



ANÁLISIS DE POLÍTICAS SOBRE PROTECCIÓN INFANTIL EN LÍNEA PARA AMS

Estudio comparativo con la participación de:
Colombia, Costa Rica, Ecuador, México, Paraguay y Perú

Diciembre del 2021



Índice

Terminología	6
Análisis de políticas sobre protección infantil en línea para AMS	14
Objetivo:	14
Proceso de implementación:.....	14
Sobre la Unión Internacional de Telecomunicaciones (UIT).....	15
Antecedentes.....	15
Programa mundial de la UIT sobre protección infantil en línea.....	15
Presentación del documento	16
Descripción del análisis	16
Alcances	16
PAÍSES PARTICIPANTES	18
COLOMBIA	18
Política Nacional Digital	19
Marco normativo / Marco Reglamentario	22
Notificaciones - contenido ilícito / Notificaciones - preocupaciones de los usuarios	24
Actores y partes interesadas.....	26
Alianzas nacionales e internacionales (sector público y privado)	28
Investigación.....	29
Educación en materia de alfabetización y competencias digitales	30
Recursos educativos.....	32
Protección de la Infancia.....	34
Sensibilización Nacional	35
Herramientas, Servicios y Ajustes.....	37
Medidas de accesibilidad.....	39
Línea de ayuda	40
Adhesión al Convenio de Budapest	41
COSTA RICA	42
Política Nacional Digital	43
Marco Normativo/Marco Reglamentario.....	47
Notificaciones-contenido ilícito / Notificaciones-preocupaciones de los usuarios	54
Actores y partes interesadas.....	57
Alianzas Nacionales e Internacionales (sector público y sector privado).....	63
Investigación.....	65
Educación en Materia de alfabetización y competencias digitales	81
Recursos educativos.....	98
Protección de la Infancia.....	100
Sensibilización Nacional	108
Herramientas, Servicios y Ajustes.....	114
Medidas de Accesibilidad	122



Línea de ayuda.....	123
Adhesión al Convenio de Budapest	124
ECUADOR	127
Política Nacional Digital	128
Marco Normativo/Marco Reglamentario.....	129
Notificaciones-contenido ilícito/Notificaciones-preocupaciones de los usuarios	135
Actores y partes interesadas.....	135
Alianzas Nacionales e Internacionales (sector público y sector privado).....	135
Investigación.....	136
Educación en Materia de alfabetización y competencias digitales	137
Recursos educativos.....	138
Protección de la Infancia.....	138
Sensibilización Nacional	140
Herramientas, Servicios y Ajustes.....	141
Medidas de Accesibilidad	141
Línea de ayuda.....	142
Adhesión al Convenio de Budapest	143
MÉXICO	144
Política Nacional Digital	145
Marco Normativo/Marco Reglamentario.....	147
Notificaciones-contenido ilícito/Notificaciones-preocupaciones de los usuarios	153
Actores y partes interesadas.....	157
Alianzas Nacionales e Internacionales (sector público y sector privado).....	159
Investigación.....	165
Educación en Materia de alfabetización y competencias digitales	165
Recursos educativos.....	170
Protección de la Infancia.....	173
Sensibilización Nacional	175
Herramientas, Servicios y Ajustes.....	181
Medidas de Accesibilidad	187
Línea de ayuda.....	189
Adhesión al Convenio de Budapest	190
PARAGUAY	191
Política Nacional Digital	192
Marco Normativo/Marco Reglamentario.....	193
Notificaciones-contenido ilícito / Notificaciones-preocupaciones de los usuarios	197
Actores y partes interesadas.....	197
Alianzas Nacionales e Internacionales (sector público y sector privado).....	198
Investigación.....	199
Educación en Materia de alfabetización y competencias digitales	199



Recursos educativos.....	199
Protección de la Infancia.....	199
Sensibilización Nacional	201
Herramientas, Servicios y Ajustes.....	201
Medidas de Accesibilidad	201
Línea de ayuda.....	201
Adhesión al Convenio de Budapest	202
PERÚ	203
Política Nacional Digital	204
Marco Normativo/Marco Reglamentario.....	204
Notificaciones-contenido ilícito/Notificaciones-preocupaciones de los usuarios	207
Actores y partes interesadas.....	208
Alianzas Nacionales e Internacionales (sector público y sector privado).....	210
Investigación.....	212
Educación en Materia de alfabetización y competencias digitales	213
Recursos educativos.....	214
Protección de la Infancia.....	214
Sensibilización Nacional	214
Herramientas, Servicios y Ajustes.....	216
Medidas de Accesibilidad	216
Línea de Ayuda.....	216
Adhesión al Convenio de Budapest	217
MATERIALES Y METODOLOGÍA DEL ESTUDIO	220
Análisis comparativo	220
Marco jurídico y reglamentario.....	222
Notificaciones-contenido ilícito / Notificaciones-preocupaciones de los usuarios	228
Educación en materia de alfabetización y competencias digitales	235
Recursos educativos.....	238
Protección de la infancia.....	239
Sensibilización Nacional	244
Cuadro 1: Ámbitos esenciales que se han de tener en cuenta	254
Buenas prácticas	255
Lecciones aprendidas	259
Modelo replicable.....	261
Desafíos regionales y posibles soluciones.....	263
MATERIAL DE REFERENCIA.....	266
Referencias ITU.....	266
Referencia Colombia	267
Referencia Costa Rica	268
Referencia Ecuador	274



Referencia México	275
Referencias Paraguay	280
Referencias Perú	281



Terminología¹

Las definiciones que figuran a continuación se basan principalmente en la terminología existente, elaborada en el marco de la Convención sobre los Derechos del Niño, de 1989, así como por el Grupo de Trabajo Interinstitucional sobre explotación sexual de niñas, niños y adolescentes, en sus Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales, de 2016² (Orientaciones de Luxemburgo), por el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual³, de 2012, así como por el Informe de Global Kids Online, de 2019⁴.

Adolescente	Es adolescente toda persona de entre 10 y 19 años de edad. Es importante señalar que, con arreglo al derecho internacional, el término adolescente no es vinculante y que las personas menores de 18 años de edad se consideran niños, mientras que las de 19 años de edad son adultos salvo que, en virtud de la ley que les sea aplicable, hayan alcanzado antes la mayoría de edad ⁵ .
Inteligencia artificial (IA)	En el sentido más amplio, el término se refiere indistintamente a los sistemas que son pura ciencia ficción (los llamados IA "fuertes" que son autoconscientes) y a los sistemas que ya están en funcionamiento y son capaces de realizar tareas muy complejas (reconocimiento facial o de voz, conducción de vehículos – estos sistemas se describen como IA "débiles" o "moderados") ⁶ .
Sistemas de IA	Un sistema de IA es un sistema basado en una máquina que, para un determinado conjunto de objetivos definidos por el ser humano, puede hacer predicciones o recomendaciones y tomar decisiones que influyen en entornos reales o virtuales, y está diseñado para funcionar con diversos niveles de autonomía ⁷ .

¹ Glosario de [las Directrices de la COP en español](https://www.itu-cop-guidelines.com/files/ugd/9ad503_ddd11b88e9fb446db04dac88def1428a.pdf) para los responsables de la formulación de políticas, Anexo 1: Terminología, p 55, disponible en: https://www.itu-cop-guidelines.com/files/ugd/9ad503_ddd11b88e9fb446db04dac88def1428a.pdf

² Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales, 2016, pág. 114, <http://luxembourguidelines.org/es/>

³ Consejo de Europa, *Protection of Children against Sexual Exploitation and Sexual Abuse* (Estrasburgo: Publicaciones del Consejo de Europa, 2012), https://www.coe.int/t/dg3/children/1in5/Source/Lanzarote%20Convention_EN.pdf

⁴ Globalkidsonline.net, *Done Right, Internet Use Can Increase Learning and Skills*, noviembre de 2019, <http://globalkidsonline.net/synthesis-report-2019/>.

⁵ UNICEF y UIT (2015), *Directrices de protección de la infancia en línea para la Industria* – [itu.int/cop](https://www.itu.int/en/cop/Documents/COP%20Guidelines_Spanish.pdf), 2015, https://www.itu.int/en/cop/Documents/COP%20Guidelines_Spanish.pdf.

⁶ Consejo de Europa, *What's AI?*, [coe.int](https://www.coe.int/en/web/artificial-intelligence/what-is-ai), inteligencia artificial, consultado el 16 de enero de 2020, <https://www.coe.int/en/web/artificial-intelligence/what-is-ai>.

⁷ OCDE, *Recommendation of the Council on Artificial Intelligence* (OCDE, 2019), <https://webcache.googleusercontent.com/search?q=cache:hTtMv9k1ak8J:https://legalinstruments.oecd.org/api/print%3Fids%3D648%26lang%3Den+&cd=3&hl=en&ct=clnk&gl=ch&client=safari>.



Interés superior del niño	Describe todos los factores necesarios para tomar una decisión en un caso específico para un niño en particular o un grupo de niños ⁸ .
Niño, niña y adolescente	De acuerdo con el Artículo 1 de la Convención sobre los Derechos del Niño, " niño " es todo ser humano menor de 18 años de edad salvo que, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad ⁹ .
Explotación y abuso sexual infantil (EASI)	Describe todas las formas de explotación y abuso sexuales (Convención sobre los Derechos del Niño, 1989, Art. 34), por ejemplo "a) la incitación o la coacción para que un niño se dedique a cualquier actividad sexual ilegal; b) la explotación del niño en la prostitución u otras prácticas sexuales ilegales; c) la explotación del niño en espectáculos o materiales pornográficos "así como el" contacto sexual que normalmente implica el uso de la fuerza sobre una persona sin consentimiento". La explotación y abuso sexuales de niños sucede cada vez más por Internet, o guarda cierta relación con el entorno en línea ¹⁰ .

⁸ ACNUDH, *Convención sobre los Derechos del Niño*, consultado el 16 de enero de 2020, <https://www.ohchr.org/SP/ProfessionalInterest/Pages/CRC.aspx>.

⁹ ACNUDH; UNICEF y UIT, *Directrices de protección de la infancia en línea para la Industria*.

¹⁰ Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.



Material de abuso (y explotación) sexual infantil (MASI)	<p>La rápida evolución de las TIC ha creado nuevas formas de explotación y abuso sexual de niños en línea, que suceden virtualmente y no tienen por qué incluir el encuentro físico con el niño¹¹. Si bien en muchas jurisdicciones todavía se clasifican las imágenes y videos de abuso sexual infantil como "pornografía infantil" o "imágenes indecentes de niños", en estas directrices englobamos ambos conceptos en el término material de abuso sexual infantil (en adelante, MASI). Esta definición está en consonancia con las Directrices de la Comisión de la Banda Ancha y el Modelo de Respuesta Nacional de la Alianza Mundial WePROTECT¹². Este término describe con mayor precisión el contenido. La pornografía se refiere a una industria legítima y comercializada y, tal como establecen las Orientaciones de Luxemburgo, el uso del término: <i>"puede (de forma involuntaria o voluntaria) contribuir a disminuir la gravedad, normalizar, o incluso legitimar lo que en realidad es abuso sexual de niñas, niños y adolescentes [...] el término "pornografía infantil" corre el riesgo de insinuar que estos actos son llevados a cabo con el consentimiento de la niña, el niño o el adolescente y es material sexual legal"</i>¹³.</p> <p>El término MASI se refiere al material que representa actos de explotación o abuso sexual de un niño. Comprende, entre otras cosas, grabaciones de abuso sexual de niños por adultos; imágenes de niños en actos sexuales explícitos; imágenes de órganos sexuales de niños producidas o utilizadas con fines principalmente sexuales.</p>
Niños y jóvenes	Toda persona menor de 18 años, siendo los niños, también llamados niños pequeños en estas directrices, los menores de 15 años y jóvenes los que tienen entre 15 y 18 años.
Juguetes conectados	Los juguetes conectados se conectan a Internet mediante tecnologías como Wi-Fi y Bluetooth, y suelen funcionar junto con aplicaciones que permiten el juego interactivo de los niños. Según Juniper Research, en 2015 el mercado de los juguetes conectados se cifró en 2 800 millones

¹¹ Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales; UNICEF, Global Kids Online Comparative Report (2019).

¹² Alianza Mundial WeProtect, Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, 2016, <https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1479255310190/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf>; Comisión de la Banda Ancha, Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019).

¹³ Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexual.



	<p>de dólares y se prevé que alcance los 11 000 millones de dólares en 2020. Estos juguetes recogen y almacenan información personal de los niños, como su nombre, geolocalización, direcciones, fotografías, grabaciones de audio y vídeo¹⁴.</p>
Ciberacoso, también denominado acoso en línea	<p>La definición del ciberacoso no está recogida en el derecho internacional. A los efectos del presente documento, el ciberacoso describe una agresión deliberada y reiterada por una persona o grupo, utilizando la tecnología digital, contra una víctima que no puede defenderse fácilmente¹⁵. Suele consistir en "utilizar la tecnología digital e Internet para publicar información dañina sobre alguien, compartir deliberadamente información privada, fotografías o vídeos con fines lesivos, enviar amenazas o insultos (por correo electrónico, mensajería instantánea, chat, mensajes de texto), difundir rumores e información falsa sobre la víctima o excluirla a propósito de las comunicaciones en línea"¹⁶. Puede tratarse de comunicaciones directas (como el envío de mensajes por chat o de texto), semipúblicas (como la publicación de mensajes en una lista de correo electrónico) o públicas (como la creación de un sitio web dedicado a burlarse de la víctima.</p>
Odio cibernético, discriminación y extremismo violento	<p>"El odio cibernético, la discriminación y el extremismo violento son un tipo distinto de violencia cibernética, que se dirige contra una identidad colectiva, en lugar de individuos [...] a menudo por motivos de raza, orientación sexual, religión, nacionalidad o situación migratoria, sexo/género y política"¹⁷.</p>
Civismo digital	<p>Por civismo digital se entiende la capacidad de participar de manera positiva, crítica y competente en el entorno digital, aprovechando las aptitudes de comunicación y creación efectivas, a fin de entablar la participación social respetando derechos humanos y la dignidad mediante el uso responsable de la tecnología¹⁸.</p>

¹⁴ Jeremy Greenberg, Dangerous Games: Connected Toys, COPPA, and Bad Security, Georgetown Law Technology Review, 4 de diciembre de 2017, <https://georgetownlawtechreview.org/dangerous-games-connected-toys-coppa-and-bad-security/GLTR-12-2017/>

¹⁵ Anna Costanza Baldry, Anna Sorrentino, y David P. Farrington, Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities, Children and Youth Services Review 96 (enero de 2019): 302-7, <https://doi.org/10.1016/j.chilcyouth.2018.11.058>

¹⁶ UNICEF, Global Kids Online Comparative Report (2019); Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.

¹⁷ UNICEF, Global Kids Online Comparative Report (2019).

¹⁸ Consejo de Europa, Digital Citizenship Education, consultado el 16 de enero de 2020, <https://www.coe.int/en/web/digital-citizenship-education/home>



Alfabetización digital	Por alfabetización digital se entiende disponer de las aptitudes necesarias para vivir, aprender y trabajar en una sociedad en la que la comunicación y el acceso a la información se realiza cada vez más a través de tecnologías digitales como las plataformas de Internet, los medios sociales y los dispositivos móviles ¹⁹ . Comprende la comunicación clara, conocimientos técnicos y pensamiento crítico.
Resiliencia digital	Este término se refiere a la capacidad del niño para afrontar emocionalmente los peligros a los que se expone en Internet. Incluye los recursos emocionales que el niño debe tener para comprender cuándo está en situación de riesgo en línea, saber qué hacer para buscar ayuda, aprender de la experiencia y recuperarse cuando las cosas salen mal ²⁰ .
Educadores	Un educador es una persona que trabaja sistemáticamente para mejorar los conocimientos de otra persona sobre un determinado tema. Comprende tanto a quienes enseñan en las aulas como a otros que, de manera más informal, por ejemplo, utilizan las plataformas y servicios de redes sociales para informar acerca de la seguridad en línea o imparten cursos comunitarios o escolares para garantizar la seguridad de los niños y jóvenes en línea. La labor de los educadores depende del contexto en el que trabajan y de la edad de los niños y jóvenes (o adultos) de los que se ocupan.
Seducción/seducción en línea	La seducción (grooming) o seducción en línea, tal como se define en las Orientaciones de Luxemburgo, hace referencia al proceso por el que una persona establece/entabla una relación con una niña, un niño o un adolescente, ya sea en persona o mediante el uso de Internet u otras tecnologías digitales, para facilitar el contacto sexual del menor, en línea o fuera de línea, con esa persona que lo convence de que tenga una relación sexual con ella ²¹ . Es un proceso destinado a engatusar a los niños para que adopten un comportamiento o entablen conversaciones de carácter sexual, con o sin su conocimiento, o un proceso caracterizado por la comunicación y la socialización entre el agresor y el niño a fin de conseguir que este último sea más vulnerable al abuso

¹⁹ Universidad de Western Sydney, Claire Urbach, What is digital literacy?, consultado el 16 de enero de 2020, https://www.westernsydney.edu.au/studysmart/home/digital_literacy/what_is_digital_literacy

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

²¹ Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.



	<p>sexual. En el derecho internacional no se establece la definición del concepto de grooming (seducción); algunos países, como Canadá, utilizan el término luring (engatusamiento).</p>
Tecnologías de la información y la comunicación (TIC)	<p>Por tecnologías de la información y la comunicación se entiende todas las tecnologías de la información centradas en la comunicación. Quedan comprendidos los servicios y dispositivos de conexión a Internet, como los ordenadores, portátiles, tabletas, teléfonos inteligentes, consolas de juego, televisores y relojes²². También incluye otros servicios como la radio, la banda ancha, los equipos de red y los sistemas de satélite.</p>
Internet y otras tecnologías conexas	<p>Hoy en día es posible conectarse a Internet mediante diversos dispositivos como los teléfonos inteligentes, las tabletas, las consolas de juego, los televisores y los ordenadores portátiles y más tradicionales. Por lo tanto, a menos que del contexto se desprenda lo contrario, se entenderá que toda referencia a Internet abarcará todos estos métodos diferentes. Para abarcar todo el vasto y complejo entramado de Internet, se utilizan indistintamente los términos "Internet y otras tecnologías conexas" y "servicios basados en Internet".</p>
Notificación y supresión	<p>Los operadores y proveedores de servicios reciben a veces notificaciones sobre contenidos sospechosos en línea emitidas por clientes, la población, los organismos responsables de hacer cumplir la ley o las organizaciones que gestionan las líneas de ayuda. Por procedimientos de notificación y supresión cabe entender los procesos que aplica una empresa para retirar rápidamente ("supresión") contenido ilícito (cuya definición será la que corresponda a la correspondiente jurisdicción) en cuanto se le informa ("notificación") acerca de la presencia de dicho contenido en sus servicios.</p>
Juegos en línea	<p>Se entiende por "juego en línea" cualquier tipo de juego digital comercial individual o multijugador a través de cualquier dispositivo conectado a Internet, incluidas las consolas de juegos, las computadoras de escritorio, los portátiles, las tabletas y los teléfonos móviles. El "ecosistema de juegos en línea" comprende ver cómo juegan otros jugadores de videojuegos a través de plataformas de deportes electrónicos, de secuenciación o de publicación de vídeos, que suelen</p>

²² UNICEF y UIT, Directrices de protección de la infancia en línea para la Industria.



	ofrecer a los espectadores la posibilidad de formular comentarios o interactuar con los jugadores y otros miembros del público ²³ .
Herramientas de control parental	Programas informáticos que permiten a los usuarios, por lo general los padres, controlar algunas o todas las funciones de una computadora u otro dispositivo que puede conectarse a Internet. Habitualmente, estos programas pueden limitar el acceso a determinados tipos o clases de sitios web o servicios en línea. Algunos de estos programas ofrecen asimismo la posibilidad de llevar a cabo una cierta gestión del tiempo, es decir, programar el dispositivo para que solamente se pueda acceder a Internet a determinadas horas. Las versiones más avanzadas de este tipo de programas pueden almacenar todos los mensajes enviados o recibidos en el dispositivo. Normalmente, estos programas están protegidos por una contraseña ²⁴ .
Padres, cuidadores y tutores	Varios sitios web se refieren a los padres de manera genérica (por ejemplo, incluyendo una "página para padres" y mencionando los "controles parentales"). Por consiguiente, sería útil definir las personas que, en un mundo ideal, deberían empoderar a los niños para aprovechar al máximo las oportunidades disponibles en línea, velando, a su vez, porque los niños y jóvenes utilicen los sitios Internet de manera segura y responsable y dándoles su consentimiento para acceder a algunos de ellos. En este documento, el término "padres" se refiere a cualquier persona (excluyendo a los educadores) que sea responsable legal del niño. En función de cada país variará el alcance tanto de la responsabilidad como de los derechos parentales.
Información personal	Este término describe la información de identificación personal que se recaba en línea. Esta información comprende el nombre completo, la información de contacto como la dirección postal y de correo electrónico, los números de teléfono, las huellas dactilares o el material de reconocimiento facial, los números de seguro o cualquier otro dato que permite entrar en contacto con una persona de manera física o en línea o localizarla. En este contexto, también se refiere a cualquier información sobre un niño y su entorno, recabada en línea por los proveedores de

²³ UNICEF, Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry, Discussion paper series: Children's Rights and Business in a Digital World, 2019, https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf

²⁴ UNICEF y UIT, Directrices de protección de la infancia en línea para la Industria.



	servicios en línea, en particular los juguetes conectados e Internet de las cosas, así como cualquier otra tecnología conectada.
Privacidad	La privacidad se suele determinar valorando la información personal que se comparte en línea, la tenencia de un perfil público en los medios sociales, la información que se comparte con personas conocidas en línea, la utilización de los parámetros de privacidad y la comunicación de contraseñas a amigos, y preocupándose por la privacidad ²⁵ .
Sexteo (sexting)	Por sexting se entiende el envío, recepción o intercambio de contenido sexual autoproducido, como imágenes, mensajes o vídeos, a través de teléfonos móviles y/o Internet ²⁶ . En la mayoría de los países, la creación, distribución y posesión de imágenes sexuales de niños es ilegal. Si se revelan imágenes sexuales de niños, los adultos no deben verlas. El hecho de que un adulto comparta imágenes sexuales con un niño es siempre un acto delictivo, y aun cuando se compartan entre niños, puede resultar dañino, por lo que puede resultar necesario informar y tomar medidas para eliminar las imágenes compartidas.
Chantaje sexual (sextorsión) o extorsión sexual de niños	El chantaje sexual (sextorsión) o extorsión sexual (también denominada "coacción y extorsión sexual en línea") ²⁷ es chantajear a "una persona valiéndose para ello de imágenes autogeneradas de esa persona con el fin de obtener favores sexuales, dinero u otros beneficios bajo la amenaza de que se compartirán dichas imágenes, independientemente de que la persona representada en ellas dé o no su consentimiento (por ejemplo, colgando las imágenes en las redes sociales)" ²⁸
Internet de las cosas (IoT)	Internet de las cosas constituye la siguiente etapa hacia la digitalización de la sociedad y la economía, en la que los objetos y las personas se interconectan a través de redes de comunicación e informan sobre su estado y/o el entorno que los rodea ²⁹ .

²⁵ Ley de Protección de la Privacidad en Línea para Niños, Ley Nº 15 del Código de los Estados Unidos, Arts. 6501 a 6505 (1998), <https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim>

²⁶ Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.

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

²⁸ Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales.

²⁹ Ntantko, The Internet of Things, 1 de octubre de 2013, Digital Single Market – Comisión Europea, <https://ec.europa.eu/digital-single-market/en/internet-of-things>



URL	Abreviatura para Uniform Resource Locator (localizador uniforme de recursos), es decir, la dirección de una página de Internet ³⁰ .
Realidad virtual	La realidad virtual es la utilización de la tecnología informática para crear el efecto de un mundo tridimensional interactivo en el que los objetos tienen un sentido de presencia espacial ³¹ .
Wi-Fi	Wi-Fi (Wireless Fidelity o fidelidad inalámbrica) es el conjunto de normas técnicas que permiten la transmisión de datos a través de redes inalámbricas ³² .

Análisis de políticas sobre protección infantil en línea para AMS

Objetivo:

Llevar a cabo un estudio con la participación de al menos cuatro países (Colombia, Costa Rica, Ecuador, México, Paraguay y Perú), y su posible difusión en la Región de las Américas, respecto a las políticas de protección y empoderamiento de los niños y jóvenes en línea, como mandato y ámbito de acción.

Proceso de implementación:

Bajo la supervisión de Pablo Palacios, en su calidad de Programmed Officer, Oficina de Área de la UIT de Chile, en estrecha coordinación con el equipo de ciberseguridad en la Sede de la UIT, y la experta designada, Claudia Ávalos, se crearon y coordinaron Grupos de Trabajo con los Puntos Focales de los Estados participantes, y que fueron considerados: Colombia, Costa Rica, Ecuador, México, Paraguay y Perú.

Se realizó la investigación y revisión multinacional de las políticas nacionales digitales / TIC; para lo cual se llevaron a cabo reuniones en línea con puntos de los Estados miembros participantes, con la finalidad de identificar y analizar prácticas y actividades de los Ministerios de TIC, reguladores de TIC, educación y cualquier otro actor gubernamental de cada país participante.

Hecho lo anterior, se coordinó el Grupo de Trabajo conformado por los puntos focales identificados y convocados, para revisar los marcos de políticas de TIC de cada país participante con un enfoque específico en los derechos del niño.

De toda la información recabada a través de dichas actividades, se hizo la revisión comparativa de las políticas TIC con enfoque de protección y empoderamiento de los niños y

³⁰ UNICEF y UIT, Directrices de protección de la infancia en línea para la Industria.

³¹ NASA, Virtual Reality, [nas.nasa.gov](https://www.nasa.gov/Software/VWT/vr.html), consultado el 16 de enero de 2020, <https://www.nasa.gov/Software/VWT/vr.html>.

³² Ley de Protección de la Privacidad en Línea para Niños.



jóvenes en línea, como mandato y ámbito de acción de cada uno de los países colaboradores, para identificar las buenas prácticas y lecciones aprendidas, y deducir un modelo replicable para los países de la Región; destacando los desafíos regionales relevantes y las posibles soluciones para el desarrollo, implementación, y el éxito de los requisitos mínimos dentro de una estrategia digital nacional que incluye la protección infantil en línea.

Del análisis anterior, se obtuvo el informe respectivo, mismo que se puso a disposición de los países participantes, para su conocimiento y con el propósito de que estén en posibilidad de retroalimentar su contenido; hecho lo anterior, se realizaron las adecuaciones pertinentes y la experta hizo la entrega de este informe final.

Agradecemos la disposición de los países participantes para colaborar en la realización del referido análisis, que sin duda es del interés de los países de la Región de las Américas.

Sobre la Unión Internacional de Telecomunicaciones (UIT)

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en lo que concierne a las tecnologías de la información y la comunicación (TIC) y se sitúa a la cabeza de la innovación de las TIC junto a sus 193 Estados Miembros y más de 900 empresas, universidades y organizaciones internacionales y regionales. Creada hace más de 150 años en 1865, la UIT es el organismo intergubernamental encargado de coordinar a escala mundial el uso compartido del espectro, promover la cooperación internacional para la asignación de órbitas de satélite, mejorar la infraestructura de telecomunicaciones en el mundo en desarrollo, y fijar las normas mundiales que garantizan la interconexión continua de una amplia gama de sistemas de comunicaciones. Desde las redes de banda ancha hasta las tecnologías inalámbricas de vanguardia, la navegación aeronáutica y marítima, la radioastronomía, la vigilancia de la tierra por medios oceanográficos y basada en satélites, así como los servicios de telefonía fija y móvil convergentes, Internet y las tecnologías de radiodifusión, la UIT se compromete a conectar el mundo. Para más información, visite la página www.itu.int.

Antecedentes

Programa mundial de la UIT sobre protección infantil en línea

El uso de la tecnología implica enormes beneficios y también diversos riesgos, respecto de los cuales, los niños no son un caso de excepción.

El objetivo de dicho programa es implementar las Directrices de protección infantil en línea (COP) en todas las regiones de la UIT. Esto se hará a través de un proyecto global y diferentes proyectos de satélites. El Proyecto Global es parte de la asociación estratégica entre la UIT y la Autoridad Nacional de Ciberseguridad (NCA) del Reino de Arabia Saudita, que lanzaron su



colaboración en diciembre de 2020 para “Crear un ciberespacio seguro y próspero para los niños”.

El programa mundial de la UIT fomentará políticas innovadoras, garantizará la mejora de las competencias, promoverá el diálogo mundial y fortalecerá los esfuerzos mundiales para implementar las Directrices de protección infantil en línea (COP) de la UIT, lanzadas en junio de 2020³³, con un enfoque de protección y empoderamiento de los niños y jóvenes en línea, como mandato y ámbito de acción.

Presentación del documento

Descripción del análisis

En el marco de la planificación anual del Fortalecimiento de Capacidades en Ciberseguridad y en el marco del plan de “Promoción de una comunidad de ciberseguridad diversa e inclusiva”, la Oficina de Área de la UIT de Chile ha considerado la implementación de un estudio que servirá como herramienta para los formuladores de políticas sobre cómo incorporar elementos de protección infantil en línea en las estrategias, políticas, legislación y regulación digitales actuales y futuras relacionadas con el fomento de la conectividad, el acceso y el uso, en asociaciones público-privadas, herramientas de implementación de proyectos relacionados con la inclusión digital y la economía digital. Llevar a cabo un estudio con la participación de al menos cuatro países (Ecuador, Perú, Paraguay, Colombia, Costa Rica y México), y su posible difusión en la Región de las Américas.

Alcances

El presente informe tiene como objetivo el poder llevar a cabo un análisis comparativo de las políticas de protección y empoderamiento de los niños y jóvenes en línea, como mandato y ámbito de acción en los países participantes de la Región, y que se trata de Colombia, Costa Rica, Ecuador, México, Paraguay y Perú.

El cuestionario enviado a los países participantes, se elaboró con base en la **Observación General No. 25 (2021)** relativa a los **derechos de los niños en relación con el entorno digital**³⁴, del Comité Sobre Derechos del Niño de la ONU; la **Ley Orgánica 8/2021 de 04 de junio de 2021, de protección integral a la infancia y la adolescencia frente a la violencia** (España); y por supuesto, en las **directrices sobre protección de la infancia en línea para los encargados de formular políticas**³⁵, emitidas por la UIT.

³³ <https://www.itu-cop-guidelines.com/implementation>

³⁴ Carta de los derechos digitales de los niños, niñas y adolescentes: <https://www.anar.org/wp-content/uploads/2019/07/Carta-Derechos-Digitales.pdf>

³⁵ Directrices sobre la protección de la infancia en línea para los encargados de formular políticas https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/Guidelines/2020-translations/S-GEN-COP.POL_MAKERS-2020-PDF-S.pdf



Asimismo, se tomó en consideración las definiciones contenidas en el Glosario de las Directrices sobre la protección de la infancia en línea para la industria <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/Guidelines/2020-translations/S-GEN-COP.IND-2020-PDF-S.pdf>, extraído principalmente de la terminología existente establecida en la Convención sobre los Derechos del Niño, 1989, así como por el Grupo de Trabajo Interinstitucional sobre explotación sexual de niñas, niños y adolescentes en las Orientaciones Terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales, 2016 (Orientaciones de Luxemburgo), por el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, 2007, así como en el Global Kids Online Report del UNICEF, 2019.

Todo lo anterior, con la finalidad de que los países participantes, puedan observar la aplicabilidad de los contenidos en sus respectivas políticas públicas.

Como definición medular del presente informe, en dicho Glosario se refiere que Niños y *jóvenes* es toda persona menor de 18 años, siendo los niños, también llamados niños pequeños en estas directrices, los menores de 15 años y jóvenes los que tienen entre 15 y 18 años.

El presente informe analizará los siguientes aspectos como **factores diferenciadores y de impacto, en las etapas de elaboración, implementación y evaluación de políticas de protección y empoderamiento de los niños y jóvenes en línea:**

- Política Nacional Digital
- Marco Normativo/Marco Reglamentario
- Notificaciones-contenido ilícito/Notificaciones-preocupaciones de los usuarios
- Actores y partes interesadas
- Alianzas Nacionales e Internacionales (sector público y sector privado)
- Investigación
- Educación en Materia de alfabetización y competencias digitales
- Recursos educativos
- Protección de la Infancia
- Sensibilización Nacional
- Herramientas, Servicios y Ajustes
- Medidas de Accesibilidad
- Línea de ayuda
- Adhesión al Convenio de Budapest



PAÍSES PARTICIPANTES

COLOMBIA

Índice de siglas en este capítulo

CAI	Centro de Atención Inmediata
CONPES	Consejo Nacional de Política Económica y Social
DIJIN	Dirección de Investigación Criminal e Interpol
ESCNNA	Explotación Sexual Comercial de Niños, Niñas y Adolescentes
EVAC	End Violence Against Children
ICBF	Instituto Colombiano de Bienestar Familiar
ISP	Proveedor de Servicios de Internet
MEN	Ministerio de Educación Nacional
MINTIC	Ministerio de Tecnologías de la Información y las Comunicaciones
PONAL	Policía Nacional
PRST	Proveedores de Redes y Servicios de Telecomunicaciones
SIC	Superintendencia de Industria y Comercio
TIC	Tecnologías de la Información y la Comunicación
DPS	Departamento de Prosperidad Social
ART	Agencia de Renovación de Tierras
SENA	Servicio Nacional de Aprendizaje
ASCUN	Asociación Colombiana de Universidades
ASOCAJAS	Asociación de Cajas de Compensación Familiar
UNICEF	Fondo de las Naciones Unidas para la Infancia
ODS	Objetivos de Desarrollo Sostenible



Política Nacional Digital

La Constitución Política de Colombia plantea que los niños, niñas y adolescentes deben gozar de una protección especial por parte del Estado, en tanto no solo se consideran titulares de derechos constitucionales y legales, sino que también, deben ser “[...] protegidos contra toda forma de abandono, violencia física o moral, secuestro, venta, abuso sexual, explotación laboral o económica y trabajos riesgosos” (Artículo 44); razón por la cual, para Colombia los derechos de los niños prevalecen sobre los derechos de los demás.

En concordancia con lo anterior, Colombia ratificó la Convención Internacional sobre los Derechos del Niño en la ley 12 de 1991, con la cual se compromete a garantizar el derecho de los menores de 18 años para desarrollarse en medios seguros³⁶. Este compromiso se extiende al actual contexto tecnológico y escenario de uso de las tecnologías de la información y las comunicaciones (TIC), dónde se promueve que estos sean medios propicios para el desarrollo individual y social de los niños y niñas en particular, y de la ciudadanía en general.

En este sentido, el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) ha asumido como una de sus funciones promover una cultura en torno al uso responsable y seguro de las TIC, entendidas como instrumentos que faciliten a los colombianos su bienestar y desarrollo personal, social y económico³⁷ (Ley 1978 de 2019, artículo 14, numeral 3). En consonancia con esta función y en correspondencia con el compromiso de garantizar los derechos de los niños y niñas, el MINTIC interviene en el sector de las TIC con el fin de: i) “Proteger los derechos de los usuarios, incluyendo a los niños, niñas y adolescentes” (Ley 1978 de 2019, artículo 4, numeral 1); ii) “Sancionar a los operadores, concesionarios de espacios de televisión y contratistas de televisión nacional cuando violen las disposiciones constitucionales y legales que amparen específicamente los derechos de la familia y de los niños” (Ley 1978 de 2019, artículo 22, numeral 30); iii) “Desarrollar e implementar la política pública para la prevención y la protección de niñas, niños y adolescentes, entendiendo las necesidades de cada tipo de población, frente a los delitos realizados a través de medios digitales, informáticos y electrónicos” (Ley 1978 de 2019, artículo 24, numeral 5).

El MINTIC desde 2010 ha implementado tres planes de política sectorial³⁸, en los cuales ha sido un tema prioritario la prevención y protección de las niñas, niños y adolescentes en los

³⁶ De igual forma Colombia ha ratificado el Convenio Internacional sobre Aspectos Civiles del Secuestro de Niños mediante la ley 173 de 1994, el Convenio 138 y 182 de la OIT sobre la edad mínima para el empleo mediante las leyes 515 de 1999 y 704 de 2001, aprobó mediante la ley 620 de 2000 la Comisión Interamericana sobre Restitución Internacional de Menores, y mediante la ley 765 de 2002 aprueba el protocolo facultativo de la convención sobre los derechos de los niños relativo a la venta de niños, la prostitución infantil y la utilización de niños en explotación sexual.

³⁷ Las funciones del MINTIC están definidas en la ley 1341 de 2009 mediante la cual se transforma el Ministerio de Comunicaciones en el Ministerio de Tecnología de la Información y las Comunicaciones. Esta ley fue modificada por la ley 1978 de 2019.

³⁸ Estos son: i) Cuaternio 2010 - 2014 Plan Vive Digital; ii) 2014 – 2018 Plan Vive Digital; iii) 2018 – 2022 Plan El Futuro Digital es de Todos.



medios digitales, informáticos y electrónicos. Las políticas del MINTIC han apostado de forma constante en construir una cultura del uso responsable y seguro de las TIC, mediante la cual sea posible prevenir prácticas de producción y consumo de contenidos en línea que vulneren los derechos de las niñas, niños y adolescentes, la interacción con personas que manipulen o inciten a los menores de 18 años a que se involucre en actividades sexuales, denunciar cualquier representación visual, gráfica o textual que involucre la participación de niñas, niños y adolescentes en actividades sexuales o eróticas.

En el 2010 se diseñó Plan Vive Digital 2010-2014 dónde se propuso “[...] promover en los usuarios de las redes de comunicaciones electrónicas, la prevención de comportamientos riesgosos, especialmente de los menores de edad, señalando responsabilidades de los padres de familia, el sector educativo y las autoridades de Policía Judicial” (Plan Vive Digital 2010 - 2014, p. 63).

Para lograr estos objetivos se planteó la creación del programa En TIC Confío, el cual se ha implementado en todo el territorio colombiano desde 2012 hasta la actualidad, y con el cual se busca proporcionar a la ciudadanía en general, conocimientos e indicaciones para la construcción de hábitos seguros en cuanto al uso de las redes de comunicaciones electrónicas. El programa En TIC Confío ha sido una apuesta del Estado colombiano en los distintos planes de política digital sectorial, de ahí que en el plan El Futuro Digital es de Todos (2018 – 2022), dicho programa continúa siendo una de las grandes apuestas, ya que contribuye significativamente a la prevención de riesgos en Internet de niñas, niños y adolescentes (p. 74).

El plan El futuro Digital es de Todos (2018 – 2022) que se encuentra en el marco del Plan Nacional de Desarrollo 2018-2022, “Pacto por Colombia, Pacto por la Equidad”, aprobado por la Ley 1955 de 2019, plantea en el numeral VII denominado el “Pacto por la Transformación Digital de Colombia: gobierno, empresas y hogares conectados con la era del conocimiento”, como uno de sus objetivos: “[...] empoderar a los ciudadanos y hogares en el entorno digital”³⁹, lo cual implica el fortalecimiento de competencias en el uso de Internet y las TIC, a partir de criterios éticos y responsables que favorezcan a los niños, niñas, adolescentes y adultos en general. Por lo anterior, le corresponde al MINTIC, como entidad del orden nacional, promover el uso y la apropiación responsable de las TIC

³⁹ “Promover la formación en habilidades digitales básicas y herramientas, aplicaciones y contenidos que les permita hacer uso productivo del entorno digital para solucionar sus problemas, generar ingresos y desarrollar sus actividades diarias. Se fomentarán estrategias para reducir barreras para la adquisición de bienes y servicios digitales, generar habilidades digitales (transversales a toda la población y productivas con enfoque regional, que reconozcan la diversidad cultural y geográfica y que impulsen el desarrollo de ecosistemas de emprendimiento digital en los territorios), fortalecer y simplificar servicios de interacción con el Estado (trámites) por canales digitales y finalmente, generar confianza hacia el entorno digital a través de estrategias sobre seguridad digital”.



Cabe destacar que en este Plan Nacional de Desarrollo, en lo referente a la niñez, se fija como estrategia, la atención integral desde la primera infancia hasta la adolescencia, el fortalecimiento del papel de la familia como garante fundamental de la protección, el afecto y los derechos de los niños, llevar atención integral de la primera infancia a la adolescencia apostándole a la construcción de proyectos de vida y un sistema de prevención y superación de la violencia infantil y las vulneraciones de los derechos de los niños.

Estas políticas sectoriales del MINTIC se articulan con documentos de política pública CONPES (Consejo Nacional de Política Económica y Social), máxima autoridad nacional de política pública del país. En el año 2011, se formuló el documento CONPES 3701 Lineamientos de Política para la Ciberseguridad y Ciberdefensa, el cual identifica como uno de los problemas de país la “[...] falta de una concientización, transmisión y cultura en el manejo seguro de la información en sectores públicos, privados y sociedad civil” (CONPES 3701, Título IV, numeral 1). De igual forma en el año 2016 el documento CONPES 3854, Política Nacional de Seguridad Digital, busca empoderar a los ciudadanos y al Estado en relación con los riesgos del entorno digital, y consolidar las capacidades del país para hacer frente al crimen, la delincuencia y otros fenómenos que afectan la seguridad nacional desde este entorno.

Por su parte en 2020, se elaboró el documento CONPES 3995 Política Nacional de Confianza y Seguridad Digital el cual tiene por objeto establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sean una sociedad incluyente y competitiva en el futuro digital. Se reconoce en este CONPES como un problema a enfrentar, que los niños y niñas colombianos se encuentran en entornos digitales con un nivel de seguridad en línea por debajo del promedio global y en alta exposición a riesgos cibernéticos.

Por esta razón, se plantean acciones para enfrentarlo relacionadas con la coordinación y diseño de una estrategia de formación en capacidades en materia de seguridad digital, en la cual se unifiquen las iniciativas de sensibilización y generación de habilidades en los ciudadanos en Colombia, que posibilite generar en la trayectoria educativa completa, el desarrollo de competencias y la formación en seguridad y confianza digital. Además, se plantea el diseño de una estrategia para la creación de hábitos de uso seguro y responsable de las TIC,

Este marco de política busca fortalecer en la ciudadanía, el conocimiento de los riesgos y delitos presentes en los entornos digitales, con el propósito de trabajar de manera conjunta con los organismos del Estado colombiano como el Instituto Colombiano de Bienestar Familiar (ICBF), la Policía Nacional (PONAL) y el MINTIC para construir entornos digitales seguros y beneficiosos para los niños, niñas y adolescentes.



Teniendo en cuenta estos lineamientos de política pública digital, el MINTIC por medio de la Dirección de Apropiación de TIC⁴⁰ lidera el programa En TIC Confío+, el cual a lo largo de sus 10 años de implementación ha beneficiado a más de trece (13) millones de colombianos. Solo en el último cuatrienio ha beneficiado a más de cuatro (4) millones de ciudadanos y en 2021 tuvo un alcance de más de dos (2) millones de niños, niñas, adolescentes, jóvenes y adultos con quienes se ha promovido el uso seguro y responsable de las TIC, a través de la sensibilización sobre los riesgos asociados a estas, tales como, Sexting, Grooming, Ciberacoso, Ciberdependencia y los delitos consecuentes como la explotación sexual infantil y la sextorsión. Así mismo, el programa desarrolla una estrategia de prevención, denuncia y cero tolerancias con el material de explotación sexual de niñas, niños y adolescentes o cualquier otra forma de violencia a menores de 18 años en Internet y otras plataformas TIC, lo que contribuye a su bienestar y seguridad, siendo estos, sujeto de especial protección por mandato constitucional.

Como resultado, la política pública de Colombia aporta a la prevención y erradicación de la Explotación Sexual Comercial de Niños, Niñas y Adolescentes (ESCNNA) como delito, en busca de generar un marco unificado de acción para el gobierno nacional y los gobiernos territoriales en materia de prevención de riesgos y restablecimiento de los derechos de niñas, niños y adolescentes víctimas de este flagelo.

Marco normativo / Marco Reglamentario

Colombia cuenta con un conjunto de normas que facilitan las acciones para alcanzar los objetivos propuestos en cuanto a la protección de los niños, niñas y adolescentes en los entornos digitales, entre las que se encuentran las siguientes:

⁴⁰ El Decreto 1064 de 2020 "Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones", establece en su artículo 25 las funciones de la Dirección de Apropiación TIC del Ministerio de Tecnologías de la Información y las Comunicaciones "1. Formular estrategias, programas, planes y proyectos encaminados a impulsar el acceso, uso productivo, apropiación y aprovechamiento de las tecnologías de la información y las comunicaciones, en la comunidad y en los sectores de la sociedad.
2. Promover el establecimiento de una cultura de uso de tecnologías de la información y las comunicaciones en el país, a través de programas y proyectos que favorezcan su incorporación a la sociedad, para facilitar el desarrollo personal y social de la comunidad.
3. Definir los mecanismos de evaluación para medir avances en la utilización y la apropiación de tecnologías de la información y las comunicaciones en todos los sectores de la sociedad.
4. Impulsar y realizar el acompañamiento técnico para la implementación del teletrabajo en el país, en coordinación con las demás entidades competentes en la materia.
5. Formular y dirigir estrategias encaminadas a realizar alfabetización digital, así como el de fomentar el desarrollo de habilidades TI y su aprovechamiento productivo en los sectores de la sociedad.
6. Formular y dirigir proyectos que fomenten la seguridad y el uso responsable de las Tecnologías de la Información y las Comunicaciones en los sectores de la sociedad.
7. Diseñar e implementar estrategias integrales de comunicación del Estado con los ciudadanos, para promover la cultura digital y el uso de tecnologías en el país.
8. Participar en los procesos de diálogo que se convoquen en atención a grupos étnicos para el uso productivo, apropiación y aprovechamiento de las tecnologías de la información y las comunicaciones.
9. Las demás que le sean asignadas, inherentes a la naturaleza de la dependencia".



Normativa	Descripción
Ley 679 de 2001	Estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores en desarrollo del artículo 44 de la Constitución Política de Colombia. Tiene por objeto dictar medidas de protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio.
Ley 1098 de 2006	Código de Infancia y Adolescencia. Establece en el artículo 47 en sus 8 numerales y párrafo, las responsabilidades especiales de los medios de comunicación, al promover y difundir información que respete los derechos y libertades de los niños, niñas y adolescentes, así como su bienestar físico y mental.
Ley 1336 de 2009	Adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Que consagra disposiciones en la lucha y prevención de la pornografía infantil.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, y se crea un nuevo bien jurídico tutelado, denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
Ley 1450 de 2011	Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014. Que regula el principio de neutralidad en la Red.
Ley 1581 de 2012	Ley de Protección de Datos Personales. En particular el artículo 7. Derechos de los niños, niñas y adolescentes, plantea que cualquier tratamiento de datos debe garantizar el respeto por los derechos prevalentes de los menores de 18 años.
Ley 1620 de 2013	Sistema nacional de convivencia escolar y formación para el ejercicio de los derechos humanos, la educación para la sexualidad y la prevención y mitigación de la violencia escolar.



	Se contempla infracciones como el matoneo por Facebook u otra red social, el cual debe ser sancionado.
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. En particular establece medidas técnicas para identificar páginas que contengan Material de Explotación Sexual de Niñas, Niños y Adolescentes.
Ley 1928 de 2018	Por medio de la cual se aprueba el “Convenio sobre la ciberdelincuencia”, adoptado el 23 de noviembre de 2001 en Budapest.
Ley 2089 de 2021	Se prohíbe el uso del castigo físico, los tratos crueles, humillantes o degradantes, así como cualquier otro tipo de violencia como método de corrección de las niñas, niños y adolescentes.

Notificaciones - contenido ilícito / Notificaciones - preocupaciones de los usuarios

Respecto de las páginas con contenido Material de Explotación Sexual de Niñas, Niños y Adolescentes, Colombia cuenta con la ley 679 de 2001⁴¹, la cual establece que los Proveedores de Redes y Servicios de Telecomunicaciones (PRST) tienen como deberes: “1. Denunciar ante las autoridades competentes cualquier acto criminal contra menores de edad de que tengan conocimiento, incluso de la difusión de material pornográfico asociado a menores; 2. Combatir con todos los medios técnicos a su alcance la difusión de material pornográfico con menores de edad; 3. Abstenerse de usar las redes globales de información para divulgación de material ilegal con menores de edad; 4. Establecer mecanismos técnicos de bloqueo por medio de los cuales los usuarios se puedan proteger a sí mismos o a sus hijos de material ilegal, ofensivo o indeseable en relación con menores de edad” (Artículo 8).

De acuerdo con la normatividad, los PRST tienen la obligación de realizar el bloqueo de las páginas con contenido proscrito, de los listados con URL con contenido de pornografía infantil emitidos por la Dirección de Investigación Criminal e Interpol (DIJIN) y que son publicados en la página web del MINTIC. De igual manera, en lo que se refiere a la vigilancia que hace el MINTIC a los PRST, el Artículo 2.2.10.3.2 Decreto 1078 de 2015⁴², establece las siguientes

⁴¹ Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores en desarrollo del artículo 44 de la Constitución Política de Colombia.

⁴² Por medio de la cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.



medidas técnicas para identificar páginas que contengan Material de Explotación Sexual de Niñas, Niños y Adolescentes:

“1. Los ISP, proveedores de servicio de alojamiento o usuarios corporativos deberán implementar sistemas internos de seguridad para su red, encaminados a evitar el acceso no autorizado a su red, la realización de spamming, o que desde sistemas públicos se tenga acceso a su red, con el fin de difundir en ella contenido relacionado con pornografía infantil.

2. Los ISP deben implementar en su propia infraestructura, técnicas de control, basadas en la clasificación de contenidos que tengan como objetivo fundamental evitar el acceso a sitios con contenidos de pornografía infantil.

La clasificación de estos contenidos se sujetará a la que efectúen las diferentes entidades especializadas en la materia. Dichas entidades serán avaladas de manera concertada por el Ministerio de Tecnologías de la Información y las Comunicaciones y el Instituto Colombiano de Bienestar Familiar (ICBF).

3. Los prestadores de servicios de alojamiento podrán utilizar herramientas tecnológicas de monitoreo y control sobre contenidos alojados en sitios con acceso al público en general que se encuentran en su propia infraestructura.

4. Los ISP y proveedores de servicios de alojamiento deberán ofrecer o informar a sus usuarios, sobre la existencia de mecanismos de filtrado que puedan ser instalados en los equipos de estos, con el fin de prevenir y contrarrestar el acceso de menores de edad a la pornografía.

Así mismo los ISP deberán facilitar al usuario el acceso a la información de criterios de clasificación, los valores y principios que los sustentan, la configuración de los sistemas de selección de contenido y la forma como estos se activan en los equipos del usuario.

5. Cuando una dirección es bloqueada por el ISP, se debe indicar que esta no es accesible debido a un bloqueo efectuado por una herramienta de selección de contenido.

6. Los ISP y proveedores de servicios de alojamiento deberán incluir en sus sitios, información expresa sobre la existencia y los alcances de la Ley 679 de 2001.

7. Los ISP y proveedores de servicios de alojamiento deberán implementar vínculos o "links" claramente visibles en su propio sitio, con el fin de que el usuario pueda denunciar ante las autoridades competentes sitios en la red con presencia de contenidos de pornografía infantil.”

De acuerdo con lo anterior, existen normas que establecen las medidas que deben adoptar los PRST, para identificar y bloquear páginas con contenido proscrito, no obstante, cada



operador tiene la libertad de implementar los mecanismos tecnológicos que considere necesarios, siempre y cuando den cumplimiento a las medidas técnicas establecidas en la normatividad, así como a los deberes dispuestos en el artículo 8 de la Ley 679 de 2001 Estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores en desarrollo del artículo 44 de la Constitución Política de Colombia y el artículo 2.2.10.2.2 del Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones.

Actores y partes interesadas

En cumplimiento del compromiso de eliminar la violencia hacia niñas, niños y adolescentes, Colombia ha avanzado en varias iniciativas, productos del consenso entre la Sociedad Civil y el Gobierno. En concordancia con ello, el 14 de mayo de 2021 se sancionó la Ley 2089 de 2021 por medio de la cual se prohíbe el uso del castigo físico, los tratos crueles, humillantes o degradantes, así como cualquier otro tipo de violencia como método de corrección de las niñas, niños y adolescentes. Esta Ley, define el castigo físico como “Aquella acción de crianza, orientación o educación en que se utilice la fuerza física y que tenga por objeto causar dolor físico, siempre que esta acción no constituya conducta punible de maltrato o violencia intrafamiliar” (Artículo 2); y los tratos crueles, humillantes y degradantes como “Aquella acción con la que se hiere la dignidad del niño, niña o adolescente o se menosprecie, denigre, degrade, estigmatice o amenace de manera cruel, siempre que no constituya conducta punible. No será causal de pérdida de la patria potestad o de la custodia, ni causal para procesos de emancipación, siempre y cuando no sea una conducta reiterativa y no se afecte la salud mental o física del niño, niña o adolescente.” (Artículo 2). Igualmente, la Ley determina que se deberá implementar una Estrategia Nacional Pedagógica y de Prevención, “[...] la cual busca identificar e ilustrar alternativas y prácticas para educar, orientar y disciplinar sin violencia” (Artículo 5).

Las bases del cumplimiento de esta ley vienen consolidándose desde agosto del año 2019, con la puesta en marcha la Alianza Nacional contra la Violencia hacia Niñas, Niños y Adolescentes, bajo el liderazgo de la Consejería Presidencial para la Niñez y Adolescencia y el ICBF, mediante la cual le es posible a Colombia vincularse a la Alianza Global para erradicar la violencia hacia la niñez. La Alianza Nacional es una estrategia de respuesta y articulación intersectorial para prevenir la violencia contra niñas, niños y adolescentes y garantizar la atención de quienes han sido víctimas de este fenómeno y de la cual el MINTIC hace parte mediante su programa En TIC Confío+. El programa toma en consideración los entornos digitales como espacios en los cuales deben prevenirse, así como denunciarse prácticas que violenten la integridad de los niños, niñas y adolescentes, razón por la cual es necesario sumar



y ordenar los esfuerzos de todos los sectores en función de garantizar una respuesta efectiva a este flagelo.

Así mismo, En TIC Confío ha desarrollado articulación técnica con las entidades que hace parte de la Alianza Nacional, orientada a desarrollar estrategias conjuntas que permitan potenciar la prevención de los riesgos presentes en el uso de Internet, las redes sociales y las plataformas digitales; así como acciones de prevención de la explotación sexual de niños, niñas y adolescentes en los medios digitales.

El Plan de Acción contra la violencia, del que hace parte En TIC Confío+, es resultado de un proceso de formulación técnica con participación de diversos actores relevantes, desarrollado en dos fases siendo estas:

Fase 1: Revisión de documentos técnicos elaborados entre 2019 y 2020 durante la puesta en marcha de la Alianza Nacional, y que sirvieron como bases del plan:

- Planes Nacionales de Acción de otros países vinculados a la Alianza Global.
- Marco normativo nacional.
- Identificación de instancias de articulación intersectoriales relacionadas con la prevención o consecuencias de la violencia hacia niñas, niños y adolescentes.
- Realización de mapeo de grupos de interés y actores clave, y abordaje metodológico del proceso de planificación.

Fase 2: Desarrollo de talleres y consultas con tres grupos de interés:

- Niñas, niños y adolescentes.
- Entidades del Estado.
- Actores con competencia en prevención de violencia (Organizaciones de Sociedad Civil, instituciones de educación superior, agencias de cooperación internacional y embajadas, y empresa privada).

El Plan busca intervenir en las causas estructurales de la violencia y dar respuesta efectiva a las necesidades diferenciales de los niños, niñas y adolescentes afectados por esta problemática. Desde el programa En TIC Confío+, el aporte al plan se encuentra en la promoción y desarrollo de habilidades digitales para que las niñas, niños y adolescentes prevengan todo tipo de violencia en el entorno digital, mediante la producción de contenidos, la divulgación de estrategias pedagógicas de prevención, la formación virtual en herramientas para la promoción del uso seguro y responsable de las TIC y el desarrollo de habilidades digitales para la transformación social desde el activismo digital positivo.



Autoridad en protección de datos personales

Colombia cuenta con la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio (SIC), autoridad de protección de datos encargada de vigilar y garantizar que las entidades públicas y privadas, respeten los principios, derechos y garantías en el tratamiento de los datos personales. Dicha autoridad, emite diversos materiales y guías para todos los sectores de la sociedad. En materia de protección de la infancia en línea, ha publicado contenidos, como la *Guía cuida tu identidad digital y protege tus datos personales* (2021), material de acceso gratuito para toda la ciudadanía, mediante la cual se informa sobre los riesgos relacionados al tratamiento de datos personales de niños, niñas y adolescentes⁴³.

De igual forma, Colombia cuenta con regulaciones sobre los datos personales como la Ley 1266 de 2008⁴⁴ y la Ley 1581 de 2012⁴⁵. Esta última en particular, plantea en el artículo 7. Derechos de los niños, niñas y adolescentes, que cualquier tratamiento de datos debe garantizar el respeto por los derechos prevalentes de los menores de 18 años, razón por la cual, resulta fundamental informar y capacitar a la ciudadanía en cuanto a los riesgos que enfrentan los menores de 18 años en cuanto se presenta un tratamiento indebido de sus datos personales, vulnerando el derecho que tienen a la privacidad y la protección de su información personal.

Alianzas nacionales e internacionales (sector público y privado)

El Programa En TIC Confío+ del MINTIC junto con la Consejería Presidencial para la Niñez y la Adolescencia, el Ministerio de Educación Nacional (MEN), el ICBF, la PONAL y la empresa TIGO, conforman la Alianza Nacional contra la Violencia hacia niñas, niños y adolescentes, en cumplimiento del Plan Nacional de Desarrollo 2018-2022 “Pacto por Colombia, Pacto por la Equidad”. Esta alianza es una apuesta de articulación interinstitucional e intersectorial, diseñada para intervenir algunas de las causas estructurales de la violencia y dar respuesta efectiva a las necesidades diferenciales de las niñas, niños y adolescentes. Además de integrar la oferta institucional, la Alianza sirve de instrumento para orientar de manera estratégica y articulada los esfuerzos del país para la prevención y atención de la violencia, y fortalecerlos a partir de la evidencia existente a nivel internacional.

En el marco de esta Alianza, el Programa En TIC Confío+, aporta de manera significativa a varios de sus lineamientos principales, entre los que se destacan: i) Fortalecer los entornos protectores: educativo, institucional, comunitario, familiar y virtual, ii) Generar capacidades de

⁴³ https://issuu.com/quioscosic/docs/guia_cuida_tu_identidad_digital_002

⁴⁴ Por medio de la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

⁴⁵ Por medio de la cual se dictan disposiciones generales para la protección de datos personales



autoprotección y empoderamiento de las niñas, niños y adolescentes. De manera adicional, en 2021 el programa En TIC Confío+ se articuló con diferentes entidades tales como: Departamento para la Prosperidad Social (DPS), el programa Jóvenes y familias en acción, la Agencia de Renovación del Territorio (ART), la Red Nacional de Reporteros Comunitarios, la Dirección de Empleo del Departamento Administrativo de la Función Pública, los programas Tecnoacademias y Tecnoparques Servicio Nacional de Aprendizaje (SENA), el Programa de Seguimiento Judicial al Tratamiento de Drogas del Ministerio de Justicia, las Asociaciones Comunitarias del Ministerio de Interior, las emisoras, Colegios y Casas de Familia de la Armada Nacional, las emisoras del Ejército Nacional, la Asociación Colombiana de Universidades (ASCUN), las Cajas de Compensación familiar (ASOCAJAS).

Esta estrategia de gestión con entidades ha logrado dar a conocer el programa En TIC Confío+ y las constantes renovaciones en sus lineamientos técnicos, metodológicos y operativos que se han consolidado fundamentalmente a partir de 2021 como parte de la renovación de este al cumplir 10 años de funcionamiento en el territorio colombiano. Dentro de las últimas propuestas se destaca la actualización de los contenidos mediante los cuales se lleva a los ciudadanos el mensaje de prevención en riesgos y delitos cibernéticos, la ampliación de la oferta a niños entre los 6 y los 11 años, como consumidores cada vez más tempranos de contenidos en línea; la creación contenidos específicos para adultos, desde su rol de cuidadores y acompañantes en el proceso de formación en el uso adecuado de las TIC y la creación de la Academia En TIC Confío+ como un escenario de formación virtual en temáticas relacionadas con el activismo digital positivo y el uso seguro de las TIC.

También se ha llevado a cabo la colaboración con el sector privado, a fin de empoderar a su población con base en experiencias en línea más seguras y positivas. En alianza con la empresa TIGO, se orientan acciones conjuntas y coordinadas que promuevan el uso seguro, responsable, creativo y positivo de Internet en la población colombiana, especialmente en los niños, niñas y adolescentes.

Investigación

En el caso de Colombia, se advierte que han llevado a cabo diversos estudios con otras organizaciones, como UNICEF en conjunto con diversas entidades gubernamentales, mediante investigaciones que han publicado en medios digitales, tales como el acceso a las páginas oficiales, así como la lectura de artículos, investigaciones y publicaciones en medios de comunicación, la cual se cita en el presente documento sin embargo, desde el programa En TIC Confío+ no se han realizado investigaciones puntuales en el tema.

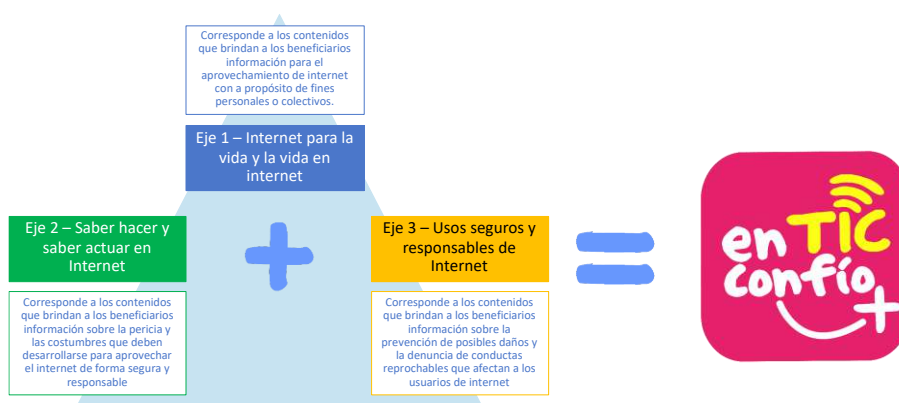


Educación en materia de alfabetización y competencias digitales

El MINTIC desde la implementación del Programa En TIC Confío+ promueve el uso y la apropiación de Internet como oportunidad para el activismo, la huella positiva en entornos digitales, y el desarrollo de las habilidades para el autocuidado respecto a los riesgos y delitos en Internet. De igual forma aporta en la prevención, denuncia y cero tolerancias frente al material de explotación sexual de niñas, niños y adolescentes o cualquier otra forma de violencia a menores de 18 años en Internet y otras plataformas TIC⁴⁶.

En concordancia con lo anterior, los contenidos del programa En TIC Confío+ se estructuran en tres ejes, los cuales definen el trabajo del programa y permiten optimizar y potenciar el acompañamiento pedagógico al establecer propósitos formativos y alcances pedagógicos diferenciados para los niños, niñas, adolescentes y adultos beneficiarios del programa. Los ejes se concretan como se representa en el siguiente esquema:

Esquema 1. Ejes estructurales de los contenidos del programa



De acuerdo con el esquema anterior cada uno de los ejes se relacionan entre sí, por lo que no son pensados como elementos aislados en la estructura de contenidos. En este sentido, los contenidos del eje 1, buscan el aprovechamiento de internet para fines personales y colectivos, por tanto, aportan en el desarrollo del eje 2, en cuanto a habilidades digitales y la construcción de hábitos para el uso seguro y responsable de internet, a la vez que el eje 1 se fundamenta en el eje 2.

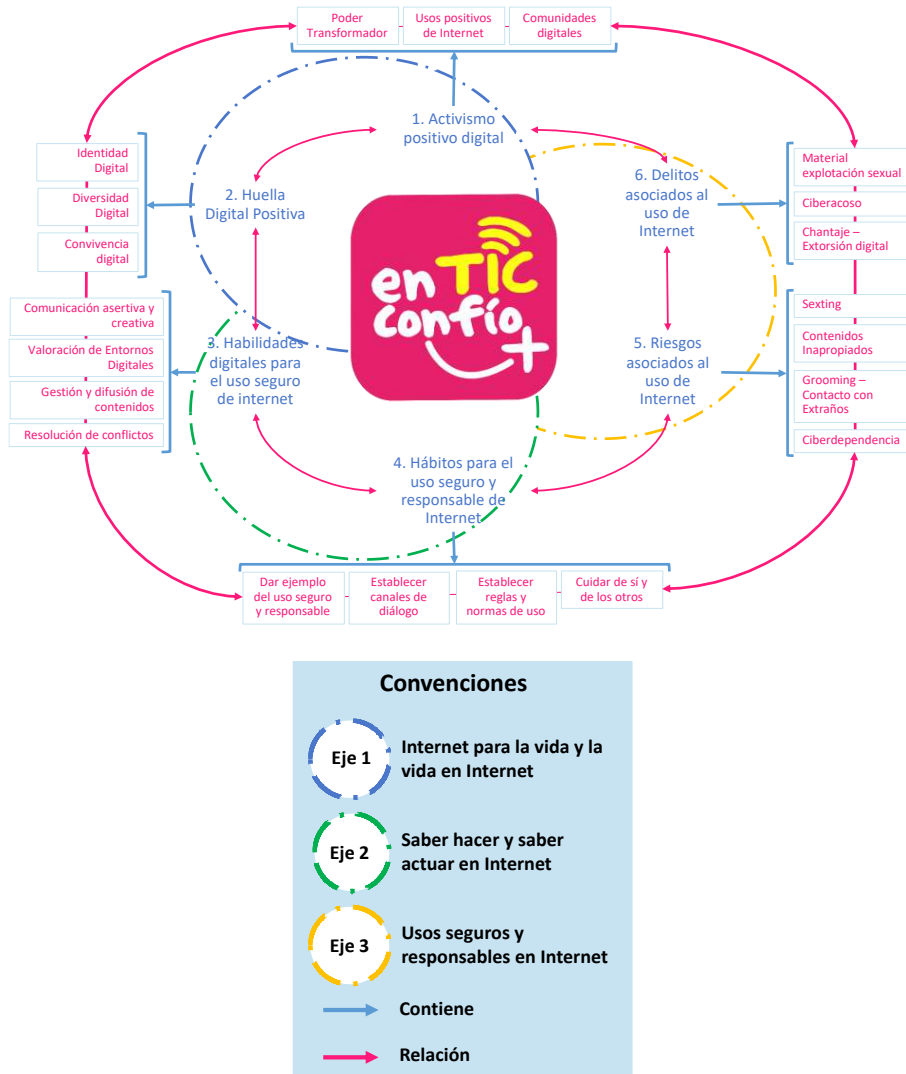
Por tanto, se considera que un activista positivo digital que cuida y deja su huella digital positiva, cuenta con habilidades para ellos y desarrolla hábitos que lo caracterizan como un usuario responsable en los entornos digitales. De igual forma, el activismo y la huella digital positiva son fundamentales para el eje 3, en tanto son la base para la prevención del riesgo y para asumir una postura crítica y responsable ante los ciberdelitos asociados al uso de internet. En este mismo sentido, la prevención del riesgo y la denuncia de delitos reafirman la posición activa positiva de los usuarios y fortalece sus habilidades y hábitos para el uso seguro

⁴⁶ <https://www.enticconfio.gov.co/>



y responsable de internet. A continuación, se presenta el esquema de contenidos del programa:

Esquema 2. Temas asociados a los ejes estructurales de los contenidos del programa



Desde esa perspectiva y por más de una década, el programa ha contribuido al fortalecimiento de la convivencia digital en los territorios, mediante el fortalecimiento de habilidades sociales y digitales en los beneficiarios, que promueven la reflexión sobre los usos positivos de Internet, las redes sociales y las plataformas digitales. Este fortalecimiento se ve reflejado en el desarrollo de habilidades como:

- La comunicación asertiva y creativa
- La evaluación de seguridad y pertinencia de los contenidos
- La resolución de problemas y ciberconflictos
- La identificación y prevención de riesgos asociados al uso inadecuado de las TIC
- La apropiación de los mecanismos de denuncia en casos de delitos



- El aprovechamiento de Internet para la vida
- La conciencia sobre la construcción de una huella positiva digital

Uno de los grandes aciertos del programa es que sus beneficiarios han variado con los años, acorde a las necesidades en la prevención de riesgos y delitos en Internet en todas las edades, implementando metodologías y narrativas que nos lleven a acercarnos a la sociedad colombiana de una manera más apropiada.

Inicialmente el programa estaba dirigido a adolescentes entre los 12 y 18 años, sin embargo, a partir de 2021 la estrategia empezó a trabajar con niños de 6 a 11 años y con la población adulta, entre la que se incluyen padres, madres, cuidadores y docentes. Los beneficiarios reconocen la oportunidad de entender las TIC como una herramienta de transformación, construcción y aporte a sus territorios, a sus proyectos de vida y a las iniciativas sociales y comunitarias que pueden potenciarse desde el uso activo, creativo y seguros de las herramientas digitales. Es así como los beneficiarios dan valía a programa, sus contenidos y las estrategias de implementación que desarrolla como un mecanismo de construcción y transformación social.

Recursos educativos

En 2021 el Programa en TIC Confío+ renovó su estrategia pedagógica y sus recursos didácticos. En este sentido amplió sus contenidos, los cuales están organizados tres ejes:

1. Internet para la vida y la vida en internet, con el cual se busca que los niños, niñas, adolescentes y adultos aprendan sobre el uso positivo de Internet y las TIC a partir del activismo positivo digital para el uso responsable y seguro de Internet y las TIC y la huella digital positiva para entornos digitales enriquecedores y amables para todos.
2. Saber hacer y saber actuar en Internet, con el cual se busca que los niños, niñas, adolescentes y adultos aprendan sobre el uso responsable de Internet y las TIC a partir de habilidades y hábitos digitales para el uso positivo y seguro de Internet y las TIC.
3. Usos seguros y responsables de Internet, con el cual se busca que los niños, niñas, adolescentes y adultos aprendan sobre el uso seguro de Internet y las TIC a partir del conocimiento de riesgos y delitos asociados al uso de Internet y las TIC, para su prevención o acción oportuna.

A partir de allí el programa ofrecer a sus beneficiarios un acompañamiento pedagógico compuesto por:

1. Encuentro pedagógico presencial o virtual, el cual es un espacio de formación pedagógica a propósito de los ejes de contenido del programa, con los que se aporta



en la construcción de una cultura de seguridad y responsabilidad en el uso activo y positivo de internet y las TIC.

2. Recursos complementarios en la página web del programa como Infografías, videos y podcast de acceso abierto para consulta y descarga a propósito de los ejes de contenido del programa, para que los beneficiarios del programa puedan ampliar información y conocer más sobre seguridad y responsabilidad en el uso activo y positivo de internet y las TIC.
3. Siete (7) cursos virtuales de acceso gratuito para toda la población colombiana que sirve de refuerzo pedagógico al trabajo que realizan los Embajadores, según los ejes de contenido del programa, para que los beneficiarios del programa puedan ampliar información y conocer más sobre seguridad y responsabilidad en el uso activo y positivo de internet y las TIC. Los cursos ofertados son:
 - a. Curso prevención de riesgos ante contenidos inapropiados en Internet (Dirigido a adultos);
 - b. Curso Estrategias de acompañamiento para adultos en el uso responsable y seguro de las TIC (Dirigido a adultos);
 - c. Curso Activismo digital para transformar el mundo (Dirigido a adultos);
 - d. Curso Tras los rastros de la huella positiva digital (Dirigido a adolescentes);
 - e. Curso Agencia misterio: protección y manejo ético de datos personales (Dirigido a adolescentes);
 - f. Curso Inteligencia artificial: el espejo de nuestras conductas en Internet (Dirigido a adolescentes);
 - g. Curso Huella D+: ser buena onda en internet (Dirigido a niños y niñas).

Los cursos están diferenciados para adultos, adolescentes y niños y niñas. Los adultos, aprenden sobre estrategias para acompañamiento de niños, niñas y adolescentes en los entornos digitales, así como la prevención de riesgos ante contenidos inapropiados y a comprender el activismo digital. Los adolescentes aprenden sobre huella digital positiva, la protección de datos personales y el papel de la inteligencia artificial como espejo de nuestras conductas en internet. Por último, los niños y niñas aprenden sobre seguridad y convivencia en los entornos digitales.

De igual forma el programa cuenta con la Academia En TIC Confío+, un entorno pedagógico virtual de autoformación gratuito para niños, niñas, adolescentes, jóvenes y adultos, en el cual además de los siete (7) cursos virtuales, se encuentra el curso de “Líderes Digitales Transformadores” mediante el cual los jóvenes aprenden a impulsar su activismo positivo



digital por medio del reconocimiento de características propias del liderazgo positivo digital y la utilidad de Internet y las TIC para la innovación para la transformación digital a partir de la construcción de una propuesta que defina metas de transformación, tiempo de implementación, recursos TIC y de Internet y beneficiarios, en áreas sociales, artísticas, culturales, de emprendimiento.

Protección de la Infancia

Desde el Programa En TIC Confío+, se proponen como desafíos claves: i) Fortalecer las capacidades de los actores para generar un uso positivo, seguro y responsable de las TIC frente a los riesgos asociados a estas, difundiendo múltiples herramientas para prevenirlos; ii) Fortalecer las capacidades de nuestros beneficiarios para usar y apropiarse del Internet como una oportunidad de generar un proyecto de vida, la movilización de causas solidarias y positivas en Internet; iii) Contribuir desde la acción directa del Programa a mantener el bienestar y seguridad digital promoviendo oportunidades de crecimiento (proyectos de vida) y participación en el entorno digital.

Para el programa, la protección de la infancia parte de la generación de conciencia en los niños, niñas y adolescentes sobre sus prácticas y hábitos en Internet que pueden resultar dañinos para sí mismo, así como reconocer las potencialidades de internet para impulsar su desarrollo individual y social. De igual forma, la protección implica el acompañamiento por parte de los adultos en el uso responsable y seguro de las TIC, padres, maestros, cuidadores deben aportar, no solo mediante el cuidado de los otros, sino también, el cuidado de sí mismo.

En este sentido, en el marco de implementación del Programa En TIC Confío+ se han definido los alcances y la caracterización de los niños, niñas, adolescentes y adultos que se benefician con el programa, a partir de lo cual es posible pensarlo como un equipo que trabaja en conjunto en pro de la protección de unos y otros:

- **Niños y niñas (6-11 años):** El programa hace el acompañamiento pedagógico con niños y niñas para enseñarles acerca de hábitos de consumo y darles a conocer alertas sobre riesgos presentes en los entornos digitales cuando como usuario de Internet y las TIC lo utilizan comúnmente para comunicarse, acceder a clases online, jugar en línea y ver videos. En general, a esta edad, su navegación busca contenidos de gratificación inmediata y facilidad en el proceso de la información.
- **Adolescentes y Jóvenes (12-18 años):** El programa hace el acompañamiento pedagógico con adolescentes para enseñarles además de hábitos de consumo y conocer alertas sobre riesgos presentes en este tipo de uso, sobre cómo desarrollar habilidades digitales que les permitan aprovechar las oportunidades de internet respetando la convivencia y los derechos de autor. Teniendo en cuenta que el uso de



Internet y las TIC que se hace en esta etapa de crecimiento está asociada a la búsqueda de un espacio personal y privado donde pueden expresarse y comunicarse. De igual forma, gracias al manejo que tienen de internet y las TIC, también apoyan a los adultos cercanos en el manejo de estas, aportando en el cierre de la brecha digital generacional.

- **Adultos:** El programa hace el acompañamiento pedagógico con adultos para enseñarles de acuerdo con su rol de cuidado, información y habilidades que les permita fortalecer el uso que hacen de internet y de las TIC, y a partir de ello, entender la importancia de definir reglas, acompañar a los niños, niñas y adolescentes en el uso de internet y las TIC para potenciar sus beneficios y reducir los riesgos, así como saber actuar en situaciones que requieran denuncia.

Sensibilización Nacional

Durante 10 años el programa En TIC Confío+ ha beneficiado a más de trece (13) millones de colombianos, aportando en la construcción de una cultura del uso positivo, seguro y responsable de Internet y las TIC. Diseñando y llevando a todos los niños, niñas, jóvenes y adultos de Colombia diferentes estrategias, entre ellas, la Charla sobre seguridad y riesgos en el uso de Internet y las TIC, con la cual se busca generar conciencia y responsabilidad en los usuarios de los entornos digitales para hacer de estos espacios amables y productivos para todos.

En 2021 el programa paso de la Charla al Encuentro Pedagógico como estrategias de sensibilización, con una apuesta metodológica por promover la construcción de una cultura del uso activo, responsable y seguro de Internet y las TIC mediante el diálogo y el desarrollo del pensamiento crítico en los participantes. Para desarrollar estos encuentros pedagógicos, el programa cuenta con un equipo de profesionales, conocidos en sus territorios como Embajadores.

En TIC Confío+ ha logrado llegar a los 32 departamentos de Colombia gracias a la confianza y respaldo de aliados institucionales, como rectores de colegios, directores de emisoras, funcionarios públicos de entidades territoriales, así como empresas privadas, quienes están convencidos que el uso activo y positivo, a la vez que seguro y responsable de Internet y las TIC es fundamental para todos los niños, niñas, adolescentes, jóvenes y adultos. Muchos son quienes han contribuido a que los niños, niñas y adolescentes hoy cuenten con herramientas para navegar seguros y de forma responsable, aprovechando Internet y las TIC para dejar una huella positiva y se líderes digitales en la transformación de sus territorios. Así las cosas, En TIC Confío+ representa más contenidos para aprender, más oportunidades para todos, más activismo digital, más huella positiva digital y claro, más seguridad y protección de la infancia y de la ciudadanía en general en los entornos digitales.



Durante los 10 años de implementación se ha logrado beneficiar mediante los contenidos del programa a propósito del uso responsable y seguro de internet y las TIC a más de trece (13) millones de colombianos, estos son algunos datos del número de beneficiarios en los últimos cuatro años:

Línea base 2018	9.674.719
2019	823.654
2020	1.117.939
2021	2.382.092
Total	13.998.404

De igual forma se han adelantado campañas de comunicación mediante las cuales se ha logrado la sensibilización de la población colombiana a propósito de la protección de la infancia y de la ciudadanía en general en los entornos digitales, realizadas por el programa En TIC Confío+:

- Campañas “[Ciberpaya y Cibercuidado](#)”, dirigidas a población mayor, donde se buscó ejemplificar el exceso de confianza, exposición y sobreexposición que jóvenes y adultos tienen en el uso de Internet.
- En alianza con Canal TR3CE y Sesame Workshop (la organización educativa sin ánimo de lucro productora de Sesame Street), se lanzó la serie Plaza Sésamo: [Monstruos en red](#). Por medio de esta serie de 26 capítulos se buscó contrarrestar los riesgos existentes en la red, diseñados para dar a conocer las ventajas y oportunidades del uso seguro de Internet y dar respuesta a las necesidades educativas y digitales que presentan los colombianos de hasta los 7 años.
- El MinTIC desde su programa “En TIC Confío+ ”lanzó el [“Pacto Nacional por la Cero Tolerancia con la Pornografía Infantil”](#) al que adhieren un amplio número de entidades públicas y privadas y en el que como parte de los compromisos que se adquirieron en este pacto se encuentra el de promover el uso responsable de las TIC de la mano de este Programa, fortalecer y apoyar los canales de denuncia y atención a los reportes de este delito en Colombia y promover el bloqueo efectivo de páginas en Internet con este contenido o cualquier forma de abuso a menores de 18 años en Internet. A esta iniciativa se vincularon actores y actrices colombianos de renombre buscando sensibilizar sobre el tema al mayor número de colombianos.
- Comercial [“Piensa antes de enviar”](#) con el fin de sensibilizar a los colombianos frente a la importancia de protegerse y hacer un uso responsable de Internet.



- [#Antropología Digital](#) una serie podcast de 10 capítulos en los que, a través de entrevistas a diversos expertos en las TIC, se reflexiona acerca de los comportamientos digitales y su impacto en la sociedad actual. La igualdad en el acceso de internet, el fenómeno del activismo digital, el uso de las redes sociales y las páginas web con enfoque de género, así como los riesgos a los que nos enfrentamos con el uso creciente de la red, son algunos de los temas que aborda la serie.
- Lanzamiento de la serie web [“EmiFan”](#), una serie web compuesta por 10 capítulos que busca prevenir los riesgos en los entornos digitales, tales como el ciberacoso y el grooming. Esta serie web juvenil representa situaciones que viven los y las adolescentes y busca generar habilidades para prevenir los riesgos, conocerlos y denunciarlos.
- Campaña [“Bajemos el tono”](#) estrategia diseñada para promover la convivencia digital. Esta iniciativa nació como un esfuerzo por generar conciencia entre los colombianos sobre los efectos de los contenidos agresivos y los abusos en las redes, promoviendo la reflexión en torno a las consecuencias que tienen sobre los demás nuestras palabras y expresiones en la red.

Herramientas, Servicios y Ajustes

Desde la puesta en marcha del programa En TIC Confío+ en una década de implementación en el territorio nacional, se han producido más de cuatro (4) millones de contenidos propios dados en infografías, videos, recursos didácticos, cursos de formación, podcast, etc., lo que demuestra una actualización constante de sus plataformas, página web, redes sociales, estrategias de encuentro y sensibilización con los beneficiarios, estrategias de gestión y articulación con el sector público y privado y en sus apoyos pedagógicos. Es así como en el Programa se desarrollan acciones encaminadas a estar permanentemente informados y actualizados en la investigación de nuestras líneas de referencia y conceptos base. Todos los contenidos producidos pueden ser descargados y revisados en:

- Página web del programa: www.enticconfio.gov.co
- Redes sociales del Programa:
 - Instagram @enticconfio
 - Facebook @enticconfio.mintic
 - YouTube @EnTicConfío+
 - Twitter @EnTICconfio

Los recursos que estarán disponibles en la página web como parte del programa y a los que podrán acudir los colombianos son:



- **Infografías:** esquemas dinámicos que precisen conceptos, rutas de acompañamiento, tips y sugerencias para el uso activo, seguro y responsable de internet.
- **Video Galería:** curaduría de los videos producidos para el programa En TIC Confío+ durante los últimos 10 años, más los videos actuales, organizados y categorizados según los ejes y temas de la estructura de contenidos del programa.
- **Podcast:** grabaciones de audio que relatan situaciones de la vida cotidiana en Internet, con indicaciones acerca de cómo actuar.
- **Enlaces de interés:** links de los aliados institucionales del programa y otras iniciativas que por su pertinencia resulten de interés para los beneficiarios.

Para el desarrollo de los encuentros pedagógicos del programa En TIC Confío+, los Embajadores del programa cuentan con una serie de herramientas de apoyo para su realización, estas son:

- **Guía metodológica:** dirigida a los embajadores del programa, en la que se describe los contenidos a desarrollar, así como sugerencias didácticas para garantizar que en el encuentro pedagógico se cumplan los propósitos formativos del programa. Actualmente el programa cuenta con dos guías metodológicas, una dirigida para los encuentros pedagógicos con adolescentes y otra para los adultos. Este material puede ser consultado en la página web y es de acceso abierto.
- **Material audiovisual:** material en formato web para apoyar el encuentro pedagógico con imágenes, textos y videos que le permitan al embajador o formador desarrollar el encuentro. Este material audiovisual se estructura según dos criterios metodológicos, en el caso de los encuentros pedagógicos para niños y niñas, se les propone imaginar que son héroes digitales y se les informa acerca de los poderes que tienen en la red para prevenir y enfrentar riesgos y delitos. En el caso de los adolescentes y en la perspectiva de generar un pensamiento crítico, se abordan los ejes de contenido del programa a partir de dilemas, es decir, situaciones que permitan la reflexión y la construcción de criterios acerca de cómo actuar en internet. Por último, en el caso de los adultos, se trabaja a partir de creencias, para desmitificar algunas que no permiten que se cumpla el rol de cuidado de la infancia y la adolescencia, así como de sí mismos en los entornos digitales.
- **Material offline:** es una estrategia dirigida a aquellos territorios en los que el acceso a Internet es escaso. En este sentido, se desarrolla mediante una metodología de escala, en la que los embajadores realizan la formación en los contenidos a un grupo de beneficiarios como por ejemplo, docentes, bibliotecarios, trabajadores sociales, por solicitud del representante de la comunidad, quienes podrán replicar los contenidos del



programa a través de la orientación de un taller de acompañamiento pedagógico, el cual estará basado en infografías y actividades de reflexión para la apropiación del contenido. Los beneficiarios una vez desarrollada la guía podrán ser reportados al representante de la comunidad, quien respaldará la realización del ejercicio e informará de manera formal al programa la realización del taller. Así las cosas, el taller de acompañamiento pedagógico guardará correspondencia con las metodologías de fases definida para los encuentros pedagógicos.

Medidas de accesibilidad

A nivel nacional, en materia de infancia y adolescencia, los Objetivos de Desarrollo Sostenible (ODS) establecen las prioridades a 2030 mediante metas e indicadores consignados. Para el caso de Colombia en el CONPES 3918, Estrategias para la Implementación de los Objetivos de Desarrollo Sostenible (ODS) en Colombia del 15 de marzo del 2018, hacen énfasis en los siguientes aspectos fundamentalmente:

- Superar la pobreza que afecta a las niñas, niños y adolescentes;
- Poner fin a todas las formas de malnutrición mediante la seguridad alimentaria;
- Garantizar educación inclusiva, equitativa y de calidad eliminando las disparidades de género y asegurando el acceso igualitario para las personas vulnerables, incluidas aquellas con discapacidad y los pueblos indígenas;
- La igualdad entre géneros y el empoderamiento a las mujeres y las niñas con la eliminación de todas las formas de violencia contra ellas, incluida la explotación sexual;
- La adopción de medidas eficaces para erradicar el trabajo forzoso y eliminar las peores formas del trabajo infantil, proporcionar acceso universal a zonas verdes y espacios públicos seguros, inclusivos y accesibles y poner fin al maltrato y, en general, a todas las formas de violencia contra niñas, niños y adolescentes.

De igual forma, el Gobierno Nacional formuló la Política Nacional de Infancia y Adolescencia la cual tiene como finalidad contribuir al desarrollo integral de las niñas, niños y adolescentes en el territorio nacional y generar las condiciones de bienestar, acceso a oportunidades con equidad e incidencia de las niñas, niños y adolescentes en la transformación del país. En dicha Política, el eje de acción no. 7 formula que todas las niñas, niños y adolescentes deben vivir en entornos seguros y protectores; por tanto, los entornos donde transcurren sus vidas deben garantizar las condiciones materiales y sociales para el ejercicio pleno de los derechos y la reducción de los riesgos y amenazas a la integridad física y psicológica de los sujetos.

Esto implica promover el desarrollo de capacidades para prevenir, evitar y también actuar de manera adecuada ante las situaciones de riesgo o amenaza contra su dignidad y desarrollo



integral, o contra otro. En este sentido la implementación del programa En TIC Confío+ se da en la perspectiva de aporta al logro de los siguientes:

ODS 4. Educación de Calidad	ODS 5. Igualdad de género
El programa aporta a la meta 4.7 de este ODS el programa aporta en la construcción de estilos de vida sostenibles, el reconocimiento de los derechos humanos, la igualdad de género, la promoción de una cultura de paz y no violencia en los entornos digitales, la ciudadanía digital y la valoración de la diversidad cultural	De acuerdo con la meta 5.2 de este ODS el programa aporta En acciones para eliminar todas las formas de violencia contra todas las mujeres y las niñas en los ámbitos público y privado, incluidas la trata y la explotación sexual, que utilizan medios digitales para ello, así como otros tipos de explotación o chantaje, como la sextorsión

Es fundamental el involucramiento parental, relaciones de cooperación y solidaridad comunitaria, apoyadas por políticas públicas coherentes con este propósito de desarrollo integral de las niñas, niños y adolescentes. Las niñas, niños, adolescentes y sus familias transitan y se desarrollan en entornos configurados por escenarios de relación confiables, seguros y protectores que los reconocen, donde se promueve desarrollo integral y se previenen los riesgos y amenazas que pueden generar vulneraciones de derechos.

Línea de ayuda

Los ciudadanos colombianos cuentan con canales de denuncia ante actividades que pongan en riesgo o vulneren los derechos de niños, niñas y adolescentes, en especial aquellos que suceden en entornos virtuales, a través de instituciones del estado como el ICBF o la PONAL. Estos canales son dados a conocer por medio de las distintas estrategias propias de dichas instituciones, así como por el programa En TIC Confío+ del MINTIC:

Línea 141- ICBF

Este canal le permite a la ciudadanía denunciar o pedir orientación sobre casos de maltrato infantil, violencia sexual, acoso escolar, trabajo infantil o consumo de sustancias psicoactivas, entre muchas otras situaciones que amenacen o afecten la vida e integridad de un niño, niña o adolescente.

Canal de denuncia de la Policía Nacional - www.adenunciar.policia.gov.co

Este canal le permite a la ciudadanía realizar denuncias en caso de: i) Hurto; ii) Delitos Informáticos; iii) Material de contenido de explotación sexual infantil; iv) Extorción; v) Falsedad en documentos y personal; vi) Estafa; vii) Violencia basada en género.

CAI virtual de la policía Nacional - www.caivirtual.policia.gov.co



Este canal le permite a la ciudadanía denunciar situaciones relacionadas con; i) hackeos de cuentas, de redes sociales; ii) accesos a sistemas informáticos; iii) cuando llegan correos electrónicos que contienen links que redireccionan a páginas fraudulentas; iv) páginas que tengan características que puedan generar riesgos para los ciudadanos o especialmente para los niños, niñas y adolescentes.

Adhesión al Convenio de Budapest

En Colombia fue aprobada la ley 1928 del 24 de julio de 2018, por medio de esta disposición el estado colombiano entró a formar parte del **CONVENIO DE BUDAPEST (OAS, 2019)**, primer tratado internacional en la historia de la humanidad sobre ciberdelincuencia, sellado el 23 de noviembre de 2001 en esta ciudad húngara de Europa Oriental y ratificado por Estados Unidos con la aprobación unánime de del Senado en el mes de agosto de 2006.

La Policía Nacional de Colombia cuenta con un apartado de Protección integral a los niños, niñas y adolescentes⁴⁷, en el que se describen los componentes del Sistema de Responsabilidad Penal para Niños, Niñas y Adolescentes, que se conforma por tres líneas de acción:

- Línea de prevención;
- Línea de vigilancia y control;
- Línea de Investigación Judicial.

Igualmente, dicha autoridad ha implementado el programa de prevención “abre tus ojos”⁴⁸, estructurado mediante una metodología pedagógica con temáticas específicas, enfocadas a las diferentes problemáticas que afectan a los niños, niñas y adolescentes dentro del contexto social actual de Colombia, y en los que se han abordado temas como principios y valores, maltrato infantil, uso adecuado de redes sociales, trabajo infantil, etc., y como población objetivo, Niños, Niñas y Adolescentes, Comunidad en general, Líderes comunales, comerciantes, trabajadores informales, entre otros.

Colombia cuenta con un Centro Cibernético Policial que depende de la Policía Nacional de Colombia, en el que se encuentra el Observatorio Cibercrimen, en el que se encuentran diversas publicaciones y materiales, como los boletines de riesgos y tendencias en Relación con el Abuso y la Explotación Sexual de los Niños, Niñas y Adolescentes⁴⁹.

⁴⁷ <https://www.policia.gov.co/proteccion-infancia/proteccion-integral>

⁴⁸ https://www.policia.gov.co/sites/default/files/informe_rendicion_de_cuentas-infancia_y_adolescencia.pdf

⁴⁹ https://caivirtual.policia.gov.co/sites/default/files/riesgos_y_tendencias_en_relacion_con_el_abuso_y_la_explotacion_sexual_de_los_n_n_a.pdf



COSTA RICA

Índice de siglas del capítulo

CEDAW	Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer
CNA	Código de la Niñez y la Adolescencia
CNNA	Consejo Nacional de la Niñez y la Adolescencia
CNSL	Comisión Nacional de Seguridad en Línea
CONACOEES	Comisión Nacional Contra la Explotación Sexual Comercial de Niños, Niñas y Adolescentes
EASNNAL	Estrategia Nacional Prevención y respuesta a la Explotación y Abuso Sexual de Niños, Niñas y Adolescentes en Línea
FANNA	Fiscalía Adjunta de Atención de Hechos de Violencia en perjuicio de Niñas, Niños y Adolescentes
ICE	Instituto Costarricense de Electricidad
INFOCOM	Cámara de Infocomunicación y Tecnología
MCJ	Ministerio de Cultura y Juventud
MEP	Ministerio de Educación Pública
MICITT	Ministerio de Ciencia, Tecnología y Telecomunicaciones
NNA	Niños, niñas y adolescentes
PANI	Patronato Nacional de la Infancia
PNDT	El Plan Nacional de Desarrollo de las Telecomunicaciones
PNDT	Plan Nacional de Desarrollo de las Telecomunicaciones
PRODHAB	Agencia de Protección de Datos de los Habitantes
UNICEF	Fondo de Naciones Unidas para la Infancia



Política Nacional Digital

Costa Rica cuenta con políticas nacionales digitales, la Ley N° 8660, Fortalecimiento y modernización de las entidades públicas del sector telecomunicaciones, establece como una de las funciones para la rectoría de Telecomunicaciones *“Coordinar las políticas de desarrollo de las telecomunicaciones con otras políticas públicas destinadas a promover la sociedad de la información”*. Con base en esto, se detallan las principales políticas:

Plan Nacional Desarrollo de las Telecomunicaciones (PNDT) 2015-2021

El Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT) 2015-2021 *“Costa Rica: Una Sociedad Conectada”*, es el instrumento guía de las acciones del sector Telecomunicaciones en el país. Dicho documento impulsa la banda ancha, la inclusión social, el empoderamiento de las y los habitantes, el gobierno electrónico abierto, cercano y transparente. Se considera que estos elementos son cruciales en la sociedad moderna como factores aglutinantes y potenciadores de las capacidades individuales y colectivas, de la transformación productiva de los diferentes sectores sobre los que descansa la economía costarricense en la búsqueda de una sociedad más justa, equitativa y próspera. Para lograrlo, se plantean 3 pilares, a saber: Inclusión Digital, Gobierno Electrónico y Transparente, Economía Digital (Costa Rica, Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2015).

Plan Nacional de Desarrollo de las Telecomunicaciones 2022-2027 "Costa Rica: Hacia la disrupción digital inclusiva"

El PNDT, es un instrumento de planificación que orienta el desarrollo del sector telecomunicaciones, este contiene elementos habilitadores de política pública, que identifican el punto de partida, para lo cual toma en cuenta datos y estadísticas a nivel nacional e internacional y con base en su análisis, define hacia dónde se quiere proyectar el país. Esta proyección se justifica y diseña considerando elementos como la convergencia tecnológica y su dinamismo, la evolución del entorno y las tecnologías emergentes, la participación de los actores que conforman el sector y, cómo a través del marco estratégico; integrado por objetivos estratégicos, metas nacionales, acciones sistemáticas, indicadores de producto, efecto e impacto medibles y evaluables, se concretan para la ejecución de las intervenciones y el cumplimiento de la visión que el Plan ha prospectado al 2027.

El objetivo general de este Plan es avanzar hacia la disrupción digital, promoviendo la gestión del espectro radioeléctrico, el despliegue y el acceso a redes de telecomunicaciones fijas y móviles; seguras, robustas, escalables y resilientes, para la reducción de la brecha digital en todos sus componentes y dimensiones, a través del desarrollo de competencias digitales para



que todas las personas puedan hacer un uso seguro, responsable e intensivo de las tecnologías digitales en el entorno de la Sociedad de la Información y el Conocimiento.

De esa forma, este instrumento se establecen 3 metas nacionales de política pública que se describen a continuación:

- Ampliar y mejorar la conectividad a Internet fija y móvil por región de planificación, al 2027;
- Incrementar la inversión del sector telecomunicaciones como proporción del Producto Interno Bruto (PIB), al 2027;
- Mejorar la adquisición de competencias digitales de la población, al 2027.

Cada una de ellas, se acompaña de una serie de indicadores que permitirán dar cuenta a través de todo el proceso de ejecución del PNDT de los avances que se están obteniendo y del alcance del resultado esperado.

Para alcanzar el objetivo principal de este Plan partirá de tres áreas estratégicas: 1. Conectividad Significativa para el bienestar. 2. Espectro Radioeléctrico para la competitividad, 3. Competencias Digitales para el desarrollo. Estas áreas son el resultado de un proceso de consulta y análisis riguroso que tienen como elemento transversal el bienestar y la mejora de la calidad de vida de las personas mediante el acceso y uso intensivo de las tecnologías digitales. (Costa Rica, Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2021).

Este Plan se encuentra en consulta pública hasta el 26 de noviembre del 2021. <https://www.micit.go.cr/micitt/publicaciones/construccion-plan-nacional-desarrollo-las-telecomunicaciones-2022-2027>

Estrategia Transformación Digital hacia la Costa Rica del Bicentenario 4.0, 2018-2022

Dicho documento busca dictar la política pública de desarrollo digital de Costa Rica, para que impacte positivamente a las personas, así como articular, coordinar y dar seguimiento a todas las iniciativas de desarrollo digital de nuestro país. Su visión es alcanzar una Costa Rica transformada digitalmente acelerando la productividad, la competitividad y el desarrollo socioeconómico, tomando ventaja de la cuarta revolución industrial y las sociedades del conocimiento, para procurar el bienestar de todos sus habitantes de manera inclusiva y potenciar el desarrollo sostenible del país (Costa Rica, Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2018).

Estrategia Nacional de Ciberseguridad, 2017

Este instrumento estratégico plantea un esfuerzo conjunto y articulado entre todos los sectores del país, para garantizar que los objetivos que se establezcan sean equilibrados,



eficaces y acordes a la realidad nacional, definiendo los principios generales que marcarán la pauta en esta materia.

El objetivo principal de esta estrategia es desarrollar un marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentado la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente a los riesgos en cuanto al uso de las TIC para lograr un entorno más seguro y confiable para todos los habitantes del país (Costa Rica, Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2017).

Política Nacional para la igualdad entre mujeres y hombres en la formación, el empleo y el disfrute de los productos de la Ciencia, Tecnología, las Telecomunicaciones y la Innovación 2018-2027 (PICTTI)

Esta política tiene como objetivo *“promover la igualdad en la participación de las mujeres respecto de los hombres en la atracción, permanencia, formación, capacitación, el empleo de calidad y la investigación, en los diferentes campos de la ciencia, la tecnología y la innovación, para facilitar el acceso y el disfrute de los avances científicos-tecnológicos”* (Costa Rica, Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2017).

Dentro de los ejes estratégicos de la política se encuentran: la atracción, formación, permanencia de las mujeres a la ciencia, la tecnología e innovación, el fomento de la investigación y el empleo de las mujeres en la ciencia, la tecnología y la innovación, y la apropiación social de la ciencia con perspectiva de género, entre otros.

Política Nacional de Sociedad y Economía basadas en el Conocimiento (PNSEBC)

Esta política tiene como objetivo fomentar, fortalecer y difundir el conocimiento, así como el desarrollo científico y tecnológico en beneficio de la sociedad costarricense, mediante los principios de respeto a los Derechos Humanos; sostenibilidad; calidad; universalidad y ética con fecha límite al período 2030, además considera como base el trabajo en 5 pilares. La política se encuentra en actualización y se espera en las próximas semanas publicar la nueva versión. (Costa Rica, Ministerio Ciencia, Tecnología y Telecomunicaciones, 2017).

En el marco de políticas de TIC, Costa Rica cuenta con un enfoque específico en los derechos del niño:

Política Nacional para la Niñez y la Adolescencia en Costa Rica, 2009-2021 (PNNA)

Esta política cuya elaboración e implementación fue liderada por el Patronato Nacional de la Infancia (PANI), comprende cuatro niveles o dimensiones de trabajo: Políticas Sociales Básicas, Políticas de Bienestar Social, Políticas de Protección Especial y Políticas de Garantías. Los ejes de la política se orientan hacia el fortalecimiento de los espacios para el



ejercicio de los derechos y la protección de las personas menores de edad, de la institucionalidad, la familia y la comunidad; e incluye el abordaje desde políticas básicas universales: educación, salud y cultura, juego y recreación; y una sección de protección especial (PANI, 2009).

Política Nacional para la Igualdad Efectiva entre Mujeres y Hombres en Costa Rica, 2018-2030

La Política Nacional para la Igualdad Efectiva entre Mujeres y Hombres en Costa Rica 2018-2030 responde a los compromisos internacionales sobre derechos humanos y la igualdad efectiva, sustentado en la convencionalidad, estos fueron ratificados por Costa Rica que protegen los derechos de las mujeres; en particular la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer (CEDAW) y, en la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra las Mujeres, así como las declaraciones, Acuerdos, Plataformas sobre la materia, y los Objetivos de Desarrollo Sostenible (ODS), que tiene como objetivo que nadie se quede atrás en el Desarrollo (Costa Rica, Instituto Nacional de la Mujeres, 2018).

Política Pública de la persona Joven, 2024

Esta política cuya elaboración y coordinación se realizó a través del Ministerio de Cultura y Juventud (MCJ) en el principal instrumento de las juventudes de 12-35 años para garantizar sus derechos y deberes en el país. En ella se definen cuatro ejes estratégicos: autodeterminación identitaria y cultural, desde la diversidad; participación activa en la esfera de lo social y ambiental; autonomía económica en ecosistemas urbanos y rurales; y protagonismo organizativo y político (Costa Rica, Ministerio de Cultura y Juventud, 2020).

Política Nacional de Discapacidad, 2011-2030 (PONADIS)

Es la política pública diseñada para procurar que todos los actores públicos y privados den cumplimiento a la normativa vigente en discapacidad, esta se dirige al mejoramiento de los derechos de las personas con discapacidad e indica el curso de acción para lograrlo. (Consejo Nacional de la Persona con Discapacidad, 2011).

Política en Tecnologías de la Información del Ministerio de Educación Pública

Tiene como objetivo principal potenciar el acceso, uso y apropiación de las tecnologías de información y la comunicación, para transformar los procesos de enseñanza-aprendizaje y la gestión educativa, en las instancias ministeriales a nivel escolar, regional y central. Está dirigida a todos los niveles y modalidades de enseñanza del sistema educativo público y tiene un claro enfoque de inclusión para toda la población estudiantil. (Ministerio de Educación Pública, 2020).



Política para la primera Infancia: Costa Rica 2015-2020

Esta política tiene como fin promover el desarrollo integral de la primera infancia en garantía del cumplimiento de sus derechos. Además, para la población de personas de 3 a 5 años, cuenta con el lineamiento de garantizar el acceso y cobertura de procesos educativos formales y no formales de calidad y adaptados a las necesidades de desarrollo, incluyendo el uso de las tecnologías de la información (TIC). (Patronato Nacional de la Infancia, 2025).

Política Nacional contra la Trata de Personas 2030

Dicho instrumento se basa en las necesidades reales y prioritarias de la población en materia de prevención, persecución y sanción del delito y establece los mejores y más eficaces procedimientos para brindarles a las víctimas detectadas y rescatadas, sean nacionales o extranjeras, la mejor asistencia y atención posibles y los mecanismos para lograr la restitución de sus derechos fundamentales y la reintegración a la sociedad.

Marco Normativo/Marco Reglamentario

Costa Rica cuenta con un robusto marco normativo y reglamentario que se describe a continuación:

Ley General de las Telecomunicaciones N° 8642

El objeto principal de esta Ley es establecer el ámbito y los mecanismos de regulación de las telecomunicaciones, que comprende el uso y la explotación de las redes y la prestación de los servicios de telecomunicaciones. Esta ley se basa en principios rectores como lo son la universalidad, solidaridad, beneficio del usuario, transparencia, publicidad, competencia efectiva, no discriminación, neutralidad tecnológica, optimización de los recursos, privacidad de la información y sostenibilidad ambiental (Ley General de Telecomunicaciones, 2008).

Legislación en vigor la seguridad en línea

En Costa Rica se ha generado una buena base normativa que le permite responder a la violencia virtual contra NNA. Pero ante los avances tecnológicos que pueden conllevar nuevos delitos, las normas existentes no son suficientes y las reformas normativas necesarias no son lo rápidas que se requiere. De la legislación vigente se puede señalar:

- **Código Penal, Ley N° 4573:** En su título III Delitos Sexuales tipifica los delitos vinculados con la explotación y abuso sexual y otras modalidades de delitos cometidos contra menores de edad, en todas sus modalidades.
- **Ley de Justicia Penal Juvenil, Ley N° 7576:** Se regulan principios, garantías y derechos fundamentales que rigen la materia penal juvenil.



- **Ley Protección de la Persona frente al tratamiento de sus datos personales, Ley N.º 8968** Esta ley tiene como objetivo garantizar, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.
- **Decreto Ejecutivo N° 36274-MICIT**, publicado en el Diario Oficial La Gaceta N° 239 de fecha 09 de diciembre de 2010: Se constituyó la Comisión Nacional de Seguridad en Línea como órgano multidisciplinario e intersectorial, conformado por representantes de distintas instituciones públicas y privadas que tienen ámbitos de competencia especial o desarrollan iniciativas referidas al uso seguro, responsable y significativo de la Internet y las Tecnologías Digitales.
- **Ley N° 10020 Ley para la Prevención del Acoso a Personas Menores de Edad por medios electrónicos o virtuales (grooming) y Reformas al Código Penal.** Esta Ley establece un marco regulatorio procura proteger contra el grooming a menores de edad del acoso cibernético y tiene como fin prevenir, combatir y sancionar la comisión de delitos sexuales a través de medios electrónicos o virtuales. También a través de dicha Ley se crea la Comisión interinstitucional para la protección para la persona menor de edad frente a delitos sexuales cometidos a través de medios electrónicos o virtuales.
- **Ley N° 8148 “Adición de los artículos 196 bis, 217 bis y 229 bis al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos”** del 9 de noviembre del 2001, que introdujo nuevos tipos penales.
- **Ley N° 9048 “Reforma de varios artículos y modificación de la Sección VIII, denominada Delitos Informáticos y Conexos, del Título VII del Código Penal”** de fecha 6 de noviembre del 2012.
- **Ley N° 9135 denominada “Reforma de los artículos 196, 196 bis, 230, 293 y 295 y adición del artículo 167 bis al Código Penal”** del 24 de abril del 2013, que introdujo el artículo 167 bis (Seducción o encuentros con menores por medios electrónicos).
- **Ley N° 7899, “Ley Contra la Explotación Sexual de las Personas Menores de edad”** del 17 de agosto de 1999.
- **Ley N° 8590 “Fortalecimiento de la Lucha Contra La Explotación Sexual de las Personas Menores de Edad mediante la reforma y adición de varios artículos al Código Penal, Ley N° 4573, y reforma de varios artículos del Código Procesal Penal, Ley N° 7594”.**



Sin embargo, a pesar de haberse promulgado diversas y variadas legislaciones específicas para combatir la ciberdelincuencia, actualmente en Costa Rica no se tiene una ley especial para esos efectos, ni tampoco una legislación especializada o enfocada en la protección de niñas, niños y adolescentes frente a la violencia en el ciberespacio, es decir lo promulgado no es suficiente, tiene un enfoque adulto centrista, y a nivel de delitos, solo se le da enfoque en delitos sexuales.

Actualmente en Costa Rica no cuenta con una legislación especializada o enfocada en la protección de niñas, niños y adolescentes frente a la violencia en el ciberespacio. Por tanto, la revisión normativa sobre ciberdelitos en perjuicio de la niñez y la adolescencia no podría estar completa si no se entiende de forma sistemática en relación con el marco jurídico convencional que ha sido firmado y ratificado por Costa Rica, tanto en materia de protección de los derechos de la niñez y la adolescencia, y en lo concerniente a la ciberdelincuencia.

De esta manera, en resumen, se pueden citar los siguientes instrumentos vigentes en materia de protección y garantía de los derechos de los niños y las niñas:

- **Convención sobre los Derechos del Niño**, Ley N°7184 del 9 de agosto de 1990 Compromiso de Estado de respetar los derechos enunciados en la Convención y asegurar su aplicación a cada niño sujeto a su jurisdicción.
- **Ley Orgánica del Patronato Nacional de la Infancia**, Ley N°7648 del 9 de diciembre de 1996 Protege especialmente y en forma integral a las personas menores de edad y sus familias.
- **Ley de Pensiones Alimentarias**, Ley N° 7654 del 19 de diciembre de 1996 Regula lo concerniente a la prestación alimentaria derivada de las relaciones familiares, así como el procedimiento para aplicarla e interpretarla.
- **Ley contra el Hostigamiento Sexual en el Empleo y la Docencia**, Ley N°7476 del 3 de febrero de 1995 Prohíbe y sanciona el acoso u hostigamiento sexual como práctica discriminatoria por razón del sexo, contra la dignidad de la mujer y del hombre en las relaciones laborales y de docencia.
- **Reglamento para prevenir, investigar y sancionar el hostigamiento sexual en el Ministerio de Educación Pública**, Decreto Ejecutivo N° 26180-MEP del 4 de julio de 1997 Establece el procedimiento disciplinario para investigar y sancionar el acoso u hostigamiento sexual como práctica discriminatoria en razón del género, que atenta contra la dignidad de la mujer y el hombre, el niño y la niña, en las relaciones jurídicas que se establecen dentro del Ministerio de Educación Pública.



- **Código de la Niñez y la Adolescencia**, Ley N° 7739 del 6 de enero de 1998 Constituye el marco jurídico para la protección integral de los derechos de las personas menores de edad.
- **Ley General de Protección a la Madre Adolescente**, Ley N° 7735 del 19 de diciembre de 1997 Regula todas las políticas, las acciones, los programas preventivos y de apoyo, que ejecuten las instituciones gubernamentales dirigidas a madres adolescentes.
- **Ley contra la explotación sexual de las personas menores de edad**, Ley N°7899 del 28 de julio de 1999 Reformas al Código Penal donde se establecen sanciones penales a tipo de delitos contra la integridad y libertad sexual de las personas menores de edad.
- **Centros de Atención Integral**, Ley N° 8022 del 21 de setiembre del 2000 Promueve la creación, el desarrollo y el financiamiento adecuado de los centros de atención integral públicos, privados y mixtos para personas hasta de 12 años, en acatamiento de la Convención de los Derechos del Niño y los alcances del Código de la Niñez y la Adolescencia.
- **Ley General de la Persona Joven**, Ley N° 8261 del 2 de mayo del 2002; Elaborar, promover y coordinar la ejecución de políticas públicas dirigidas a crear las oportunidades, a garantizar el acceso a los servicios e incrementar las potencialidades de las personas jóvenes para lograr su desarrollo integral y el ejercicio pleno de su ciudadanía, en especial en el campo laboral, la educación, la salud preventiva y la tecnología.
- **Aprobación del protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres, niñas y niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional**, Ley N° 8315 del 4 de noviembre del 2002.
- **Reglas sobre conformación y funcionamiento de los Equipos Interdisciplinarios previstos en el Código Procesal Penal y el Circular N°13- 98** emitida por Corte Plena el 14 de julio de 1998 Creación de equipos interdisciplinarios expertos en la atención de personas menores y mujeres víctimas de cualquier tipo de agresión y delitos sexuales.
- **Ley de Justicia Penal Juvenil, N° 7576**, serán sujetos de esta ley todas las personas que tengan una edad comprendida entre los doce años y menos de dieciocho años al momento de la comisión de un hecho tipificado como delito o contravención en el Código Penal o leyes especiales.

Legislación en la que se exprese la voluntad política de dar prioridad a la PleL (Protección Infantil en Línea).



Desde la adopción de la Convención sobre los Derechos del Niño en 1990, Costa Rica se ha comprometido formalmente a respetar los derechos de las personas menores de edad, a quienes considera personas sujetas de derechos. Varias leyes nacionales e internacionales responden a este compromiso y constituyen el Sistema Nacional de Protección Infantil, que, a través de la participación de una serie de actores institucionales, procura coordinar las acciones para la protección de los derechos civiles, políticos, económicos, sociales y culturales que requiere esta población. Costa Rica ha aprobado una serie de leyes que protegen a la niñez: la Ley contra la Violencia Doméstica (1996), la Ley General de Protección a la Madre Adolescente (1997), la actualización de la gestión del Patronato Nacional de la Infancia (PANI) (1997), el establecimiento del Código de la Niñez y la Adolescencia (1998) y la Ley contra la Explotación Sexual de Personas Menores de Edad (1999).

Sin embargo, la base jurídica de la protección de la niñez en línea en Costa Rica la provee, principalmente, la Ley de Protección de la Niñez y la Adolescencia frente al Contenido Nocivo de Internet y Otros Medios Electrónicos (N° 8934, del 27/04/2011). Las disposiciones de esta ley se extendieron a los cibercafés el 23 de marzo de 2012 mediante el Decreto Ejecutivo N° 31763, Reglamento de Control y Regulación de Locales que ofrecen Servicio Público de Internet. Además, la Ley N° 9135 de 2013 modificó el Código Penal con la adición del Artículo 167 bis (Seducción o encuentros con menores por medios electrónicos), que sanciona con dos o tres años de prisión a quien, a sabiendas y con conocimiento del carácter del material, establece una comunicación que incluya contenido pornográfico por medios digitales con una persona menor de edad. El Decreto Ejecutivo N° 31764 del 26 de abril de 2004 introdujo el Reglamento de Funcionamiento de las Salas de Videojuegos o Juegos Cibernéticos y la Clasificación de los Juegos según el Nivel de Violencia, que dispone normas para su etiquetado y clasificación de acuerdo con las normas internacionales (OCDE 2020).

- **Ley N° 7184, Convención sobre los Derechos del Niño:** Costa Rica ratificó la Convención sobre los Derechos del Niño del 20 de noviembre de 1989, mediante Ley N° 7184 del 9 de agosto de 1990.
- **Ley N° 8172, Protocolo Facultativo de la Convención sobre los Derechos del Niño,** en el año 2002 se ratificó el protocolo en lo relativo a la venta de niños, la prostitución infantil y utilización de niños en la pornografía mediante.
- **Ley N° 8122, Convenio N° 182 de la Organización Internacional del Trabajo sobre "La Prohibición de las Peores Formas de Trabajo Infantil y la Acción Inmediata para su Eliminación".**
- **Ley N° 8934, Protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos.** Esta es aplicable a los locales con acceso



al público, destinados al uso público de computadoras conectadas a Internet u otras formas de comunicación en red, sea por medio de computadoras y de cualquier otro medio electrónico, que sean utilizados por personas menores de edad.

- **Ley N° 9452 Convenio de Budapest:** En el campo propiamente de los delitos informáticos, en el año 2017 se ratificó la Convención sobre Ciberdelincuencia (Convenio de Budapest) ratificada mediante la citada ley de fecha 03 de julio del 2017.
- **Decreto Ejecutivo N° 36274 del 17 de noviembre de 2010,** Creación de la Comisión Nacional de Seguridad en Línea. Esta Comisión, se encargará de diseñar las políticas necesarias sobre el buen uso de Internet y las Tecnologías Digitales contribuyendo a generar una cultura de comprensión, análisis y responsabilidad personal, que les permita beneficiarse de las ventajas de su utilización, y tener una actitud consciente y proactiva frente a los riesgos inherentes al uso de estos recursos.
- **Ley N° 9952, Día nacional de la lucha contra el "grooming",** se declaró en Costa Rica el 13 de noviembre de cada año como Día Nacional de la Lucha contra el "Grooming". Además, se estableció que Corresponde al Consejo Superior de Educación (CSE) la realización de actos informativos, de capacitación y formación para los alumnos y padres de familia, a efectuarse en los centros educativos públicos y privados del país, en los niveles de educación básica y diversificada, que permitan técnicas y formas de cómo reconocer y evitar el "grooming". Asimismo, se designó al Consejo Superior de Educación (CSE) como el ente que realizará campañas informativas alusivas a la celebración de este día, mediante exposiciones, ferias, concursos literarios, charlas, publicaciones en redes sociales y cualquier otro medio o mecanismo que permita que la población en general conozca la importancia de luchar contra la práctica del "grooming" (Asamblea Legislativa, 2021).

Por otro lado, en el marco de la celebración de este día los medios de comunicación masiva, que utilizan el espectro radioeléctrico para sus operaciones radiales y televisivas, estarán obligados, según lo establecido en el artículo 11 de la 1758, Ley de Radio, de 19 de junio de 1954, a brindarle de forma gratuita al Consejo Superior de Educación para que el Ministerio de Educación (MEP) utilice el espacio mínimo de media hora, que le corresponde por semana, para la divulgación de informaciones, acciones, programas, cápsulas informativas, así como los proyectos que se han realizado en el país para la erradicación de la práctica del "grooming" (Asamblea Legislativa, 2021).

- **Ley para la prevención del acoso a personas menores de edad por medios electrónicos o virtuales (Grooming) y reformas al Código Penal, Ley N° 10020:** Establece un marco regulatorio de referencia para prevenir, combatir y sancionar la



comisión de delitos sexuales a través de medios electrónicos o virtuales conocido como grooming, con el fin de proteger a las personas menores de edad del acoso, así como incrementar las penas que castigan los delitos de corrupción y seducción de la persona menor de edad o incapaz por medios electrónicos o virtuales, regulados en la Ley 4573, Código Penal, de 4 de mayo de 1970. Entre los principales puntos de esta ley se señalan los siguientes:

- **Creación de Comisión Interinstitucional.** Se crea la Comisión interinstitucional para la protección para la persona menor de edad frente a delitos sexuales cometidos a través de medios electrónicos o virtuales. Estará adscrita al PANI y contará con integrantes del Ministerio de Educación, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones y Organismo de Investigación Judicial.
- **Reformas al Código Penal.** Con la nueva ley se reforman los artículos 167, 167 bis, 168, 173, 173 bis y 174 de la Ley 4573, Código Penal, de 4 de mayo de 1970. Algunas de las reformas con las que se amplían las sanciones son las siguientes:
 - **Artículo 167 Corrupción.** Se establece que será sancionado con pena de prisión de cuatro a nueve años quien mantenga o promueva la corrupción de una persona menor de edad o incapaz, con fines eróticos, pornográficos y obscenos, en exhibiciones o espectáculos públicos o privados, aunque la persona menor o incapaz lo consienta. La pena será de seis a doce años de prisión, si el actor, utilizando las redes sociales o cualquier otro medio informático o telemático, busca encuentros de carácter sexual para sí o para otros, con una persona menor de edad o incapaz, aunque la víctima consienta participar.
 - **Artículo 167 bis. Seducción o encuentros con persona menor o incapaz por medios electrónicos.** Será reprimido con prisión de dos a cuatro años quien, por cualquier medio, establezca comunicaciones de contenido sexual o erótico con una persona menor de edad o incapaz. La misma pena se impondrá a quien suplantando la identidad de un tercero o mediante el uso de una identidad falsa, por cualquier medio, procure establecer comunicaciones de contenido sexual o erótico, ya sea que se incluyan o no imágenes, videos, textos o audios, con una persona menor de edad o incapaz. La pena será de tres a cinco años, en las conductas descritas en los dos párrafos anteriores, cuando el actor procure un encuentro personal en algún lugar físico con una persona menor de edad o incapaz. La legislación incrementa también las penas al reformar otros artículos del Código Penal sobre corrupción agravada, fabricación, producción o



reproducción de pornografía, tenencia de material pornográfico con presencia de un menor de edad o incapaz o por difusión de pornografía (UNICEF, 2021).

Notificaciones-contenido ilícito / Notificaciones-preocupaciones de los usuarios

Sí, existe normativa que regula este tipo de contenidos, sin embargo, a continuación, se explica el detalle del marco normativo e institucional que estipula las circunstancias bajo las cuales se regulan dichos actos.

El país cuenta con un marco normativo que rige al Sector de Telecomunicaciones, en particular, la **Ley General de Telecomunicaciones Nº 8642**, desarrolla el régimen de privacidad y de protección de los derechos e intereses de los usuarios finales de los servicios de telecomunicaciones. Los acuerdos entre operadores, lo estipulado en las concesiones, autorizaciones y, en general, todos los contratos por servicios de telecomunicaciones que se suscriban de conformidad con esta Ley tendrán en cuenta la debida protección de la privacidad y los derechos e intereses de los usuarios finales. En este caso le corresponde a la Superintendencia General de Telecomunicaciones velar porque los operadores y proveedores de estos servicios cumplan lo establecido en este capítulo y lo que reglamentariamente se establezca (LGT, 2008).

De este modo, establece en el artículo 42 lo siguiente en relación con la privacidad de las comunicaciones y protección de datos personales:

“Los operadores de redes públicas y proveedores de servicios de telecomunicaciones disponibles al público, deberán garantizar el secreto de las comunicaciones, el derecho a la intimidad y la protección de los datos de carácter personal de los abonados y usuarios finales, mediante la implementación de los sistemas y las medidas técnicas y administrativas necesarias. Estas medidas de protección serán fijadas reglamentariamente por el Poder Ejecutivo.

Los operadores y proveedores deberán adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios. En caso de que el operador conozca un riesgo identificable en la seguridad de la red, deberá informar a la Sutel y a los usuarios finales sobre dicho riesgo. Los operadores y proveedores deberán garantizar que las comunicaciones y los datos de tráfico asociados a ellas, no serán escuchadas, gravadas, almacenadas, intervenidas ni vigiladas por terceros sin su consentimiento, salvo cuando se cuente con la autorización judicial correspondiente, de conformidad con la ley” (LGT, 2008).

Por otro lado, desde el punto de vista del rol de las instituciones MICITT y PANI son responsables de promover el diseño, implementación y ejecución de políticas de protección de la niñez según la legislación. Asimismo, tal como se explicó anteriormente, el ente



regulador del sector de telecomunicaciones, la normativa establece que la SUTEL, es la entidad responsable de la ejecución de las disposiciones relativas a la normativa en materia de daños contenidos en Internet y otros medios electrónicos. El Poder Ejecutivo es responsable de coordinar las políticas y asegurar el cumplimiento. Cuando el PANI tenga conocimiento de una situación que vulnere los derechos de uno o más menores, utilizando medios digitales en Internet, debe coordinarse con las instituciones relevantes y remitir asunto a la Corte. Esta entidad se apoya en las disposiciones del Código de la Niñez y la Adolescencia, Artículo 111. (OECD, 2020).

Seguidamente, el país a través de la **Ley N° 8934 para la Protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos**, la cual será aplicable a los locales con acceso al público, destinados al uso público de computadoras conectadas a Internet u otras formas de comunicación en red, sea por medio de computadoras y de cualquier otro medio electrónico, que sean utilizados por personas menores de edad.

De esta forma en el artículo 2 se establece que las personas propietarias y las personas encargadas de la administración de los establecimientos regulados, en esta Ley, deberán instalar filtros en todas las computadoras destinadas a personas menores de edad, incluidos los navegadores, los servicios de comunicación en red por computadora o cualquier medio electrónico de comunicación, y en los programas de intercambio o los programas especiales para bloquear el acceso a sitios y comunicaciones cuyo contenido incluya:

- a. *Sitios que muestren o promuevan la pornografía en general y la infantil, en particular.*
- b. *Sitios que promuevan el lenguaje obsceno.*
- c. *Sitios que promuevan la agresión y la violencia física, sexual y emocional.*
- d. *Sitios que promuevan la construcción de armas o explosivos.*
- e. *Sitios que promuevan e inciten el uso de drogas de uso no autorizado.*
- f. *Sitios que promuevan actividades bélicas.*
- g. *Sitios que promuevan el racismo, la xenofobia o cualquier otra forma de discriminación contraria a la dignidad humana, de conformidad con el artículo 33 de la Constitución Política y los instrumentos internacionales de derechos humanos vigentes en Costa Rica.*
- h. *Los programas o la información que puedan ser usados para mirar, descargar, distribuir, adquirir e intercambiar pornografía en general e infantil, en particular (Asamblea Legislativa, 2011).*

El Estado, por medio de las instituciones dedicadas a la protección de la niñez y la adolescencia, facilitará el acceso a los filtros y programas señalados de manera gratuita o a



bajo costo. Además, mediante la presente ley se establece la obligación de los proveedores de servicios de Internet, donde todo proveedor de servicios de acceso a Internet que ofrezca o venda estos servicios al público deberá incluir, dentro de su oferta de servicios, la opción de adquirir los filtros y demás programas especiales para bloquear el acceso a sitios con los contenidos indicados en el artículo citado anteriormente. Asimismo, en el artículo 4 de la ley supracitada se define el detalle de los procesos de fiscalización, regulación y control de los requerimientos y las estipulaciones le corresponderá a la Sutel, de conformidad con la Ley N° 8642, de 30 de junio de 2008, así como a las municipalidades y al Ministerio de Salud, en lo que se refiere al otorgamiento de las patentes municipales y los permisos sanitarios respectivos. De igual forma, será competencia de la Sutel lo siguiente:

- a. *Resolver el procedimiento administrativo procedente para determinar el incumplimiento de dichos requerimientos y proceder a la imposición de la sanción que corresponda, o bien, a la cancelación de la autorización de funcionamiento respectiva, en su caso. Lo anterior, sin demérito de las competencias que al efecto tengan el Ministerio de Salud y las municipalidades, de conformidad con el ordenamiento jurídico vigente.*
- b. *Certificar, como locales libres de pornografía y contenidos nocivos, a los establecimientos que instalen filtros o programas en todas sus computadoras, según lo estipulado en el artículo 2, los cuales quedarán exentos de realizar la adecuación de cubículos señalada en el segundo párrafo del artículo 3 de la presente Ley (Asamblea Legislativa, 2011).*

Además, en el documento “*Mapeo de la Capacidad institucional en prevención y respuesta a la explotación y abuso sexual en línea, 2018*” se indicó que en relación con los procedimientos de alerta y remoción de contenido local y bloqueo de contenido de Explotación Sexual en Línea es un asunto implica que la Industria de tecnología y telecomunicaciones, incluso por iniciativa propia toma medidas para bloquear información, datos, videos u otros vinculados a esta violencia. En este aspecto la industria no ha enviado registro a las autoridades nacionales (PANIAMOR, 2018).

De igual forma, la FANNA señaló que existe coordinación entre este ente y los operadores mediante los procesos de monitoreo y en coordinación con las instancias judiciales correspondientes.

En ese sentido, según el *Mapeo de la Capacidad Institucional en prevención y respuesta a la explotación y abuso sexual en línea* realizado en 2018, en lo referente a la industria, no hay registro oficial de remoción local y bloqueo de contenido de Explotación Sexual en Línea, por iniciativa propia de los operadores móviles⁵⁰.

⁵⁰https://crianzatecnologica.paniamordigital.org/sites/default/files/recursos_apoyo%20paniamor_prevenccion_y_respuesta.pdf



Asimismo, se señala que existen protecciones estatutarias que permiten a la industria reportar completa y efectivamente los casos, incluyendo transmisión de contenidos a fuerzas policiales o autoridad competente. Esto se refiere a que es la misma Industria la que denuncia los casos de Explotación Sexual en Línea, sin embargo, a la fecha, desde el MICITT no se dispone de registro de estas acciones, aunque la legislación nacional lo permite.

En relación con este tema, el ICE señaló que cuenta con servicios de monitoreo que permiten identificar y bloquear páginas maliciosas o tráfico irregular a nivel empresarial. También existen herramientas para el control parental, no obstante, mediante la coordinación interinstitucional se deben robustecer estas medidas desde colegios, escuelas y espacios para padres familia.

Si bien es cierto, no existen estudios específicos sobre el conocimiento y eficacia de los mecanismos de denuncia e información sobre delitos de EASNNAL; en el Sondeo desarrollado por el MICITT en 2020 se consultó a las personas menores de edad participantes si sabían cómo actuar al enfrentar una situación incómoda, peligrosa o violenta en internet, a lo que el 84% respondió afirmativamente.

Por otra parte, actualmente no existe una línea de ayuda o denuncia específica para los casos de violencia en línea. Tampoco existen protocolos de atención específicos para personas menores de edad y sus familias a la hora de hacer la denuncia. Asimismo, muchos funcionarios no están sensibilizados sobre las nuevas formas de ciberdelincuencia y no cuentan con capacidad instalada necesaria para atender a las demandas de la población, en especial a aquellos grupos en condiciones de vulnerabilidad. Además, es importante resaltar que los centros educativos por medio de protocolos y espacios organizativos establecidos en las dinámicas de estos centros.

Actores y partes interesadas

En Costa Rica aún no está designada una sola autoridad para la protección de la infancia en línea, en primera instancia el **Patronato Nacional de la Infancia (PANI)** es la institución rectora en materia de derechos de la niñez y la adolescencia, y cuenta con normativa nacional e internacional que se deriva principalmente de la Convención sobre los Derechos del Niño, ratificada por Costa Rica en 1990, el Código de la Niñez y la Adolescencia (Ley N° 7739) de 1977 y su Ley Orgánica (Ley N° 7648) de 1996, que se constituyen en el marco legal mínimo para la protección de los derechos de la niñez y la adolescencia en Costa Rica.

Otras entidades desde su competencia ejecutan acciones referidas a la protección en los entornos digitales, principalmente en el marco del **Consejo Nacional de la Niñez y la Adolescencia (CNNA)**, un órgano interinstitucional, intersectorial y colegiado, no desconcentrado, adscrito a la Presidencia de la República.



El CNNA se crea de conformidad con el artículo 170 de la Ley 7739 Código de la Niñez y la Adolescencia, y su funcionamiento se regula mediante el Decreto N° 41452-MP Reglamento del Consejo Nacional de la Niñez y la Adolescencia, publicado en La Gaceta N° 227 del 06 de diciembre del 2018, modificado mediante el Decreto N° 42549-MP del 30 de junio, publicado en La Gaceta N. 228 el 11 de setiembre de 2020.

Dentro de las funciones del CNNA, establecidas en el artículo 171 del Código de la Niñez y la Adolescencia, se encuentra la función de coordinar la acción interinstitucional e intersectorial en la formulación de las políticas y la ejecución de los programas de prevención, atención y defensa de los derechos de las personas menores de edad, conforme con la política de protección integral.

El artículo 172 del Código de la Niñez y la Adolescencia establece que el CNNA estará integrado por nueve ministerios, diez instituciones y cinco representantes de la sociedad civil, para un total de veinticuatro integrantes, quienes cuentan con capacidad de deliberación y decisión sobre los asuntos conocidos en dicho Órgano.

Representación en el CNNA

Ministerios	Ministerio de Educación Pública (MEP)
	Ministerio de Salud (MS)
	Ministerio de Cultura y Juventud (MCJ)
	Ministerio de Trabajo y Seguridad Social (MTSS)
	Ministerio del Deporte (MIDEPOR)
	Ministerio de Justicia y Paz (MJP)
	Ministerio de Seguridad Pública (MSP)
	Ministerio de Planificación y Economía Política (MIDEPLAN)
	Ministerio de Gobernación y Policía (MGP)
Instituciones	Patronato Nacional de la Infancia (PANI)
	Instituto Mixto de Ayuda Social (IMAS)
	Caja Costarricense de Seguro Social (CCSS)
	Instituto Nacional de Aprendizaje (INA)
	Instituto Nacional de las Mujeres (INAMU)
	Instituto de Fomento y Asesoría Municipal (IFAM)
	Consejo Nacional de Personas con Discapacidad (CONAPDIS)
	Dirección Nacional de Desarrollo de la Comunidad (DINADECO)
	Consejo Nacional de la Política Pública de la Persona Joven (CPJ)
	Consejo Nacional de Rectores (CONARE)
Sociedad Civil	Confederación Costarricense de Trabajadores Democráticos (CCTD)
	Unión de Cámaras y Asociaciones del Sector Empresarial Privado (UCCAEP)
	Asamblea Nacional de la Red Nacional Consultiva de la Persona Joven
	Unión de Instituciones Privadas de Atención a la Niñez (UNIPRIN)
	Coalición Costarricense de Organizaciones Sociales para el Seguimiento de la Convención sobre los Derechos del Niño (COSECODENI)
Invitados especiales	Consejos Participativos de la Niñez y la Adolescencia
	Poder Judicial
	Defensoría de los Habitantes de la República (DHR)
	Fondo de las Naciones Unidas para la Infancia (UNICEF)

Varios ministerios y agencias participan en el desarrollo de políticas sobre temas relacionados con la protección en línea de los niños y las niñas. El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) es el órgano rector en el campo de las tecnologías de la información y la comunicación (TIC) y coordina las actividades de la Comisión Nacional



de Seguridad en Línea establecida en 2010 por el Decreto Ejecutivo N° 36274. El objetivo de la Comisión es promover el uso seguro, significativo y productivo de las TIC por parte de las personas menores de edad y empoderar a familias y niños y niñas a través de programas educativos específicos. El Ministerio de Educación Pública (MEP) y el Ministerio de Cultura y Juventud (MCJ) también son miembros de la Comisión Nacional de Seguridad en Línea. El Patronato Nacional de la Infancia (PANI) de Costa Rica, establecido en 1930, es el órgano responsable de la implementación de políticas para niños y niñas y adolescentes; esto incluye planes, programas y proyectos para promover y garantizar los derechos y el desarrollo integral de las personas menores de edad y sus familias, con la participación de instituciones estatales y otros actores sociales. Junto con la sociedad civil, el PANI participa en acciones para salvaguardar la integridad física y emocional de los niños y niñas y adolescentes que se exponen a situaciones de alto riesgo y cuyos progenitores no pueden cuidarlos adecuadamente. El Consejo Nacional de la Niñez y la Adolescencia, un organismo creado por la Ley N° 7739 en 1998, está adscrito al Poder Ejecutivo y provee un espacio para el debate, la consulta y la coordinación entre el Ejecutivo, las instituciones estatales descentralizadas y las organizaciones comunitarias representativas. Tiene el poder de garantizar que la formulación y la implementación de políticas públicas sean consistentes con la visión del país de un marco jurídico integral para la protección de los derechos de las personas menores de edad, de conformidad con el Código de la Niñez y la Adolescencia (CNA) y de acuerdo con los principios establecidos. La Comisión Nacional Contra la Explotación Sexual Comercial de Niños, Niñas y Adolescentes (CONACOES) también participa en la prevención de la explotación sexual en línea de niños, niñas y adolescentes. La CONACOES pertenece al Consejo Nacional de la Niñez y la Adolescencia. Recibe su legitimidad del Patronato Nacional de la Infancia.

Las organizaciones no gubernamentales (ONG), las empresas y la sociedad civil desempeñan una función central en el desarrollo y la implementación de políticas y están representadas tanto en el Consejo Nacional de la Niñez y la Adolescencia como en la Comisión Nacional de Seguridad en Línea.

Las ONG más importantes de la Comisión Nacional de Seguridad en Línea son la Fundación Paniamor y la Fundación Omar Dengo, ambas creadas en 1987 como entidades sin fines de lucro. El Ministerio de Relaciones Exteriores designó en 2005 a la Fundación Paniamor como la institución con mejores prácticas en cooperación internacional. Su misión es catalizar cambios duraderos en la calidad de vida de los niños y niñas para promover el cumplimiento de las leyes que protegen los derechos de la niñez en Costa Rica. La Fundación Omar Dengo tiene como objetivo desarrollar y mejorar la calidad de la educación a través de la informática y la aplicación de nuevas tecnologías en el sistema educativo costarricense (OCDE 2020).



En efecto, Costa Rica cuenta con diversas organizaciones que representan a la sociedad civil y al mismo tiempo desarrollan programas para la sensibilización, desarrollo de habilidades y destrezas digitales, así como el fortalecimiento del ejercicio de la ciudadanía digital; en ese sentido, también se destaca que Fundación Paniamor, World Vision, Aldeas SOS y Pueblito Costa Rica forman parte de las organizaciones aliadas en el marco de la implementación de la Estrategia EASNNAL.

A continuación, se menciona en detalle su rol dentro de las comunidades costarricenses y su marco de acción:

1. Fundación PANIAMOR⁵¹

Esta organización de sociedad civil centra su quehacer en el desarrollo y cabildeo de Tecnologías Sociales costo-efectivas para el enfrentamiento de desafíos en el ámbito de su especialidad, identificados como prioritarios para el país en dos ejes fundamentales: la prevención de violencias y exclusión social. Es así que promueve la Cultura Tecnológica como un modo de vida basado en un conjunto de saberes, prácticas, rutinas, conocimientos, relaciones psicosociales que le permiten a la persona, sin importar su edad, la decodificación del lenguaje y normas que rigen las tecnologías de la información y comunicación (TIC).

Bajo la premisa de que la persona es más competente y más productiva cuanto más acceso y capacidad tiene de seleccionar y construir información, desde el año 1998 Paniamor ha venido fortaleciendo el programa de Cultura Tecnológica para promover el conocimiento y el acceso a los recursos de la sociedad de la información a las personas menores de edad, y sus familias. El Programa Cultura Tecnológica ha incursionado por más de dos décadas en el desarrollo de un conjunto de innovaciones sociales basadas en el uso de las Tecnologías Digitales como herramientas para el mejoramiento de la calidad de vida, la seguridad personal, y el disfrute de ciudadanía digital de niñas, niños y adolescentes, desde los enfoques de derechos y responsabilidades de las personas menores de edad (PANIAMOR, 2021).

De igual forma durante estos años ha articulado con instancias gubernamentales para incorporar el enfoque de los derechos humanos de las niñas, niños y adolescentes en las acciones para la promoción de un uso seguro, responsable, crítico y reflexivo de las tecnologías, a través de estrategias de información, sensibilización y formación a las personas menores de edad, sus referentes familiares e institucionales. A través de los años ha instalado capacidades en diversas entidades con mandatos relacionados a asegurar la inclusión digital, tanto en el acceso y uso de las tecnologías como en la apropiación de estas. Desde el paradigma de la Ciudadanía digital en alianzas público - privadas ha desarrollado diversas estrategias de incidencia política y movilización social para la reforma de leyes, creación de

⁵¹ <http://www.paniamor.org>



política pública y articulación con otros actores no tradicionales para el desarrollo conjunto de planes de acción país.

2. Fundación Quirós Tanzi⁵²

Esta es una organización no gubernamental sin fines de lucro que promueve oportunidades educativas y de desarrollo en escuelas públicas de Costa Rica, por medio de la implementación de las tecnologías móviles. Además, cuenta con diferentes iniciativas y servicios en pro de la innovación y capacitación en el área educativa-tecnológica en el país. Actualmente, forma parte de las organizaciones aliadas en el marco de la implementación de la Estrategia EASNNAL (FQT, 2021).

3. Fundación Omar Dengo⁵³

Esta organización tiene como misión contribuir al mejoramiento de la calidad y equidad de las oportunidades de aprendizaje de la población, para potenciar su desarrollo humano, mediante propuestas y modelos educativos innovadores centrados en las personas y el aprovechamiento de las tecnologías digitales. Además, cuentan con una línea estratégica de Ciudadanía Digital la cual utiliza las tecnologías digitales para que todos sus estudiantes tengan la oportunidad de participar de forma activa en la era digital, igualmente se basan en la construcción de un mundo más justo y pacífico cuando los niños y jóvenes aprenden a interactuar y comunicarse, utilizan la red para debatir, compartir ideas o experiencias e impulsan acciones colaborativas para resolver problemáticas sociales. También forma parte de las organizaciones aliadas en el marco de la implementación de la Estrategia EASNNAL (FQT, 2021).

4. World Vision⁵⁴

Esta es una organización que trabaja por el bienestar de la niñez y adolescencia. Se enfoca en impulsar espacios a nivel nacional y local donde se vele por sus derechos y el desarrollo de habilidades para la vida, creyendo que esos dos elementos les dará un viaje más seguro para sus vidas (World Vision, 2021).

5. Aldeas SOS⁵⁵

Esta es una ONG con más de 40 años de funcionar en Costa Rica, la cual brinda entornos afectivos y protectores a casi 350 niños, niñas y adolescentes que han perdido el cuidado familiar o están en riesgo de que esto suceda, procurando, siempre que sea posible, que se reintegren a sus familias y comunidades (Aldeas SOS, 2021).

⁵² <https://es-la.facebook.com/fundacionquirosanzi/>

⁵³ <https://fod.ac.cr>

⁵⁴ <https://www.worldvision.cr/quienes-somos>

⁵⁵ <https://www.aldeasinfantiles.or.cr/conocenos>



6. Pueblito CR⁵⁶

Es una organización no gubernamental sin fines de lucro localizada en Paraíso, en Cartago. Se constituye como una alternativa de protección de estancia prolongada, alberga en forma permanente a más de 115 niños, niñas y adolescentes, que por distintas circunstancias de riesgo social fueron referidos por el Patronato Nacional de la Infancia (PANI) para ser atendidos en la institución.

7. Defensa de Niños Internacional (DNI)⁵⁷

Este es un movimiento internacional, que nació en 1979 con la finalidad de impulsar la vigencia plena de los derechos humanos de las niñas y los niños en la comunidad internacional y en los Estados. DNI cuenta con un Secretariado Internacional localizado en Ginebra, Suiza, que desempeña acciones de incidencia y presión política dentro de los sistemas y mecanismos de las Naciones Unidas. También dispone de Secciones Nacionales y miembros asociados en 4 continentes (África, Oriente Medio, Europa y América), mismos que encuentran su coordinación en las oficinas regionales, integradas por Vicepresidencias y Desk regionales.

En las Américas, DNI está presente en Argentina, Bolivia, Brasil, Canadá, Colombia, Costa Rica, Trinidad y Tobago y Uruguay, en este último país se mantiene actualmente la Vicepresidencia. Las Secciones Nacionales de DNI son organizaciones de base que identifican y desarrollan programas en respuesta directa a las necesidades y prioridades de las niñas y niños de sus respectivos países. DNI tiene cuatro prioridades temáticas: Justicia para NNA; Eliminación de la violencia contra NNA; NNA en situación de migración; NNA afectados por conflictos armados. También identificamos tres cuestiones transversales de gran relevancia en nuestro trabajo diario: NNA privados de libertad; igualdad de género; participación de NNA (DNI, 2021).

8. Federación de Organizaciones Sociales⁵⁸

Esta es una plataforma de las ONG y Empresas Sociales de Costa Rica, fundada desde 1969, en ese entonces bajo el nombre de Federación de Organizaciones Voluntarias. Relanzada en el 2015 como la Federación de Organizaciones Sociales. Desde su inicio se dedican al fortalecimiento del sector no lucrativo de Costa Rica y a la atención prioritaria de las causas que atienden las ONG del país como organización sombrilla del sector.

Por parte del Poder Judicial son Ministerio Público, Juzgados de Familia, también se destaca el Juzgado de Niñez y Adolescencias, Salas de la Corte Suprema de Justicia.

⁵⁶ <https://www.pueblitocr.com/quienes-somos>

⁵⁷ <https://www.end-violence.org/members/defensa-de-ninas-y-ninos-internacional-dni-costa-rica>.

⁵⁸ <http://www.foscr.org/nosotros/>



Al crearse la Comisión Nacional de Seguridad en Línea, y encomendarse el diseño de las políticas necesarias sobre el buen uso de Internet y las Tecnologías Digitales, se designa al MICITT para presidir dicho grupo por lo que el grado de responsabilidad sobre el tema es alto, sin que esto se contraponga ante la rectoría en temas de infancia que posee el Consejo Nacional de Niñez y Adolescencia.

Autoridad en materia de protección de datos personales

En Costa Rica mediante la Ley N° 8968, Protección de la Persona frente al Tratamiento de sus Datos Personales publicada en el diario oficial La Gaceta N°170 del 5 de setiembre del 2011, se creó la **Agencia de Protección de Datos de los Habitantes (Prodhab)**, institución de desconcentración máxima adscrita al Ministerio de Justicia y Paz, con independencia de criterio y personalidad jurídica instrumental propia en el desempeño de las funciones y en la administración de sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones.

Su principal objetivo es garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes. Asimismo, orienta al ciudadano a ejercitar sus derechos y a las entidades públicas y privadas que manejan bases de datos, a cumplir con las obligaciones que establece dicha Ley. (Agencia de Protección de Datos de los Habitantes. 2021).

Alianzas Nacionales e Internacionales (sector público y sector privado)

En el año 2010 mediante Decreto Ejecutivo N° 36274-MICIT, se creó la Comisión Nacional de Seguridad en Línea (CNSL), la cual es la encargada del diseño de las políticas necesarias sobre el buen uso de Internet y las Tecnologías Digitales, contribuyendo a generar una cultura de comprensión, análisis y responsabilidad personal, que le permita a la población, beneficiarse de las ventajas de su utilización, y tener una actitud consciente y proactiva frente a los riesgos inherentes al uso de estos recursos.

La comisión es coordinada por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones y lo integran representantes del Ministerio de Educación Pública, Ministerio de Cultura y Juventud, Superintendencia de Telecomunicaciones, Poder Judicial, Patronato Nacional de la Infancia, Fundación Paniamor, Fundación Omar Dengo y la Cámara Costarricense de Tecnologías de la Información y la Comunicación.

Además, de esta Comisión se han integrado organizaciones tanto del sector público, privado, académico y sociedad civil, está orientado a generar acciones para mitigar los riesgos del



ciberspacio para las personas menores de edad. (Decreto Ejecutivo N° 36274-MICIT Creación de la Comisión Nacional de Seguridad en Línea, 2010).

En relación a este rubro, el Instituto Costarricense de Electricidad (ICE) agregó que como parte de una Dirección de Ciberseguridad de un operador de telecomunicaciones como el ICE, mediante la identificación de amenazas a las que estamos expuestos basándonos en las debilidades de los sistemas actuales con el fin de identificar controles que minimicen los riesgos, mediante planes de concientización a la población laboral que trascienden no solo al cuidado o la seguridad de la información a nivel laboral sino también a la esfera personal y familiar.

Por otra parte, la Fiscalía Adjunta de Atención de Hechos de Violencia en perjuicio de Niñas, Niños y Adolescentes (FANNA) señaló que se encuentra proponiendo iniciativas legislativas, capacitando en tipologías de delitos, así como los riesgos a los que se exponen las personas menores de edad (PME).

En relación con convenios con las empresas operadoras de telecomunicaciones los alcances han estado mayormente relacionados a iniciativas en el marco de la prevención. En el año 2015, se desarrolló el Taller "*Construyendo Espacios Seguros con las TIC: Propuesta de acción para la protección de la niñez y la adolescencia*", celebrado los días 21 y 22 de setiembre, por parte del MICITT, la empresa MILLICOM Cable Costa Rica S. A. /TIGO y la Fundación Paniamor. Esta actividad tuvo como objetivo, construir propuestas de acción para la protección y seguridad en línea de la niñez y la adolescencia, a partir de la presentación de experiencias tanto nacionales como internacionales, que se encuentran en curso y cuya característica principal fuese el enfoque de prevención y protección de dicha población en el uso de las TIC (Escalante, A. C., 2019). Como parte de sus resultados, surge la iniciativa de constituir el Comité Consultivo del Sector Privado y la Propuesta de Acción para la Protección de la Niñez y Adolescencia, con la participación de las empresas que ofrecen servicios de telecomunicaciones y el apoyo de la Asociación de Empresas para el Desarrollo, UNICEF y *Global System for Mobile Communications Association* conocida como GSMA. Al mismo tiempo, el ICE, CLARO CR Telecomunicaciones S. A., Telefónica Costa Rica TC S.A. y MILLICOM Cable Costa Rica S. A. /TIGO firmaron una "*Carta de Compromiso de los Operadores de Telecomunicaciones de Costa Rica para Apoyar la Estrategia de Seguridad en Línea de la Niñez y Adolescencia Costarricense*" en colaboración con la CNSL con el propósito de impulsar acciones coordinadas que promuevan el uso seguro, responsable y productivo de las tecnologías digitales, por parte de la población en general (MICITT, 2021).

En 2021, se oficializó por parte de los principales operadores del país, en conjunto con las cámaras empresariales de tecnología la iniciativa Código E- mentores.



El Código E- mentores, es un mecanismo de autorregulación que se establece a partir de una adhesión voluntaria por parte del sector industria de las telecomunicaciones y de la sociedad civil que promueve el cumplimiento de estándares para la prevención y respuesta del abuso y la explotación sexual en línea. El Código es una iniciativa liderada por Fundación PANIAMOR con el apoyo institucional del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT); y el Instituto Mixto de Ayuda Social (IMAS). Es una alternativa sostenible para multiplicar acciones orientadas al uso seguro y responsable del Internet por parte de niñas, niños y adolescentes, y sus familias. El proceso de construcción de esta herramienta fue liderado por la Fundación PANIAMOR, en alianza estratégica con Claro, CoopeGuanacaste, Kölbi, Tigo, IBM Costa Rica y Fundación Quirós Tanzi, entidades fundadoras que proponen el cumplimiento de una serie de compromisos por incluir en sus prácticas para la promoción de la inclusión digital y la crianza tecnológica, principios transversales del Código, esta es denominada la Red de Actores. El proceso contó, con el apoyo financiero de End Violence Against Children, The Fund en el marco de la Iniciativa País: Costa Rica dice No a la Explotación y Abuso Sexual en Línea de Niñas, Niños y Adolescentes'; y con el respaldo de la Cámara de Infocomunicación y Tecnología (INFOCOM).

Dentro de los criterios a evaluar para formar parte del programa destacan: la existencia de protocolos que prevengan y respondan ante situaciones de explotación o abuso sexual en línea de niñas, niños y adolescentes; la garantía de contar con capacidades internas para considerar la explotación y abuso sexual en línea de niñas, niños y adolescentes como parte de sus planes estratégicos, tácticos u operativos y finalmente la posibilidad de Multiplicación social o promoción de los principios del Código E- mentores en su cadena de valor y entre sus partes interesadas, sea públicamente o por medio de comunicaciones específicas.

Investigación

Según los resultados de la Encuesta Kids on Line, aplicada en Costa Rica, y publicada en 2018; en uno de los apartados se indagó en la percepción de experiencias de desagrado, molestia y discriminación en Internet, incluyendo contacto con contenido sexual y con personas desconocidas. Específicamente se estudiaron las siguientes experiencias o conductas: 1. Experimentar haberse sentido discriminado 2. Motivos atribuidos a la discriminación 3. Experimentar contenidos en internet que resultaron molestos o incómodos 4. Comunicar a otras personas lo que le hizo sentir mal 5. Ser molestado en Internet 6. Ser tratado de manera desagradable por alguien de la escuela o el colegio 7. Tratar a otros de forma desagradable 8. Tratar a otros de forma desagradable de la escuela o colegio 9. Presenciar a alguien siendo discriminado en Internet 10. Ver imágenes de personas desnudas (solo para adolescentes) 11. Conocer a alguien que haya recibido mensajes de contenido sexual 12. Conocer a alguien que haya enviado mensajes de contenido sexual 13. Recibir



mensajes con contenido sexual 14. Tener contacto con personas desconocidas 15. Tener encuentros personales con personas desconocidas 16. Tener encuentros con personas que son contactos de amigos o familiares. Para ello se consideraron determinantes parentales, comportamentales y contextuales relevantes que permitieran entender estas experiencias o comportamientos.

Por otro lado, en los resultados del sondeo para la construcción e implementación de la Estrategia para la prevención y respuesta a la Explotación y Abuso Sexual de Niñas, Niños y Adolescentes en Línea ejecutado por el MICITT en 2020 destaca el hecho que una gran mayoría de las personas que respondieron (87,3%) aseguró haber recibido orientación e información por parte de personas adultas sobre temas relacionados con el uso seguro de Internet y dispositivos, siendo el entorno familiar (93,4%) y educadores (73,1%) quienes les facilitaron dicha información. A nivel general hay un sentimiento de seguridad propia en el uso de Internet entre las personas menores de edad que participaron del sondeo, pues el 77,7% expresó sentirse seguro utilizando esta herramienta, sin embargo, al ser consultados sobre si otros niños, niñas y adolescentes están seguros en Internet solamente el 25% respondió que sí. El 25% de los niños, niñas y adolescentes que participó en el sondeo afirmaron haber experimentado una situación incómoda, peligrosa o violenta en Internet.

Y si bien no observa un proceso formalmente establecido en Costa Rica para medir y evaluar regularmente la eficacia de las políticas e iniciativas. Los desarrollos y las necesidades emergentes son monitoreados a través de encuestas ad hoc e investigación por centros académicos e instituciones (OECD, 2020).

Sin embargo, en febrero de 2020, la OCDE oficializó el Informe *Digital Economy Policy in Costa Rica*, elaborado por la Secretaría de este ente, como un documento de antecedentes para el examen de adhesión de Costa Rica realizado por el Comité de Políticas para la Economía Digital. En el mismo se incluye un apartado de valoración y recomendaciones del Comité relativas a la protección en línea de los niños y niñas [OCDE/LEGAL/0389] (OCDE, 2020).

Según el documento: *“El principal objetivo de las políticas de Costa Rica para la protección de los niños y niñas en línea es extender a Internet la protección que se les brinda fuera de línea. Los marcos jurídicos sobre protección infantil y comunicaciones reflejan valores fundamentales e incluyen regulaciones específicas para la protección de las niñas y niños en línea”*. Además, destaca el rol fundamental del MICITT, MEP y PANI en dichas acciones, asimismo enfatiza la participación activa que han asumido la Fundación Paniamor y la FOD en la implementación de medidas para empoderar y educar a los niños, niñas, personas adolescentes, docentes, madres y padres, para la concienciación de los medios (MICITT, 2021).



También reconoce que la conformación de la CNSL es “*un buen medio para mejorar la coordinación de los diferentes actores que participan en el desarrollo y la implementación de políticas para la protección en línea de los niños y niñas*”. La recomendación que se brinda al respecto es: “*Mejorar el seguimiento y la medición regular de la evolución de la alfabetización digital de los niños y niñas, promover el crecimiento de una base empírica y analítica sólida para el desarrollo y la implementación de políticas basadas en la evidencia*” (MICITT, 2021).

Indicadores de protección de la infancia en línea:

En particular se cuenta con indicadores base derivados de buenas prácticas internacionales como los estudios de la Red Global Kids Online, cuyo objetivo hacer una medición y diagnóstico periódico de los tipos de usos de la Internet, considerando los usos beneficiosos, oportunidades, limitaciones y riesgos de la Internet en niñas, niños y adolescentes entre los 9 y los 17 años. Sin embargo, se cuenta con datos relacionados al acceso y uso de los distintos servicios de telecomunicaciones y datos relacionados con los actos delictivos en línea dirigidos a personas menores de edad reportados al Organismo de Investigación Judicial. A continuación, el detalle de dichos datos obtenidos de los diversos estudios realizados:

1. Acceso y uso a los servicios de telecomunicaciones e Internet para personas menores de edad entre los 5 y 18 años en Costa Rica, 2020-2021

En la ENAHO del 2021, emitida por el INEC se determinó que la población entre los 5 y 18 años corresponde a 1.045.621 habitantes, representan un 20,2% de la población total en el país (Instituto Nacional de Estadística y Censos, Costa Rica, 2021)⁵⁹. Por otro lado, en cuanto al acceso y uso de los servicios de telecomunicaciones e Internet por parte de las personas menores de edad, que van de los 5 a los 18 años en Costa Rica durante el 2020, esta población correspondió al 81% de las personas usuarias de Internet. En la siguiente ilustración, se muestra el detalle de los datos.

Resumen datos Acceso y uso a los servicios de telecomunicaciones e Internet para personas menores de edad entre los 5 y 18 años en Costa Rica, período 2020-2021



Fuente: Elaboración propia, con datos de la ENAHO, INEC, 2020, 2021.

⁵⁹ <https://www.inec.cr>



2. Resultados del sondeo para la construcción e implementación de la Estrategia Nacional para la Prevención y Respuesta a la Explotación y Abuso Sexual de Niños, Niñas y Adolescentes en Línea, 2021

Como parte del proceso de construcción de la *"Estrategia Nacional para la Prevención y Respuesta a la Explotación y Abuso Sexual de niños, niñas y adolescentes en Línea"*, se realizó una Consulta Pública no vinculante con personas menores de edad, mediante la aplicación de un formulario en línea llevado a cabo entre el 05 y 25 de mayo del 2021.

Este formulario se distribuyó entre esta población con el apoyo de: Asociación Guías y Scout de Costa Rica, Cruz Roja Costarricense, Redes de Desarrollo Local en Región Caribe del Instituto de Formación y Capacitación Municipal de la Universidad Estatal a Distancia, Fondo de Naciones Unidas para la Infancia (UNICEF) y sus redes de colaboración, así como mediante mensajería de texto.

El objetivo del sondeo consistió en obtener opiniones y experiencias de niños, niñas y adolescentes costarricenses entre los 9 y 17 años, tomando como base los contenidos de cada uno de los ejes definidos para la estrategia. En resumen, el cuestionario, contó con 32 preguntas de las cuales 22 fueron preguntas cerradas divididas en cuatro secciones: 1. información básica sobre la persona menor de edad, 2. acceso y uso de Internet y herramientas digitales, 3. riesgos y situaciones enfrentadas en Internet y 4 opiniones sobre las acciones de distintos actores implicados para que Internet sea un lugar más seguro. Asimismo, el cuestionario incluyó un total de 10 preguntas abiertas, en aras de que la persona menor de edad tuviera la oportunidad de expresar sus opiniones y sentimientos o ampliar alguna de las respuestas.

Como resultado del sondeo se obtuvo un total de 400 respuestas de personas menores de edad, distribuidas en las 7 provincias y 58 cantones del país, siendo San José la provincia con mayor respuesta y Puntarenas con la de menor respuesta. Adicionalmente, cerca del 25% afirmaron haber contado con el apoyo de una persona mayor de edad para responder el cuestionario.

El 64% de las personas que respondieron se identificaron como mujeres y 31% como hombres y 5% no se identificaron con algún género. El rango de edad se ubica entre los 9 años a 17 años, en detalle el grupo de 9 a 12 años o menos, corresponde al 47% y de 13 a 17 años, corresponde al 53%.

En términos generales, la población que respondió el sondeo utiliza Internet muy a menudo y realiza un uso intensivo y constante principalmente en el celular (casi 40%), WhatsApp (89%), YouTube (86,5%) y Google (80,3%) fueron las plataformas de mayor uso por parte de las niñas, niños y adolescentes que participaron del sondeo. Un resultado que llamó la atención



fue que el 87,3% aseguró haber recibido orientación e información por parte de personas adultas sobre temas relacionados con el uso seguro de Internet y dispositivos, siendo el entorno familiar (93,4%) y educadores (73,1%) quienes les facilitaron dicha información.

Entre otros hallazgos, se mostró que a nivel general existe un sentimiento de seguridad propia en el uso de Internet entre las personas menores de edad que participaron del sondeo, pues el 77,7% expresó sentirse seguro utilizando esta herramienta, mientras que el 22,3% manifestó que no. Por otra parte, al ser consultados sobre si otros NNA están seguros en Internet solamente el 23,2 % respondió que sí, y el 76,8 % contestó que no. Además, el 25% de los NNA afirmaron haber experimentado una situación incómoda, peligrosa o violenta en Internet.

Sobre la opinión en cuanto a las acciones de distintos actores implicados para que Internet sea un lugar más seguro, algunos comentarios destacaron que el Gobierno debería realizar reformas para conocer cómo se pueden denunciar los delitos de violencia digital que se presentan en este espacio, además que deben contar con un equipo profesional capacitado que se encargue de este tipo de delitos.

Como parte de las soluciones los NNA propusieron la creación de una aplicación o página web para realizar denuncias y a su vez que puedan ayudar a los NNA que sufrieron violencia en Internet, o bien un protocolo o plan para que este sea un espacio seguro y enfatizaron en la necesidad de charlas o capacitaciones sobre los riesgos y el uso correcto del Internet, tanto para los NNA como para los padres, las madres o personas encargadas de crianza.

Los NNA igualmente expresaron que es necesario que los maestros (as) y profesores (as) estén actualizados con lo que pasa en Internet; enseñar y orientar a las personas estudiantes sobre los riesgos, consecuencias y medidas del uso de esta red, atender las acciones de la forma de actuar de algunos (as) estudiantes y brindar la confianza a los NNA para dialogar con ellos, en caso de que tengan un problema o estén siendo víctimas de un riesgo en Internet.

Otra de las medidas que los NNA participantes sugieren es que se realicen videos explicativos sobre las consecuencias de lo que puede pasar en las redes sociales y que se establezcan reglamentos sobre el buen uso del Internet a los niveles de escuelas y colegios.

Por otro lado, los NNA señalaron entre las principales acciones que las empresas de la industria de tecnologías y telecomunicaciones deben realizar destacan: brindar información sobre los riesgos y oportunidades de Internet (79%) seguido de ayudar a las autoridades en las investigaciones que realizan (53%) asimismo ofrecer más filtros y contenidos de seguridad en sus plataformas (44%). Finalmente, los temas de capacitación de personal de las empresas de telecomunicaciones fueron señalados como necesarios por el 36,6% de los participantes.



Entre otras acciones que se podrían implementar, destacó la creación de portales y plataformas seguras exclusivos para personas menores de edad; la detección y filtro de contenido inapropiado; (avisos de seguridad); la colaboración y denuncia de casos a las autoridades, así como el establecimiento de canales directos para denunciar contenidos y situaciones, así como el desarrollo de campañas de información y prevención.

Aproximadamente, el 60% de los NNA participantes respondió que los medios de comunicación informan poco o nada sobre los peligros del uso de Internet, por lo tanto recomiendan que estos colaboren con su seguridad en línea con material de comunicación dirigido a esta población, también consideran que se debe dar una mayor visibilidad de casos relacionados con explotación y abuso sexual de NNA en línea, sus denuncias, cómo se resuelven y su seguimiento, pedir cuentas a las autoridades gubernamentales, difundir consejos y programas más educativos sobre esta temática. Del mismo modo, sugieren más campañas preventivas en medios de comunicación y que éstos apoyen los esfuerzos que se realizan desde las instituciones.

Las acciones planteadas en la Estrategia coinciden con las inquietudes manifestadas por las personas menores de edad que participaron en el sondeo, lo cual es de suma importancia pues asegura que ésta será un instrumento que permitirá atender las necesidades y trabajar hacia la construcción de entornos virtuales más seguros para las personas menores de edad. Asimismo, plantea el reto de incorporar de forma permanente su participación y consulta en el proceso de implementación de dicha Estrategia.

3. Estudio: Usos de tecnología móvil y violencia en línea, Kids Online, Costa Rica 2019

En el 2019, se realizó en Costa Rica, la Encuesta Kids Online, ejecutada por el Instituto de Investigaciones Psicológicas de la Universidad de Costa Rica (IIP-UCR) en conjunto con la Fundación Paniamor cuyo objetivo fue hacer una medición y diagnóstico periódicos de los tipos de usos de la Internet, considerando sus oportunidades, limitaciones riesgos y usos beneficiosos en NNA entre los 9 y los 17 años. La muestra fue de 1.008 personas distribuidos en dos grupos de edad 9 a 12 años y de 13 a 17 años. Además, se incluyó una muestra de 1.008 personas adultas responsables primarias de su cuidado.

Entre los principales hallazgos se destacó que las habilidades digitales, medidas dentro de una escala de 0-10, presentan una considerable variabilidad. Las habilidades digitales totales o generales tienen un puntaje promedio de 6.18; es decir, puede haber algunos NNA con puntajes mayores a 8.5 como aquellos con puntajes menores a 4.

Se destaca que las diferencias son debido a su condición socioeconómica y la zona de residencia, siendo las personas con mayores habilidades digitales las personas adolescentes con mayor condición económica y que habitan en zonas urbanas. También, se encontró que



el entretenimiento, información y comunicación son los principales usos, caracterizados por una variabilidad en su empleo, por tanto, se recomienda promover los usos beneficiosos educativos, sociales y de participación ciudadana mediante la generación de programas que favorezcan la promoción y el uso en contextos escolares como la ciencia, la tecnología y la participación democrática.

Los NNA, desde edades tempranas están expuestos a contenido sexual por Internet, el estudio destaca que el 4% de las personas entre los 9 y 12 años vieron o recibieron mensajes con contenido sexual, mientras que el 16% de las personas entre los 13 y 17 años vieron o recibieron mensajes con contenido sexual, mostrando así que este contenido es más propenso a llegar a adolescentes que a niños y niñas, además se recalca que este aspecto requiere atención por parte de las personas responsables de la crianza de esta población.

El estudio resume que a mayores habilidades digitales y con una mediación parental menos restrictiva los expone a riesgos tanto de recibir mensajes con contenido sexual, contactar a personas desconocidas, así como conductas de discriminación. De lo anterior es posible concluir la importancia de que las habilidades digitales permiten a los menores identificar los riesgos, aunque a su vez los expone a estos mismos. De allí que se requiera de un acompañamiento adecuado por parte de personas cuidadoras que cuentan con un dominio alto de habilidades digitales que puedan mediar las interacciones de los NNA en el uso de las TIC para que puedan disfrutar de sus beneficios y ejercer su ciudadanía digital.

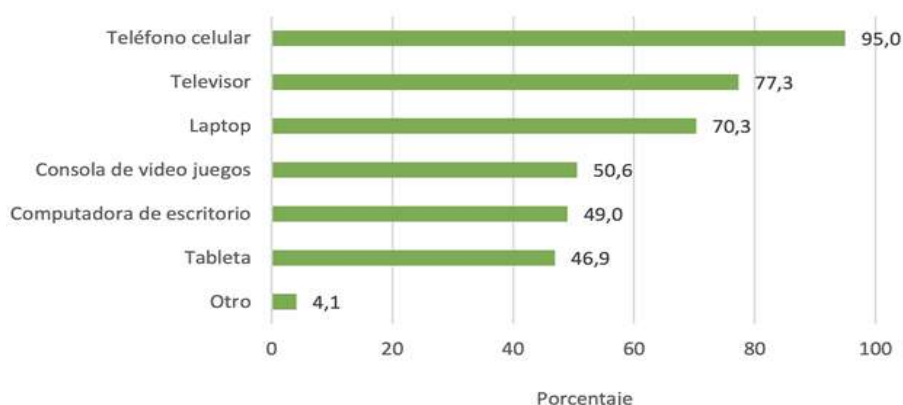
4. Estudio sobre Acceso y Uso de los Dispositivos Móviles e Internet en Niños, Niñas y Jóvenes 2018-2019

En el marco de las competencias de generar información sobre la evolución de las TIC en diferentes poblaciones, el MICITT, desarrolló el estudio "Acceso y Uso de los Dispositivos Móviles e Internet en Niños, Niñas y Jóvenes 2018-2019" (2020), el cual se aplicó a 1.962 personas estudiantes de II ciclo, III ciclo y educación diversificada tanto de escuelas y colegios públicos y privados distribuida a nivel nacional.

Como parte de sus resultados, se obtuvo que el 96,6% de los estudiantes entrevistados han utilizado Internet. El 95,0% de los estudiantes entrevistados utiliza el teléfono celular para acceder a Internet, el 77,3% utiliza el televisor y la computadora portátil (laptop) es usada por el 70,3% como se muestra en el siguiente gráfico.



Distribución porcentual de los estudiantes entrevistados que han usado Internet según dispositivo utilizado para acceder a Internet, período 2018-2019



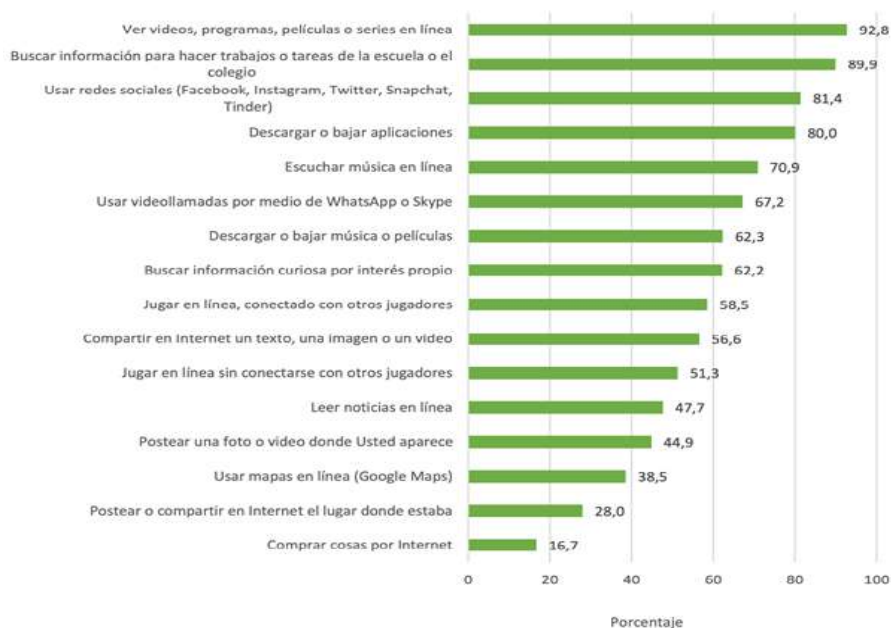
Con respecto a las habilidades computacionales según la zona, los estudiantes de zonas urbanas presentan porcentajes significativamente más altos con respecto a los estudiantes de zonas rurales en las habilidades de uso, exceptuando la de utilizar código para el bloqueo de la pantalla del celular cuyo porcentaje es igual entre estudiantes de zona urbana y rural (75,9 en ambas zonas). Estos resultados evidencian la brecha de conocimiento y uso de estas herramientas computacionales por zona geográfica.

En detalle, las habilidades computacionales que se presentan con mayor frecuencia, entre las que se tienen; conectarse a una red inalámbrica (82,9%); utilizar código para bloquear la pantalla del celular (75,9%); borrar fotos que compartió o recibió (74,4%); eliminar personas de su lista de contactos (71,3%). El índice de habilidades y conocimiento computacional tiene una media nacional de 6,7; este índice oscila en una escala de valores entre 0 y 10. Tanto las personas estudiantes de instituciones y colegios privados presentan una media del índice superior a la media nacional.

Además, se observó que las actividades de uso de Internet que realizan con mayor frecuencia las personas estudiantes son: ver videos, programas, películas o series en línea (92,8%), buscar información para hacer trabajos o tareas (89,9%), usar redes sociales (81,4%) y descargar o bajar aplicaciones (80,0%).



Distribución porcentual de los estudiantes entrevistados según actividades realizadas en Internet, período 2018-2019



Fuente: MICITT, 2020.

Sobre las personas estudiantes de instituciones privadas, en relación con aquellas de instituciones públicas, estas utilizan más Internet para realizar compras; jugar en línea; buscar información, para hacer trabajos o por interés propio; y usar mapas en línea.

También, destaca que las actividades de Internet realizadas por las mujeres con mayor frecuencia que los hombres son: la búsqueda de información para hacer trabajos o tareas; usar redes sociales; escuchar música; y hacer videollamadas. Mientras que las actividades de Internet que los hombres utilizan en mayor proporción que las mujeres son: descargar aplicaciones; jugar en línea y comprar artículos.

Para todas las actividades, los estudiantes de colegio, así como los estudiantes de zonas urbanas, presentan porcentajes de utilización más altos al compararlos con estudiantes de escuela y estudiantes de zonas rurales, respectivamente.

En relación con las actividades de uso se evidencia mediante la media de la escala a nivel nacional es de 6,21 y se observa que los estudiantes de instituciones privadas poseen un nivel en la escala que es significativamente mayor (6,82) al compararlos con los estudiantes de instituciones públicas (6,16), esto debido a que la media de esta población sobrepasa el límite superior de la escala a nivel nacional. Este resultado indica que los estudiantes de instituciones privadas están realizando más actividades utilizando Internet.



5. Uso de Internet en prácticas culturales y formación de estudiantes de secundaria en Costa Rica

En el año 2018, el MICITT realizó un estudio exploratorio con una submuestra de 309 personas con edades entre los 13 y 18 años que asisten a la educación secundaria a partir de los datos de la Encuesta Nacional de Cultura (ENC) 2016.

El objetivo del estudio, denominado *“Uso de Internet en prácticas culturales y formación de estudiantes de secundaria en Costa Rica”* (MICITT, 2018) consistió en identificar las actividades en Internet de formación y prácticas culturales que hacen las personas estudiantes secundaria en Costa Rica, así como conocer los principales determinantes socioeconómicos de las diferencias en su uso e igualmente profundizar el aprovechamiento de las TIC por parte de esta población en los distintos contextos sociales y culturales, y de acuerdo con sus diferentes capacidades, motivaciones e intereses.

Entre los principales resultados destacó que 9 de cada 10 estudiantes de secundaria entrevistados utilizaron la red durante los 30 días anteriores a la aplicación de la encuesta (2016). Este hallazgo pone en evidencia cómo el uso de las TIC está inmerso en la vida cotidiana de las personas y, en particular, en la de las personas jóvenes. Otro hallazgo que se deriva del análisis es el uso más intensivo de Internet que realiza esta población en redes sociales, lúdicas y recreativas; y que en menor medida lo utilizan para adquirir habilidades estratégicas digitales tales como formación y cultura, éstas últimas están más relacionadas con una reducción de la brecha digital desde su perspectiva de apropiación y de uso productivo.

También, se destaca en esta investigación, que cada vez más los centros educativos han incorporado en sus planes de estudio y material didáctico el uso de la red. Además, el acceso a Internet permite compartir contenidos audiovisuales y escritos que transmiten el conocimiento que constantemente se genera en diferentes áreas de la educación.

Asimismo, el estudio pone en evidencia cómo las variables zona de residencia, región de planificación, sexo y tipo de centro educativo (público o privado) son relevantes a la hora de explicar el uso de Internet en las personas jóvenes para formarse y acceder a prácticas culturales.

Al estudiar las diferencias de uso según zona de residencia, se evidencia que, en la rural, el 76,7% de las personas jóvenes utilizan Internet; mientras que, en la zona urbana se registró un uso de 94,4% (18 puntos porcentuales (p.p.) más que en la rural). En relación con el nivel de acceso de acuerdo con la región de planificación, las mayores diferencias se observan entre jóvenes residentes de la Región Huetar Norte como los de menor acceso relativo, con diferencias que oscilan entre los 16 p.p. (respecto a la Región Brunca) y los 31 p.p. de las



Regiones Central y Chorotega. Los resultados que consideran variables de corte regional muestran cómo, acorde con la evidencia empírica, persisten brechas territoriales, una de ellas es el uso de Internet. Para el análisis, los usos de Internet se agrupan en tres categorías: 1. Redes Sociales, 2. Ocio y Diversión y, 3. Cultura y Formación, como se observa en la siguiente ilustración.

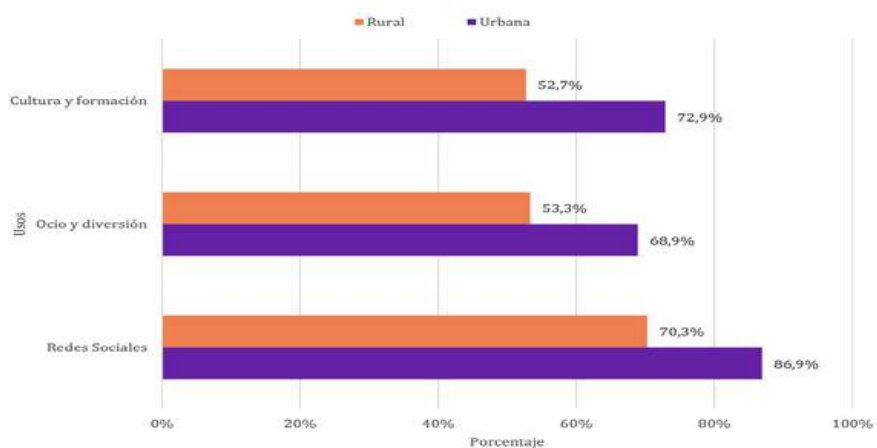
Agrupación de los usos de Internet según categorías



Fuente: MICITT, 2018

Se evidenció que las personas jóvenes de la zona urbana utilizan más Internet que aquellas de la zona rural, indistintamente del grupo de actividades analizado. La diferencia más marcada se observó en la categoría Cultura y formación, donde las personas jóvenes de la zona urbana realizaron alguna actividad de esta categoría 20 p.p. más que aquellas de zona rural, como se muestra en el siguiente gráfico. El menor uso de la red en actividades formativas y en prácticas culturales en las zonas rurales pone en evidencia que en el país persisten inequidades territoriales que se reflejan en diferencias al adquirir habilidades digitales estratégicas.

Porcentaje de jóvenes que usaron Internet en los últimos 30 días según zona por categorías de uso de Internet, año 2016



Fuente: MICITT, 2018



En cuanto al uso de Internet en las prácticas culturales, se encontró que es reducido; solo una quinta parte de las personas jóvenes utilizó Internet para llevarlas a cabo. La práctica más común fue la toma de fotografías; del total de jóvenes que la realizó, sólo 13,0% utilizó Internet. Por otra parte, cerca un tercio de quienes practicaron canto o tocaron un instrumento musical emplearon Internet para ello (31,1% y 32,0%, respectivamente).

6. Uso de Internet en prácticas culturales y formación de estudiantes de primaria en Costa Rica

Con el objetivo de conocer el uso de Internet en Costa Rica por parte de los y las estudiantes de educación primaria en la realización de actividades educativas y prácticas culturales, el MICITT, a través del VT, publicó el estudio “Uso de Internet en prácticas culturales y formación de estudiantes de primaria en Costa Rica” (2020), el cual utiliza los datos de la ENC 2016, realizada por el INEC de Costa Rica. Se analizó una submuestra de 1303 personas con edades entre los 5 y 12 años que asisten a la educación primaria.

Entre los principales resultados, se encontró que 62,1% de los y las estudiantes de 5 a 12 años usaron Internet durante los últimos 30 días, observándose una diferencia de casi 30 puntos porcentuales con respecto al grupo de jóvenes de 13 a 18 años.

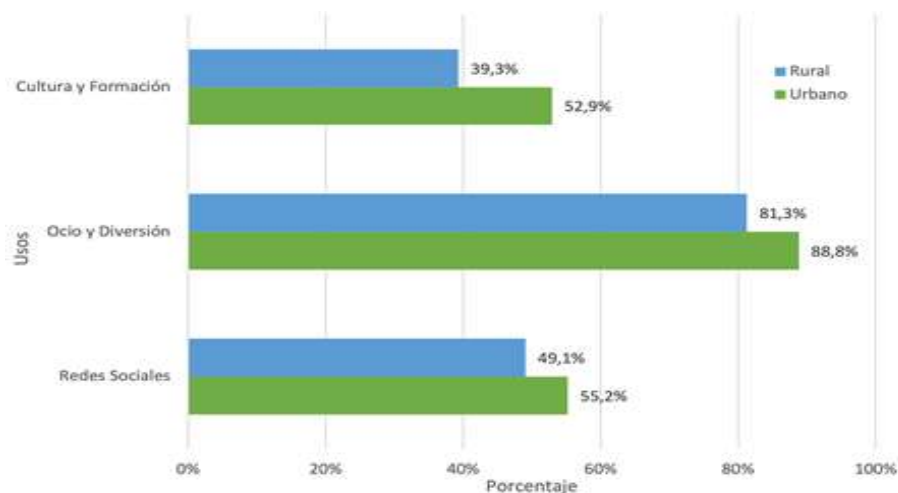
El 69,1% de los niños y niñas que residían en la zona urbana utilizaron Internet en los últimos 30 días, mientras que solo el 45,0% de quienes residían en la zona rural lo hicieron.

Por sexo, se observó que el porcentaje de niñas que usaron Internet fue superior al porcentaje de niños (4,1 puntos porcentuales de diferencia). Según edad, se apreció una tendencia creciente en cuanto al uso de esta herramienta a mayor grupo de edad.

De las actividades realizadas por Internet por los niños y niñas entrevistados, el 87,2% utilizó esta herramienta para actividades de Ocio y Diversión, seguidas de aquellas relacionadas con Redes Sociales (53,9%) y la mitad lo utilizó para actividades de Cultura y Formación como se observa en el siguiente gráfico.



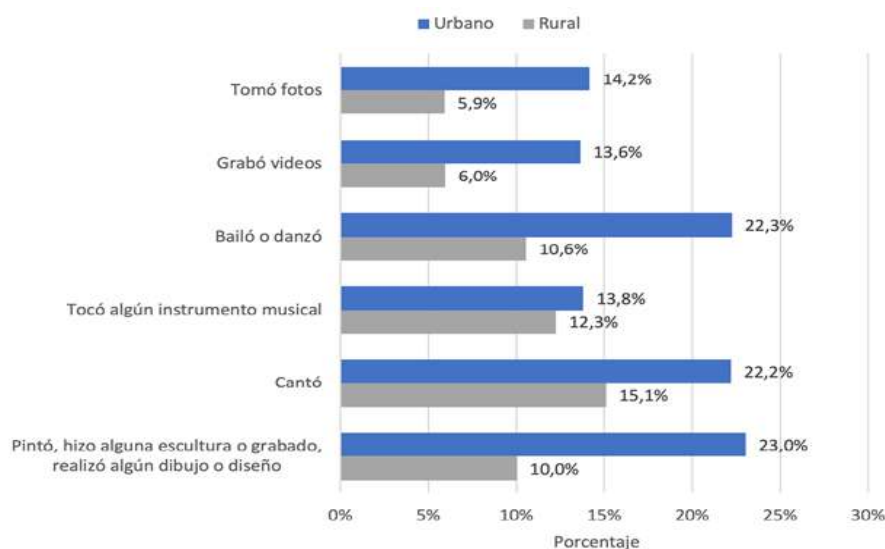
Porcentaje de niños y niñas que usaron Internet en los últimos 30 días según zona por categorías de uso de Internet, año 2016



Fuente: MICITT, 2020

La mayoría de los niños y las niñas que llevaron a cabo prácticas culturales utilizando Internet residían en la zona urbana.

Porcentaje de niños y niñas que realizaron prácticas culturales utilizando Internet según práctica por zona de residencia, año 2016



Fuente: MICITT, 2020.

Este apartado sobre el uso de las telecomunicaciones e Internet enfocado en población menor de edad hace un repaso por los resultados de diversas consultas realizadas a dicha población.

Con base en estos resultados, se ha evidenciado el actual estado en temas como el acceso, los usos, las prácticas culturales y de formación, los retos en materia de seguridad en línea, las destrezas y habilidades con que cuentan y las necesidades que ellos mismos demandan de atención para contar con un entorno más seguro para su desarrollo mediado por las TIC.



Estas solicitudes de los NNA, así como las que surgen en este contexto para los adultos, son fundamentales para el abordaje transversal en el proceso de planificación del PNDDT y fomentar un ejercicio responsable de la ciudadanía digital en su conjunto.

7. Proceso de consulta y participación con niños, niñas y adolescentes sobre brecha y alfabetización digital para la incidencia en la formulación de políticas públicas de Telecomunicaciones. DNI para UNICEF (2021)

En el marco de la construcción del Plan Nacional de Desarrollo de las Telecomunicaciones 2022-2027, la oficina de UNICEF Costa Rica manifestó su interés de contratar una consultoría para realizar un proceso de consulta a población NNA con el fin de recoger insumos que pudieran ser incorporados en dicha política pública y que a la vez pudieran ser aprovechados por UNICEF. Para su ejecución se contrató a la organización Defensa de la Niñez Internacional (DNI) de esto se realizó una consulta abierta a adolescentes y jóvenes con el fin de conocer sus percepciones sobre el contexto, realidades y experiencias sobre el uso de las Tecnologías de Información y Comunicación durante los meses de julio y agosto de 2021. Se contó con la participación de 116 personas entre los 10 y 24 años de edad de las 7 provincias del país con diferentes características sociodemográficas.

Como productos concretos de este proceso la población NNA participante creó contenido creativo digital, donde expresaron sus opiniones finales, por medio de imágenes, videos, audios, etc., y por parte del equipo consultor se elaboraron informes de hallazgos y resultados.

Video: <https://drive.google.com/file/d/1bGqow-gpoBRdR7IOEil1iDsMnoFUOJEd/view?usp=sharing>

Libro cuento:

<https://drive.google.com/file/d/1a6YBmJquS16GR1emC3I4tamT0w4yYO8F/view?usp=sharing>

Perfil Informativo en Instagram: https://www.instagram.com/ntc_costa_rica/

Para las y los participantes el uso de Internet y las TIC representan grandes beneficios tales como la posibilidad de vinculación con sus familias y entre sus pares, en especial por la situación de la pandemia; reconocen en el uso de Internet un derecho y una oportunidad de crecimiento; destacan la necesidad de acompañamiento y guía que requieren para su uso y la necesidad de disminuir las brechas para que todas y todos los niños, niñas y jóvenes puedan tener buenas alternativas de conectividad y acceso a la información.

Como principales barreras en su uso citan limitantes en la cobertura por parte de los programas estatales por miembros de la familia, conectividad baja o escasa, mala calidad de señal en algunos poblados, falta de infraestructura en algunas zonas; dificultades para la adquisición de equipos; falta de acceso en centros educativos y necesidad de capacitación para mayor aprovechamiento.



En cuanto a las vivencias y usos de la población parte del sondeo destacan la incidencia de eventos de riesgo y llama la atención un 25,6% de ellos y ellas que manifiesta haber recibido burlas, amenazas o agresiones verbales.

Situaciones y vivencias de riesgo relacionado al uso de Internet y tecnología



Información vrs Protección



Fuente: DNI, 2021

Asimismo, se les consultó a las personas participantes sobre el conocimiento y acceso a información sobre situaciones que podrían violentar sus derechos o prácticas en el uso del Internet y dispositivos móviles poco más de la mitad de las personas adolescentes y jóvenes conocen qué es *sexting*; *grooming*, *cyberbullying* y *sextorsión*.

Además, afirmaron conocer sobre la práctica de intercambio o solicitud de fotos a chicas o chicos a cambio de dinero o favores sexuales. En general, la población consultada considera que el uso de tecnología debe darse bajo supervisión adulta y un acompañamiento en las escuelas, regulando el tiempo de uso, generando más seguridad y restricciones según edad, y a su vez brindando más información de uso y riesgos. Al respecto apuntan la necesidad de acciones relacionadas con acompañamiento, información adecuada para conocer sobre

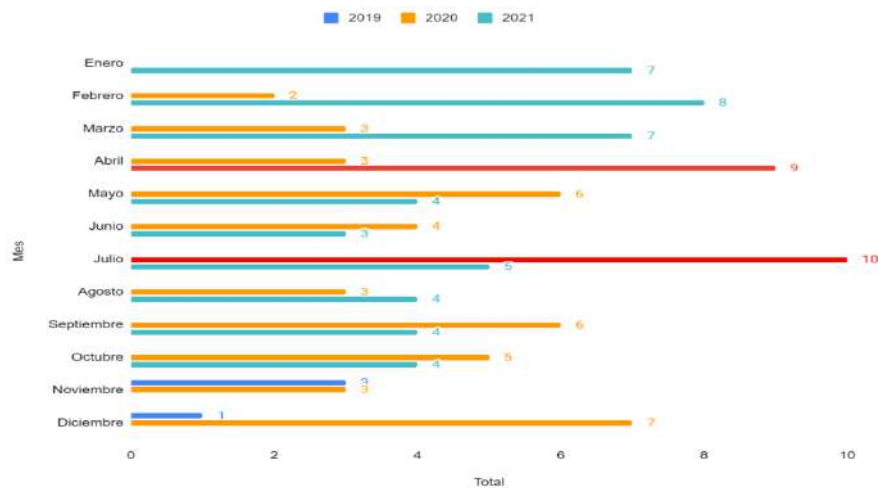


riesgos, manejo de rutas de denuncia, enseñanza de habilidades para el uso de las aplicaciones y programas; mismas percepciones para el tema de la tecnología en adolescentes y jóvenes.

8. Datos Organismo de Investigación Judicial, Unidad de Análisis Criminal

El Organismo de Investigación Judicial reportó el siguiente análisis de la información, seducción o encuentro con personas menores de edad por medios electrónicos, del cual se encuentra el siguiente gráfico que muestra la cantidad de casos por delito de grooming reportados desde el 01 de noviembre de 2019 al 31 de octubre de 2021, mostrando así que en los meses de julio de 2020 y abril de 2021 han sido los meses con mayor número de casos reportados durante este periodo.

Cantidad de casos acumulados en el periodo 2019 a 2021

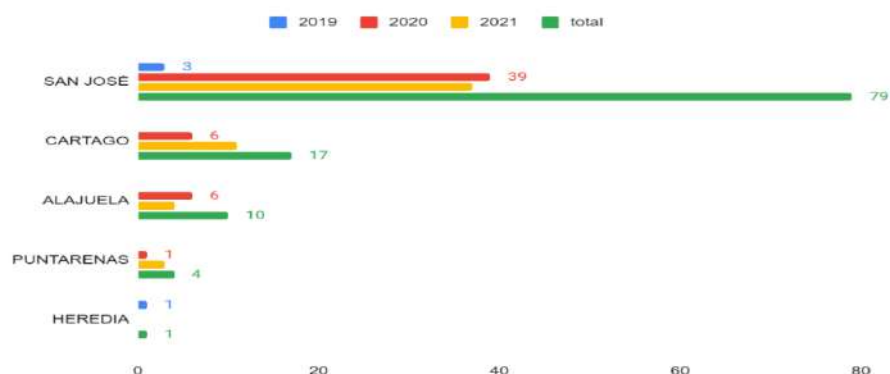


Fuente: OIJ, 2021

Por otro lado, se cuenta con el detalle de los casos de acuerdo al lugar de procedencia se muestra que el total de casos reportados se concentra en mayor número en la provincia de San José, seguidamente el mayor número de casos se concentra en Cartago, luego en Alajuela, seguido de Puntarenas y Heredia siendo estas las dos provincias con menor número de casos reportados. En cuanto a las provincias de Limón y Guanacaste no presentan ningún caso reportado a esta entidad judicial. Es importante aclarar que en la mayoría de las ocasiones en este tipo de delitos la provincia pertenece al lugar de residencia del denunciante.



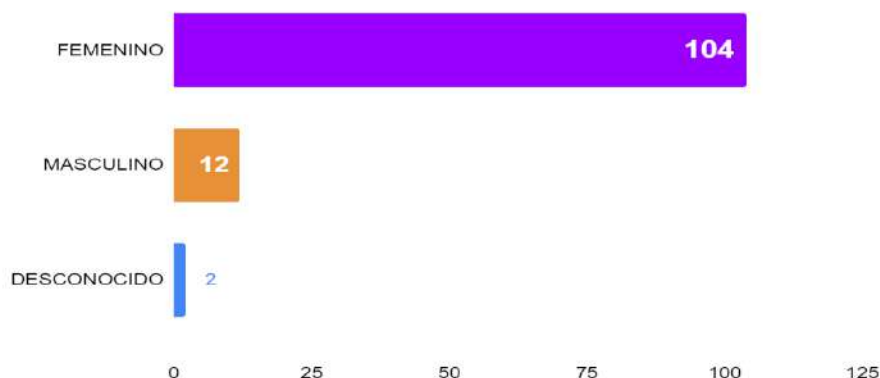
Casos de seducción o encuentro con personas menores de edad por medios electrónicos denunciados por provincia según año



Fuente: OIJ, 2021. Con base en datos tomados del 01/11/2019 al 31/10/2021

Por otro lado, en cuanto al género, la mayoría de las víctimas corresponden al género femenino con 104 casos reportados y del género masculino se reportaron 12 víctimas y 2 casos de quienes no aportaron esta información.

Número de casos reportados según género, 2019-2021



Fuente: OIJ, 2021

Educación en Materia de alfabetización y competencias digitales

Actividades que se realizan en Costa Rica para apoyar la seguridad en línea.

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT) 2015-2021, Costa Rica.

Como parte de la ejecución del Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT), se diseñaron e implementaron actividades para el desarrollo de capacidades, habilidades y destrezas dirigidas a promover el uso seguro, productivo y responsable de Internet por parte de la población. Entre las actividades ejecutadas que se suman a los compromisos asumidos por el MICITT en materia de prevención de la explotación y abuso



sexual de la niñez en línea. Con base en lo anterior, se mencionan los resultados alcanzados de las actividades ejecutadas en el periodo 2020 y 2021.

- **Campaña de comunicación sobre el uso seguro, productivo y significativo de Internet, 2020**

En el mes de junio de 2020, se inició una campaña de comunicación digital con el objetivo de brindar mensajes con información actualizada y con contenidos de calidad para sensibilizar, posicionar conceptos y mantener actualizadas a las personas que han participado en los procesos de capacitación y sensibilización sobre temas de seguridad en línea. Estos mensajes se difundieron, a través de la cuenta de correo electrónico institucional de la Dirección de Evolución y Mercado de Telecomunicaciones y publicaciones realizadas en el perfil de Facebook del Viceministerio de Telecomunicaciones.

- **Actividades virtuales para la promoción y prevención de la seguridad en línea, 2020**

Con el fin de seguir trabajando en la promoción y prevención de la seguridad en línea, y debido al cambio digital que provocó la pandemia del COVID-19, la Dirección de Evolución y Mercado de Telecomunicaciones (DEMT) programó diversas actividades virtuales sobre este tema, tanto de manera proactiva como en conjunto con otras instancias (MICITT, 2021). A continuación, se presentan a detalle cada una:

- **Charla informativa Seguridad en línea y Programa e-mentores dirigida a la Red Apoyo Pyme, Zona Norte, 11 agosto, 2020**

En el marco del Programa de Emprendimiento de la Dirección de Apropiación Social del Conocimiento de MICITT, se colaboró con una charla informativa sobre temas de seguridad en línea y los alcances del Programa e-mentores a las personas que integran la Red de Apoyo a PYMES de la Zona Norte, esto con motivo de promover la formación de nuevos (as) mentores. En la misma participaron alrededor de 20 personas representantes de distintas organizaciones tanto públicas como privadas de la zona. Esta charla informativa se dio en el marco de la reunión de la Red y la cual se encuentra disponible en el siguiente enlace: <https://www.youtube.com/watch?v=qE6xXzICrks&feature=youtu.be>

- **Webinar: Riesgos y oportunidades para nuestras familias frente al uso de los videojuegos en tiempos de COVID-19, 30 junio 2020**

En el contexto mundial a raíz de las medidas sanitarias de la pandemia de COVID-19, tal como el caso del distanciamiento físico, el Fondo de las Naciones Unidas para la Infancia (UNICEF), informó que la empresa Steam, distribuidora de juegos digitales, obtuvo un aumento considerable de personas usuarias alcanzando un récord de 23.5 millones de personas usuarias a principios de abril de 2020, mostrando así que, los videojuegos en línea



se han convertido en una herramienta que permite a las personas continuar conectadas y compartir actividades lúdicas con otras.

Por ello, el MICITT en aras de abordar esta situación como un aporte al trabajo que se ha venido realizando en conjunto con la Comisión Nacional de Seguridad en Línea (CNSL), cuyo objetivo de generar un espacio de sensibilización y análisis del impacto de los videojuegos dirigido a padres y madres de personas menores de edad, a partir de un enfoque de seguridad en línea que considera la identificación de oportunidades, riesgos y buenas prácticas, desarrolló una charla sobre la materia.

Se contó con la participación de la Sra. Gabriela Salas, Psicóloga experta en Gaming y bloguera, fundadora del sitio Psicogamer y el Sr. David Santiváñez, CEO y fundador de GameMetron, Abogado y Consultor, asimismo participó la Sra. Maricruz León, funcionaria de la DEMA en representación de la voz de los padres y madres de familia de NNA.

A esta actividad se invitó a personas encargadas de CECI inscritas en los programas de capacitación de e-mentores 2019-2020, personas que forman parte de la CNSL y público en general. La misma se realizó mediante el Facebook Live del MICITT, y se puede encontrar en el siguiente enlace:

<https://www.facebook.com/548389708518468/videos/997682314001840>

- **Foro virtual: “Promoción de entornos digitales seguros para las niñas, niños y adolescentes”, Comisión Nacional de Seguridad en Línea, 09 setiembre 2020**

Con motivo de celebrar el Día de los Niños y las Niñas en Costa Rica, se realizó un foro virtual como espacio para ayudar a tomar conciencia sobre la importancia de garantizar y respetar los derechos de las personas menores de 18 años, no solamente en el ámbito físico, sino también en el digital donde como sociedad cada vez se desarrollan más.

En esta actividad se realizó la presentación de las Guías de Protección de la Niñez en línea de la Unión Internacional de Telecomunicaciones (UIT), por parte de personas representantes de esta organización, entre ellas la Sra. Sylvia Poll, Jefa de la División de Sociedad Digital de la UIT, en conjunto con el Sr. Pablo Palacios y la Sra. Fanny Rotino, trabajaron como parte del equipo que lideró el proceso de construcción. Siendo Costa Rica el primer país en el cual se presentaron las Directrices desde su lanzamiento oficial en junio del 2020. Los representantes de UIT expusieron que dichas directrices forman parte de un conjunto integral de recomendaciones para todas las partes interesadas en la construcción de un entorno seguro y empoderador en línea para la niñez y juventud, estas consideran modelos que pueden ser adaptables para cada país.

Además, se contó con la presentación magistral de la Sra. Pilar Ramírez, Directora de Protección Infantil y Asuntos Legales del Centro Internacional para Niños Desaparecidos y



Explotados (ICMEC), quien expuso sobre los conceptos y riesgos de la seguridad en línea para niñas, niños y adolescentes, presentando el marco general de cómo algunos países de la región en conjunto con el ICMEC han estado avanzando en acciones de información, involucramiento y sensibilización. También, participaron Natanael Díaz y Melany Rojas, dos jóvenes residentes de Aldeas SOS quienes comentaron su experiencia en el uso de herramientas digitales y brindaron recomendaciones a sus pares sobre cómo desenvolverse en las redes de manera segura.

Enlace: <https://www.youtube.com/watch?v=Qlhb2jtd3qU>

- **Charla virtual: El abordaje de la seguridad en línea, MICITT y Colegio de Periodistas de Costa Rica, 9 setiembre 2020**

En el mes de febrero de 2020, se solicitó la participación de representantes de los medios de comunicación del país a fin de colaborar con la construcción de una Estrategia Nacional para la prevención y atención de la Explotación y Abuso Sexual en Línea de niños, niñas y adolescentes que desarrolla la Comisión Nacional de Seguridad en Línea. Los medios de comunicación son aliados estratégicos fundamentales en la lucha contra el abuso y la explotación sexual debido a su capacidad de hacer llegar los mensajes a las distintas poblaciones, incluso influir en la adopción de valores y conductas de las personas, en la estrategia se incluye un eje referido a la participación de los medios de comunicación. Por lo tanto, los medios de comunicación se vuelven indispensables a la hora de sentar las bases de una cultura digital que rechace abiertamente las conductas que generan la explotación y el abuso sexual en línea de niños, niñas y adolescentes (EASNNAL).

A partir del acercamiento con el Colegio de Periodistas de Costa Rica (COLPER) se desarrollaron actividades de sensibilización de estas temáticas dirigidas a sus agremiados (as), con el propósito de sensibilizar sobre la problemática y el uso correcto del lenguaje a partir de las definiciones técnicas que permiten atender este tipo de delitos y con ello proteger la integridad de las víctimas, evitando procesos de revictimización, y así fortalecer la labor profesional en este campo de las personas que miembros (as) de COLPER.

Una primera sesión celebrada el pasado 09 de septiembre, esta fue dirigida de forma exclusiva a este gremio, es decir, se realizó por inscripción con cupo limitado y se contó con la participación de profesionales de amplia trayectoria profesional en esta materia, entre ellas la Sra. Angélica Chinchilla, Directora de Evolución y Mercado de Telecomunicaciones (DEMT) del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), la Sra. Betilde Muñoz-Pogossian, Directora del Departamento de Inclusión Social de la Secretaría de Acceso a Derechos y Equidad de la Organización de los Estados Americanos (OEA) y la Sra. Pilar



Ramírez, Directora de Protección Infantil y Asuntos Legales en el Centro Internacional para Niños Desaparecidos y Explotados (ICMEC⁶⁰).

- **Webinar gratuito: ¿Cómo hacer un uso responsable y productivo de la tecnología en niños, niñas y adolescentes? MICITT- Grupo INS, 17 setiembre 2020**

Actualmente para las personas menores de edad, Internet representa un entorno tan natural como cualquier otro, que complementa o mejora la variedad de espacios en los que pueden comunicarse o divertirse. Les permite relacionarse con otras personas de su edad y combinar una gran cantidad de actividades de forma simultánea sin importar su ubicación geográfica. Estos espacios virtuales y públicos les permiten relacionarse entre sus pares teniendo cierta sensación de privacidad y autonomía, sin la supervisión de las personas adultas. En un escenario ideal, es deseable que tengan experiencias digitales estimulantes, que les ayuden a crecer con seguridad en un mundo hiperconectado con las destrezas adecuadas para enfrentar riesgos.

Con base en estas preocupaciones, se atendió la propuesta realizada por el personal de Instituto Nacional de Seguros (INS), con la finalidad de sensibilizar al personal docente y del sector académico y otras personas involucradas en procesos de crianza tecnológica con el apoyo de información actualizada sobre los riesgos en entornos virtuales, así como consejos prácticos para navegar en Internet de forma segura. Esta actividad se trabajó en conjunto con el Departamento de Respuesta e Incidentes de Seguridad Informática (C-SIRT) del MICITT.

- **Webinar “La comunicación en la atención y denuncias de delitos de la Explotación y Abuso Sexual en Línea de niños, niñas y adolescentes en Costa Rica”, MICITT- Colegio de Periodistas de Costa Rica (COLPER) 23 de setiembre 2020**

Esta sesión se desarrolló mediante un webinar específicamente para personas profesionales del ámbito de la comunicación, sin embargo, este se transmitió de manera abierta para público en general. Esta actividad se desarrolló en conjunto con el personal del Colegio de Periodistas de Costa Rica (COLPER) debido a la latente necesidad de continuar llevando a cabo procesos de sensibilización y de capacitación en esta área, cuyo resultado se vea reflejado en la calidad de la información periodística y sobre todo en el impacto que ejercen en la prevención y atención de los delitos de explotación sexual en línea cuando las víctimas sean personas menores de edad.

Los medios de comunicación tiene un papel importante en cuanto a apoyar a las autoridades nacionales responsables de la investigación criminal aportando datos útiles o denunciando y dando seguimiento a las denuncias de este tipo de delitos ante las autoridades competentes, evaluando las alternativas de protección a las víctimas, reflexionando sobre su enfoque o

⁶⁰ <https://www.icmec.org>



efectividad, divulgando las iniciativas que tienen lugar en otros países, utilizando el lenguaje apropiado y la terminología correcta, evitando el empleo de imágenes y titulares sensacionalistas, debido a que este tipo de material ejerce una fuerte influencia en la forma de pensar de una sociedad, por lo tanto, se deben evitar expresiones que refuerzan los mitos o estereotipos que contribuyan con el círculo de abuso.

De lo anterior, se deriva la motivación para la creación de este espacio para sensibilizar sobre la problemática y sus diversas perspectivas, desde la labor que desempeñan las personas periodistas, profesionales en comunicación, líderes de opinión y la población en general sobre el abordaje en los medios de comunicación social costarricenses de los delitos de explotación y abuso sexual de niños, niñas y adolescentes en línea (EASNNAL).

En el espacio se contó con la participación de Patricia Gómez Pereira, Coordinadora de la Comisión de Capacitación, (COLPER), Angélica Chinchilla, directora de la Dirección de Evolución y Mercado de Telecomunicaciones, (DEMT), Evelyn Varela, funcionaria de la DEMT del MICITT, y Licda. Angie Bartels Calderón, Jefa de la Sección Especializada en Violencia de Género, Trata de Personas y Tráfico Ilícito de Migrantes (MICITT, 2021). Esta charla se transmitió vía Facebook Live y a su vez, a través del canal del MICITT disponible en YouTube. Se llevó a cabo el 23 de setiembre a las 6:00 p.m. (hora Costa Rica). El webinar quedó grabado en los siguientes enlaces:

Facebook: <https://www.facebook.com/548389708518468/videos/829099121234936> y

YouTube: <https://www.youtube.com/watch?v=sYeizzbdpe8>

- **Charla virtual: Usos seguros de las aTIC dirigida a emprendedoras Zona Norte, 29 septiembre, 2020**

Como resultado de la charla informativa brindada en la Cámara de Comercio, Turismo e Industria de la Zona Norte el 11 de agosto de 2020, se gestionó el apoyo de la Dirección de Evolución y Mercado de Telecomunicaciones para brindar una charla sobre usos seguros, productivos y responsables para niños, niñas y adolescentes.

La misma contó con una participación de 10 mujeres emprendedoras de esta zona, quienes manifestaron un interés en los contenidos debido a que muchas de ellas también son madres de familia y eso les facilitó compartir sus experiencias de su vida tanto empresarial como familiar.

- **Charlas Mes Ciberseguridad 2020**

La Dirección de Evolución y Mercado de Telecomunicaciones en colaboración con la Dirección de Gobernanza Digital impartieron charlas de Seguridad en Línea para todo el público de manera virtual en el marco del Mes de la Ciberseguridad, enfocadas especialmente para



niños, niñas, adolescentes y padres, madres y encargados de familia. Este ciclo de charlas se desarrolló en el mes de octubre de 2020 y de igual forma se llevó a cabo un nuevo ciclo de estas charlas en octubre de 2021. Estas se llevaron a cabo mediante la plataforma Zoom y se transmitieron a través de Facebook Live y el canal de YouTube del MICITT. A continuación, se adjunta el detalle de cada una de estas charlas:

Charla virtual	Detalle	Fechas	Enlaces
Ciberseguridad Niños y Niñas	Esta charla se enfocó en población menor de edad entre los 7 y los 12 años,	13 octubre, 2020	Facebook: https://www.facebook.com/203950599615339/videos/711369182794284 You Tube: https://www.youtube.com/watch?v=pN8gFqEljpY
Ciberseguridad para Jóvenes	Esta charla se dirigió a público adolescente, con edades entre los 13 y los 17 años	20 octubre, 2020	Facebook: https://www.facebook.com/203950599615339/videos/1261902944183617 YouTube: https://www.youtube.com/watch?v=uqX2NFIBk5w
Ciberseguridad para Padres y Madres	Esta charla se realizó otra sesión dirigida a padres y madres de familia	27 octubre, 2020	Facebook: https://www.facebook.com/203950599615339/videos/776721919844312 YouTube: https://www.youtube.com/watch?v=3sLwsHXifpg

• Ciclo de charlas virtuales Coocique

Para el mes de octubre, Coocique empresa cooperativa de ahorro y crédito abierta cuenta con su Programa Nueva Generación (NG), conformado por personas asociadas menores de 12 años y además, de un grupo de personas adolescentes. Asimismo, se incluyó una charla virtual dirigida a personas adultas mayores, quienes también se han visto vulnerabilizados durante los procesos de transformación digital. Entre sus funciones se encuentra ofrecer talleres bajo los siguientes ejes de acción, se citan; ambiental, financiero, social y digital. Por lo tanto, se mostraron interesados en contar con charlas con contenidos sobre seguridad en línea para esta población.

A continuación, se muestra el detalle de cada una de estas actividades.



Actividad	Fecha
Charla virtual: Uso seguro, responsable y productivo de la tecnología en niños y niñas	22 de octubre 2020
Charla virtual: Uso seguro, responsable y productivo de la tecnología en personas adolescentes	22 de octubre 2020
Charla virtual: Uso seguro, responsable y productivo de la tecnología en padres y madres de familia	29 de octubre, 2020
Charla virtual: Uso seguro, responsable y productivo de la tecnología, Generación Dorada	2 de diciembre, 2020

En resumen, durante el año 2020 el MICITT a través de la Dirección de Evolución y Mercado de Telecomunicaciones, intensificó las acciones que buscan la sensibilización y el incremento de conciencia en personas menores de edad, padres, madres de familia, personal docente, personal de organizaciones enfocadas en la protección de la niñez, adolescencia y personas adultas mayores, en cuanto a las oportunidades y riesgos derivados del uso de la Internet.

Es relevante destacar que la institución ante la emergencia sanitaria provocada por la pandemia de COVID-19 gestionó dichas actividades de manera virtual, utilizando plataformas sincrónicas y asincrónicas que permitieron un amplio alcance a los distintos grupos permitiendo, así democratizar el acceso a la información y a su vez mantener al tanto a la población en general sobre estos temas mediante los diversos canales de comunicación, como correo electrónico, redes sociales, entre otros.

En general los resultados obtenidos del desarrollo de estas actividades muestran que:

- Se realizaron un total de 12 actividades virtuales, que se clasifican en 8 charlas virtuales, 3 webinar, 1 foro virtual y 3 publicaciones en medios de comunicación digital;
- Las charlas virtuales alcanzaron de forma directa 307 personas sensibilizadas, en un rango de edad de 7 años en adelante;
- Según las métricas generadas de las transmisiones en vivo en el perfil de la red social Facebook, se contabilizaron 451 reacciones, 202 comentarios y las actividades se compartieron alrededor de 114 veces;
- Los comentarios recibidos en general tienen una percepción positiva, manifestando su interés en los contenidos y agradeciendo la existencia de este tipo de espacios para informarse y conocer con mayor profundidad los riesgos que conlleva el uso de Internet.

Aunado a ello, durante el desarrollo de las actividades se constató que las personas menores de edad requieren de acompañamiento constante que incluya información y orientación sobre



los nuevos riesgos que surgen derivados del uso de la Internet, acorde a los acelerados avances tecnológicos. De igual forma se logró determinar que los grupos que están encargados de la crianza de las personas menores de edad también requieren fortalecer sus habilidades y destrezas para brindar un adecuado acompañamiento y una mejor guía para el buen uso de la Internet, así como para enfrentar los riesgos a los que se ven expuestos las personas menores de edad.

Además, permitió evidencia que se requiere continuar difundiendo información sobre las oportunidades y los riesgos que se presentan con el uso de Internet, brindando facilidades de participación y más canales para que las personas puedan acceder a los contenidos informativos y educativos de la seguridad en línea (MICITT, 2021).

- **Publicaciones realizadas en medios de comunicación sobre seguridad en línea, 2020**

Además, de las actividades ejecutadas se realizaron diversas publicaciones alusivas al tema de la seguridad en línea que implica información sobre los riesgos y cuidados que deben tener las personas en general cuando acceden y utilizan la Internet. A continuación, se muestra el resumen de estas.

- **Publicación en Periódico Informativo JBS: Recomiendan "el control parental cibernético para evitar atentados contra nuestros hijos"**

El día 10 de junio 2020, el señor Alberto Cabezas realizó una solicitud de información mediante el envío de un cuestionario, con el objetivo de realizar una entrevista, como resultado de esta, el día 22 de junio de ese mismo, se publicó la nota en el Periódico Informativo JBS. En resumen, la nota contiene información sobre grooming, control y filtro parental y cómo identificar noticias falsas. Esta publicación puede ser consultada en el siguiente enlace: <http://informativojbs.com/recomiendan-el-controlpaternal-cibernetico-para-evitar-atentados-contra-nuestros-hijos/>

- **Entrevista para Telemundo Las Vegas: La pandemia estaría poniendo a sus hijos más cerca de los depredadores sexuales en línea, 30 de junio 2020**

El medio de comunicación Telemundo Las Vegas realizó una entrevista a la Sra. Angélica Chinchilla Medina, Directora de la DEMA, con el fin de brindar información sobre el incremento de casos de grooming que se aceleró con los confinamientos de la pandemia COVID-19. La entrevista se encuentra disponible en el siguiente enlace: <https://www.telemundolasvegas.com/fotosyvideos/alertan-sobre-depredadores-sexuales-enlinea/2089405/>



- **Publicación "Apoyemos el uso seguro, productivo y responsable de la tecnología en niños, niñas y adolescentes", Revista Cima Digital**

Por otro lado, el grupo editor del periódico vocacional "En la Cima" otorgó un espacio en la última edición del año 2020, en este medio es posible encontrar importante información sobre temas relacionados con uso seguro, responsable y productivo de las tecnologías de información y comunicación. La publicación se realizó En la Cima Digital, edición Número 93, en el mes de noviembre de 2020, se incluyó dentro del Apartado Pizarra Científica y Tecnológica, página 11 con el título "*Apoyemos el uso seguro, productivo y responsable de la tecnología en niños, niñas y adolescentes*".

Este artículo se compartió con los miembros de la CNSL, con el fin de divulgar contenidos de dichas temáticas con la población estudiantil, padres, madres y personas cuidadoras. Esta publicación se realizó con la colaboración de Noemy Coto, funcionaria de la DEMA.

Enlace:<https://www.miguiavocacional.com/periodicos/93.%20noviembre%202020.pdf>

- **Actividades virtuales para la promoción y prevención de la seguridad en línea, 2021**

En el año 2021 se enumeran las siguientes actividades.

- **Día de la Internet Segura, 2021**

El Día de Internet Segura, "Safer Internet Day" (SID, por sus siglas en inglés) es un evento promovido por la red INSAFE/INHOPE con el apoyo de la Comisión Europea, que se celebra cada mes de febrero con el objetivo de promover un uso seguro y positivo de las tecnologías digitales, especialmente entre niños, niñas y jóvenes. El SID se celebra cada año el segundo día de la segunda semana de febrero y reúne a millones de personas de todo el mundo para impulsar cambios positivos y concienciar acerca de la seguridad en Internet, organizando distintos eventos y actividades.

Este día no solo pretende generar conciencia para contar con una Internet más segura, sino una Internet mejor, como espacio en el que todas las personas hagamos uso de la tecnología de manera responsable, respetuosa, crítica y creativa. El SID se dirige a niños, niñas y jóvenes, padres y tutores, profesores, educadores y trabajadores sociales, así como a las empresas y responsables políticos, animándolos a participar de forma activa en la creación de una Internet mejor.

- **Conversatorio virtual "Una Internet mejor comienza contigo: más conectad@s, más segur@s"**

Evento virtual dirigido a adolescentes, entrevistas a 2 personas menores de edad, que pueden ser líderes o *influencers* en el campo de la ciberseguridad acerca de cómo estar más



conectados, pero más seguros en los entornos digitales (gestión de riesgos en Internet, relaciones afectivas, sexting y ciberbullying en la adolescencia a través de medios digitales)

Enlace: https://www.youtube.com/watch?v=B9ihCV18W_c

- **Taller para personas de la comunidad de Curridabat sobre seguridad en Línea, 9 de febrero 2021, 2:00 p.m.**

En conjunto Municipalidad de Curridabat, acordar alguna fecha febrero 2021, a través de FB Live.

Enlace:

<https://www.facebook.com/centrodedesarrollohumanoelhogar/videos/439432810532812/>

- **Campaña de stickers:**

Diseño de paquete de stickers para compartir el Día Internet Segura, se diseñó un paquete de stickers para niños, niñas, personas jóvenes, padres, madres, tutores (as), profesores (as), empresas, instituciones y público en general que impulsen experiencias más seguras en Internet con mensajes divertidos y diferentes para contestar a sus contactos con conciencia sobre usos positivos de las tecnologías.

Enlace: <https://www.micit.go.cr/noticias/costa-rica-se-une-conmemoracion-del-dia-la-internet-segura>

- **Día Internacional de las Niñas en las TIC, 2021**

El Viceministerio de Telecomunicaciones a través de la Dirección de Evolución y Mercados de Telecomunicaciones en conmemoración del Día Internacional de las Niñas en las TIC y como parte de las actividades para la celebración de la Semana de la Innovación y la Creatividad, como parte de la promoción de los beneficios de la sociedad de la información y el conocimiento se requiere que los países impulsen el desarrollo de destrezas y competencias digitales desde edades tempranas, cuenten con una amplia variedad de talentos, y fomentar una mayor participación de las niñas en carreras profesionales que les permita en el futuro insertarse de manera exitosa en el sector TIC. Además, se hace trascendental fomentar soluciones que procuren la generación de habilidades que propicien el empoderamiento de estas y a su vez ambientes seguros en línea para las niñas y mujeres (MICITT, 2021).

Sumado a la necesidad de una mayor participación de mujeres en el sector, la sociedad enfrenta el reto de fortalecer las capacidades y destrezas de esta población para la protección de sus derechos dado que diversos estudios revelan que las formas de violencia en el mundo físico se han trasladado de manera intensiva a los entornos digitales (MICITT, 2021).

De este modo, la institución se planteó realizar dos actividades virtuales, a saber:



- **Webinar: Conversemos sobre habilidades digitales para niñas creadoras, usuarias e innovadoras**

Dirigido a público en general, para generar un diálogo y exponer las necesidades actuales y visión a futuro de acciones, políticas e iniciativas que puedan sumarse como soluciones a los obstáculos que siguen presentándose como limitantes para el pleno empoderamiento de las mujeres y niñas del desarrollo tecnológico.

Enlace: <https://www.youtube.com/watch?v=Je3WYkudsyg>

- **Taller: Construyendo entornos digitales seguros, creativos e innovadores para empoderar a nuestras niñas**

Dirigido a niñas de 10 a 13 años, con el fin de potenciar sus destrezas y desarrollar su imaginación mediante actividades prácticas. (MICITT, 2021).

- **Webinar Ciberacoso: expresión de violencia de género para personas menores de edad**

Como parte de las actividades realizadas en el marco de la conmemoración del Mes de la Ciberseguridad, mismo que se celebra durante el mes de Octubre de 2021. Se planteó realizar un Webinar para abordar el tema del **ciberacoso** entendiendo que este es una conducta donde se utiliza la tecnología para amenazar, avergonzar, intimidar o criticar a otra persona (Kids Health, 2018). En otras palabras, es todo aquello que se publica en Internet con la intención de hacer daño, avergonzar o molestar a otra persona. La mayoría de las personas expertas están de acuerdo en que implica acoso repetido y algún tipo de desequilibrio de poder.

Esto se convierte en una forma de expresión de violencia en línea la cual ocurre de diferentes maneras, tales como el envío de correos electrónicos amenazantes o de acoso, mensajes instantáneos o publicación de información en línea y tiene como blanco a una persona específica, ya sea contactándola directamente o difundiendo información personal suya, causándole angustia, miedo o enojo (OEA, 2019). Los términos equivalentes que se utilizan son “acoso en línea” y “acoso cibernético”. Ante estas conductas las mujeres y las personas menores de edad se ven expuestas.

El objetivo se centró en comprender el alcance y el funcionamiento de los instrumentos legales en Costa Rica para la resolución de los casos de acoso tanto para personas menores de edad como para personas adultas. En este espacio se contó con la participación de Jessica Velarde, Responsable del Observatorio de Trata de Persona, Bolivia y Miguel Ramírez López, Fiscal Adjunto y Fiscalía Adjunta de Fraudes y Ciberdelitos de Costa Rica quienes expusieron acerca de este tema.



Enlace Facebook:

<https://www.facebook.com/100064629341808/videos/1069413467204047>

Enlace You Tube: <https://www.youtube.com/watch?v=0T5q5Uo2a5s>

- **Charla en Casa con Ageco Aprenda acerca de Ciberseguridad y personas adultas mayores: ¿Qué puedo hacer para estar más segur@ en línea?**

Sumado a las diversas actividades desarrolladas en el mes de la Ciberseguridad el Viceministerio de Telecomunicaciones a través de la Dirección de Evolución y Mercados de Telecomunicaciones planteó realizar un webinar dirigido a las personas adultas mayores, con el fin de realizar un acercamiento con dicha población y brindar consejos y recomendaciones para una interacción más segura en Internet y el mundo digital. El estudio "Fifty Plus Booms Online", realizado antes de que se desarrollara la pandemia de COVID-19, analizó el comportamiento en línea de las personas entre 50 a 75 años en los Estados Unidos, reveló que los navegantes de más de 50 años estaban invirtiendo un promedio de cinco horas por día en línea. La encuesta también mostró que el 80% de los adultos mayores estaban utilizando redes sociales. De los adultos mayores en línea, más de la mitad aseguró haber compartido voluntariamente información personal con personas que nunca han conocido en persona. Esta tendencia se incrementó con las medidas sanitarias adoptadas por la crisis sanitaria, donde Internet y las redes sociales se convirtieron en la principal herramienta de contacto para la mayoría de las personas, incluida la población adulta mayor. En este período también digitalizó muchos de los trámites que se realizaban a nivel público lo que obligó a muchas personas a adaptarse a las nuevas tecnologías.

Esta tendencia se incrementó con las medidas sanitarias adoptadas por la crisis sanitaria, donde Internet y las redes sociales se convirtieron en la principal herramienta de contacto para la mayoría de las personas, incluida la población adulta mayor. En este período también digitalizó muchos de los trámites que se realizaban a nivel público lo que obligó a muchas personas a adaptarse a las nuevas tecnologías.

En Costa Rica, la población adulta mayor, según datos estimados del INEC se conforma por un total de 476 756 personas, representando así el 9,2% de la población total, donde el 52,9% son mujeres y el 47,1% son hombres. Asimismo, en cuanto al acceso a Internet de esta población un 38,2% de las mujeres cuentan con una conexión a este servicio y el 41,3% por parte de los hombres. En cuanto a la tenencia de computadora, el 13,3% de mujeres cuenta con este dispositivo mientras que en los hombres este dato correspondió al 11, 2%. Por otro lado, en cuanto al acceso a teléfono, el porcentaje de acceso a conectividad en este dispositivo un 66,4% correspondió a mujeres mientras que por parte de los hombres fue del 66,3%. Siendo así que el país se encuentra por debajo del promedio de la región en



conectividad para esta población. Y aunque Internet brinda excelentes oportunidades para las personas mayores, en especial para que sigan en contacto con amigos y familiares, al igual que todos los grupos de edad, esta población puede ser víctima de una serie de riesgos que es importante conocer y prevenir.

De esta forma, el objetivo es brindar consejos y recomendaciones a la población adulta mayor para realizar un uso más seguro y significativo de Internet y las herramientas digitales. **Enlace:** <https://www.facebook.com/AGECOCR/live/>

- **Charlas Mes Ciberseguridad 2021**

La Dirección de Evolución y Mercado de Telecomunicaciones en colaboración con la Dirección de Gobernanza Digital impartieron charlas de Seguridad en Línea para todo el público de manera virtual en el marco del Mes de la Ciberseguridad, enfocadas especialmente para niños, niñas, adolescentes y padres, madres y encargados de familia. Este ciclo de charlas se desarrolló en el mes de octubre de 2021. Estas se llevaron a cabo mediante la plataforma Zoom y se transmitieron a través de Facebook Live y el canal de YouTube del MICITT. A continuación, se adjunta el detalle de cada una de estas charlas:

Charla virtual	Detalle	Fechas	Enlaces
Ciberseguridad Niños y Niñas	Esta charla se enfocó en población menor de edad entre los 7 y los 12 años.	11 de octubre, 2021	Facebook: https://www.facebook.com/watch/live/?ref=watch_permalink&v=870382343644315 You Tube: https://www.youtube.com/watch?v=M85mr8vTQEY
Ciberseguridad para Jóvenes	Esta charla se dirigió a público adolescente, con edades entre los 13 y los 17 años	18 de octubre, 2021	Facebook: https://www.facebook.com/watch/live/?ref=watch_permalink&v=580275299841304 YouTube: https://www.youtube.com/watch?v=NN7eGfaWLnU
Ciberseguridad para Padres y Madres	Esta charla se realizó otra sesión dirigida a padres y madres de familia	25 de octubre, 2021	Facebook: https://www.facebook.com/watch/live/?ref=watch_permalink&v=291864868839648 You Tube: https://www.youtube.com/watch?v=tGWZLw9lrOA

Fuente: Elaboración propia, 2021.



- **Día Nacional de la lucha contra el Grooming.**

El pasado 13 de noviembre a través de la Comisión Nacional de Seguridad en Línea se compartió información sobre este delito, a través de la difusión de un afiche informativo y un video que se muestra en el siguiente enlace:

<https://www.facebook.com/100064629341808/videos/pcb.250991730398470/4504346679631966>

- **Charla Oportunidades y Riesgos del Internet: Coopejudicial-MICITT**

Se coordinó una serie de charlas virtuales con el objetivo de sensibilizar a los niños, niñas, madres, padres y personas encargadas sobre el uso seguro, productivo y responsable de las tecnologías digitales. La primera de ellas se impartió el pasado 25 de noviembre de 2021.

- **Manifiesto: La voz de las niñas, niños y adolescentes ante el Estado y la sociedad NNA, Patronato Nacional de la Infancia, 2021**

En el 2021, la Fundación Paniamor lideró y desarrolló con fondos de End Violence Against Children este Manifiesto, con el respaldo del PANI, y la participación de 30 personas adolescentes pertenecientes a los consejos consultivos del PANI, de todo el país, quienes se sensibilizaron sobre la importancia de cómo confiar en Internet, a partir de información a la que están expuestos y que comparten. Como producto final de estos espacios, se desarrolló un Manifiesto donde estos adolescentes expresaron sus responsabilidades como personas menores de edad y activas en el ecosistema digital, a través de sus interacciones con las demás personas, desde la promoción de una cultura de paz. Este Manifiesto se dividió en cuatro secciones:

- 1) Su compromiso como NNA en el uso de Internet;
- 2) Su responsabilidad para con sus pares;
- 3) La necesidad de acompañamiento y escucha de parte de sus familias en el uso de tecnologías;
- 4) La solicitud de apoyo a las instituciones del Estado y la Sociedad para hacer un uso participativo de las TIC.

En resumen, se plantearon algunas recomendaciones importantes en relación con el uso de las TIC, tales como detectar información falsa en Internet, no compartir información sensible o personal con terceros, desconfiar de plataformas digitales de dudosa procedencia, verificar la información, no compartir información falsa y tener pensamiento crítico. Además, el documento indica las necesidades de las personas adolescentes en cuanto a conexión a Internet, espacios formativos y de reflexión sobre cómo confiar en Internet y el acompañamiento de sus referentes adultos e institucionales para saber cómo sentirse parte



de este ecosistema. Finalmente, hacen algunas recomendaciones al Estado y a la sociedad para que les apoyen a hacer un uso participativo de las TIC, en función de ejercer su ciudadanía digital. Cabe destacar que este documento fue declarado de interés nacional por la Comisión Nacional de Niñez y Adolescencia.

Enlace: <https://pani.go.cr/ninas-ninos-y-adolescentes-entregan-recomendaciones-al-estado-para-un-mejor-aprovechamiento-de-la-internet/>

Fundación Paniamor

A continuación, se detallan algunas de las actividades que ha realizado la Fundación Paniamor:

1. **Webinar 'Prevenemos el Bullying y el Cyberbullying Parte 2: Violencias en línea y delitos informáticos'.** https://www.youtube.com/watch?v=ibO_uC9t-cY
2. **Encuentros virtuales Sexting: Desinformación vs Realidad**
<https://www.facebook.com/paniamor.org/videos/2936907686619721>
3. **Taller 'Apps para el bien'**
<https://www.facebook.com/paniamor.org/photos/a.156361261084600/4256843041036381/>
4. **Charla 'Salud Mental en ecosistemas digitales seguros y promotores'**
<https://www.facebook.com/inie.ucr/videos/3072310192988444>
5. **Campaña Sexteen:** La Fundación PANIAMOR y el Ministerio de Educación Pública (MEP) lanzaron una campaña, con el propósito de fomentar procesos de diálogo y reflexión con y entre las personas adolescentes y sus familias, sobre los riesgos y las responsabilidades de la práctica del Esto, a partir de la comprensión de las experiencias e interacciones entre sus pares, que reportan las personas adolescentes en distintos espacios. La campaña está planteada desde un Enfoque de Derechos de Niñez y Adolescencia, así como de una perspectiva de género que orientan el tratamiento de la temática e incluyen mensajes diferenciados para adolescentes mujeres y hombres, que recuperan y reelaboran sobre sus experiencias de vida.
<https://www.facebook.com/hashtag/campa%C3%B1asexteen>
6. **Podcast Paniamor:** La fundación cuenta con un canal en la plataforma Sound cloud, donde por medio de entrevistas a profesionales, historias brindan a toda la población mensajes y consejos en temas sobre seguridad en línea, género, derechos, especialmente dirigidos a la población de niñez y juventud.
https://soundcloud.com/fundacion_paniamor



7. Crianza Tecnológica: Es una plataforma de autoformación interactiva que se basa en el enfoque de ciudadanía digital, y sus cuatro dimensiones: Uso Seguro, Responsable, Productivo y para Empoderar. Está compuesta de una serie de recursos pedagógicos multimedia innovadores para acompañar a mamás, papás, personas docentes y otras personas con roles de crianza y formación de niñas, niños y para las personas adolescentes.

<https://crianzatecnologica.paniamordigital.org/curriculum/index.html>

CLARO Costa Rica

La empresa CLARO en conjunto con la Fundación Paniamor, realizó una serie de cápsulas denominadas 'Así o más Claro', donde se comparte información sobre riesgos, consejos y rutas para denunciar las manifestaciones de violencia en línea. Estos episodios se pueden observar en los siguientes enlaces:

- Crianza Tecnológica: <https://www.youtube.com/watch?v=KJDZYt3Mjjo>
- Redes Sociales, Riesgos y Oportunidades: https://youtu.be/jCMrC_wUako
- Sexting: <https://youtu.be/k6o2LIJQGwQ>
- Cyberbullying: <https://youtu.be/MMamNtQdUak>
- Grooming: <https://youtu.be/Zcib6fHCxCw>
- Phishing: <https://youtu.be/GeBiBEQnFJQ>
- Rutas de denuncia: <https://www.youtube.com/watch?v=IHQtlvBX1jQ>

Kolbi -ICE

La empresa Kölbi y Fundación Paniamor realizaron la campaña denominada “De peligroso lo tiene todo”, la cual tenía como objetivo concientizar a las madres, padres y las personas encargadas de crianza de personas menores de edad, sobre el uso seguro de las TIC. Esta campaña desarrolló temas, términos y simbologías que pueden ser nuevos o desconocidos para las personas encargadas de crianza, como cyberbullying, sexting, sextorsión y grooming, así como el manejo de las redes sociales y la presencia de contenidos nocivos. En el siguiente enlace se puede ver el comunicado de prensa de la actividad:

<https://www.facebook.com/GrupoICECR/posts/3236847276428837/>

Videos con mensajes sobre riesgos:

Grooming: <https://www.facebook.com/GrupoICECR/videos/994820894340358>

Sexting: <https://www.facebook.com/GrupoICECR/videos/330028644954173>



Tribunal Supremo de Elecciones

Curso Ciudadanía Digital Responsable: El Instituto de Formación y Estudios en Democracia (IFED) del TSE ofrece un curso virtual denominado “Ciudadanía Digital Responsable”. Este es auto gestionado y consta de cuatro módulos. Este curso se realizó para que los usuarios de redes sociales y de internet aprendan cómo identificar la desinformación, proteger sus datos y a dialogar respetuosamente, son los tres principales objetivos que persigue el Tribunal Supremo de Elecciones (TSE) con un nuevo esfuerzo de formación digital.
<https://ifedvirtual.tse.go.cr/>

Agencia de Protección de Datos de los Habitantes (Prodhab)

Realiza charlas, eventos, y campañas en conjunto con otras instituciones, para culturizar en la protección de los datos personales y afines, a centros educativos, instituciones públicas y privadas de todo tipo y a la población en general.

Fiscalía Adjunta de Atención de Hechos de Violencia en perjuicio de Niñas, Niños y Adolescentes (FANNA)

Realiza capacitaciones en hospitales, escuelas, colegios, tanto a profesores como estudiantes.

Recursos educativos

Plan Nacional para el Desarrollo de Estrategias de Prevención y Erradicación de la Violencia Contra Niños, Niñas y Adolescentes, Costa Rica (2017-2019)

Este plan busca delimitar el concepto integral de prevención de la violencia contra las niñas, niños y adolescentes, se han interrelacionado varias fuentes de información, desde la literatura, los talleres participativos y las entrevistas, buscando avanzar a una delimitación concreta y operativa que guiaría el plan de acción (UNICEF, 2017).

Enlace: <https://www.unicef.org/costarica/media/341/file/Plan-nacional-para-desarrollar-estrategias-de-prevencion-y-erradicacion-de-la-violencia.pdf>

Además, en relación con el ICE mencionó que ha emitido los comunicados que han salido sobre los peligros latentes a los que se enfrenta la niñez mediante el uso de Internet. Por parte la Fiscalía de Género y la Fiscalía de Trata de Personas y Tráfico Ilícito de migrantes, así como la Fiscalía Penal Juvenil, han emitido algunas políticas.

30. ¿Tiene guías/soportes formativos/protocolos de actuación de respuesta ante riesgos de la infancia en línea?

El Ministerio de Educación Pública (MEP) ha asumido el reto de que los centros educativos sean espacios seguros para el aprendizaje de una convivencia basada en la equidad y la



justicia con un enfoque de derechos humanos y libres de toda forma de violencia y discriminación, en los que se generen oportunidades de desarrollo integral, se rechace la exclusión y, de esta manera, se construya y fortalezca una cultura de paz.

Siendo así que es imperioso contar con herramientas para atender las situaciones excepcionales de violencia que puedan presentarse en el ambiente educativo, por lo que brindamos a la comunidad educativa nacional los protocolos de actuación para la atención de situaciones de violencia y riesgo en los centros educativos.

Estos protocolos están mediados pedagógicamente y están constituidos por temas vitales de la convivencia en nuestras instituciones:

- Pautas generales para protocolos de actuación en situaciones de violencia y riesgo en los centros educativos;
- Protocolo de actuación en situaciones de bullying;
- Protocolo de atención del bullying contra la población LGTBI inserta en los centros educativos;
- Protocolo de actuación en situaciones de hallazgo, tenencia y uso de armas;
- Protocolo de actuación en situaciones de hallazgo, tenencia, consumo y tráfico de drogas;
- Protocolo de actuación en situaciones de violencia física, psicológica, sexual, acoso y hostigamiento sexual;
- Protocolo de atención a la población estudiantil que presenta lesiones autoinfligidas y/o en riesgo por tentativa de suicidio;
- Atención del embarazo y maternidad en personas menores de edad insertas en el sistema educativo;
- Protocolo de actuación institucional para la restitución de derechos y acceso al sistema educativo costarricense de las personas víctimas de sobrevivientes del delito de trata de personas y sus dependientes;
- Protocolo de actuación en situaciones de discriminación racial y xenofobia.

Estos protocolos constituyen una herramienta sencilla y práctica que busca apoyar al personal de centros educativos, a la propia población estudiantil y a la comunidad educativa en general, para que puedan enfrentar mejor estas amenazas.

Enlace: <https://www.mep.go.cr/protocolos-de-actuacion>



Protección de la Infancia

Se cuenta con una serie de proyectos, programas y políticas públicas, a continuación, el detalle:

1. Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT) 2015-2021: Pilar Inclusión Digital

De acuerdo con lo establecido en la Ley N°8642, Ley General de Telecomunicaciones que establece que le corresponde al Poder Ejecutivo la definición de metas y prioridades del sector sobre acceso, servicio universal y solidaridad mediante, el “*Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT) 2015-2021: Costa Rica: Una sociedad conectada*”, contempló dentro del Pilar de Inclusión digital una línea de acción enfocada en el empoderamiento de la población en cuanto al uso de las TIC con el fin de incrementar el uso y la apropiación responsable, segura y productiva de las tecnologías digitales de la población en general, de este modo en esta misma línea se han llevado a cabo capacitaciones tanto a personas adultas como actividades dirigidas a personas menores de edad (MICITT, 2021).

2. Comisión Nacional de Seguridad en Línea

A partir de la apertura del sector de telecomunicaciones, surgieron un conjunto de nuevas necesidades en relación con los procesos de alfabetización los cuales se encaminan hacia el mundo digital, propiciando en el año 2010, la creación de la Comisión Nacional de Seguridad en Línea (CNSL) mediante el Decreto Ejecutivo N° 36274-MICIT, publicado en el Diario Oficial La Gaceta N° 239 de fecha 09 de diciembre de 2010, marcando así el inicio de una serie de acciones que se constituyen en hitos que reflejan los esfuerzos nacionales realizados en materia de seguridad en línea, atención y prevención de la Explotación y Abuso Sexual de Niños, Niñas y Adolescentes en Línea (EASNNAL).

Este es un órgano multidisciplinario e intersectorial, conformado por representantes de distintas instituciones públicas y privadas que tienen ámbitos de competencia especial o desarrollan iniciativas en este campo. Se encarga del diseño de las políticas necesarias sobre el buen uso de Internet y las TIC, contribuyendo a generar una cultura de comprensión, análisis y responsabilidad personal, que le permita a la población beneficiarse de las ventajas de la utilización de la Internet, y tener una actitud consciente y proactiva frente a los riesgos inherentes al uso de estos recursos. La comisión está liderada por el MICITT y la integran además MEP, Ministerio de Cultura y Juventud, PANI, Poder Judicial, SUTEL, Cámara de Tecnologías de Información y Telecomunicaciones, la Fundación Omar Dengo (FOD) y la Fundación Paniamor.



Por lo tanto, según lo señalado por el Decreto Ejecutivo N° 36274-MICIT, las acciones de la Comisión se enfocan en generar una cultura de comprensión, análisis y responsabilidad personal de las tecnologías digitales en línea por parte de poblaciones vulnerables, entre ellas la niñez y adolescencia de todo el país (MICITT, 2021).

3. “Costa Rica dice No a la Explotación y el Abuso Sexual en Línea de Niñas, Niños y Adolescentes” (CR-NEXST)

La iniciativa Costa Rica dice No a la Explotación y Abuso Sexual en Línea (CR-NEXST), surge en el 2018 a partir de un trabajo impulsado por la Fundación Paniamor, con el apoyo del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) y otras entidades públicas y privadas, el Instituto Mixto de Ayuda Social (IMAS) del Ministerio de Desarrollo Humano e Inclusión Social, el Patronato Nacional de la Infancia (PANI) y el Sistema de Emergencias 9-11 cuya finalidad consiste en promover acciones para la protección de niñas, niños y adolescentes (NNA) frente a la explotación y abuso sexual en línea (MICITT, 2021) y a su vez debido a la necesidad de realizar esfuerzos hacia la democratización de acceso a las tecnologías y la inclusión digital, como supuesto a cumplir para el cierre de brechas socioeconómicas y de conocimiento que limitan el desarrollo sostenible de la nación costarricense (PANIAMOR, 2021).

Dicha iniciativa es financiada por el Fondo End Violence Partnership & Fund, y desde su construcción ha contado con la asesoría técnica de ECPAT International. También ha trabajado en alianza estratégica con el Fondo de Naciones Unidas para la Infancia (UNICEF-CR). La misma se planteó en tres componentes: 1. el fortalecimiento del Programa Hogares Conectados, 2. el fortalecimiento del Sistema Nacional 9-1-1, y 3. el desarrollo de un modelo nacional para la prevención y respuesta de la explotación y abuso sexual en línea de NNA (MICITT, 2021).

4. Estrategia Nacional Prevención y Respuesta a la Explotación y Abuso Sexual de Niños, Niñas y Adolescentes en línea 2021-2027

En el 2021, se emitió la "*Estrategia Nacional Prevención y Respuesta a la Explotación y Abuso Sexual De Niños, Niñas y Adolescentes en Línea 2021-2027*", cuyo objetivo general es fortalecer la capacidad país en los entornos digitales mediante la coordinación y articulación interinstitucional e intersectorial para garantizar la protección de la niñez y la adolescencia frente a la explotación y el abuso sexual en línea.

Esta Estrategia contiene 6 ejes de acción, a saber; Políticas Públicas y Gobernanza, Justicia Penal, Víctimas, Sociedad Civil, Industria y Medios de Comunicación, cada uno con un objetivo y un total de 21 resultados esperados, desagregados en 51 acciones y 65 indicadores de medición, así como el detalle de los responsables. La ejecución se lleva bajo un modelo



de participación activa y responsable de múltiples partes interesadas y su ejecución es responsabilidad compartida entre las entidades públicas, la Sociedad Civil, Academia, Sector Privado y demás actores que deseen aliarse, para garantizar la protección y el pleno disfrute de los derechos de la población niñez y adolescencia. De lo expuesto en materia de seguridad en línea, se destacan los esfuerzos del país para determinar las necesidades de la población menor de edad respecto del tema uso seguro, mediante el trabajo interinstitucional a través de la CNSL (MICITT, 2021).

5. Proyectos de Ley

De parte de la Fiscalía Adjunta de Atención de Hechos de Violencia en perjuicio de Niñas, Niños y Adolescentes (FANNA) del Ministerio Público de Costa Rica se propuso un proyecto de Ley especial para proteger a las NNA, y se incluyeron nuevas tipologías de esa materia, así mismo en la Política de Persecución Penal, se incluyeron también.

Prioridades en materia de seguridad en línea

Siguiendo el Modelo We Protect, en 2018, la Fundación Paniamor en conjunto con el MICITT, lideraron la realización de un mapeo que evalúa el desempeño país en seis áreas temáticas: Políticas Públicas y Gobernanza; Justicia Penal; Víctimas; Sociedad; Industria; Medios de Comunicación para la protección de las personas menores de edad en materia de seguridad en línea.

En total contempla 21 indicadores para la evaluación de desempeño. Dentro de los resultados obtenidos destaca la existencia en Costa Rica de un robusto cuerpo normativo orientado a la protección de los derechos de personas menores de edad, pero que carece de la tipificación adecuada de los nuevos delitos que se generan a partir de las Tecnologías de la Información y la Comunicación (TIC).

Por su parte, la Estrategia Nacional de prevención y atención del Abuso y Explotación Sexual de Niños, Niñas y adolescentes en Línea (EASNNAL) oficializada en el país en agosto 2021, propone como objetivo general *“Fortalecer la capacidad país en los entornos digitales mediante la coordinación y articulación interinstitucional e intersectorial para garantizar la protección de la niñez y la adolescencia frente a la explotación y el abuso sexual en línea”*

Para ello plantea como sus objetivos específicos:

- Construir entornos digitales seguros, en coordinación con la institucionalidad pública, la empresa privada y la sociedad civil;
- Implementar medidas integrales para la prevención y respuesta a delitos asociados a EASNNAL, siguiendo el Modelo “WePROTECT”;



- Reducir los riesgos que puedan derivarse del desconocimiento, incomprensión o uso inadecuado de las tecnologías digitales, por parte de las poblaciones meta;
- Es decir, las prioridades del país están enfocadas en la sensibilización de la población sobre los riesgos en línea; el desarrollo de habilidades y destrezas digitales en todos los segmentos de la población y la promoción del ejercicio de una ciudadanía digital responsable.

Por su parte OCDE (2020) señala que el enfoque de las políticas para la protección de la niñez en línea en Costa Rica se articula en torno a cuatro acciones principales: i) fortalecer el marco regulatorio; ii) fortalecer la coordinación interinstitucional; iii) identificar e implementar proyectos que promueven una cultura de protección en línea; y iv) apoyar la investigación y la evaluación de los impactos de los planes nacionales. Las políticas en áreas relacionadas como la protección de datos, la investigación penal, la educación, la distribución de películas y juegos de computadora también incorporan la protección en línea de los niños y niñas.

Por otro lado, el MEP mantiene como prioritario las acciones de educación de personas adultas en rol de crianza, así como profesionales en función de acompañamiento a procesos formativos y a su vez la Fundación Paniamor trabaja para potenciar la incorporación de la cultura de los derechos de la niñez y la adolescencia en la acción política y social de la nación, desde los Paradigmas de la Movilización Social, la Responsabilidad Estatal, la Responsabilidad Social y la Articulación Público-Privada, el programa Cultura Tecnológica desarrolla un conjunto innovaciones sociales basadas en el uso de las Tecnologías Digitales como herramientas para el mejoramiento de la calidad de vida, la seguridad personal, y el disfrute de ciudadanía digital de niñas, niños y adolescentes, desde los enfoques de derechos y responsabilidades de las personas menores de edad.

El Instituto Costarricense de Electricidad (ICE, operador incumbente del Estado) señala como sus prioridades la integridad, confidencialidad y disponibilidad de los datos mediante el uso seguros de los servicios para tener certeza jurídica.

Asimismo, la Fiscalía Adjunta de Atención de Hechos de Violencia en perjuicio de Niñas, Niños y Adolescentes (FANNA) indicó que se deben tipificar más delitos, no solo en materia sexual. Aunado a esto se debe capacitar más al personal que trabaja esta materia e implementar controles parentales, y capacitar a las personas que ostentan la responsabilidad parental.

Por otra parte, se han creado comisiones interinstitucionales con el fin de trabajar diseño, implementación y evaluación de políticas de protección de la infancia en línea, entre estos equipos de trabajo se pueden destacar:



- **Consejo Nacional de la Niñez y la Adolescencia (CNNA)**

Es un órgano interinstitucional, intersectorial y colegiado, no desconcentrado, adscrito a la Presidencia de la República. El CNNA se crea de conformidad con el artículo 170 de la Ley 7739 Código de la Niñez y la Adolescencia, y su funcionamiento se regula mediante el Decreto N° 41452-MP Reglamento del Consejo Nacional de la Niñez y la Adolescencia, publicado en La Gaceta N. 227 del 06 de diciembre del 2018, modificado mediante el Decreto N° 42549-MP del 30 de junio, publicado en La Gaceta N. 228 el 11 de setiembre de 2020.

Dentro de las funciones del CNNA, establecidas en el artículo 171 del Código de la Niñez y la Adolescencia, se encuentra la función de coordinar la acción interinstitucional e intersectorial en la formulación de las políticas y la ejecución de los programas de prevención, atención y defensa de los derechos de las personas menores de edad, conforme con la política de protección integral. (Patronato Nacional de la Infancia, 2021).

- **Comisión Nacional contra la Explotación Sexual Comercial de Niños, Niñas y Adolescentes, en adelante (CONACOES)**

Es una Comisión Técnica Articuladora y Coordinadora que fue reglamentada mediante el Decreto N° 33028-MTSS-MSP-MNA de reglamentación del Consejo Nacional de la Niñez y la Adolescencia del 14 de noviembre del 2005, Decreto que fue derogado tácitamente por el Decreto N° 37205-MP del 9 de enero del 2012, por lo cual se hace necesario emitir el presente Reglamento, con la finalidad de darle un marco jurídico al funcionamiento de la CONACOES.

Esta Comisión agrupa instituciones públicas centralizadas y descentralizadas, organismos internacionales y organizaciones no gubernamentales en la lucha por erradicar la explotación sexual comercial. (Reglamento N° 37563-MTSS, 2013).

- **Foro: Modelo de seguimiento al cumplimiento del Código de Niñez y Adolescencia**

Es liderado por la Dirección de Niñez y Adolescencia de la Defensoría de los Habitantes de Costa Rica. En este foro participan todas las instituciones que tienen responsabilidades en materia de niñez y adolescencia desde sus mandatos institucionales y, por lo tanto, en el cumplimiento del Código de la Niñez y la Adolescencia. (Ministerio de Planificación Nacional y Política Económica, 2021).

- **Comisión Nacional de Seguridad en Línea**

La Comisión Nacional de Seguridad en Línea (CNSL) se crea mediante el Decreto Ejecutivo N° 36274-MICIT, publicado en el Diario Oficial La Gaceta N° 239 de fecha 09 de diciembre de 2010, marcando así el inicio de una serie de acciones que se constituyen en hitos que reflejan los esfuerzos nacionales realizados en materia de seguridad en línea. Este es un órgano multidisciplinario e intersectorial, conformado por representantes de distintas instituciones



públicas y privadas que tienen ámbitos de competencia especial o desarrollan iniciativas en este campo. Se encarga del diseño de las políticas necesarias sobre el buen uso de Internet y las TIC, contribuyendo a generar una cultura de comprensión, análisis y responsabilidad personal, que le permita a la población beneficiarse de las ventajas de la utilización de la Internet, y tener una actitud consciente y proactiva frente a los riesgos inherentes al uso de estos recursos. La comisión está liderada por el MICITT y la integran además MEP, Ministerio de Cultura y Juventud, PANI, Poder Judicial, SUTEL, Cámara de Tecnologías de Información y Telecomunicaciones, la Fundación Omar Dengo (FOD) y la Fundación Paniamor. (MICITT, 2021).

- **Comisión interinstitucional para la protección de la persona menor de edad frente a delitos sexuales cometidos a través de medios electrónicos o virtuales (Grooming)**

Es una Comisión interinstitucional que se crea mediante la Ley N° 10020, que tiene entre sus funciones coordinar las políticas, acciones, estrategias y actuaciones de las entidades involucradas, para asegurar la protección efectiva de las personas menores de edad ante la comisión de delitos sexuales en medios electrónicos o virtuales, recomendar a la Asamblea Legislativa, cuando corresponda, la modificación y/o actualización del marco jurídico aplicable para garantizar que se adecúe al cambio tecnológico y a la forma en que se detecte que operan los delincuentes sexuales, con el objetivo de prevenir y sancionar efectivamente las prácticas que violenten la seguridad e integridad de las personas menores de edad, impulsar programas de concientización en los centros educativos, para dar a conocer a los estudiantes, docentes y padres de familia los riesgos que enfrenta la población menor de edad ante el uso de medios electrónicos y la forma de prevenir la comisión de delitos sexuales que puedan afectarlos y promover estrategias de concientización con los operadores y prestatarios de servicios de telecomunicaciones, para que colaboren con las autoridades y desarrollen mecanismos que coadyuven en la prevención, detección y persecución de delincuentes sexuales que utilicen medios electrónicos o virtuales para cometer actos en perjuicio de personas menores de edad o incapaces. (Ley N° 10020, 2021).

- **Observatorio Temático Interuniversitario de Derechos de la Niñez y la Adolescencia**

Tiene la labor de observar la condición de vida, el desarrollo integral y acceso a los Derechos Humanos de la niñez, la adolescencia y la juventud en el país. En este proyecto participan la Universidad Estatal a Distancia (UNED), la Universidad Nacional de Costa Rica (UNA), y la Universidad de Costa Rica (UCR). El objetivo principal de este observatorio es conocer la situación en materia de Derechos Humanos y calidad de vida de Niñas, Niños, y Adolescentes



que viven en Costa Rica. <https://pridena.ucr.ac.cr/observatorio-tematico-interuniversitario-de-derechos-de-la-ninez-y-adolescencia/>

- **Red Interinstitucional para la Niñez y la Adolescencia en Costa Rica (RINA, UCR)**

se conforma de un conjunto de instituciones gubernamentales y no gubernamentales vinculadas con el interés de promover espacios de análisis y reflexión en torno a los derechos de la niñez y la adolescencia en Costa Rica, con el fin de generar acciones en defensa de los mismos y a la vez favorecer su desarrollo integral.

- **Coalición Nacional contra el Tráfico Ilícito de Migrantes y la Trata de Personas (CONATT)**

Cuenta con un Plan Estratégico 2022-2027 para prevenir el tráfico ilícito de migrantes y la trata de personas, así como atender y proteger a las víctimas, y ejecutar la persecución y la sanción de los responsables del delito. Con este Plan Estratégico también se potencia la implementación del Plan de trabajo en materia de tráfico ilícito de migrantes (2019-2025). Como parte de las recomendaciones de la Fundación Paniamor, se enfatiza incluir procesos de sensibilización y empoderamiento sobre cómo prevenir, responder y denunciar las nuevas formas delictivas en línea por parte del crimen organizado.

El Plan Estratégico se encuentra estructurado en 5 ejes: a) Eje de atención y protección a víctimas; b) Eje de prevención; c) Eje de procuración de justicia; d) Eje de información, análisis e investigación; e) Eje de coordinación institucional. Contempla objetivos estratégicos, resultados, indicadores estratégicos y acciones operativas con sus metas, las instituciones responsables y los productos. Para cumplir con las metas y los productos las comisiones o instituciones responsables definirán las actividades y proyectos puntuales en planes de trabajo anuales.

La CONATT es la institución responsable de promover la formulación, la ejecución, el seguimiento y la evaluación de políticas públicas nacionales, regionales y locales, representada por 21 instituciones estatales y cuenta con participación en calidad de observadores de organizaciones de la sociedad civil, organismos internacionales y de cooperación internacional, así como organismos no gubernamentales.

- **Modelo Crianza Tecnológica**

Desde sus inicios el proyecto Crianza Tecnológica ha contado con la cooperación técnica y financiera del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) a través del Consejo Nacional para Investigaciones Científicas y Tecnológicas (CONICIT).

Este promueve: Posicionar los recursos pedagógicos multiplataforma del portal Crianza Tecnológica a lo interno de los sistemas primarios de socialización-familias, escuela y



comunidad-como herramientas de valor agregado para potenciar la participación de las familias hacia un uso seguro y responsable de las tecnologías digitales, en la prevención y respuesta de la explotación y abuso sexual en línea, a través de una estrategia de promoción.

- Instalar capacidad en personas de roles de cuidado y acompañamiento a través de la plataforma electrónica Crianza Tecnológica, por medio un proceso de formación acción en modalidad cascada que permita orientación oportuna sobre crianza tecnológica.
- Impulsar la acción y el compromiso de actores políticos y sociales clave para garantizar el derecho de las familias a un uso seguro y responsable de las tecnologías digitales, a través del fortalecimiento de capacidades en la prevención y respuesta a la explotación y abuso sexual en línea de niñas, niños y adolescentes.

Enlace: <http://paniamor.org/Product/detail/21/crianza-tecnologica>

- **Modelo Tecnobus**

Desde sus inicios ha contado con el respaldo del MICITT. Esta estrategia llega a las comunidades del país a través de una plataforma móvil equipada con tecnología de punta. Consiste en una intervención costo efectiva y replicable para incidir en la brecha digital que afecta a las personas menores de edad en comunidades en desventaja social. Busca que los y las adolescentes logren identificar y desarrollar un conjunto de competencias tecnológicas para ser parte de un ecosistema. Este promueve:

- *Proceso de Formación en Competencias Tecnológicas:* trabajo de facilitación y acompañamiento en pro de la generación de un espacio socio afectivo que le permita a la persona adolescente desarrollar un conjunto de competencias tecnológicas;
- *Proceso de Movilización Comunitaria:* tiene como objetivo la generación de masas críticas de personas adultas en las comunidades donde se desarrolla el Modelo -padres, madres, líderes comunales y otras.

Enlace: <http://paniamor.org/Product/detail/20/modelo-tecnobus>

Desde la labor del ICE indicó que ha tenido que brindar desde su marco de acción apoyo interinstitucional con el OIJ. Además, con el PANI han desarrollado acciones concientización sobre los peligros latentes del ciberespacio y el control parental.

Asimismo, la **Fiscalía Adjunta de Atención de Hechos de Violencia en perjuicio de Niñas, Niños y Adolescentes (FANNA)** señaló que coordina esfuerzos con la Subcomisión de acceso de Niñez y Adolescencia.



Sensibilización Nacional

Costa Rica dice No a la Explotación y Abuso Sexual en Línea (CR-NEXST)

La iniciativa Costa Rica dice No a la Explotación y Abuso Sexual en Línea (CR-NEXST), surge en el 2018 a partir de un trabajo impulsado por la Fundación Paniamor, con el apoyo del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) y otras entidades públicas y privadas, el Instituto Mixto de Ayuda Social (IMAS) del Ministerio de Desarrollo Humano e Inclusión Social, el Patronato Nacional de la Infancia (PANI) y el Sistema de Emergencias 9-11 cuya finalidad consiste en promover acciones para la protección de niñas, niños y adolescentes (NNA) frente a la explotación y abuso sexual en línea (MICITT, 2021) y a su vez debido a la necesidad de realizar esfuerzos hacia la democratización de acceso a las tecnologías y la inclusión digital, como supuesto a cumplir para el cierre de brechas socioeconómicas y de conocimiento que limitan el desarrollo sostenible de la nación costarricense (PANIAMOR, 2021).

Dicha iniciativa es financiada por el Fondo End Violence Partnership & Fund, y desde su construcción ha contado con la asesoría técnica de ECPAT International. También ha trabajado en alianza estratégica con el Fondo de Naciones Unidas para la Infancia (UNICEF-CR).

La misma se planteó en tres componentes: 1. el fortalecimiento del Programa Hogares Conectados en alianza estratégica con el IMAS, 2. el fortalecimiento del Sistema Nacional 9-1-1, y 3. el desarrollo de un modelo nacional para la prevención y respuesta de la explotación y abuso sexual en línea de NNA (MICITT, 2021).

Para el desarrollo del primer componente, se creó el **Programa E-mentores**, el cual cuenta con una plataforma web cuyo objetivo es impulsar la acción y el compromiso de actores políticos y sociales claves para promover el ejercicio del derecho de las familias a un uso seguro y responsable de las tecnologías digitales, a través del fortalecimiento de sus capacidades en la prevención y respuesta a las conductas que propician la explotación y el abuso sexual en línea de niñas, niños y adolescentes (MICITT, 2021).

En junio de 2019, se firmó una **Carta de Entendimiento entre el MICITT y la Fundación Paniamor**, con el objetivo de generar un compromiso para apoyar en el proceso de desarrollo de capacidades de facilitadores activos en la prevención del abuso y explotación sexual de la niñez en línea (MICITT, 2021).

Los compromisos asumidos por el Ministerio de Ciencia, Tecnología y Telecomunicaciones en el marco del Programa E-mentores se derivan de la Carta de Entendimiento suscrita con la Fundación Paniamor, y tienen como principal objetivo el desarrollo de capacidades en



materia de prevención del abuso y explotación sexual de la niñez en línea, los cuales se enumeran a continuación:

- 1 *"Instalar el enlace a la Caja de Herramientas e-Mentores en la página web del MICITT, en coordinación con la Dirección de Evolución y Mercado de Telecomunicaciones.*
- 2 *Coordinar la instalación del enlace de la Caja de Herramientas e-Mentores en la plataforma de capacitaciones de los Centros Comunitarios Inteligentes (CECI) con la Dirección de Apropiación Social del Conocimiento.*
- 3 *Capacitar a las personas funcionarias del MICITT en el curso e-mentores a través de la Dirección de Evolución y Mercado de Telecomunicaciones.*
- 4 *Divulgar actividades externas que considere conveniente el programa e-mentores a través de la Dirección de Evolución y Mercado de Telecomunicaciones.*
- 5 *Brindar fuentes de verificación a Paniamor sobre la cantidad de personas capacitadas en las herramientas e-mentores a través de la Dirección de Evolución y Mercado de Telecomunicaciones." Carta Compromiso 2019" (MICITT, 2021)".*

En el año 2020, se presentó el Informe técnico N° MICITT-DEMT-INF-003-2020 Resultados de los Compromisos del Ministerio de Ciencia, Tecnología y Telecomunicaciones con el Programa e-mentores, Periodo 2019, con el avance de los compromisos alcanzados en ese año y el reporte del cumplimiento de la instalación de la caja de herramientas en el sitio web del MICITT.

De acuerdo con los avances de estos compromisos de la institución con el programa e-mentores se resumen de la siguiente manera:

1. *En relación con la instalación del enlace a la Caja de herramientas e-Mentores en la página web del MICITT, se realizó la gestión a través del Memorando MICITT-DEMT-MEMO-020-2019, con fecha de 22 de julio 2019, dirigido a la Unidad de Servicios Tecnológicos con el fin de incluir el enlace <https://www.ementores.org/> de la plataforma e-mentores en la página web mencionada, este compromiso se considera cumplido.*
2. *Sobre la instalación del enlace a la Caja de Herramientas e-Mentores en la plataforma de capacitaciones de los Centros Comunitarios Inteligentes (CECI), se procedió a integrar la plataforma de familias, dentro de la currícula de capacitaciones de los CECI. El acceso ha sido integrado a la plataforma web: http://ceci.go.cr/zf_Web/Index/academiamicitt El cual ha generado un total de 129 visitas, entre el periodo 2019 y hasta el 05 enero de 2020, y la instalación del enlace de la Caja de Herramientas e-Mentores en la plataforma de capacitaciones de los Centros Comunitarios Inteligentes (CECI).*



3. *El cual se incorporó con el Código: 2020-EMF cuyo nombre designado es esta plataforma fue E-mentores para familias a partir del 17 de marzo de 2020 todos los CECI del país que impartan este curso, deberán calendarizar el mismo con la información antes mencionada de este modo, este compromiso se considera cumplido.*
4. *Sobre el compromiso para capacitar a las personas funcionarias del MICITT como gestores del programa e-mentores, al finalizar el 2019 se capacitaron 18 personas, siendo la meta final para el 2021 de un total de 142 personas que conforman el personal de la institución. Se espera continuar con el proceso en el primer trimestre de 2020.*
5. *Además, se extendió esta formación a las personas encargadas de la gestión de los Centros Comunitarios Inteligentes para que se conviertan en mentores, y así cuentan con las capacidades para fungir como agentes multiplicadores de este conocimiento dentro de sus respectivas comunidades, y hagan un mejor aprovechamiento de la Caja de Herramientas. En la primera etapa, se capacitaron las personas encargadas de los CECI ubicados en Guanacaste, San Ramón, Zona Sur, Puntarenas, Zona Norte y Limón. Como resultado de esta fase se convocaron 484 personas encargadas de un total de 137 CECI. Como resultado de este proceso se capacitaron un total de 79 personas encargadas de CECI, de las cuales 48 personas finalizaron el curso. El grupo de personas facilitadoras se conformó por el equipo de la DEMA, los cuales se organizaron en equipos de trabajo, con dos o tres integrantes quienes facilitaron la capacitación. En el 2020 se espera capacitar a los encargados de los CECI faltantes.*
6. *Divulgación, se han realizado actividades asociadas a la seguridad en línea en las cuales se ha promovido el uso de la plataforma y sus contenidos. Este compromiso se considera es de carácter permanente (MICITT, 2020).*

Posteriormente, en cuanto a la atención de los compromisos 3, 4 y 5 que se ejecutaron en el periodo de enero a diciembre 2020, entre los que se destacan:

- La capacitación y sensibilización al personal del MICITT, a través de charlas impartidas por el Grupo E-mentores del MICITT abarcando un total de 111 personas funcionarias.
- Se concluyó con la formación de personas encargadas de la gestión de los Centros Comunitarios Inteligentes en el periodo 2020, capacitando 15 personas, que se convirtieron en gestores de E-mentores, con las capacidades para fungir como agentes multiplicadores de este conocimiento dentro de sus respectivas comunidades, y puedan hacer un mejor aprovechamiento de la Caja de Herramientas.
- Se han realizado actividades asociadas a la seguridad en línea en las cuales se ha promovido el uso de la plataforma y sus contenidos (MICITT, 2021).



- **Programa E-Mentores**

El Programa e-mentores es un espacio que brinda a padres, madres o familiares de personas menores de edad, la información y herramientas necesarias para que logren acompañarlos en el uso seguro de los recursos tecnológicos e Internet. Este programa forma parte del primer componente de la iniciativa *Costa Rica dice No a la Explotación y Abuso Sexual en Línea* (CR-NEXST), el cual cuenta con una plataforma web cuyo objetivo es impulsar la acción y el compromiso de actores políticos y sociales clave para garantizar el derecho de las familias a un uso seguro y responsable de las tecnologías digitales, a través del fortalecimiento de sus capacidades en la prevención y respuesta a las conductas que propician la explotación y el abuso sexual en línea de niñas, niños y adolescentes.

Está basado en una plataforma virtual que permite la alfabetización y democratización del conocimiento sobre temáticas de seguridad en línea disponible para todas las personas que pertenecen a instituciones públicas, empresas de tecnología y telecomunicaciones quienes a su vez han generado iniciativas dirigidas a poblaciones vulnerables como niñez y adolescencia incluyendo a aquellas relacionadas con su crianza.

Como parte de este programa la Fundación Paniamor cuenta con diferentes estrategias de sensibilización y cajas de herramientas integradas con recursos didácticos y pedagógicos innovadores. A continuación, algunas de sus Caja de Herramientas.

- **Familias Ementoras:** Espacio interactivo de autoformación para personas con roles de cuidado y acompañamiento para promover el uso seguro de las TIC. **Enlace:** <http://www.ementores.org/familias/>
- **Agentes e-mentores:** curso virtual en plataforma moodle diseñado para instalar capacidades en referentes institucionales en su rol de agente de prevención y respuesta del abuso y la explotación sexual en línea. **Enlace:** <https://e-mentores.moodle.school/login/index.php>
- **Ecompa:** Espacio interactivo para personas adolescentes para realizar un uso seguro en Internet y promover un uso responsable con sus pares. **Enlace:** <http://www.ementores.org/ecompa/>
- **Crianza Tecnológica:** Proceso de autoformación para personas con roles de cuidado y acompañamiento para modelar una crianza activa y responsable con las personas menores de edad, desde el paradigma de la ciudadanía digital. **Enlace:** <https://crianzatecnologica.paniamordigital.org/>
- Dicha iniciativa se encuentra vigente desde el año 2019 la cual logró un alcance nacional de 53.463 niños y niñas, 6.545 adolescentes, 41.196 madres, padres y personas cuidadoras y 3.343 personas funcionarias capacitadas.



- **Código E- Mentores:** El Código e-mentores consiste en un programa de responsabilidad y acción social en Costa Rica para la prevención y respuesta del abuso y la explotación sexual en línea. Esta iniciativa es liderada por Fundación PANIAMOR con el apoyo institucional del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT); y el Instituto Mixto de Ayuda Social (IMAS). El programa se basa en un mecanismo de autorregulación a partir de una adhesión voluntaria por parte del sector industria de las telecomunicaciones y de la sociedad civil que promueve el cumplimiento de estándares para la prevención y respuesta del abuso y la explotación sexual en línea.

Es una alternativa sostenible para multiplicar acciones orientadas al uso seguro y responsable del Internet por parte de niñas, niños y adolescentes, y sus familias. El proceso de construcción de esta herramienta fue liderado por la Fundación PANIAMOR, en alianza estratégica con organizaciones del sector privado, tales como: Claro, CoopeGuanacaste, Kölbi, Tigo, IBM Costa Rica y Fundación Quirós Tanzi, estas se convirtieron en las entidades fundadoras que proponen el cumplimiento de una serie de compromisos por incluir en sus prácticas para la promoción de la inclusión digital y la crianza tecnológica, principios transversales del Código. El proceso contó, además, con el apoyo financiero de End Violence Against Children, The Fund en el marco de la Iniciativa País: Costa Rica dice No a la Explotación y Abuso Sexual en Línea de Niñas, Niños y Adolescentes'; y con el respaldo de la Cámara de Infocomunicación y Tecnología (INFOCOM).

Dentro de los criterios a evaluar para formar parte del programa destacan: la existencia de protocolos que prevengan y respondan ante situaciones de explotación o abuso sexual en línea de niñas, niños y adolescentes; la garantía de contar con capacidades internas para considerar la explotación y abuso sexual en línea de niñas, niños y adolescentes como parte de sus planes estratégicos, tácticos u operativos y finalmente la posibilidad de Multiplicación social o promoción de los principios del Código e-mentores en su cadena de valor y entre sus partes interesadas, sea públicamente o por medio de comunicaciones específicas.

- **¡Qué gato con las TIC!, Defensa de Niños Internacional**

Se trata del programa de Defensa de Niños Internacional (DNI) sobre el uso de redes sociales digitales y cómo prevenir la explotación sexual comercial en línea. Su modelo plantea un proceso pedagógico que estimula el desarrollo de factores protectores, comprendidos estos como el auto cuidado y autogestión del aprendizaje e interaprendizaje, con la finalidad de que las personas adolescentes puedan navegar de forma segura en las redes digitales y así puedan identificar los diferentes riesgos presentes en el espacio virtual, los cuales aumentan la vulnerabilidad para ser víctimas de explotación sexual comercial. Para ello realizan procesos de formación con estudiantes de colegios públicos y privados sobre la prevención



de la explotación sexual comercial de niños, niñas y adolescentes (ESCNNA) mediada por las TIC; capacitación dirigida a personal docente, usando metodología bimodal avalada por la Dirección General de Servicio Civil, en la cual cada docente recibe hasta 15 horas de capacitación en temáticas como la inclusión de las TIC en procesos de enseñanza y aprendizaje, abordaje psicosocial de problemáticas mediadas por las TIC (sexting, cyberbullying, privacidad, entre otros) y marco jurídico y normativo de las TIC en Costa Rica. Además, desarrollan trabajo con padres y madres de la GAM y zonas rurales en temáticas tales como parentaje y TIC, privacidad de hijas e hijos y abordaje de riesgos. Investigación alrededor de la dimensión relacional de las TIC y la defensa de los derechos de niñas, niños y adolescentes.

- **Proyecto Conectándonos en Línea, Fundación Quirós Tanzi**

Tiene por objetivo ofrecer mejores oportunidades de inclusión social digital a los niños, y que su proceso de aprendizaje en la etapa escolar sea realmente significativo y beneficioso para su desarrollo, gracias al potencial que tiene la tecnología brindada en distintos espacios educativos cambiantes. Se desarrolla por la Fundación Quirós Tanzi en asocio con el Ministerio de Educación Pública. A través de la iniciativa se brinda espacios presenciales y virtuales de desarrollo profesional a los docentes, que permiten un acercamiento a las herramientas tecnológicas (computadoras, proyectores interactivos, kits de robótica) presentes en la institución. Además, se capacita y asesora en la integración de la tecnología en los planeamientos didácticos. Para familias, se habilitan talleres y cursos gratuitos, con el fin de abordar temas relacionados con el uso de las tecnologías móviles, Internet seguro, educación financiera, ofimática, emprendedurismo, entre otros.

- **Curso Ciudadanía Digital Responsable, Fundación Omar Dengo y el Instituto de Formación Ciudadana del Tribunal Supremo de Elecciones**

Las organizaciones Fundación Omar Dengo y el Instituto de Formación Ciudadana del Tribunal Supremo de Elecciones desarrollaron un curso virtual dirigido a cualquier persona interesada en estas temáticas a partir del mes de agosto de 2021, este curso constará de cuatro módulos los cuales requieren de un total aproximado de 6 a 8 horas de dedicación cuyos objetivos consistieron en conocer conceptos y herramientas para proteger la información, identificar las desinformaciones en redes sociales así como desarrollar habilidades para actuar bajo principios, valores y prácticas democráticas.

- **Capacidades sobre ciberseguridad y violencia de género, Instituto Nacional de las Mujeres, UNICEF Costa Rica**

El Instituto Nacional de las Mujeres (INAMU), UNICEF Costa Rica y la organización Nosotras Women Connecting desarrollaron un Taller para jóvenes entre los 12 y los 23 años,



conformados en campamentos virtuales de tres días con el fin de dotar a las participantes de herramientas digitales para uso seguro de Internet y sobre violencia de género.

Herramientas, Servicios y Ajustes

Al considerarse a los niños, niñas y adolescentes una población de protección especial se han llevado a cabo acciones afirmativas en lo político, normativo y en relación con las estrategias de acceso a bienes y servicios específicamente adaptados a sus necesidades. En lo correspondiente al análisis de las herramientas de política pública relacionadas a TIC mencionadas con anterioridad se identifican los siguientes elementos:

Plan Nacional Desarrollo de las Telecomunicaciones (PNDT) 2015-2021

<p>Visión 2021: Transformar a Costa Rica en una sociedad conectada, a partir de un enfoque inclusivo del acceso, uso y apropiación de las tecnologías de la información y las comunicaciones, de forma segura, responsable y productiva.</p>		
<p>Pilar de Inclusión Digital</p>		
<p>Objetivo: Reducir la brecha digital de acceso, uso y apropiación de las Tecnologías Digitales, con el fin de que la población en condiciones de vulnerabilidad disfrute de los beneficios de las Telecomunicaciones /TIC como herramienta para la superación, el desarrollo personal y el ejercicio de sus derechos.</p>		
<p>Línea de Acción Alfabetización Digital: Fomentar el empoderamiento de las Telecomunicaciones/TIC por parte de la población con la participación interinstitucional.</p>		
<p>Programa: Empoderamiento de la Población en TIC</p>	<p>Objetivo: Incrementar el uso y la apropiación responsable, segura y productiva de las tecnologías digitales de la población en general</p>	<p>Resultado: Disminución en la brecha de uso de las tecnologías digitales de la población, de manera que se logre un uso responsable y seguro y se fomente la innovación social</p>
<p>Meta 16: 100% de ejecución de los componentes del Programa de Empoderamiento de la Población en Tecnologías Digitales al 2018</p>		
<p>Pilar de Gobierno Electrónico y Transparente</p>		



Objetivo: Avanzar hacia una relación más cercana y abierta entre la administración pública y los habitantes de manera que incremente la eficiencia estatal, facilite el acceso a servicios públicos innovadores, promueva la transparencia, toma de decisiones del Estado y la participación activa de la Sociedad.		
Línea de Acción Gobierno Cercano: Digitalización de trámites y servicios brindados por el Gobierno mediante plataformas y terminales tecnológicas y que a su vez se relaciones con el teletrabajo.		
Programa: Impulsar el Gobierno Electrónico	Objetivo: Lograr un Gobierno Electrónico Abierto, interconectado que permita brindar servicios interactivos de calidad para propiciar el empoderamiento y la participación de la sociedad civil	Resultado: Desarrollo de aplicaciones utilizando las TIC para lograr una plataforma de Gobierno Electrónico accesible a la población, que fomente la participación de la ciudadanía y la rendición de cuentas
Meta 20: 100% de cumplimiento del programa para impulsar la ciberseguridad como un eje de desarrollo del Gobierno Electrónico.		

Estrategia de transformación digital

Visión: Una Costa Rica transformada digitalmente acelerando la productividad, la competitividad y el desarrollo socio-económico, tomando ventaja de la cuarta revolución industrial y las sociedades del conocimiento, para procurar el bienestar de todos sus habitantes de manera inclusiva y potenciar el desarrollo sostenible del país.
Lineamiento rector 3: Servicios digitales inclusivos, integrados y seguros
Eje: Sociedad Innovadora
Objetivo: Promover la innovación social a través de la utilización de nuevas tecnologías y el empoderamiento de los actores de la sociedad.
Línea de acción 2: Potenciar las destrezas y habilidades digitales de la sociedad costarricense.



<p>Meta: Desarrollar programas de formación continua desde una perspectiva de género y maximizar el aprovechamiento de la base instalada de centros públicos ciudadanos para potenciar la adopción de las tecnologías digitales al servicio del arte, de la cultura y de la sociedad.</p>				
<p>Promoción de equidad de género en el aprovechamiento de las tecnologías digitales para crear valor agregado.</p>				
<p>Mejorar la oferta de programas para potenciar las destrezas y habilidades digitales.</p>	<p>Maximizar el uso de los centros públicos ciudadanos para desarrollar capacidades en las empresas y los ciudadanos.</p>	<p>Disminuir la brecha digital en los sectores sociales más vulnerables.</p>	<p>Mejorar la divulgación en materia de oportunidades y nuevos conocimientos tecnológicos.</p>	<p>Disminución de la brecha de género en el aprovechamiento de las tecnologías digitales.</p>
<p>Eje: Buena Gobernanza</p>				
<p>Objetivo: Garantizar la buena gobernanza mediante la participación ciudadana y la transparencia de la gestión pública impulsando la rendición de cuentas.</p>				
<p>Línea de acción 4: Adaptación del marco normativo nacional a las nuevas tecnologías.</p>				
<p>Meta: Propiciar los cambios sustantivos en materia de la normativa nacional vigente para permitir el aprovechamiento de las tecnologías digitales disruptivas en el quehacer de los diferentes sectores de la sociedad costarricense.</p>				
<p>Normativa para la gestión de la información ciudadana (habeas data, privacidad).</p>	<p>Observatorio de normativa.</p>	<p>Potenciar la utilización de nuevas tecnologías para el mapeo de la normativa vigente.</p>	<p>Sistemas de búsqueda e identificación de normativa vigente con tecnologías disruptivas.</p>	



Mejorar la seguridad jurídica en las relaciones entre los usuarios y los servicios de gobierno digital.	Aumentar la fiscalización ciudadana y la discusión sobre la normativa vigente.	Mejorar la capacidad de consulta y aprovechamiento de los instrumentos normativos mediante plataformas digitales.
---	--	---

Estrategia de Ciberseguridad

Objetivo principal: Desarrollar un marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentando la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente a los riesgos en cuanto al uso de las TIC para lograr un entorno más seguro y confiable para todos los habitantes del país.	
Colaboración interinstitucional para la identificación y respuesta de situaciones de riesgo	
Objetivo específico 1: Coordinación Nacional: Coordinar con todas las partes interesadas para establecer su papel y línea de acción tanto en el proceso de mitigación como gestión, recuperación y continuidad en caso de un incidente de seguridad cibernética.	Objetivo Específico 6: Gestión del Riesgo: Promover la implementación de un modelo de gestión de riesgo que se adapte a las necesidades propias de cada institución u organización.
Mejora de legislación en caso de explotación y abuso en línea	
Objetivo Específico 4. Fortalecimiento del marco jurídico en Ciberseguridad y TIC: Realizar una revisión del marco jurídico existente y proponer los ajustes necesarios para llevar a cabo procedimientos legales y medidas institucionales que garanticen una adecuada investigación y el enjuiciamiento efectivo.	
Educación digital para uso de tecnologías de forma segura	



<p>Objetivo Específico 2: Conciencia pública: Desarrollar y/o implementar campañas de concienciación y educación sobre seguridad cibernética que fomenten la responsabilidad de la protección digital como un deber de todos los usuarios de las tecnologías digitales.</p>	<p>Objetivo Específico 3. Desarrollo de la Capacidad Nacional de Seguridad Cibernética: Realizar campañas de capacitación exclusivas para el sector público que tengan como objetivo educar a los usuarios finales en conceptos y buenas prácticas sobre seguridad cibernética y preparar a usuarios expertos (desarrolladores, administradores, directivos) en técnicas de seguridad cibernética.</p>
<p>Línea estratégica 2.1: Desarrollar campañas de concienciación en ciberseguridad para los habitantes de Costa Rica de modo que se habitúen y acojan buenas prácticas como parte de su cultura, considerando el fortalecimiento de acciones para la protección de grupos poblacionales en condición de vulnerabilidad como niñez y adolescencia, adultos mayores, población indígena, población con discapacidad. Todo ello en alianza con el sector privado, sociedad civil y organizaciones no gubernamentales dedicadas a la protección de la infancia y adolescencia.</p>	
<p>Objetivo Específico 8: Implementación, Seguimiento y Evaluación: Diseñar y aplicar una metodología de implementación y seguimiento que permita evaluar el cumplimiento de las líneas de acción y proponer los ajustes según se requiera.</p>	
<p>Línea estratégica 8.2. Realizar una revisión y actualización de la Estrategia Nacional de Ciberseguridad cada dos años o según sea necesario.</p>	

PICTI

<p>Objetivo: Promover la igualdad en la participación de las mujeres respecto de los hombres en la atracción, la permanencia, la formación, la capacitación, el empleo de calidad y la investigación, en los diferentes campos de la ciencia, la tecnología y la innovación, para facilitar el acceso y el disfrute de los avances científicos-tecnológicos.</p>
<p>Eje 4: Apropiación social de la ciencia con perspectiva de género.</p>
<p>Objetivo específico 4: 4. Estimular la apropiación social de la ciencia y la tecnología, mediante el apoyo a proyectos e investigaciones científico - tecnológicos con perspectiva de género en todas las áreas del desarrollo humano que cuenten con participación activa</p>



de mujeres en el planteamiento y solución de problemas, considerando los diferentes contextos socioculturales.			
Acción específica 4.4. Incentivar la investigación aplicada para la creación de ciberespacios seguros que reduzcan la vulnerabilidad de las mujeres.			
4.4.1. Porcentaje de avance en la creación de ley para la protección de los derechos de las mujeres en el espacio digital.	4.4.2. Porcentaje del personal de la sección de delitos informáticos capacitado para la atención de la violencia de género, riesgo y vulnerabilidad digital.	4.4.3. Número de páginas web dirigidas a la prevención de la violencia, que integran el tema de la violencia digital contra las mujeres.	4.4.4. Número de plataformas web que desarrollan contenido y servicios digitales con enfoque de género, seguros para las mujeres, en funcionamiento para todo el país.

Política de Sociedad y Economía Basada en el Conocimiento

Principios rectores	Respeto a los Derechos Humanos	Sostenibilidad	Calidad	Universalidad	Ética
Pilar 5: Tecnología Digital					
Habilitar un entorno que propicie las condiciones necesarias para un mayor crecimiento del ecosistema digital, requiere la generación de políticas públicas que fomenten la participación de todos los actores sociales, brinde seguridad jurídica, y favorezca la expansión de las inversiones y la competencia efectiva en el mercado, tanto desde el punto de vista de las políticas públicas como en materia de regulación en telecomunicaciones.					
Línea de Acción 14: Generar capacidades y habilidades en el uso de las tecnologías digitales por parte de todos los actores que integran la sociedad					
Línea de acción 15: Implementar un modelo de Gobernanza Digital cada vez más cercano a los ciudadanos, empresas y organizaciones.					

El país cuenta con una serie de protocolos en materia de atención de casos de violencia en personas menores de edad, específicamente no cuenta con un protocolo en específico para



atención de casos de abuso de niños, niñas o adolescentes en línea, sin embargo, se considera que estos protocolos tienen alcance para estas situaciones.

- **Protocolo de actuación en situaciones de violencia física, psicológica, sexual, acoso y hostigamiento sexual, Ministerio de Educación Pública**

El Protocolo establece que los centros educativos son espacios privilegiados para la promoción del desarrollo integral de niños, niñas, adolescentes y jóvenes: para el aprendizaje de formas sanas de convivir y relacionarse con otras personas; pero también son espacios donde, pueden darse hechos de violencia, o bien conocerse manifestaciones de ésta, en perjuicio de la población estudiantil. Con el apoyo de UNICEF, la Dirección de Vida Estudiantil del MEP desarrolló estos protocolos de acatamiento obligatorio en los Centros Educativos (MEP, 2015).

Enlace: <https://www.mep.go.cr/sites/default/files/protocolo-situaciones-violencia.pdf>

- **Guía de atención integral a niños, niñas y adolescentes víctimas de abuso, Caja Costarricense de Seguro Social**

Esta Guía incluye información relativa al proceso general de atención integral de las personas menores de edad en situaciones de abuso que asisten a los diferentes servicios de salud de la Caja Costarricense de Seguro Social.

La Guía incluye aspectos generales de la Guía, entre ellos antecedentes históricos internacionales y nacionales, cuyo objetivo es situar en el tiempo el esfuerzo nacional en la atención integral contra niños, niñas y adolescentes víctimas de abuso, además se presenta el marco conceptual abarcando definiciones generales y específicos de abuso, lo que tiene como meta fomentar el manejo de un lenguaje común en torno a la temática de abuso a niños, niñas y adolescentes en los servicios de salud.

Esta parte es fundamental, en tanto, uno de los principales problemas que existen en el abordaje de las situaciones de abuso es la diferencia de criterios sobre los principales tipos de abuso y los procesos relacionados. Además, se anotan indicadores, factores de riesgo y determinantes relacionados con el fenómeno de la violencia contra niños, niñas y adolescentes. Aquí se hace énfasis en que generalmente, un indicador, criterio diagnóstico, factor de riesgo o determinante, no es suficiente por sí solo para establecer el diagnóstico de abuso, promoviendo su uso en forma integral junto con otras evidencias y análisis realizado en equipo interdisciplinario. De igual manera, abarca las consideraciones generales a tomar en cuenta en el proceso de atención integral general en la Red de Servicios, lo que incluye consideraciones ético-legales, el marco organizativo y la coordinación con otras instituciones como el PANI y el Ministerio Público, lo cual supone la existencia de un Comité de Estudio Integral de Niños, Niñas y Adolescentes Agredidos (CEINNAA) tal como se establece en el



Artículo 48 del Código de la Niñez y la Adolescencia. Comité cuya principal función es la coordinación de dicha atención. Además, incorpora actividades generales que se deben llevar a cabo en los EBASIS, las sedes de Áreas de Salud Hospitales, Regionales, Periféricas, Nacionales y Especializados manteniendo el principio de trabajo en red de acuerdo a la capacidad resolutoria de cada nivel de atención, lo que incluye los principios de la Atención Primaria en Salud.

Enlace: <https://www.binasss.sa.cr/protocolos/victimasabuso.pdf>

- **Protocolo de atención legal a víctimas de delitos sexuales y violencia doméstica cometidos por personas menores de edad, Ministerio Público Poder Judicial**

Este es un instrumento que permitirá brindar un mejor servicio a las víctimas de delitos relacionados con la violencia sexual y doméstica, logrando así la reducción de la revictimización secundaria en las diligencias realizadas por el Ministerio Público. Los presentes protocolos forman parte del proyecto de Reducción de la Revictimización de personas víctimas de delitos sexuales y violencia intrafamiliar que forman parte de la ejecución del Convenio de Préstamo 1377/OC-CR entre el Gobierno de la República de Costa Rica y el Banco Interamericano de Desarrollo, destinado a financiar la segunda etapa del Programa de Modernización de la Administración de Justicia. La segunda etapa de este programa comprende el componente de Fortalecimiento del Ministerio Público, cuyo objetivo es, mejorar la actividad persecutoria que ese órgano desempeña. Las personas tienen el derecho a no ser revictimizadas y maltratadas, por lo que el Poder Judicial decidió definir normas de protocolos de servicios dirigidos a alcanzar esto.

El propósito que se pretende cumplir con los protocolos es crucialmente que el servicio de Administración de Justicia no sea un mecanismo más de revictimización. Además, se pretende uniformar y controlar el cumplimiento de las rutinas de trabajo y evitar alteraciones arbitrarias, simplificar la determinación de responsabilidades por fallas o errores, facilitar las labores de auditoría, la evaluación del control interno y su vigilancia; que tanto las/os empleadas/os como sus jefas/es conozcan si el trabajo se está realizando adecuadamente; reducir los costos al aumentar la eficiencia general. Con la protocolización de las actuaciones judiciales se pretende que en todo el Poder Judicial, cualquier profesional siga las mismas pautas de actuación, facilitando las acciones judiciales y sociales a la víctima. Favoreciendo la denuncia de estas agresiones, sensibilizando al personal ante estos casos, protegiendo la intimidad y facilitando la información de la persona víctima de la violencia intrafamiliar o delitos sexuales y la correcta obtención de la prueba necesaria para la investigación de los delitos.



Enlace: https://sitiooij.poder-judicial.go.cr/images/Documentos/Otras-Normativas/Protocolo_de_Atencion_Legal_Victimas_de_Delitos%20Sexuales_Violencia_Domestica_cometidos_por_Menores_de_Edad.pdf

En este sentido, de parte del **ICE** indicó dentro de sus buenas prácticas que su área de seguridad ha participado en procesos de concientización en coordinación con Gestión de Marca visitando escuelas y colegios para hablar sobre los peligros latentes a los que se encuentra expuesta la niñez mediante el uso del internet y cómo establecer buenas prácticas. Y la **Fiscalía Adjunta de Atención de Hechos de Violencia en perjuicio de Niñas, Niños y Adolescentes (FANNA)** señaló como buena práctica para la detección de estos casos en las investigaciones penales realizadas con la Sección de Cibercrimen del OIJ.

Medidas de Accesibilidad

Desde el Poder Judicial se señaló que aún no cuentan a nivel penal con este material, por el momento está en proceso la aprobación de las políticas de persecución penal para niñez y adolescencia, así como para personas en condición de discapacidad.

En general tanto para personas menores de edad como para padres, educadores y cuidadores es importante indicar que Costa Rica en materia de accesibilidad a la información y a la comunicación cuenta con la **Ley 8661, Ratificación de la Convención sobre los derechos de las personas con discapacidad**, desde el 2008 y la **Ley 7600, Igualdad de oportunidades para las personas con discapacidad, desde el año 1996**. No obstante, en cuanto al tema de accesibilidad web, es hasta la puesta en marcha del Plan Nacional de Desarrollo de las Telecomunicaciones PNDT 2015-2021 que se establece una meta referente al desarrollo de una estrategia para la aplicación de criterios de accesibilidad y diseño universal en las tecnologías de la información y la comunicación, dirigida a las instituciones del Gobierno Central al 2021, de la cual se deriva la **Directriz 051 MTSS-MICITT Implementación de la accesibilidad de sitios web en el sector público, cuyo objetivo es oficializar la utilización de los criterios de accesibilidad establecidos en la norma WCAG 2.1 "Pautas de Accesibilidad para el Contenido Web"** y sus posteriores versiones, en las páginas de los sitios web de las instituciones del Estado, facilitando a las personas con discapacidad el acceso a la información y a las Tecnologías de Información y Conocimiento (TIC), de manera oportuna y sin costo adicional al usuario final, en formatos accesibles y con las tecnologías adecuadas a los diferentes tipos de discapacidad, con el objeto de garantizar la igualdad real de oportunidades y trato, evitando así todo tipo de discriminación. Asimismo, se han desarrollado otras acciones como la generación de 19 normas técnicas complementarias, entre las que se cuenta la tropicalización de la norma WGAC 2.1 y diversas actividades de asesoría y capacitación en el tema.



Línea de ayuda

En Costa Rica, el Patronato Nacional de la Infancia (PANI) cuenta con el **Centro de Orientación e Información (COI)**, donde se reciben denuncias, se atienden consultas y a su vez se brinda orientación a personas menores de edad y adultas en situaciones relacionadas a la violación de derechos de niños, niñas y adolescentes. Busca alternativas para la garantía del ejercicio de los derechos.

Además, el Centro facilita orientación e información a los y las usuarias, así como la direccionalidad de las denuncias de una manera integral, coordinando en el ámbito intrainstitucional e interinstitucional para brindar una respuesta que garantice el cumplimiento de los derechos de las personas menores de edad.

También, tiene espacios específicos para que los niños, niñas y adolescentes tengan una participación activa en la garantía y restitución del ejercicio de sus derechos, mediante líneas telefónicas gratuitas. En detalle estas líneas corresponden a la línea telefónica **1147** y una línea de atención vía WhatsApp 8989-1147, también puede utilizarse el servicio de emergencias 9-1-1. Por otro lado, es pertinente aclarar que estas líneas de atención se utilizan para denunciar situaciones violatorias de derechos hacia un niño, niña o adolescente (PANI, 2021). Asimismo, se ofrecen los siguientes servicios:

- **Atención directa al público:** En las instalaciones del COI, los profesionales brindan orientación e información de primera instancia a la población que lo requiera, en temas relacionados a la garantía de los derechos de las personas menores de edad. Este servicio se ofrece de lunes a viernes, de 7:30 a.m. a 4 p.m.
- **Consultas mediante la Central Telefónica:** Es un servicio institucional que permite recibir la demanda de usuarios y usuarias, quienes solicitan orientación, consultas e información sobre servicios institucionales a través de los números de la Central Telefónica. Las mismas son debidamente canalizadas a profesionales. Central Telefónica: 2523-0700 / 2523-0800/ 2523-0900. Horario: De lunes a viernes de 7:30 a.m. a 4 p.m. (PANI, 2021).

Por otro lado, la **Oficina de Recepción de Denuncias (ORD) del Organismo de Investigación Judicial** es la dependencia que se encarga, en el Área Central de San José, de recibir las denuncias de las personas víctimas de delito, convirtiéndose en el primer enlace formal entre la persona usuaria y los servicios de atención de la institución. Se reciben denuncias tanto típicas como atípicas. Las denuncias que se reciben son remitidas dos veces por día en las diferentes Oficinas del Poder Judicial, O.I.J, Fiscalías, Juzgados Contravencionales (OIJ, 2021).



El horario de atención al público es de lunes a domingo, las 24 horas del día, los 365 días del año 2295-3644 fax 2295-3114 o bien mediante el siguiente correo electrónico oij_denuncias@poder-judicial.go.cr

Adhesión al Convenio de Budapest

Mediante decreto ejecutivo N° 40546 del 3 de julio de 2017, Costa Rica se adhiere al Convenio.

Ley N° 9452 Convenio de Budapest: En el campo propiamente de los delitos informáticos, en el año 2017 se ratificó la Convención sobre Ciberdelincuencia (Convenio de Budapest) ratificada mediante la citada ley de fecha 03 de julio del 2017.

PANI-Poder Judicial, de igual forma Costa Rica ha creado mecanismos para la atención a víctimas de delitos, a nivel judicial, cuenta con la Ley de protección a víctimas, testigos y demás sujetos intervinientes en el proceso penal y con una **Oficina de Atención y Protección a la Víctima en el Ministerio Público**, que implementó dos programas: **Programa de Atención y Programa de Protección**, los cuales son gratuitos, voluntarios y confidenciales. Es importante que se prevean servicios de atención mental y médica para NNA víctimas de Explotación Sexual en Línea, además de los servicios de apoyo para los miembros de familia de la víctima, para ayudarles durante el proceso de recuperación (PANIAMOR, 2018).

Además, la Fiscalía Adjunta de Atención de Hechos de Violencia en perjuicio de Niñas, Niños y Adolescentes (FANNA) indicó que la **Fiscalía Adjunta de Género (FAG Ministerio Público)** atiende e investiga ese tipo de delitos.

Según **OCDE** (2020) Costa Rica necesita mejorar el seguimiento y la medición regulares de la evolución de la alfabetización digital de los niños y niñas y promover el crecimiento de una base empírica y analítica sólida para el desarrollo y la implementación de políticas basadas en la evidencia.

Considerando la evaluación realizada en 2018 sobre la aplicación del **Modelo We Protect**, se requiere además fortalecer los mecanismos de cuenta el apoyo a las víctimas en todo el proceso de investigación e incluso después. NNA que hayan sido seducidos por Internet puede sentirse responsable o pensar que se merece este abuso, lo que hace más difícil que lo revele. Por lo tanto, es importante que se prevean servicios de atención mental y médica para NNA víctimas de explotación sexual en línea para NNA, además de los servicios de apoyo para los miembros de familia de la víctima, para ayudarles durante el proceso de recuperación.



Otro aspecto que se requiere fortalecer es el incremento en la designación de recursos humanos y financieros suficientes para atender la explotación sexual en línea de NNA, a fin de facilitar mucha más información y empoderar a la población.

Además, el principal desafío para las autoridades gubernamentales, en particular para el **MICITT**, será el cumplimiento del 100% de las acciones que emana de la Estrategia EASNAL incluida en el nuevo PNDT 2022-2027, la cual se ejecutará en este mismo periodo.

Asimismo, desde el punto de vista de las organizaciones estas indican que es un desafío contar con recursos para financiar campañas accesibles en varios formatos que realmente sean un recurso de información para todas las poblaciones y sus diversidades. Acceso real a las TIC en las comunidades (Internet, dispositivos, asesoría articulada de las instituciones), brindando mayor apoyo y recursos a las poblaciones con factores socioeconómicos, culturales, discapacidad, entre otros.

Igualmente, la **Fundación Paniamor** prioriza los siguientes desafíos:

- Acceso al internet, en igualdad de condiciones, sin discriminación alguna. En especial en zonas rurales y costeras.
- Alfabetización digital que permita a la población desarrollar habilidades digitales para un uso crítico y reflexivo de las tecnologías digitales
- Fomento del ejercicio de la ciudadanía digital por parte de la población, a través de acciones afirmativas que brinden acceso a espacios de expresión, participación y colaboración desde el enfoque de los derechos humanos y la promoción de valores de paz.

Por parte del **ICE**, desde su punto de vista señaló que:

- El acceso universal al internet y las posibilidades de crecimiento mediante la innovación tecnológica.
- La integridad y confidencialidad de los datos personales en el mundo en línea, así como la seguridad de los datos institucionales.
- Minimizar los ciberdelitos a los que está expuesta la población mediante el ciberespacio y fomentar accesos seguros, mediante una mayor concientización de la población sobre peligros latentes en el ciberespacio y como propiciar accesos seguros.

La Fiscalía Adjunta de Atención de Hechos de Violencia en perjuicio de Niñas, Niños y Adolescentes (FANNA) mencionó como desafíos:

- Capacitación a funcionario que trabaja con esta población, así como a los encargados de la responsabilidad parental, sensibilización, control parental y escolar.



Áreas de oportunidad en el mundo en línea para Costa Rica

Se puede indicar que las oportunidades que se tienen son las siguientes:

- El alcance del acceso a servicios de telecomunicaciones e Internet permite el desarrollo de una gran cantidad de actividades que promueven el desarrollo como son el acceso a la salud, la educación, el comercio, los servicios, entre otras, representando así una oportunidad de gestar entornos digitales seguros, productivos y responsables en coordinación con la institucionalidad pública, la empresa privada y la sociedad civil.
- Otra oportunidad es la posibilidad de acceder a los recursos que se generan en otras latitudes y en especial la articulación y colaboración con actores nacionales e internacionales para apoyar el desarrollo de habilidades y destrezas para realizar un uso productivo, significativo y seguro de los recursos digitales.
- Diseño de políticas públicas visionarias e innovadoras para promover el desarrollo de entornos seguros sobre la base de las experiencias y buenas prácticas que se llevan a cabo en el mundo.

Por otro lado, en este rubro se suma la perspectiva de distintos actores nacionales involucrados, según se indica a continuación:

- **La Fundación Paniamor** considera que las oportunidades en línea son infinitas Priorizando las oportunidades , las personas menores de edad y sus referentes familiares tienen la oportunidad de: Acceder a recursos didácticos de calidad para ejercer su derecho a la información, conocimiento, formar parte de un ecosistema digital que les permita a las personas menores de edad y sus familias a ejercer su derecho a la expresión , participación y ser tomados en cuenta para la toma de decisiones en asuntos que les competen, y también espacios para la creación e innovación que permita a las niñas, niños y adolescentes ser prosumidores y participantes activos de soluciones de problemas de su comunidad.
- El **Instituto Costarricense de Electricidad (ICE)** mencionó como oportunidades: 1. El acceso a la información y actualización constante, 2. La innovación y facilitación de trámites 3. El alcance exponencial que por su naturaleza genera el ciberespacio que permite comunicarnos masivamente.
- La **Fiscalía Adjunta de Atención de Hechos de Violencia en perjuicio de Niñas, Niños y Adolescentes (FANNA)** indicó como oportunidades, el acceso de información para retroalimentarse, comunicación inmediata independientemente de la distancia, aporte al medio ambiente por el no uso de papel.



ECUADOR

Índice de siglas del capítulo

ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones
CCPD	Consejos Cantonales de Protección de Derechos
CDN	Convención sobre los Derechos del Niño
CNII	Consejo Nacional para la Igualdad Intergeneracional
CONADIS	Consejo Nacional para la Integración de la Persona con Discapacidad
COOTAD	Código Orgánico de Organización Territorial Autonomía Descentralización
DECE	Departamento de Consejería Estudiantil
DINARDAP	Dirección Nacional de Registros Públicos
FENPIDEC	Organización de base comunitaria, promotora de la protección integral y Derechos de los niños, niñas, adolescentes y jóvenes del Noroccidente de Pichincha
FOFOUSI	Formación de Formadores en el Uso Seguro del Internet
MILTEL	Ministerio de Telecomunicaciones y de la Sociedad de la Información
OEA	Organización de los Estados Americanos
SNDPINA	Sistema Nacional Descentralizado de Protección Integral de la Niñez y Adolescencia
TIC's	Tecnologías de la Información y Comunicación



Política Nacional Digital

Desde 2011 Ecuador cuenta con su estrategia “Ecuador Digital”, lanzada dentro del Plan Nacional Para el Buen Vivir, y que ha tenido diversas actualizaciones para mejoramiento de la calidad de vida de los ecuatorianos, con el objetivo de que las TIC se utilicen de manera efectiva en el proceso de desarrollo productivo, social y solidario, para el bienestar de todos.

Cuenta con tres programas de acción:

- Ecuador Conectado;
- Ecuador Eficiente y Ciberseguro;
- Ecuador Innovador y Competitivo.

Dicha estrategia se encuentra a cargo del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MILTEL)⁶¹.

El Consejo Nacional para la Igualdad Intergeneracional (CNII) en el marco de las atribuciones establecidas en la Constitución y en la Ley Orgánica para los Consejos Nacionales para la Igualdad; conjuntamente con la actual Dirección Nacional de Registros Públicos, el Ministerio de Telecomunicaciones y de la Sociedad de la Información en conjunto con 22 instituciones públicas, privadas y organismos internacionales, con el propósito de implementar la política pública de uso seguro de internet para niñas, niños y adolescentes, han sumado esfuerzos para desarrollar, presentar e implementar la “Política Pública por el Uso Seguro de Internet para Niñas, Niños y Adolescentes”.

El Ministerio de Educación ejecuta la Agenda Educativa Digital, un instrumento de política pública orientado a la transformación digital de la educación en el Ecuador. Esta agenda propone la planificación, ejecución y evaluación de estrategias y acciones destinadas al desarrollo del Aprendizaje Digital y a la consolidación de la Ciudadanía Digital en todos los miembros de la comunidad educativa (estudiantes, docentes, personal educativo, directivos y familias). A través de este documento, el ministerio traza el camino para generar las condiciones necesarias para el establecimiento de una comunidad que aprende acerca y mediante herramientas tecnológicas en entornos digitales.

El objetivo de la Agenda Educativa Digital es:

- Diseñar planes, políticas y programas educativos enfocados en el Aprendizaje Digital, la Alfabetización Digital y la Ciudadanía Digital en el Sistema Nacional de Educación.

Sus objetivos específicos son:

⁶¹Estrategia “Ecuador Digital”: <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2019/05/PPT-Estrategia-Ecuador-Digital.pdf>



- Impulsar el Aprendizaje Digital a través de procesos de formación, creación y gestión de recursos digitales y acceso oportuno a entornos digitales en la comunidad educativa;
- Promover la Alfabetización Digital y la construcción de una Ciudadanía Digital universal, incluyente e intercultural en la comunidad educativa.

Para conseguir estos objetivos se establecen dos ejes: a. Aprendizaje Digital y Alfabetización Digital y b. Ciudadanía Digital, que engloban estrategias y acciones que permitirán alcanzar la transformación digital educativa del país. La Agenda Educativa Digital 2021 – 2025 se presentará oficialmente en diciembre del 2021.

En este marco se ejecuta la campaña El Mundo Virtual de Eugenia, la cual está enfocada en promover el uso adecuado de las tecnologías digitales y la prevención de riesgos durante la navegación en internet. Esta iniciativa institucional plantea una metodología que permite, conocer, identificar y prevenir los riesgos, generando espacios de reflexión, participación y consulta para todos los miembros de la comunidad educativa. El Ministerio de Educación es parte del Pacto por un Internet Seguro, a través del cual se han unido varios esfuerzos interinstitucionales para construir e implementar la política pública de uso seguro de internet para niñas, niños y adolescentes.

Marco Normativo/Marco Reglamentario

En materia de protección integral de derechos de niñas, niños y adolescentes el **Ecuador** tiene su Constitución⁶², aprobada en 2008 refuerza el rol del Estado, la sociedad y la familia como garantes del ejercicio de derechos y con la obligación de brindar protección, apoyo y promover el desarrollo integral de niñas, niños y adolescentes, enmarcado en el principio de interés superior del niño, además, recibirán atención prioritaria y especializada en los ámbitos públicos y privados. Así mismo en su artículo 340 determina que la protección integral de sus habitantes se realizará a través del **sistema nacional de inclusión y equidad social**, que es el conjunto articulado y coordinado de sistemas, instituciones, políticas, normas, programas y servicios que aseguran el ejercicio, garantía y exigibilidad de los derechos reconocidos en la Constitución y el cumplimiento de los objetivos del régimen de desarrollo y específicamente para niñas, niños y adolescentes ha definido el Sistema Nacional Descentralizado de Protección Integral de la Niñez y Adolescencia (SNDPINA), mismo que está vigente desde el año 2003 a través de su ley especializada el Código de Niñez y Adolescencia⁶³ y se constitucionaliza en el 2008. Son parte de este sistema organismos públicos y privados encargados de la protección integral de este grupo poblacional en los ámbitos de prevención, atención, protección y restitución.

⁶² https://www.asambleanacional.gob.ec/sites/default/files/documents/old/constitucion_de_bolsillo.pdf

⁶³ <https://www.registrocivil.gob.ec/wp-content/uploads/downloads/2014/01/este-es-06-CÓDIGO-DE-LA-NIÑEZ-Y-ADOLESCENCIA-Leyes-conexas.pdf>



En ese contexto a nivel territorial el Código Orgánico de Organización Territorial Autonomía descentralización COOTAD⁶⁴ determina a todos los 221 gobiernos autónomos descentralizados municipales y metropolitano el implementar el sistema de protección integral de derechos, que incluye la conformación y financiamiento de organismos especializados en protección como los consejos cantonales de protección de derechos, juntas cantonales y redes de protección de derechos (artículos 54;j y 84;j y 598).

Al momento existen **215 Consejos Cantonales de Protección de Derechos** conformados, cuya competencia es de formulación, transversalización, seguimiento, evaluación y observancia de las políticas públicas de protección integral a niñas, niños y adolescentes en su cantón. Los CCPD coordinarán con las entidades, así como con las redes interinstitucionales especializadas en protección de derechos.

En casi todos los cantones se han conformado espacios que se denominan redes o mesas de articulación y coordinación interinstitucional en casi todos los casos liderados por los Consejos Cantonales de protección de derechos, en donde se tratan temas de interés del cantón ya sean políticas públicas o análisis de casos de amenaza y/o vulneración de derechos.

Las Juntas Cantonales de protección de derechos son los organismos especializados que entre otras competencias tienen la de conocer, de oficio o a petición de parte, los casos de amenaza o violación de los derechos individuales de niños, niñas y adolescentes dentro de la jurisdicción del respectivo cantón; y disponer las medidas administrativas de protección que sean necesarias para proteger el derecho amenazado o restituir el derecho violado; b) Interponer las acciones necesarias ante los órganos judiciales competentes en los casos de incumplimiento de sus decisiones; d) Requerir de los funcionarios públicos de la administración central y seccional, la información y documentos que requieran para el cumplimiento de sus funciones; c) Denunciar ante las autoridades competentes la comisión de infracciones administrativas y penales en contra de niños, niñas y adolescentes. Al momento existen **187 JCPD conformadas en todo el país**.

La Política pública por una internet segura para niños, niñas y adolescentes, mediante un acceso y uso sano, seguro y constructivo de la internet, se enfoca garantizar el interés superior del niño, niña y adolescente consagrado en la Constitución de la República del Ecuador, así como también, en los instrumentos normativos nacionales e internacionales.

La intención de esta política pública es de potenciar las oportunidades y habilidades que ofrecen las tecnologías digitales en la vida de las niñas, niños y adolescentes, y así, promover

⁶⁴ <https://www.gob.ec/regulaciones/codigo-organico-organizacion-territorialcootad>



el aprovechamiento de los usos y beneficios de las TIC en un marco de derechos (digitales), dignidad e integridad física, psicológica, emocional y sexual.

La política definida por el Ministerio de Educación se enfoca en la promoción de derechos de niñas, niños y adolescentes en el uso seguro de Internet desde las familias y la institución educativa. Las líneas de acción definidas a través de la Agenda Educativa Digital y la Campaña El Mundo Virtual de Eugenia se enfocan en docentes, estudiantes, familias, cuidadores o adultos referentes, con el propósito de fortalecer las capacidades y competencias de la comunidad educativa desde un enfoque de garantía y protección de derechos.

El trabajo institucional se sustenta en la necesidad de que las y los adultos responsables y garantes de derechos de niñas, niños y adolescentes (docentes tutores, directivos, madres, padres, cuidadoras, adultos referentes) conozcan y promuevan derechos, acompañen activamente el acceso y uso seguro de Internet, informen a sus hijas e hijos sobre los riesgos que existen en la web para prevenir situaciones de violencia, discriminación y escenarios de vulneración de derechos.

El trabajo ministerial propone realizar con madres, padres, cuidadoras, adultos responsables, un proceso de animación socioeducativa que contempla: (1) actividades de socialización de la temática al interior de la comunidad educativa y de las familias, mediante una campaña permanente (2) actividades de talleres o webinars para madres, padres, cuidadoras, adultos responsables que tengan la oportunidad de conocer los derechos de niñas, niños y adolescentes en el uso seguro de Internet, los riesgos que existen en la web, y adquirir herramientas o pautas de acompañamiento seguro a hijas e hijos; y (3) gestión de recursos educativos para el abordaje de la temática y para su aprovechamiento dentro y fuera de clase.

En el marco del proceso de construcción del Informe de primer debate de la reforma al Código Orgánico de Niñez y Adolescencia, se propuso articulado sobre los diferentes tipos de violencia en las nuevas tecnologías de la información y la explotación sexual en línea. Además, como parte del Colectivo público-privado contra la explotación sexual comercial, liderado por el CNII se envió observaciones para el proceso de creación del Informe de Segundo debate sobre los tipos de violencia incluida la violencia en los medios digitales.

En materia de niñez y adolescencia, la Convención sobre los Derechos del Niño es un instrumento jurídico internacional orientado a proteger específicamente los derechos de la niñez y la adolescencia. Ecuador, como Estado miembro, se convirtió en garante de las condiciones necesarias para que los niños y sus familias puedan gozar y reivindicar el cumplimiento de sus derechos. El 20 de noviembre de 1989 Ecuador firmó la Convención sobre los Derechos del Niño (CDN) y fue el primer país en América Latina en suscribirla en



19901, lo que significó una ruptura con la anterior forma de ver y actuar con respecto a la niñez y la adolescencia, asumiendo el rol de garante en la promoción y protección de los derechos de niñas, niños y adolescentes de acuerdo a su autonomía progresiva acorde a su edad y competencias. Esta reconoce a los niños, niñas y adolescentes como sujetos de derecho y al mismo tiempo, reconoce a las familias como garantes y sujetos de derechos que requieren protección y asistencia de las instituciones del Estado para poder asumir plenamente sus responsabilidades de cuidado y protección (CEPAL, 2018).

La ratificación de la Convención por parte del Ecuador significa que el país ha asumido, tanto el postulado de que todos los niños, niñas y adolescentes tienen derechos y deben ser capaces de exigir su cumplimiento, así como la obligación de respetar y proteger esos derechos y generar las condiciones para que la niñez y adolescencia puedan exigir su cumplimiento (CEPAL, 2018).

Esto implicó que los niños, niñas y adolescentes dejaran de ser vistos como “objetos de necesidades” u “objeto de protección”, para reconocerlos como “sujetos de derechos”, dando paso a la Doctrina de Protección Integral, intentando dejar atrás la Doctrina de Situación Irregular. Además, significó avanzar en la normativa específica para la garantía y protección de sus derechos; el Código de la Niñez y Adolescencia fue publicado oficialmente el 03 de enero del 2003, con la convicción de que permitió la creación de un sistema especializado de protección como: la Ley Orgánica de Educación Intercultural, Ley Orgánica de Salud, Ley Orgánica de los Consejos Nacionales para la Igualdad, Reformas al Código de la Niñez y Adolescencia, Código Orgánico de la Función Judicial, Código Orgánico Integral Penal, entre otras, normativa que incorpora los principios de protección integral y la implementación de servicios orientados al aseguramiento del ejercicio de sus derechos.

La Constitución, aprobada en 2008 refuerza el rol del Estado, la sociedad y la familia como garantes del ejercicio de derechos y con la obligación de brindar protección, apoyo y promover el desarrollo integral de niñas, niños y adolescentes, enmarcado en el principio de interés superior del niño, además, recibirán atención prioritaria y especializada en los ámbitos públicos y privados.

El Ministerio de Educación, al ser el órgano rector de la educación nacional, maneja los protocolos y rutas de actuación frente a situaciones de violencia detectadas o cometidas en el Sistema Educativo, incluyendo las cometidas en entornos virtuales.

Esta normativa define las líneas de acción institucional para la prevención y sanción (administrativa). Además, existe una acción conjunta entre varias instituciones del estado para su sanción legal considerando los cuerpos normativos anteriormente mencionados.



Existen mecanismos legales estipulados en la legislación ecuatoriana que tienen un valor resumido a la seguridad en línea, además cuenta con políticas nacionales digitales, como la ley orgánica de telecomunicaciones y la ley orgánica de protección de datos personales.

La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), mediante Resolución No. ARCOTEL-2018-0716 de 16 de agosto de 2018, expidió la Norma técnica que regula las condiciones generales de los contratos de adhesión, del contrato negociado con clientes y del empadronamiento de abonados y clientes, en este instrumento entre otros aspectos, se establecen en el artículo 4, las condiciones generales que deben cumplir los prestadores de servicios, puntualmente en el número 26, se indica:

“26) Protección de los niños, niñas, y adolescentes e Inclusión de herramientas para control parental⁶⁵.- Los prestadores de servicios de telecomunicaciones y servicios de radiodifusión por suscripción, se obligan a:

- a. Protección a niñas, niños y adolescentes;
- b. Los acuerdos que se suscriban entre los prestadores de servicios de telecomunicaciones, servicios de radiodifusión por suscripción y los proveedores de contenido, deberán contener cláusulas específicas donde se establezcan las condiciones relativas a control de acceso a la información;
- c. Acuerdos con proveedores de contenidos y difusión;
- d. Los acuerdos que se suscriban entre los prestadores de servicios de telecomunicaciones, radiodifusión por suscripción y los proveedores de contenido, deberán contener cláusulas específicas donde se establezca que la publicidad relativa a la provisión de contenidos deberá incluir en forma clara el precio o tarifas de provisión de dichos servicios, los mecanismos de contratación y de suscripción o cancelación de la contratación realizada;
- e. Acceso y Seguridad;
- f. Los prestadores de servicios de telecomunicaciones y de radiodifusión por suscripción, podrán ofrecer a sus abonados y clientes que lo soliciten, el servicio de control y bloqueo de contenidos que atenten contra la ley, o a la protección de niños, niñas y adolescentes, informando claramente al usuario cual es el alcance, tarifa o precio y modo de funcionamiento de estos”.

Aunque la Convención sobre los Derechos del Niño fue aprobada en 1989, antes de que el Internet se convirtiera en una herramienta que usamos todos los días, la CDN sigue siendo

⁶⁵ Disponible en: <https://www.hallo.ec/uploads/GUIA-CONTROL-PARENTAL--ARCOTEL.pdf>



una herramienta pertinente cuando se trata de promover y proteger los derechos de niñas, niños y adolescentes en sus actividades online.

Con el rápido desarrollo de las TIC's (Tecnologías de la Información y Comunicación) en la última década, estos derechos están más vigentes que nunca. Ecuador ha ratificado los siguientes protocolos facultativos de la Convención de los derechos de la niñez:

- Ratificación del 1er Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la participación de niños en los conflictos armados: 7 de junio de 2004;
- Ratificación del 2do Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía: 30 de enero de 2004;
- Ratificación del 3er Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo al procedimiento de comunicaciones: 19 de septiembre de 2018. Esta herramienta tiene como objetivo establecer un procedimiento internacional de denuncia de violaciones de los derechos de niñas, niños y adolescentes ante el Comité de los Derechos del Niño de Naciones Unidas.

Por otra parte, el Comité sobre los Derechos del Niño (CRC-Ecuador 2017) realizó algunas observaciones y recomendaciones al país referente la situación de los derechos de la niñez y adolescencia:

- El Comité recuerda al Estado parte que todos los derechos consagrados en la Convención son indivisibles e interdependientes, y hace hincapié en la importancia de todas las recomendaciones que figuran en las presentes observaciones finales. Asimismo, desea señalar a la atención del Estado parte las recomendaciones relativas a las siguientes esferas, respecto de las cuales deben adoptarse medidas urgentes: coordinación (párr. 9); violencia, malos tratos y descuido (párr. 25); violencia de género (párr. 27); salud de los adolescentes (párr. 35); niños pertenecientes a minorías étnicas y/o grupos indígenas (párr. 41); y justicia juvenil (párr. 44).

Sobre el acceso a la información pertinente, el Comité recomienda que el Estado:

- a. Tome medidas para mejorar el acceso de los niños a la información pertinente, en particular de los que viven en zonas lejanas o rurales, los que pertenecen a pueblos y nacionalidades indígenas, los afroecuatorianos y los refugiados, en función de su edad, madurez y contexto cultural;
- b. Adopte medidas para proteger a los niños frente a la información y los productos nocivos y los riesgos en línea, y a la denigración y la discriminación en su contra;
- c. Instruya a los comunicadores sociales y los periodistas sobre los derechos del niño;



d. Amplíe el acceso a Internet y a la información de los niños que viven en zonas rurales.

Estas definiciones nos obligan a plantear programas, planes y proyectos que apunten a la alfabetización digital y a la formación de una ciudadanía digital que promuevan un uso seguro de las tecnologías. A esta necesidad responde la Agenda Educativa Digital, la cual incluye dentro de sus líneas de acción la definición de orientaciones sobre cómo proteger y garantizar el uso seguro de Internet en un contexto de uso de medios tecnológicos para la continuidad y fortalecimiento del proceso de enseñanza – aprendizaje.

El Código de la Niñez y Adolescencia tiene como fin proteger y garantizar el goce y ejercicio de los derechos, deberes y responsabilidades de las niñas, niños y adolescentes del Ecuador, dentro de un marco de libertad, dignidad y equidad; a su vez dentro de la ley orgánica de protección de datos se establece la protección de niños.

Notificaciones-contenido ilícito/Notificaciones-preocupaciones de los usuarios

No se tiene información de la que se advierta la posibilidad de llevar a cabo dichas notificaciones.

Actores y partes interesadas

La política pública es un trabajo mancomunado entre varios ministerios y otros actores del sector público, se han identificado a las siguientes entidades como responsables de su implementación:

- Ministerio de Telecomunicaciones y de la Sociedad de la Información;
- Dirección Nacional de Registros Públicos;
- Agencia de Regulación y Control de las Telecomunicaciones;
- Consejo de la Judicatura;
- Ministerio de Gobierno (Policía Nacional);
- Fiscalía General del Estado;
- Ministerio de Educación (en el contexto educativo);
- Grupos especializados en ciberseguridad de las fuerzas públicas.

La institución que tiene la autoridad en protección de datos personales es la Dirección Nacional de Registros Públicos (DINARDAP).

Alianzas Nacionales e Internacionales (sector público y sector privado)

El Ministerio de Educación ha brindado su apoyo técnico para la gestión de guías, normativas y herramientas digitales desarrolladas por instituciones públicas y privadas. Por ejemplo, el



desarrollo del portal de web de Internet Segura en el link: <https://internetsegura.gob.ec/>, mismo que busca fortalecer un vínculo entre las y los ciudadanos en torno al uso seguro de internet, precautelando siempre la integridad de niñas, niños y adolescentes del país.

Como se mencionó anteriormente, el CNII, en colaboración con otras instituciones, ha sumado esfuerzos para desarrollar, presentar e implementar la “Política Pública por el Uso Seguro de Internet para Niñas, Niños y Adolescentes”.

El Ministerio de Educación trabaja con varias instituciones para la gestión de este proceso: OEA -IIN, OEI, UNICEF, UNESCO, BID, Universidades nacionales (ESPE, EPN, UDLA, UNAE), Fundación ADELA (Plan Ceibal – Uruguay), Ministerio de Telecomunicaciones y Sociedad de la Información, Consejo Nacional para la Igualdad Intergeneracional – CNII, Profuturo – Fundación Telefónica, ChildFun, Plan Internacional, entre otras.

Investigación

Hay varias instituciones que trabajan con el CNII y en prevención de riesgos como: CHILDFUND, Profuturo, Plan Internacional, UNESCO, OEI, DirecTV, Fundación Telefónica Movistar, Plan Internacional y Universidades públicas y privadas, entre otras.

Actualmente, el CNII, en colaboración con otras instituciones, ha sumado esfuerzos para desarrollar, presentar e implementar la “Política Pública por el Uso Seguro de Internet para Niñas, Niños y Adolescentes”.

El Ministerio de Educación trabaja, de manera permanente, con el proyecto “El Mundo Virtual de Eugenia”, el cual está enfocado en conocer, identificar y prevenir riesgos. Sin embargo, la Agenda Educativa Digital define el desarrollo de competencias digitales para todos los miembros de la comunidad educativa a partir de procesos de formación y empoderamiento.

Actualmente no se cuenta con indicadores de protección de la infancia en línea; sin embargo, como parte del seguimiento a la implementación de la política pública se tiene planificación la construcción de estos.

En febrero de 2018, el Informe de Impacto DQ se publicó en asociación con el Foro Económico Mundial. Ese informe evaluó la seguridad en línea y la ciudadanía digital entre 38 mil niños de 8 a 12 años en 29 países del mundo.

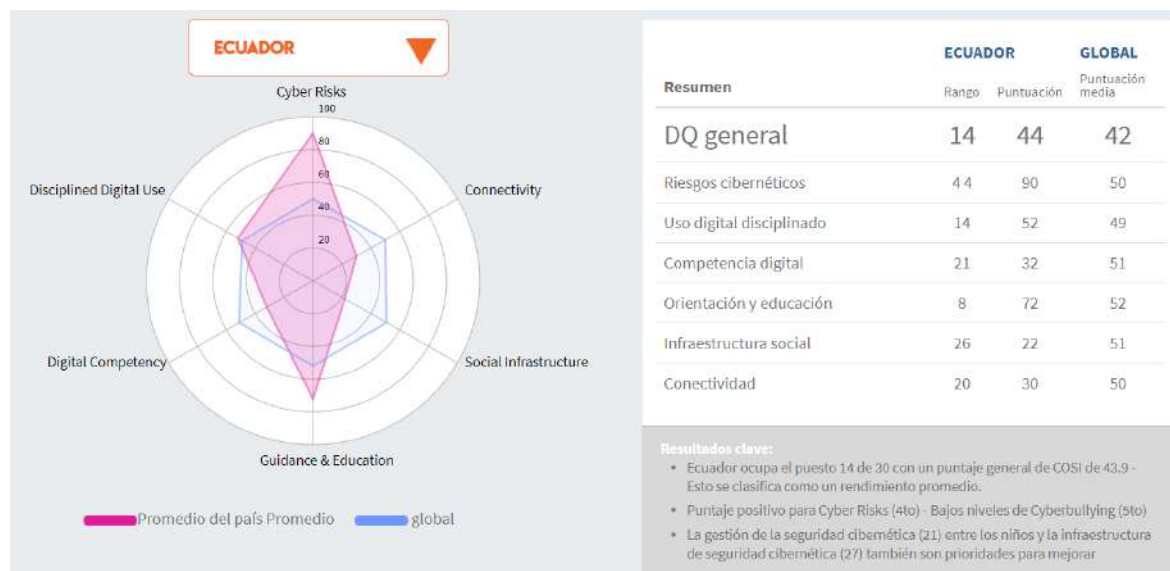
En ese informe se establece que el 56% de niñas, niños y adolescentes estaban expuestos a al menos un riesgo cibernético (incluidos riesgos como el acoso cibernético, el trastorno del juego, las reuniones fuera de línea con extraños y agresiones sexuales en línea).

En los dos años siguientes, febrero de 2020, se amplió la cobertura e indicadores a seis pilares de apoyo para la seguridad en línea. EL Ranking COSI 2020 compara los resultados en 30 países e incluye datos de más de 145 mil niños, así como de otras fuentes externas como la



Unión Internacional de Telecomunicaciones (UIT), el Sistema Global para la Asociación de Comunicaciones Móviles (GSMA), la Unidad de Inteligencia Economista y otras instituciones internacionales.

Según el Ranking COSI, Ecuador ocupa el puesto 14 (de un total de 30 países) con una puntuación total de 43.9.



Según este mismo índice, Ecuador posee un “bajo riesgo” de cyberbullying. Mientras que las prioridades a mejorar corresponden a la gestión de la seguridad cibernética y su infraestructura.

Sin embargo, este panorama corresponde a la gestión de indicadores a partir de una muestra que no obedece a la realidad nacional, por lo que sus resultados se toman como una referencia. El manejo de indicadores es vital para la gestión de política pública. Por lo tanto, es necesaria la definición de estándares que den cuenta de la realidad nacional con relación al acceso y manejo del internet seguro.

El Ministerio de Educación ha planificado el levantamiento de una línea base sobre el desarrollo de competencias digitales, la cual puede servir como un primer acercamiento para conocer la realidad nacional. Este levantamiento dependerá de la disponibilidad técnica y presupuestaria.

Educación en Materia de alfabetización y competencias digitales

Ecuador conjuga sus esfuerzos desde diversas aristas para fomentar una sociedad que genere y administre conocimiento. El Código de Economía Social de los Conocimientos, la Creatividad y la Innovación brinda un marco legal, pero es la comunidad la encargada de darle vida a ese objetivo. Consolidar una sociedad que genere y administre conocimiento exige una educación que vaya en el mismo rumbo. El Ministerio de Educación aporta en este sentido no



solo desde lo curricular y metodológico sino también desde el fomento a las iniciativas, la innovación. La educación y las tecnologías de la información y comunicación son un gran desafío pedagógico en la sociedad del conocimiento actual.

El enfoque de la Agenda Educativa Digital⁶⁶ es una estrategia del Ministerio de Educación que establece los lineamientos para la inclusión de las Tecnologías de la Información y Comunicación, para producir cambios que apunten a la transformación mediante el paso de las TIC a las TAC como un proceso de innovación pedagógica.

Recursos educativos

El CNII, junto con instituciones público y privadas, han desarrollado el portal web de Internet Segura⁶⁷, mismo que busca fortalecer un vínculo entre padres, docentes y el Estado brindando conocimientos y herramientas que permitan usar la Internet de una manera segura, precautelando siempre la integridad de niñas, niños y adolescentes del país.

Protección de la Infancia

El CNII, en el marco de las atribuciones contempladas en la Constitución de la República del Ecuador y en la Ley Orgánica de los Consejos Nacionales para la Igualdad, dentro del ciclo de la política pública, nos encontramos en la prioridad de realizar el seguimiento a la Implementación de la “Política Pública por el Uso Seguro de Internet para Niñas, Niños y Adolescentes”.

El Ministerio de Educación prioriza las siguientes acciones:

- Desarrollo de competencias digitales en todos los miembros de la comunidad educativa;
- Protección de la información relacionadas a docentes, estudiantes y familias;
- Conocer, identificar y prevenir los riesgos relacionados al uso de dispositivos tecnológicos y a la navegación en internet;
- Integración de las tecnologías digitales para el fortalecimiento del proceso de formación;
- Proponer políticas de seguridad en línea más rígidas que se ambienten a la realidad nacional.

El CNII, en el marco de las atribuciones contempladas en la Constitución de la República del Ecuador y en la Ley Orgánica de los Consejos Nacionales para la Igualdad, dentro del ciclo de la política pública, encuentra en la prioridad de realizar el seguimiento a la Implementación de la “Política Pública por el Uso Seguro de Internet para Niñas, Niños y Adolescentes”.

El ministerio implementa las siguientes acciones:

⁶⁶Agenda educativa digital <https://educacion.gob.ec/wp-content/uploads/downloads/2017/11/Agenda-Educativa-Digital.pdf>

⁶⁷ Portal web de Internet Segura: <https://internetsegura.gob.ec/>




- Campaña permanente “El Mundo Virtual de Eugenia” para conocer, identificar y prevenir riesgos. En este contexto se ha desarrollado un micrositio de consulta con más de 140 recursos educativos (videos, podcast, guías para docentes, entre otros; enlace: <https://recursos2.educacion.gob.ec/euinicio/>);
- Gestión de webinars y talleres nacionales para docentes, estudiantes y familias;
- Definición y socialización de normativa para protección de datos;
- Procesos de formación para docentes de IE de sostenimiento fiscal enfocadas en el desarrollo de competencias digitales;
- Cooperación con otras instituciones (públicas y privadas) para desarrollo de planes y programas complementarios.

ChildFund junto a su socio local FENPIDEC apoyó el proceso de construcción y aprobación de la ordenanza para un internet seguro que norma especialmente los servicios de cybercafés y define espacios de prevención de violencia en internet. El plan de trabajo a nivel local incluye la réplica de esta iniciativa en los cantones de Pedro Vicente Maldonado y Puerto Quito. Además, en Pedro Vicente Maldonado se trabaja de forma conjunta con el CNII para implementar la metodología FOFIOUSI.

El Ministerio de Educación maneja el sistema REDEVI para la identificación, prevención y seguimiento de casos de violencia identificados a través del sistema educativo. Actualmente se trabaja en su evaluación técnica para mejorar su alcance y funcionalidad.

En el ámbito de promoción de derechos y prevención de vulneración de derechos en contra de niñas, niños y adolescentes específicamente el CNII desarrolló algunas campañas educacionales, dirigidas a la sociedad en general, en el tema:

Tema	Contenidos y acceso
Niñez Protegida con Internet Segura	https://www.igualdad.gob.ec/ninez-prottegida-con-internet-segura/ ¿Sabes cuáles son los delitos más comunes contra la integridad sexual y reproductiva de niñas, niños y adolescentes y cómo les pueden afectar en su vida? Aquí te contamos más sobre ello para que puedas estar informado y prevenir que sean víctimas de ello.
#NiñezProtegida	https://www.igualdad.gob.ec/ninezprottegida/

	<p>Niñez Protegida Lo que más preocupa a gobiernos, sociedades y familias es el crecimiento sistemático de la explotación sexual contra niñas, niños y adolescentes.</p>
<p>Uso seguro de la internet para niñez y adolescencia</p>	<p>https://www.igualdad.gob.ec/uso-seguro-de-la-internet-para-ninez-y-adolescencia/</p> 

También se elaboró la Guía de control parental realizada por ARCOTEL, de manera conjunta con el Consejo Nacional para la Igualdad Intergeneracional:

https://www.hallo.ec/uploads/GUIA-CONTROL-PARENTAL-_-ARCOTEL.pdf.

La Guía conceptualiza al control parental como una herramienta que busca monitorear, restringir o bloquear el acceso de niños, niñas y adolescentes a sitios web, cuyo contenido sea inapropiado o ponga en riesgo su integridad. También permite establecer un tiempo límite para el uso de dispositivos como computadoras, TV, smartphones, tablets, y cualquier otro equipo que tenga acceso a una red WiFi.

Sensibilización Nacional

La emergencia sanitaria causada por la Covid-19 provocó que la digitalización sea mucho más acelerada, y con ello el incremento de riesgos en su uso, nuevas formas de amenazas y vulneración de derechos, sobre todo para los niños, niñas y adolescentes⁶⁸.

En ocasiones, resulta incontrolable la divulgación de los mensajes y el contacto que extraños pueden tener con niños, niñas y adolescentes. Esta falta de “control” en el uso de internet, hace que atraviesen un doble riesgo y exposición al peligro (ciberacoso, grooming, pornografía infantil, sexting y sextorsión, entre otros); y con ello, la consecuente vulneración de sus derechos (vida, integridad, dignidad, libertad); entonces, la corresponsabilidad de los distintos actores de la sociedad, demanda crear estrategias conjuntas para proteger a ese grupo poblacional.

⁶⁸ <https://www.arcotel.gob.ec/por-un-internet-seguro-para-ninos-ninas-y-adolescentes/>



Herramientas, Servicios y Ajustes

Telefónica pone a disposición una plataforma con el objetivo de fomentar un entorno seguro en Internet y concientizar a la Sociedad sobre la importancia de aprender a sacar el máximo provecho de estas herramientas en el día a día, desarrollado el portal web Dialogando⁶⁹.

Dialogando es un espacio para debatir sobre todo lo que ocurre alrededor de la Red y los dispositivos conectados. Desde cómo pueden ayudar a los menores a gestionar su identidad digital, hasta cómo debemos gestionar nuestra privacidad. Sobre cómo relacionamos a través de la tecnología, el uso excesivo que hacemos de Internet.

Medidas de Accesibilidad

El 13 de diciembre de 2006, la Asamblea General de Naciones Unidas (ONU) adoptó la Convención para promover y proteger los derechos y la dignidad de las personas con discapacidad.

Ecuador, como estado Parte, ha ratificado esta Convención y su Protocolo Facultativo a través de la Asamblea Nacional Constituyente en abril del 2008, a partir de su publicación en el Registro Oficial Nro. 329 del 5 de Mayo del 2008. Aunado a lo anterior cuenta con una propuesta de políticas públicas para accesibilidad web⁷⁰.

La Convención se compone de 50 artículos. El Protocolo Facultativo, también se constituye en un instrumento internacional compuesto por 18 artículos. El documento en mención hace referencia en varias ocasiones a los derechos de las personas con discapacidad al acceso a la información y a la comunicación en condiciones de igualdad, con el apoyo de los recursos disponibles cuando fuese necesario. El Artículo 9 (Accesibilidad), establece que los estados parte deben **“Promover el acceso de las personas con discapacidad a los nuevos sistemas y tecnologías de la información y las comunicaciones, incluida Internet”**. El artículo 2 de la presente convención incluye “facilitar a las personas con discapacidad información dirigida al público en general, de manera oportuna y sin costo adicional, en formatos accesibles y con las tecnologías adecuadas a los diferentes tipos de discapacidad”.

La Constitución Ecuatoriana garantiza los derechos humanos sin discriminación alguna. Art 3, todos somos iguales y tenemos los mismos derechos, deberes y obligaciones. Art. 11, El Estado adoptará medidas de acción afirmativa que promuevan la igualdad real en favor de los titulares de derechos que se encuentren en situación de desigualdad. En su Art. 47 y 48, el estado garantizará y adoptará políticas para la inclusión social de personas con discapacidad.

⁶⁹ <https://www.dialogando.com.ec/guia-de-control-parental/>

⁷⁰ <http://redenti.ups.edu.ec/observatorio/resources/pdf/PROPUESTA%20DE%20POLITICAS%20PUBLICAS%20PARA%20ACCESIBILIDAD%20WEBv4.pdf>



La ley orgánica de discapacidades aprobada mediante Registro Oficial No. 796 del 25 de septiembre del 2012 señala en su Art. 4 numeral 8 garantizar la accesibilidad a la información y comunicación incluido los sistemas y las tecnologías de la información y comunicación, facilitando las condiciones necesarias para procurar autonomía en sus vidas. En su Art. 17 señala que El Estado adoptará medidas de acción afirmativa en el diseño y la ejecución de políticas públicas necesarias para garantizar el ejercicio pleno de las personas con discapacidad y que se encontraran en situación de desigualdad. Art. 58 señala garantizar la accesibilidad y utilización de servicios eliminando barreras. En su Art 63. El estado promocionará las ayudas técnicas y tecnológicas garantizando la inclusión y participación de personas con discapacidad. Art 65. Las instituciones públicas y privadas que presten servicios públicos incluirán en sus portales web un enlace de acceso para las personas con discapacidad (CONADIS - Vicepresidencia, 2013).

Línea de ayuda

Sobre el tema de participación de niñas, niños y adolescentes, se han realizado consultas nacionales para definir estrategias y campañas sobre temas como el internet seguro y acciones para prevenir y combatir delitos cometidos en la red, así como se ha promocionado mecanismos de denuncia a través de la línea 1800 335486 y página www.fiscalia.gob.ec, con consejos consultivos ya sea nacional o cantonales. Al momento se ha identificado 1 consejo consultivo nacional de niñas y niños y 1 de adolescentes conformados a nivel nacional sobre la base de los consejos consultivos cantonales.

En el ámbito nacional el Consejo Nacional para la Igualdad Intergeneracional ha conformado 2 consejos consultivos nacionales integrados por niñas, niños y adolescentes. A manera de ejemplo:



Igualmente, se cuenta con la entidad denominada Servicio Integrado de Seguridad ECU 911, quien gestiona en todo el territorio ecuatoriano, la atención de las situaciones de emergencia



de la ciudadanía, reportadas a través del número 911, mediante el despacho de recursos de respuesta especializados pertenecientes a organismos públicos y privados articulados al sistema, con la finalidad de contribuir, de manera permanente, a la consecución y mantenimiento de la seguridad integral ciudadana (<https://www.ecu911.gob.ec/mision-y-vision/>).

En su portal informa que durante el 2021, se han reportado 103.516 emergencias de violencia intrafamiliar (<https://www.ecu911.gob.ec/en-2021-al-9-1-1-se-han-reportado-103-516-emergencias-de-violencia-intrafamiliar/>).

Adhesión al Convenio de Budapest

No se encuentra adherido.

La entidad competente de atender víctimas de abuso en línea es la Fiscalía General del Estado mediante la recepción de denuncias presentadas. Desde el Ministerio de Educación, se trabaja con El Departamento de Consejería Estudiantil (DECE), la instancia responsable de la atención integral de las y los estudiantes. Su propósito es brindar apoyo y acompañamiento psicológico, psicoeducativo, emocional y social, en concordancia con el marco legal vigente.



MÉXICO

Índice de siglas del capítulo

ARCO	Acceso, Rectificación, Cancelación, Oposición
CAS	Centro de Atención a la Sociedad del INAI
CGPU	Coordinación General de Política del Usuario del IFT
CNDH	Comisión Nacional de Derechos Humanos
CPEUM	Constitución Política de los Estados Unidos Mexicanos
DIF	Sistema Nacional para el Desarrollo Integral de las Familias
DOF	Diario Oficial de la Federación
EDN	Estrategia Digital Nacional
ENCS	Estrategia Nacional de Ciberseguridad
GN	Guardia Nacional
IFT	Instituto Federal de Telecomunicaciones
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LGDNNA	Ley General de los Derechos de Niñas, Niños y Adolescentes
LGPDPSSO	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
NNA	Niños, Niñas y Adolescentes
RLFPDPPP	Reglamento Ley Federal de Protección de Datos Personales en Posesión de los Particulares
SEGOB	Secretaría de Gobernación
SEP	Secretaría de Educación Pública
SICT	Secretaría de Infraestructura, Comunicaciones y Transportes
SIPINNA	Sistema Nacional de Protección Integral de niñas, niños y adolescentes
SNT	Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
SSPC	Seguridad Ciudadana de la Ciudad de México



Política Nacional Digital

Estrategia Digital Nacional⁷¹, en materia de tecnologías de la información y comunicaciones, y en la seguridad de la información.

El 8 de mayo de 2014, se publicó en el Diario Oficial de la Federación (DOF) el “Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias”, el cual en su Anexo único presenta el Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información cuyo objeto es:

“Definir los procesos con los que, en las materias de TIC y de seguridad de la información, las Instituciones deberán regular su operación, independientemente de su estructura organizacional y las metodologías de operación con las que cuenten”.

- **Estrategia Nacional de Ciberseguridad (ENCS)⁷²**

El 13 de noviembre de 2017, se publicó en el portal de Internet del Gobierno de México, la Estrategia Nacional de Ciberseguridad (ENCS), el cual es el documento que establece la visión del Estado mexicano en la materia, a partir del reconocimiento de:

- a. La importancia de las tecnologías de la información y comunicación (TIC) como un factor de desarrollo político, social y económico de México; en el entendido de que cada vez más individuos están conectados a Internet y que, tanto organizaciones privadas como públicas desarrollan sus actividades en el ciberespacio;
- b. Los riesgos asociados al uso de las tecnologías y el creciente número de ciberdelitos;
- c. La necesidad de una cultura general de ciberseguridad.

La ENCS tiene por objetivo el fortalecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano; define cinco objetivos y ocho ejes transversales, plasma los principios rectores, identifica a los diferentes actores involucrados y da claridad sobre la articulación de esfuerzos entre individuos, sociedad civil, organizaciones privadas y públicas

⁷¹ Publicada en el Diario Oficial de la Federación el 08 de mayo de 2014, disponible en el vínculo electrónico siguiente: http://www.dof.gob.mx/nota_detalle.php?codigo=5343881&fecha=08/05/2014

⁷² Disponible para su consulta en: <https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad>



en materia de ciberseguridad; además señala el modelo de gobernanza para la implementación, seguimiento y evaluación de la Estrategia.

- **Estrategia Digital Nacional 2021-2024**⁷³

La Estrategia Digital Nacional 2021-2024, publicada en agosto de 2021, es un plan de acción del Ejecutivo Federal (coordinado por Presidencia), enfocado en aprovechar el potencial de las tecnologías de la información y comunicación (TIC), incluidos los servicios de banda ancha e Internet, como elemento catalizador del desarrollo del país, mediante su incorporación a la vida cotidiana de las personas, y a la Administración Pública Federal, mediante el uso de la informática y el desarrollo del gobierno digital.

- Hoja de Ruta 2021-2025 del Instituto Federal de Telecomunicaciones⁷⁴. Este documento establece el marco estratégico que permite planificar y focalizar las acciones del Instituto Federal de Telecomunicaciones (IFT) en un horizonte temporal de cinco años.
- Programa Anual de Trabajo⁷⁵. En este documento el IFT emite de manera anual un instrumento a través del cual el IFT establece su agenda de trabajo, se precisan los objetivos, estrategias y prioridades regulatorias e institucionales para el beneficio de los usuarios y audiencias de los sectores de las Telecomunicaciones y la Radiodifusión.

El 06 de septiembre del presente año, se publicó en el DOF la EDN⁷⁶ 2021-2025, misma que aborda distintos objetivos generales y específicos, y líneas de acción en dos ejes de acción: la Política Digital en la Administración Pública Federal (APF) y en la Política Social Digital.

En cuanto a los objetivos generales y específicos, por lo que respecta al primer eje de acción, su objetivo general se centra en transformar la APF mediante el uso y aprovechamiento de las Tecnologías de la Información y de la Comunicación (TIC) para mejorar y transparentar los servicios gubernamentales que se otorgan a la ciudadanía. Por lo que respecta a sus objetivos específicos, estos son; mejorar y armonizar el marco normativo de la política digital de la APF a través de una articulación integral y simplificada de las directrices tecnológicas para el país, que permitan lograr eficiencia técnica y económica; estandarizar las compras de TIC a través de acciones transparentes, austeras y efectivas que generen ahorros y maximicen el ejercicio responsable de los recursos públicos; promover la autonomía e independencia tecnológicas para establecer la rectoría del Estado en la definición de sus TIC; obtener el máximo aprovechamiento

⁷³ Disponible para su consulta en: https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021

⁷⁴ Disponible para su consulta en: <http://www.ift.org.mx/conocenos/hoja-de-ruta-2021-2025>

⁷⁵ Disponible para su consulta en: <http://www.ift.org.mx/conocenos/programa-anual-de-trabajo>

⁷⁶ Publicada el 06 de septiembre de 2021 en el Diario Oficial de la Federación, disponible en el vínculo electrónico siguiente: https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021.



de aplicativos de cómputo e infraestructura mediante el intercambio de información y la colaboración tecnológica; promover una cultura de seguridad de la información que genere certeza y confianza a las personas usuarias de los servicios tecnológicos institucionales y gubernamentales y promover la continuidad y mejora de proyectos y programas a partir de la integración de información estructurada disponible en la Institución.

Por lo que refiere al segundo eje de acción, su objetivo general es el de incrementar la cobertura de Internet a todo el país para combatir la marginación y comunicar las zonas más pobres y alejadas, facilitando con ello su integración a las actividades productivas.

Y en cuanto a sus objetivos específicos se encuentran: impulsar la integración e iluminación de la fibra óptica en posesión de las instancias públicas para el transporte de señales y la reducción de la brecha digital en el país; promover el despliegue de Internet a todas las zonas sin cobertura, para lograr la cobertura universal de Internet a la población; mejorar la calidad de los programas sociales mediante soluciones tecnológicas que faciliten y acompañen las acciones encaminadas al bienestar de la población.

Marco Normativo/Marco Reglamentario

A nivel nacional se tiene la siguiente legislación:

De acuerdo con lo señalado en el artículo 4, párrafo noveno, de la Constitución Política de los Estados Unidos Mexicanos CPEUM⁷⁷ se señala que "en todas las decisiones y actuaciones del Estado se velará y cumplirá con el principio del interés superior de la niñez, garantizando de manera plena sus derechos".

En la misma disposición constitucional se establece que los niños y las niñas tienen derecho a la satisfacción de sus necesidades de salud, educación y sano esparcimiento para su desarrollo integral, por lo que este principio debe guiar el diseño, ejecución, seguimiento y evaluación de las políticas públicas dirigidas a la niñez.

El 04 de diciembre de 2014, se publicó en el Diario Oficial de la Federación la Ley General de los Derechos de Niñas, Niños y Adolescentes (LGDNNA)⁷⁸, la cual tiene como objeto principal el

⁷⁷ Publicada en el Diario Oficial, Órgano del Gobierno Provisional de la República Mexicana, el 05 de febrero de 1917, disponible en el vínculo: https://www.dof.gob.mx/index_113.php?year=1917&month=02&day=05, cuyo texto puede obtenerse del vínculo siguiente: http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum/CPEUM_orig_05feb1917.pdf, basado en el contenido de la información que se desprende de la imagen original disponible en el enlace: http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum/CPEUM_orig_05feb1917_ima.pdf; última reforma publicada en el Diario Oficial de la Federación el 28 de mayo de 2021, disponible en el siguiente vínculo electrónico: http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_251_28may21.pdf; texto consolidado por la Cámara de Diputados del H. Congreso de la Unión en formato de documento portable, denominado como pdf por sus siglas en inglés, incorporando las diversas reformas de dicho ordenamiento jurídico en el sitio siguiente: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_280521.pdf.

⁷⁸ Publicada en el Diario Oficial de la Federación el 04 de diciembre de 2014, disponible para su consulta en:

https://www.dof.gob.mx/nota_detalle.php?codigo=5374143&fecha=04/12/2014, última reforma el 11 de enero de 2021, texto disponible por



reconocer a las niñas, niños y adolescentes como titulares de derechos, pero también el reconocerles la capacidad de goce de los mismos.

A través de dicha Ley, se busca poder garantizar el pleno ejercicio, respeto, protección y promoción de los derechos humanos que le asisten a las niñas, niños y adolescentes, los cuales se encuentran reconocidos tanto como en la CPEUM, así como en los tratados internacionales de los cuales México forma parte, como en el caso particular lo es la Convención sobre los Derechos del Niño⁷⁹ (Convención).

La citada Convención reconoce expresamente el papel de los padres y cuidadores, incluidos los familiares, tutores y otras personas con responsabilidad legal, en la protección y promoción del interés superior de la niñez. También reconoce el derecho de las niñas, niños y adolescentes a la privacidad, el acceso a la información, la asociación con otros y el juego para apoyar su desarrollo, así como su derecho a tener voz en los asuntos que lo afectan.

En este mismo sentido, es de resaltar que la LGDNNA, reconoce en su artículo 1, fracción IV, que dentro de su objeto se encuentra establecer los principios rectores y criterios que orienten la política nacional en materia de derechos de niñas, niños y adolescentes, así como las facultades, competencias, concurrencia y bases de coordinación entre la Federación y las entidades federativas, los municipios y las demarcaciones territoriales de la Ciudad de México; y la actuación de los Poderes Legislativo y Judicial, y los organismos constitucionales autónomos.

En consonancia con lo anterior, en el artículo 114 de la LGDNNA se prevé que las autoridades federales, de las entidades federativas, municipales, de las demarcaciones territoriales de la Ciudad de México, y de los organismos constitucionales autónomos, en el ámbito de su competencia, deberán establecer y garantizar el cumplimiento de la política nacional en materia de derechos de niñas, niños y adolescentes.

Por otro lado, la mencionada Ley, establece que las autoridades tienen obligación de realizar acciones y tomar medidas para garantizar un enfoque integral, transversal y con perspectiva de derechos humanos de los menores de edad. Para ello, tienen que considerar los aspectos culturales, éticos, afectivos, educativos y de salud de las niñas, niños y adolescentes en todo aquello de su incumbencia.

Asimismo, la LGDNNA establece en su artículo 13, entre otros, los derechos de las niñas, niños y adolescentes, a la intimidad, libertad de expresión y de acceso a la información, asociación y

parte de la Cámara de Diputados del H. Congreso de la Unión disponible para su consulta en:

http://www.diputados.gob.mx/LeyesBiblio/pdf/LGDNNA_110121.pdf.

⁷⁹ Publicado en junio de 2006, disponible para su consulta en: <https://www.un.org/es/events/childrenday/pdf/derechos.pdf>



reunión, salud, educación, esparcimiento, y acceso a las tecnologías de la información y comunicación; en su fracción XX⁸⁰, establece el derecho al acceso de las tecnologías de la información y comunicación, incluidas la banda ancha e Internet a este sector de la población.

Adicionalmente, el Artículo 101 Bis 1 establece que el Estado garantizará a niñas, niños y adolescentes su integración a la sociedad de la información y el conocimiento. De igual forma, el Artículo 101 Bis 2 estipula su derecho al acceso y uso seguro del Internet para ejercer sus derechos a la información, comunicación, educación, salud, esparcimiento.

Al respecto, la LGDNNA establece en su Capítulo Décimo Séptimo, el derecho a la intimidad, lo cual contempla a la intimidad personal y familiar, así como a la protección de sus datos personales.

En este sentido, se señala que las niñas, niños y adolescentes no podrán ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia; tampoco de divulgaciones o difusiones ilícitas de información o datos personales, incluyendo aquella que tenga carácter informativo a la opinión pública o de noticia que permita identificarlos y que atenten contra su honra, imagen o reputación. Quienes ejerzan la patria potestad, tutela o guarda y custodia, deberán orientar, supervisar y, en su caso, restringir, las conductas y hábitos de niñas, niños y adolescentes, siempre que atiendan al interés superior de la niñez.

En relación con lo anterior, es importante señalar que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), en su carácter de organismo constitucional autónomo garante del derecho humano a la protección de datos personales, es una de las autoridades obligadas a garantizar los derechos de los menores de edad, en el entendido que tanto la privacidad como la protección de datos personales forman parte de la gama de derechos humanos, considerando que un indebido tratamiento de sus datos personales puede afectar severamente a la esfera más íntima de las niñas, niños y adolescentes, lo cual repercutiría en su desarrollo social y en el ejercicio de otros derechos fundamentales.

Robustece lo anterior el hecho que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados⁸¹ (LGPDPPO) en su artículo 7, segundo párrafo, reconoce que en el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior

⁸⁰ Disponible para su consulta en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGDNNA_110121.pdf Publicada en el Diario Oficial de la Federación el 04 de diciembre de 2014: https://www.dof.gob.mx/nota_detalle.php?codigo=5374143&fecha=04/12/2014, última reforma el 11 de enero de 2021, texto disponible por parte de la Cámara de Diputados del H. Congreso de la Unión disponible para su consulta en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGDNNA_110121.pdf.

⁸¹ Publicada en el Diario Oficial de la Federación el 26 de enero de 2017, disponible en el siguiente vínculo electrónico: http://dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017, sin reformas; texto consolidado en formato de documento portable, pdf por sus siglas en inglés, por parte de la Cámara de Diputados del H. Congreso de la Unión, en el vínculo siguiente: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>



de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables, situación que reconoce la aplicabilidad en la materia de la Ley en comento, como normatividad específica para el tratamiento de información personal de niñas, niños y adolescentes.

Asimismo, la Hoja de Ruta 2021-2025 del IFT, contempla la diversificación de usuarios, en la cual se incluye también a los niños. Esta consideración, es primordial para garantizar los derechos de todos los usuarios y la calidad de los servicios prestados.

Reconociendo que las TIC se constituyen cada vez más como parte fundamental en la sociedad, específicamente considerando el uso que realizan los menores de edad y su participación en línea y debido a que, las TIC se utilizan para el proceso, administración y distribución de la información a través de elementos tecnológicos necesarios en una sociedad cada vez más digital, conlleva a que haya un importante flujo de datos personales.

La sociedad de la información conduce a que cada vez, en mayor medida, todas las generaciones realicen actividades en forma digital, es por ello que, la adquisición de competencias desde una edad temprana para el cuidado de los datos personales es de suma relevancia para manejarse en estos espacios cada vez más habituales.

En esta vertiente, el derecho a la protección de datos personales es un elemento principal para considerarse en las interacciones que se dan mediante el uso de las TIC. En México, el derecho a la protección de datos personales se encuentra reconocido como derecho fundamental en el artículo 16 de la CPEUM, así como en LGPDPPSO y sus Lineamientos Generales aplicables al sector público⁸² (Lineamientos) a nivel federal y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares⁸³ (LFPDPPP) y su Reglamento (RLFPDPPP)⁸⁴ aplicable al sector privado, en las cuales se prevé la observancia de principios, deberes y obligaciones orientados a la protección de datos personales de todas las personas, entre las cuales se encuentran menores de edad, y respecto de los cuales, por ejemplo, en el caso de los responsables del sector público,

⁸² Publicados en el Diario Oficial de la Federación el 26 de enero de 2018 disponible en los siguientes vínculos electrónicos: https://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018 y <http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf>, modificados por última vez el 25 de noviembre de 2020, disponible en el vínculo electrónico https://www.dof.gob.mx/nota_detalle.php?codigo=5605789&fecha=25/11/2020, www.dof.gob.mx/2020/INAI/ACT-PUB-11-11-2020-05.pdf, <https://home.inai.org.mx/wp-content/documentos/AcuerdosDelPleno/ACT-PUB-11-11-2020.05.pdf>

⁸³ Publicada en el Diario Oficial de la Federación el 5 de julio de 2010 disponible en el siguiente vínculo electrónico: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010, sin reformas; texto consolidado en formato de documento portables, pdf por sus siglas en inglés, por parte de la Cámara de Diputados del H. Congreso de la Unión, en el siguiente vínculo electrónico: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>.

⁸⁴ Publicado en el Diario Oficial de la Federación el 21 de diciembre de 2011, disponible en el siguiente vínculo electrónico: http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011; sin reformas; texto consolidado en formato de documento portable, pdf por sus siglas en inglés, por la Cámara de Diputados del H. Congreso de la Unión, disponible en el vínculo siguiente: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf.



se establece que se deberá privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables.

En congruencia con lo anterior, cabe destacar lo dispuesto por el segundo párrafo del artículo 7 de la LGPDPSO, de conformidad con el cual “en el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables”.

Ello supone la aplicación del principio del interés superior de la niñez (también llamado interés superior del menor o de los niños, niñas y adolescentes), previsto en el párrafo noveno del artículo 4º de la CPEUM, conforme al cual deben orientarse todas las decisiones y actuaciones del Estado.

La Ley Federal de Telecomunicaciones y Radiodifusión⁸⁵ en su artículo 145, fracción III, establece que:

“Artículo 145. Los concesionarios y autorizados que presten el servicio de acceso a Internet deberán sujetarse a los lineamientos de carácter general que al efecto expida el Instituto conforme a lo siguiente:

...

III. Privacidad. Deberán preservar la privacidad de los usuarios y la seguridad de la red:

...”

En ese sentido, el 5 de julio de 2021, el IFT publicó en el DOF el “Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos para la gestión de tráfico y administración de red a que deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet” (Lineamientos de Gestión y Administración de Tráfico)⁸⁶, el cual tiene por objeto establecer los criterios a los que deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet, mediante redes públicas de telecomunicaciones, al implementar gestión de tráfico y administración de red.

La normatividad mexicana en materia de protección de datos personales se regula a través de dos piezas legislativas diferenciadas a partir de los sujetos a quienes le son aplicables, la LFPDPPP y la LGPDPSO. Teniendo así que, el sector privado es regulado por la LFPDPPP y

⁸⁵ Disponible en el siguiente vínculo http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014

⁸⁶ Publicado en el Diario Oficial de la Federación el 05 de julio de 2021, disponible en el siguiente vínculo electrónico: http://dof.gob.mx/nota_detalle.php?codigo=5622965&fecha=05/07/2021



el sector público federal le es aplicable la LGPDPPSO y demás normatividad que derive de ambos ordenamientos.

Por un lado, la LFPDPPP se constituye en el marco general que contempla una serie de reglas, requisitos, condiciones y obligaciones mínimas para garantizar un adecuado manejo de los datos personales por parte de los responsables de carácter privado que, durante el desarrollo de sus actividades, procesos operativos, comerciales o de servicios, o bien, funciones estatutarias utilicen datos personales.

Asimismo, la LGPDPPSO, establece las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos en el ámbito federal.

Ambas piezas legislativas consideran como tratamiento de datos personales a cualquier operación o conjunto de operaciones relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales tanto en soportes físicos como automatizados.

Por lo tanto, la normatividad señalada contempla las acciones tanto físicas como en línea, que pudieran constituirse como tratamiento de datos personales, por lo que la aplicabilidad de la normativa citada, tanto para el sector público como privado, garantiza la salvaguarda del derecho reconocido en el artículo 16 constitucional.

Aunado a lo anterior, es importante tener presente que, en septiembre de 2018, se publicó en el Diario Oficial de la Federación, el Decreto Promulgatorio del Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos⁸⁷ (Convenio 108) y su Protocolo Adicional, a través del cual México se adhirió a dicho instrumento internacional por medio del cual se prevé garantizar la protección efectiva de los derechos humanos y de las libertades fundamentales, y en particular, el derecho al respeto a la vida privada, en relación con los constantes intercambios transfronterizos de datos personales.

En este sentido, y de acuerdo con el artículo 133 de la CPEUM, los tratados celebrados con aprobación del Senado se constituyen como la Ley Suprema de toda la Unión, por lo que la

⁸⁷ Publicado en el Diario Oficial de la Federación el 28 de septiembre de 2018, disponible para su consulta en: https://www.dof.gob.mx/nota_detalle.php?codigo=5539474&fecha=28/09/2018.



normatividad aplicable en la materia en México, no solo se limita al ámbito nacional, sino que adquiere tintes internacionales con la citada adhesión.

Notificaciones-contenido ilícito/Notificaciones-preocupaciones de los usuarios

El micrositio de Ciberseguridad para Usuarios de Servicios de Telecomunicaciones,⁸⁸ que tiene como objetivo de promover la confianza en el ecosistema digital, cuenta con un apartado denominado “*Reporte Ciudadano*” en el que los usuarios podrán encontrar los datos de contacto de las policías cibernéticas adscritas a los diferentes estados de la república y, con ello, recibir asesoría o reportar los incidentes cibernéticos que presenten durante su navegación por Internet.

El INAI cuenta con múltiples canales de atención para el público, entre ellos el “Centro de Atención a la Sociedad (CAS)”, el cual, entre otros servicios, brinda asesoría a las personas sobre el ejercicio del derecho a la protección de datos personales, así como asesoría para presentar denuncias por vulneración o inadecuado tratamiento de datos personales por parte de responsables del sector público y privado. Además, el Instituto cuenta con canales de comunicación vía telefónica, presencial, correo electrónico y postal.

Asimismo, el INAI es la autoridad garante del derecho a la protección de datos personales, por lo tanto, se puede acudir ante esta autoridad cuando se tenga conocimiento de un tratamiento indebido de los datos personales, y hacer uso de los procedimientos señalados en la LFPDPPP y LGPDPPSO.

Los procedimientos que sustancia el Instituto, vinculados con la protección de los datos personales son:

- **Sector privado**

Los procedimientos que sustancia el Instituto, vinculados con la protección de los datos personales incluyen los procedimientos de Investigación y Verificación que aplican cuando un particular quiera denunciar un tratamiento indebido de datos personales por parte de un responsable del sector privado. Con la presentación de la denuncia, inicia el Procedimiento de Investigación, a través del cual se determinará si se considera que el responsable vulneró o no los principios o deberes señalados en la ley; en caso de que se haya considerado que existen vulneraciones por parte del responsable, se da continuidad al trámite de denuncia a través del Procedimiento de Verificación, en el cual una vez que el INAI, considere que ya cuenta con los elementos suficientes para determinar si efectivamente existió una vulneración por parte del responsable a los principios o deberes que señala la ley, el Pleno del Instituto, emitirá la

⁸⁸ Disponible en el siguiente vínculo <https://ciberseguridad.ift.org.mx/>



resolución correspondiente, pudiendo ordenar el inicio del procedimiento de imposición de sanciones o en su caso concluir el procedimiento de verificación.

- **Sector público**

En términos de lo dispuesto por el artículo 16, párrafo segundo, de la CPEUM toda persona tiene derecho a la protección de sus datos personales, y al derecho de ejercer sus derechos de acceso, rectificación, cancelación y oposición, en los términos que fije la ley. Estos derechos se conocen como derechos ARCO los cuales se podrán hacer valer ante el responsable que tenga en su posesión sus datos personales.

Por lo que respecta, al derecho de cancelación, el artículo 46 de la LGPDPSO establece que el titular de los datos personales tiene el derecho de solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

Por otro lado, en cuanto al derecho de oposición, el artículo 47 establece que el titular de los datos personales podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:

- Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular; y
- Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

En este tenor y para el ejercicio de los derechos ARCO, será necesario que se acredite la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante. Asimismo, el ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.

Por su parte, la LFPDPPP, es importante hacer de su conocimiento que los derechos de cancelación y oposición se encuentran reconocidos concretamente en los artículos 25 y 26 de la LFPDPPP y 105, 106 y 108 del RLFPDPP, disposiciones de las cuales se desprende que toda persona tiene derecho a cancelar sus datos personales en cualquier fase de la utilización de éstos, cuando considere que los mismos no están siendo manejados conforme a los principios y



deberes que establece las disposiciones jurídicas en materia de protección de datos, salvo que se actualice alguna de las siguientes excepciones:

- Cuando los datos personales se refieran a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;
- Cuando los datos personales deben ser utilizados por disposición legal;
- Cuando se obstaculicen actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, investigación y persecución de delitos o actualización de sanciones administrativas;
- Cuando la información personal sea necesaria para proteger los intereses jurídicamente tutelados de la persona a quien le concierne ésta;
- Por cuestiones de interés público;
- Cuando los datos personales sean necesarios para cumplir con una obligación legalmente adquirida por la persona a quien le concierne éstos;
- Para la prevención, diagnóstico médico o gestión de servicios de salud, siempre que se realice por un profesional de la salud sujeto a un deber de secreto.

En este sentido, la cancelación de datos personales implica la supresión o eliminación de éstos de los registros, archivos, expedientes o sistemas de información de la persona física o moral de carácter privado que los posee, previo bloqueo.

En ese sentido, es posible advertir que el periodo de bloqueo tiene como propósito impedir la utilización de los datos personales, a través de la implementación de una serie de medidas de seguridad encaminadas a su inutilización, salvo el almacenamiento o posible acceso de alguna persona.

Por su parte, de conformidad con los artículos 27 de la LFPDPPP y 109 de su RLFPDPP, el derecho de oposición implica que el individuo a quien le conciernan los datos personales pueda solicitar, amparado en una causa legítima, que sus datos personales no sean utilizados para ciertos fines, como podría ser por ejemplo la divulgación de sus datos personales en Internet.

En otro contexto, el Procedimiento de Verificación ante el INAI sólo aplica cuando un particular quiera denunciar un tratamiento indebido de datos personales por parte de un responsable del sector público federal, es decir su objeto es denunciar que los datos personales se están tratando de manera indebida o no se están respetando los principios y deberes de la LGPDPPSO. El Instituto podrá ordenar medidas cautelares, si durante la verificación se advierte un daño



inminente o irreparable en materia de protección de datos personales, y tendrán una finalidad correctiva y serán temporales hasta que el responsable atienda las recomendaciones que emita el INAI. El procedimiento de verificación concluirá con la resolución que emita el Instituto, en la cual, se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma determine.

Al respecto, sobre los procedimientos del INAI o el derecho de protección de datos personales en general, el INAI cuenta con los siguientes canales de comunicación:

- IFAI-Prodatos: <https://www.datospersonales.org.mx/>
- Mediante el número, 800 835 4324 gratuito.
- CAS en la siguiente dirección: Av. Insurgentes Sur 3211, Col. Insurgentes Cuicuilco, Coyoacán, C.P. 04530, Ciudad de México.
- Vía correo electrónico: atencion@inai.org.mx
 - 1 Sector privado: verificacion@inai.org.mx
 - 2 Sector público: investigayverifica@inai.org.mx

Cuando una institución pública estatal realice un tratamiento indebido de tus datos personales se deberá acudir al Órgano Garante local.

La Guardia Nacional, cuenta con el número 088, en donde se brinda la asesoría técnica y legal a la ciudadanía, en seguimiento a los reportes sobre delitos y conductas antisociales que se cometen a través del Internet, en agravio de niñas, niños y adolescentes. Así también cuenta con medios cibernéticos de contacto:

- 1 Correos electrónicos: cnac@gn.gob.mx; guardia.nacional@gn.gob.mx
- 2 Red social Twitter: @CNACGN y @GNMEXICO
- 3 Red social Facebook: @GUARDIA.NACIONAL.MX
- 4 Red social Instagram: @gnmexico
- 5 Plataforma YouTube: /GuardiaNacionaldeMexico

De todo lo anterior, se concluye que en México no se tiene una normatividad específica para la retirada de los contenidos que atenten contra los niños, niñas y adolescentes, como el caso de la pornografía infantil; sin embargo, se cuenta con un criterio de la Suprema Corte de Justicia de la Nación que, aunado a las políticas de privacidad de los proveedores y convenios con los mismos, permiten la gestión correspondiente.



“BLOQUEO DE UNA PÁGINA ELECTRÓNICA (INTERNET). DICHA MEDIDA ÚNICAMENTE ESTÁ AUTORIZADA EN CASOS EXCEPCIONALES. Como lo ha sostenido el Consejo de Derechos Humanos de la Organización de las Naciones Unidas, el bloqueo de una página de Internet implica toda medida adoptada para impedir que determinados contenidos en línea lleguen a un usuario final. Al respecto, debe tenerse en cuenta que las restricciones al derecho humano de libertad de expresión no deben ser excesivamente amplias, por el contrario, deben referirse a un contenido concreto; de ahí que las prohibiciones genéricas al funcionamiento de ciertos sitios y sistemas web, como lo es el bloqueo, son incompatibles con el derecho humano de libertad de expresión, salvo situaciones verdaderamente excepcionales, las cuales podrían generarse cuando los contenidos de una página de Internet se traduzcan en expresiones prohibidas, esto es, tipificadas como delitos acorde con el derecho penal internacional, dentro de las que destacan: (I) la incitación al terrorismo; (II) la apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia -difusión del "discurso de odio" por Internet-; (III) la instigación directa y pública a cometer genocidio; y (IV) la pornografía infantil. Asimismo, la situación de excepcionalidad a la prohibición de restricciones genéricas al derecho de expresión también podría generarse cuando la totalidad de los contenidos de una página web resulte ilegal, lo que lógicamente podría conducir a su bloqueo, al limitarse únicamente a albergar expresiones no permisibles por el marco jurídico”.

Amparo en revisión 1/2017. Alestra, S. de R.L. de C.V. 19 de abril de 2017. Unanimidad de cuatro votos de los Ministros Alberto Pérez Dayán, Javier Laynez Potisek, José Fernando Franco González Salas y Eduardo Medina Mora.

Impedida: Margarita Beatriz Luna Ramos. Ponente: Alberto Pérez Dayán. Secretario: Isidro Emmanuel Muñoz Acevedo. Esta tesis se publicó el viernes 16 de junio de 2017 a las 10:22 horas en el Semanario Judicial de la Federación

Actores y partes interesadas

- Secretaría de Gobernación (SEGOB)⁸⁹.
- Secretaría de Educación Pública (SEP)⁹⁰.
- Sistema Nacional de Protección Integral de niñas, niños y adolescentes (SIPINNA)⁹¹.
- Comisión Nacional de Derechos Humanos (CNDH)⁹².

⁸⁹ Disponible para su consulta en: <https://www.gob.mx/segob>

⁹⁰ Disponible para su consulta en: <https://www.gob.mx/sep>

⁹¹ Disponible para su consulta en: <https://www.gob.mx/sipinna>

⁹² Disponible para su consulta en: <https://www.cndh.org.mx/>



En México existen distintas autoridades que podrían resultar competentes en materia de protección de menores de edad en línea. Sin embargo, por lo que refiere específicamente al derecho humano a la protección de datos personales, el INAI, es el organismo constitucional autónomo garante de este derecho. Así, en aras de la salvaguarda de este derecho, el INAI es la autoridad competente para garantizar el derecho a la protección de datos personales, así como el ejercicio y tutela de los derechos de acceso, rectificación, cancelación y oposición que toda persona tiene con respecto a su información.

En este sentido, el INAI, realiza esfuerzos constantes con el fin de promover una cultura en materia de protección de datos personales en cualquiera de sus ámbitos, incluyendo cuando se dé el tratamiento de información personal en línea.

Es importante señalar, que, en la actuación del INAI, como organismo garante del derecho a la protección de datos personales, por lo que se refiere al caso particular de niñas, niños y adolescentes, resulta necesaria la colaboración con otros actores involucrados, situación que habilitaría la competencia concurrente en un caso específico.

- 1 Sistema Nacional de Protección de Niñas, Niños y Adolescentes (SIPINNA)
- 2 Sistema Nacional para el Desarrollo Integral de las Familias (DIF)
- 3 Fiscalía General de la República (FGR)
- 4 Fiscalías y Procuradurías de las Entidades Federativas
- 5 Unidades de Policías Cibernéticas de las Entidades Federativas
- 6 La Guardia Nacional
- 7 Comisión Ejecutiva de Atención a Víctimas
- 8 Comisión Nacional de los Derechos Humanos (CNDH)

El INAI, es el organismo constitucional autónomo garante del cumplimiento de dos derechos fundamentales: el de acceso a la información pública y el de protección de datos personales; teniendo en cuenta que, el sector privado es regulado por la LFPDPPP y el sector público federal por la LGPDPPSO.

Existen Organizaciones no gubernamentales dedicadas a la protección de la infancia en línea, como:

- Social TIC⁹³

⁹³ Disponible para su consulta en: <https://socialtic.org/>



- WOMCY⁹⁴
- UNICEF México⁹⁵, misma que trabaja en coordinación con el gobierno, las organizaciones de la sociedad civil y el sector privado para lograr que todas las niñas, niños y adolescentes vean garantizados sus derechos. De igual forma, ha desarrollado material informativo en cuanto a la seguridad de niñas, niños y adolescentes en línea como su reciente titulado “Mantener seguros a niñas, niños y adolescentes en internet”⁹⁶. Así como su reciente campaña con Facebook “#SinViolenciaEnLínea” en donde a través de la difusión de temas como la violencia en internet contra la niñez y la adolescencia se busca prevenirla.
- “Save the Children⁹⁷” México, encargada de defender los derechos de la niñez, protegiéndolos de violencia infantil, desnutrición, acoso, maltrato, explotación y otros más, además de fomentar su educación e inclusión.
- Red por los Derechos de la Infancia⁹⁸, coalición conformada por 72 Organizaciones de la Sociedad Civil, la cual desarrolla programas a favor de niñas, niños y adolescentes mexicanos en situaciones de vulnerabilidad teniendo como fin la promoción y defensa de los derechos de la infancia en México para que éstos conozcan, ejerzan y disfruten sus derechos, a través de acciones de incidencia y exigibilidad buscando un cambio jurídico, social y cultural, entre algunas otras más organizaciones.

Alianzas Nacionales e Internacionales (sector público y sector privado)

El IFT ha llevado algunas acciones de colaboración con otras instituciones, en materia de seguridad digital, como son las siguientes:

- Plan de Acciones en materia de Ciberseguridad⁹⁹. En marzo de 2019, el Instituto publicó un documento con el que se pretende contribuir a un ecosistema digital seguro. Dicho Plan, fue sometido a un mecanismo de participación ciudadana con el objeto de conocer los comentarios, opiniones y aportaciones de la academia, la industria, la sociedad civil y cualquier otro interesado, con la finalidad de obtener insumos para robustecer el contenido de dicho documento. Actualmente, las áreas involucradas trabajan en su actualización.
- Micrositio de Ciberseguridad para usuarios de Servicios de Telecomunicaciones. El 17 de noviembre de 2021 el IFT presentó el Micrositio de Ciberseguridad para Usuarios de

⁹⁴ Disponible para su consulta: <https://www.womcy.org/es/inicio/>

⁹⁵ Disponible para su consulta en: <https://www.unicef.org/mexico/>

⁹⁶ Disponible para su consulta en: <https://www.unicef.org/mexico/mantener-seguros-niñas-niños-y-adolescentes-en-internet>

⁹⁷ Disponible para su consulta en: <https://www.savethechildren.mx/>

⁹⁸ Disponible para su consulta en: <http://derechosinfancia.org.mx/v1/sobre-nosotros/>

⁹⁹ Disponible para su consulta en: <http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/upr-planaccionesiberseguridad.pdf>



Servicios de Telecomunicaciones, como una acción del regulador para promover la confianza en el ecosistema digital, en seguimiento a las estrategias establecidas en el documento denominado Hoja de Ruta 2021-2025 del Instituto.

En el Micrositio se conjuntan materiales de información en torno a la seguridad digital generada por el IFT y la Unión Internacional de Telecomunicaciones (UIT), el Instituto Nacional de Ciberseguridad de España (INCIBE), la Guardia Nacional (GN), el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), la Secretaría de Infraestructura, Comunicaciones y Transportes (SICT), el Sistema Nacional de Protección de Niñas, Niños y Adolescentes (SIPINNA) y la Secretaría de Seguridad Ciudadana de la Ciudad de México (SSPC), entre otros.

- Comisión para el Seguimiento de las Recomendaciones del Comité de los Derechos del Niño de Naciones Unidas del Sistema Nacional de Protección Integral de Niñas, Niños y Adolescentes (SIPINNA). El Instituto forma parte de este Comité, el cual tiene como objetivo realizar esfuerzos conjuntos a nivel nacional a fin de dar cumplimiento a las Recomendaciones, mediante acciones concretas de conformidad con la competencia de cada Instancia mexicana. A través de ciclos de conferencias, talleres, grupos de trabajo, entre otros, realizadas con las múltiples partes interesadas en el tema. Es preciso destacar que el IFT, continúa participando y apoyando activamente en la actualización de la ENCS; asimismo, lideró el grupo de trabajo correspondiente al objetivo estratégico “Sociedad y derechos” de la estrategia en comento, en coordinación con el Sistema Nacional de Protección Integral de Niñas, Niños y Adolescentes (SIPINNA); también es invitado permanente de la Subcomisión de Ciberseguridad. En este contexto, se coordinaron mesas de trabajo con la participación de organizaciones públicas y privadas, así como de la sociedad civil a efecto de:
 - Identificar áreas de oportunidad y recomendaciones de mejores prácticas en materia de Ciberseguridad en el uso y aprovechamiento de las TIC para el fortalecimiento de políticas públicas con perspectiva de derechos humanos y no discriminación.
 - Establecer acciones con un enfoque basado en gestión de Riesgos en materia de Ciberseguridad que permitan identificar las principales amenazas, vulnerabilidades, Riesgos y ataques a los que la población se encuentra expuesta, así como las organizaciones públicas y privadas con la finalidad de concientizar e incentivar un uso responsable de las TIC.



- Recomendar mecanismos y ruta crítica para la actualización y armonización del marco jurídico en el ámbito de la Ciberseguridad con perspectiva de derechos humanos y no discriminación.

Asimismo, el INAI ha establecido coordinación con diversas instituciones del sector público y privado, con el objetivo de establecer coordinación y apoyo para coadyuvar en campañas de difusión, promoción y sensibilización respecto a la protección de datos personales y la seguridad en el uso de las TIC, dirigidas a la ciudadanía.

Al respecto, en coordinación con la Universidad Nacional Autónoma de México, lanzó la historieta didáctica “Ina y el cuervo de nunca más” dirigida principalmente a jóvenes adolescentes para advertir sobre los riesgos en el uso del internet y las redes sociales y fomentar el conocimiento, la prevención, la protección y defensa de la privacidad y los datos personales en el ámbito virtual.

De igual forma en coadyuvancia con diversos actores de instituciones públicas y privadas, nacionales e internacionales, se ha establecido acciones para organización, promoción, difusión y operación de concursos dirigidos al fomento de la cultura en protección de datos personales en menores de edad tal como el “Concurso para ser Comisionada y Comisionado Infantil y formar parte del Pleno Niñas y Niños”, el cual tienen como objetivo principal promover la importancia de la privacidad y protección de datos personales entre los menores de edad, como parte de la campaña de educación cívica para el ejercicio del derecho de protección de datos personales.

En el ámbito internacional, el INAI ha establecido comunicación con distintas autoridades de protección de datos personales con el objetivo específico de realizar a adaptación de materiales dirigidos a niñas, niños, adolescentes, personal educativo y prestadores de servicios en línea con el objetivo de difundir el conocimiento sobre los derechos a la privacidad y protección de datos personales destacando las siguientes autoridades: Oficina del Comisionado de Privacidad de Canadá, Oficina del Comisionado de la Información en Reino Unido y la Comisión de Protección de Datos Personales de Singapur. De igual forma en el marco de las distintas redes y organizaciones en las que el INAI participa se han impulsado distintas iniciativas sobre temáticas relacionadas con la seguridad en línea.

El micrositio de ciberseguridad por parte del IFT, es un ejemplo de la colaboración entre los múltiples actores, ya que integra la información disponible en materia de seguridad digital generada por el propio IFT, la Unión Internacional de Telecomunicaciones (UIT), el Instituto Nacional de Ciberseguridad de España (INCIBE), la Guardia Nacional (GN), el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), la Secretaría de Infraestructura, Comunicaciones y Transportes (SICT), el Sistema Nacional de Protección de



Niñas, Niños y Adolescentes (SIPINNA) y la Secretaría de Seguridad Ciudadana de la Ciudad de México (SSPC), entre otros.

Con el objetivo de garantizar de manera amplia el derecho a la protección de datos personales de la ciudadanía mexicana, incluyendo a la población menor de edad y considerando que las telecomunicaciones y las TIC, incluyendo el acceso a internet y las plataformas, aplicaciones, servicios y actividades que se ofrecen a través de las mismas, brindan grandes y diversas oportunidades de desarrollo a la sociedad, facilitan el comercio y las demás actividades económicas, el INAI ha firmado convenios como el celebrado con el IFT, el cual tiene como principal objetivo establecer las bases generales de coordinación y colaboración, para que, a través del máximo aprovechamiento de sus recursos humanos, materiales y financieros en el desarrollo de acciones, se puedan realizar programas, eventos y trabajos, que tengan como finalidad promover la cultura de la protección de datos personales, la competencia económica y su interrelación con otras actividades gubernamentales y sociales, generando promoción, confianza y el uso responsable y seguro de las telecomunicaciones, las TIC y los servicios digitales; conforme a sus respectivas atribuciones y ámbitos de competencia.

Asimismo, el INAI, en atención a la transversalidad del derecho a la protección de datos personales con otras materias, ha colaborado en diversas ocasiones con Guardia Nacional para organizar y desarrollar campañas de difusión sobre temáticas de ciberseguridad y protección de datos personales.

Por otro lado, el 24 de agosto de 2017, el INAI junto con el Sistema Nacional para el Desarrollo Integral de las Familias, DIF Nacional, suscribieron un Convenio General para fortalecer la Transparencia y la Protección de Datos Personales. En dicho instrumento ha servido para promover los programas que el INAI ha creado para cuidar a los niños de los peligros que enfrentan al tener acceso a las tecnologías de la información. En este sentido, se buscó que el convenio suscrito ayudara para que las familias mexicanas, en la parte más delicada, que es la niñez, se sientan más protegidas.

Asimismo, el citado Convenio, demostró el interés de las dos instituciones involucradas de aprender de manera conjunta la tarea de ser transparentes y poner ante la mirada de la sociedad cada acción y gestión empleada.

Por último, es importante recalcar que, de conformidad con el artículo 93 de la LGPDPSO, faculta tanto al INAI como a los organismos garantes locales para promover que en los programas y planes de estudio, libros y materiales que se utilicen en las instituciones educativas de todos



los niveles y modalidades del Estado, se incluyan contenidos sobre el derecho a la protección de datos personales, así como una cultura sobre el ejercicio y respeto de éste.

Al respecto, es conveniente resaltar que de la mano con la Secretaría de Educación Pública se han desarrollado Jornadas de Sensibilización en escuelas de nivel secundaria, las cuales se han planteado como objetivos primordiales el promover el ejercicio del derecho a la protección de datos personales principalmente entre adolescentes, como parte de la población prioritaria, y el difundir información práctica y de utilidad para la protección de datos personales en el entorno digital. Para ello, se contemplaron instituciones educativas tanto del sector público como privado.

En este sentido el INAI establece coordinación con el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT) y de forma específica con los Organismos Garantes de las entidades federativas, así como de las Coordinaciones Regionales, la Comisión de Protección de Datos Personales y la Comisión de Asuntos de Entidades Federativas y Municipios para promover la privacidad y protección de los datos personales.

El INAI, en el interés de fomentar la educación y propiciar el conocimiento en cuanto a la importancia de la protección de los datos personales, ha celebrado convenios de colaboración con el sector privado buscando crear un ambiente cultura participativa y colaborativa, es por ello que el 25 de octubre de 2016, se aprobó mediante sesión del Pleno del INAI la celebración de un contrato para la adquisición de la licencia para el uso del programa “Plaza Sésamo: Monstruos en Red” por parte del Instituto, mismo que encuentra sustento en las atribuciones con las que cuenta este organismo garante como es difundir el conocimiento del derecho que salvaguarda, promover su ejercicio y el debido cumplimiento de la Ley en materia de protección de datos personales, entre otras.

La organización educativa sin fines de lucro *Sesame Workshop* o Plaza Sésamo desarrolló el programa “Monstruos en red”, que se trata de una iniciativa en múltiples plataformas (serie de televisión, guías interactivas, juegos en línea, libros electrónicos, entre otros), diseñada para apoyar a niños y niñas, familias y educadores en la formación de buenos hábitos de uso y aprovechamiento de las nuevas tecnologías de la información y las comunicaciones.

En coordinación con el INAI se realizó el ajuste a dicho material, para hacer énfasis en los temas de privacidad y protección de datos personales de los menores para una navegación segura y un mejor aprovechamiento de las TIC, y contextualizar los contenidos para el entorno mexicano.

El programa está dirigido a niños de entre tres y siete años, pero también para familias y educadores de buenos hábitos en el uso y aprovechamiento de las tecnologías de la información



y la comunicación y para la difusión de este proyecto, televisoras y plataformas de videos brindaron su apoyo.

El 4 de septiembre de 2017, inició la transmisión de la serie Monstruos en Red a través de Canal Once, Once Niños y por el canal de YouTube Kids, las redes sociales del INAI, así como de los canales en YouTube de Sésamo e INAI.

La población infantil tiene acceso a contenidos y plataformas digitales a edades progresivamente más tempranas, lo que hace indispensable poner a su disposición herramientas que les permitan interactuar de manera segura con los mismos. Es por lo que, continuando con el mismo objetivo y en el ejercicio de dichas atribuciones y a efecto de apoyar a la población a la formación de buenos hábitos de uso seguro y aprovechamiento de nuevas tecnologías de la información y comunicaciones, el 11 de noviembre del 2020, se aprobó la celebración de la extensión de la licencia del mismo programa con Sesame Workshop, buscando seguir contribuyendo a la educación de este derecho fundamental en México.

Los personajes de la asociación civil sin fines de lucro, Plaza Sésamo, son ampliamente reconocidos y queridos por la niñez mexicana y de muchos otros países y gozan de gran confianza por parte de padres y educadores gracias a su trayectoria de más de 40 años generando contenidos educativos y atractivos para la televisión.

Debido a la conexión emocional que generan con los niños, éstos son vehículos ideales para promocionar temas de salud, bienestar, educación, entre otros, lo cual se encuentra ampliamente respaldado por numerosas investigaciones en México y alrededor del mundo.

Además de lo anterior, el INAI cuenta con el “Programa Aliados INAI: por una cultura de la Protección de Datos Personales”, el cual consiste en una estrategia continua de capacitación impulsada por el INAI, dirigida a responsables del sector privado, que inicio a partir del año 2018. Su objetivo es ofrecer capacitación estratégica y continua a responsables y encargados de la LFPDPPP.

De manera adicional se han realizado colaboraciones con distintas asociaciones y organizaciones del sector privado enfocadas en los derechos de los menores de edad en el marco de la realización de las distintas actividades de promoción, difusión y sensibilización del derecho a la protección de datos personales como por ejemplo los concursos dirigidos a este sector de la población.

La Guardia Nacional mantiene estrecha colaboración con aliados estratégicos, entre las que se encuentran las Unidades de Policía Cibernética de las Secretarías de Seguridad Pública y Fiscalías de las entidades federativas, que conforman el Comité de Ciberseguridad de Unidades



de Policía Cibernética; también se cuenta con la participación de otros aliados de los sectores gubernamentales, privados, académicos y organizaciones nacionales e internacionales. Se mantiene estrecha colaboración con la Fiscalía General de la República, las Fiscalías y Procuradurías de las 32 Entidades Federativas, para la investigación y combate de los Ciberdelitos, teniendo como resultado el rescate de víctimas menores de edad, y la detención de los agresores sexuales o ciberdelincuentes.

Investigación

En México, el IFT realiza la Encuesta Nacional de Consumo de Contenidos Audiovisuales 2019¹⁰⁰; igualmente, el Instituto Nacional de Estadística y Geografía, en colaboración con la Secretaría de Comunicaciones y Transportes (SCT) y el IFT, publica la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020¹⁰¹.

La Guardia Nacional cuenta con el área funcional de Ciberdelitos, con capacidades de prevención e investigación de conductas delictivas que se cometen a través de las tecnologías de la información y comunicación e Internet; cumple con la misión de prevenir, atender e investigar delitos o conductas antisociales en perjuicio a la ciudadanía, resaltando las que se cometen en agravio de Niñas, Niños y Adolescentes, como el grooming, sexting, sextorsión, amenazas, robo de identidad, corrupción de menores, trata de personas, pornografía Infantil, entre otras.

Además, en la presente administración la G.N., implementó el "Operativo Salvación", que consiste en realizar acciones de prevención, capacitación y coordinación entre la Guardia Nacional con la Fiscalía General de la República (FGR) y con las Fiscalías y Procuradurías de las 32 Entidades Federativas, para llevar a cabo labores de investigación para el combate a la Pornografía Infantil en México y demás conductas antisociales que se cometen a través del Internet, en agravio de niñas, niños y adolescentes, lo que permite el rescate de víctimas menores de edad del delito de Pornografía Infantil, y poner a los probables responsables o agresores sexuales en manos de la Justicia.

Educación en Materia de alfabetización y competencias digitales

Algunas acciones realizadas por el IFT son las siguientes:

- El Programa para Promover la Confianza en el Entorno Digital, trata de un programa de trabajo interinstitucional e intersectorial que se realiza a través de reuniones y mesas de

¹⁰⁰ Encuesta Nacional de Consumo de Contenidos Audiovisuales 2019 <https://conectadas.org/encuesta-nacional-de-consumo-de-contenidos-audiovisuales/>

¹⁰¹ Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020. https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH_2020.pdf



trabajo con diferentes actores, entre ellos, organismos gubernamentales, asociaciones civiles y la iniciativa privada, para que a través de la suma de esfuerzos de los diversos entes que participan en el ecosistema digital, se dialogue, comparta e identifiquen los principales riesgos y amenazas de dicho entorno, y se diseñen acciones a ejecutar desde el ámbito de competencia de cada uno de los actores, con la finalidad de promover confianza en el entorno digital, el uso informado y responsable de Internet.

- **Micrositio de ciberseguridad para usuarios de servicios de telecomunicaciones. Sección: niñas, niños y adolescentes.** El material elaborado y elegido para esta sección fue diseñado con el objetivo de brindar recomendaciones amenas y puntuales que contribuyan a que los usuarios de este rango de edad tengan una navegación en línea segura, respetuosa, divertida y agradable. Las subsecciones que integran este apartado son:

Riesgos en línea: a través de videos e infografías, los menores de edad que exploren esta subsección, podrán conocer diferentes tipos de riesgos que pueden enfrentar cuando realizan sus actividades en línea.

Consejos: sencillas recomendaciones dirigidas a promover una navegación segura y divertida de niñas, niños y adolescentes.

Ciber Club IFT: cómic interactivo, elaborado por el Instituto, integrado por 6 episodios que tienen como objetivo informar a niños, usuarios de los servicios de telecomunicaciones, sobre diversos conceptos y recomendaciones en materia de ciberseguridad. El comic puede consultarse en video animado, historieta para leer y cuadernillo para colorear.

Sitios e información de interés: apartado que presenta sitios web, de otras instituciones, en los que niñas, niños y adolescentes encontrarán sencillas recomendaciones de seguridad digital.

Proyectos de sensibilización en protección de la infancia en línea con los que cuenta el INAI:

Concursos:

- **Concurso Nacional de Cuento Juvenil. Ciberconvivencia responsable.** Es una campaña de sensibilización cuyo objetivo es promover entre estudiantes de la secundaria, bachillerato y preparatoria, el uso consciente y responsable de la información personal en las redes sociales, a través de la creación literaria.

Disponible para su consulta en: <http://concurso.inai.org.mx/cuento/>



- **Concurso Nacional de Trabajo Universitario.** Año con año se convoca a estudiantes universitarios de licenciatura y posgrado, inscritos en escuelas públicas y privadas de todo el país a elaborar un trabajo de investigación que podrá ser: análisis, ensayo, reporte, o reportaje, entre otro en el que se ejemplifique la utilidad de la transparencia y del ejercicio del derecho de acceso a la información, en los distintos sectores sociales y/o en comunidades.

Disponible para su consulta en: <https://concurso.inai.org.mx/universitario/index.php/bases>

- **Concurso “60 segundos para informarme”.** Tiene por objetivo que personas interesadas, especialmente los jóvenes, produzcan contenido en TikTok que muestre los principios de transparencia, acceso a la información, protección de datos personales o gobierno abierto y su importancia como herramientas para fortalecer la democracia y contribuir a la formación de una sociedad más informada y participativa.

Disponible para su consulta en: https://concurso.inai.org.mx/snt2021/wp-content/uploads/2021/09/60seg_convocatoria.pdf

- **Concurso Nacional de Spot de Radio.** Se convoca a todos los estudiantes de licenciatura y posgrado mayores de 18 años que cursen sus estudios en escuelas e instituciones de educación superior tanto de carácter público como privado a elaborar un spot de radio de manera individual o colectiva, donde se muestre la importancia y la utilidad social de la transparencia y de los derechos de acceso a la información y a la protección de datos personales, a fin de sensibilizar a la población mexicana sobre la conveniencia de incorporar estos temas en su vida cotidiana y en su entorno.

Disponible para su consulta en: <https://concurso.inai.org.mx/spot/>

- **Concurso de Arte Urbano y Neomuralismo.** Está dirigido a jóvenes de entre 15 y 25 años de edad para que, a través de un boceto expresen artísticamente algún mensaje relacionado con la protección de los datos personales y los riesgos de compartir información personal en la era digital con el fin de impulsar las expresiones creativas entre la juventud y promover entre la ciudadanía el derecho a la protección de los datos personales y el uso responsable de su información personal.

Disponible para su consulta en: <https://concurso.inai.org.mx/artearbano/index.php/bases>

- **Concurso para ser Comisionada y Comisionado Infantil y formar parte del Pleno Niñas y Niños.** El INAI y el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT) a través de los Organismos Garantes de



las entidades federativas, así como de las Coordinaciones Regionales, la Comisión de Protección de Datos Personales y la Comisión de Asuntos de entidades federativas y Municipios promueven la promover la importancia de la privacidad y protección de los datos personales entre los menores de edad, como parte de la campaña de educación cívica para el ejercicio del derecho a la protección de datos personales.

Disponible para su consulta en: <https://concurso.inai.org.mx/plenoninos/>

Programas:

- **Programa Plaza Sésamo: Monstruos en Red.** El INAI, desde 2016 adquirió la licencia para el uso de dicho programa, el cual se trata de una iniciativa en múltiples plataformas (serie de televisión, guías interactivas, juegos en línea, libros electrónicos, entre otros) diseñada para apoyar a niños y niñas, familias y educadores en la formación de buenos hábitos de uso y aprovechamiento de las nuevas tecnologías de la información y las comunicaciones. En coordinación con el INAI se ha ajustado dicho material, para hacer énfasis en los temas de privacidad y protección de datos personales de los menores para una navegación segura y un mejor aprovechamiento de las tecnologías de la información, y contextualizar los contenidos para el entorno mexicano.

El 4 de septiembre de 2017, inició la transmisión de la serie Monstruos en Red a través de Canal Once, Once Niños y por el canal de YouTube Kids, así como de los canales en YouTube de Sésamo e INAI.

Disponible para su consulta en

<https://www.youtube.com/playlist?list=PLAhw62t2Z4CrPGs5rNHdAiE32oeRgJUqy>

Micrositios:

- **Micrositio ¡CLIC!**, es un micrositio habilitado y alojado en la página web oficial del INAI para promover la importancia de la privacidad y protección de datos personales entre las niñas, niños y adolescentes, mismo que incorpora en un solo espacio los diversos materiales que este Instituto ha desarrollado para este sector de la población. De igual manera, se constituye como un canal de comunicación con padres y madres, personas tutoras y educadoras para poner a su disposición materiales que les ayudarán a acompañar a las niñas, niños y adolescentes en el cuidado de sus datos personales. El contenido de cada apartado se encuentra redactado en un lenguaje sencillo para su mayor comprensión. A detalle, el micrositio ¡CLIC! se conforma de 8 secciones que dan acceso a distintos tipos de materiales que van desde videos hasta materiales de lectura sobre el tema referido.



Dentro de sus secciones, el micrositio comparte material educativo, guías y herramientas dirigidas a padres y personas tutoras, proporcionando apoyo para una supervisión parental organizada, que servirá para la enseñanza oportuna en materia de protección de los datos personales. Además, las niñas, niños y adolescentes podrán visualizar las convocatorias de los concursos que el Instituto organiza, para que consulten las bases en los temas de su interés. Disponible para su consulta en: <https://micrositios.inai.org.mx/clic/>

- **Micrositio Aprende y enseña datos personales: Conocimientos y habilidades en protección de datos personales.** Diseñado con el objetivo de brindar información a las y los profesores de educación básica y secundaria, así como, a sus alumnas y alumnos, para que conozcan, con cierta profundidad, los conceptos básicos y el marco jurídico mexicano relacionado con el derecho fundamental de protección de datos personales, y a su vez, adquieran las habilidades necesarias para ejercer su derecho a la protección de datos personales y eviten colocarse en una situación, dentro del entorno digital, que pueda comprometer su información personal y ponerlos en riesgo. Disponible para su consulta: <https://micrositios.inai.org.mx/marcocompetencias/>
- **Micrositio Identidad Segura.** Diseñado para que las personas cuenten con herramientas que les ayuden a saber cómo proteger sus datos personales y reducir el riesgo de que su identidad sea robada, así como referencias para saber qué hacer y ante quién acudir en caso de haber sido víctimas de robo de identidad. El micrositio Identidad Segura se divide en los siguientes segmentos: ¿qué es el robo de identidad?; métodos utilizados para el robo de identidad; ¿cómo me protejo del robo de identidad?; ¿cómo actúo ante un robo de identidad? y el apartado conoce más.
- Disponible para su consulta: <https://micrositios.inai.org.mx/identidadsegura/>

Guías, materiales y recomendaciones:

- **Guía de herramientas de supervisión parental.** Tiene por objetivo brindar información sobre distintas herramientas que permitan a los padres: 1) supervisar la actividad de sus hijos en línea, para que tengan una experiencia positiva en el uso del Internet; 2) establecer límites claros sobre los hábitos de navegación y uso de Internet; 3) supervisar los datos personales que comparten en los diferentes sitios o aplicaciones, y 4) restringir contenidos o aplicaciones no aptos para su edad.

Disponible para su consulta en: <http://inicio.inai.org.mx/Guias/GuiaSupervisionParental.pdf>



- **Guía para la configuración de privacidad en redes sociales.** Busca que los usuarios aprendan a proteger los datos personales que publican o comparten en estas redes, a través de una configuración de privacidad adecuada en sus perfiles y describe paso a paso las instrucciones para configurar la protección a su información en cinco redes sociales principales.

Disponible para su consulta en:

http://inicio.inai.org.mx/Guias/Guia_Configuracion_RS.PDF

- **Material para educadores sobre datos personales.** Son una serie de presentaciones las cuales consisten en una traducción del material elaborado por la Office of the Privacy Commissioner of Canada, dirigido para niñas, niños y jóvenes de nivel primaria, secundaria y preparatoria, que incluye consejos sobre la protección de datos personales al navegar en internet y utilizar dispositivos móviles, redes sociales, etc.

Disponibles para su consulta en:

http://inicio.inai.org.mx/Guias/Material_Primeria_4o_6o.pptx,

http://inicio.inai.org.mx/Guias/Material_Secundaria.pptx, y

http://inicio.inai.org.mx/Guias/Material_Preparatoria.pptx.

- **Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital.** Tienen por objeto explicar, de manera clara y sencilla, una serie de consejos prácticos sobre configuraciones de seguridad, aplicaciones móviles y software en general (gratuito o con costo), que se consideran útiles para que los usuarios o titulares de los datos personales mantengan segura su privacidad y sus datos personales en el entorno digital. Este documento contiene diez recomendaciones para los titulares de los datos personales. Cada una de ellas explica por qué es importante seguir la recomendación y cuáles son los mecanismos o la mejor práctica que seguir para implementarla.

Disponible en:

<https://home.inai.org.mx/wp->

[content/documentos/GuiasTitulares/5RecomendacionesPDP_Web.pdf](https://home.inai.org.mx/wp-content/documentos/GuiasTitulares/5RecomendacionesPDP_Web.pdf)

Recursos educativos

El INAI ha elaborado y publicado distintos materiales de concientización respecto a la protección de datos personales de menores en línea, entre las que se encuentran:



Infografías

- Los dispositivos y juguetes conectados a internet¹⁰².
- Recomendaciones a autoridades educativas para el tratamiento seguro de imágenes de niñas, niños y adolescentes en eventos escolares¹⁰³.
- Recomendaciones para el tratamiento seguro de imágenes de niñas, niños y adolescentes en eventos escolares¹⁰⁴.
- Recomendaciones a padres o tutores para el tratamiento seguro de imágenes de niñas, niños y adolescentes en eventos escolares¹⁰⁵.
- Derecho a la Intimidad de niñas, niños y adolescentes y el manejo de su imagen¹⁰⁶.
- Si eres pequeño y navegas en internet. Esto debes saber¹⁰⁷.
- La intimidación personal y familiar¹⁰⁸.
- Cuidate del doxing¹⁰⁹.

Guías y recomendaciones

- Recomendaciones para proteger datos personales de menores de edad en preinscripciones escolares por internet¹¹⁰.
- Herramientas o aplicaciones de Supervisión Parental en Internet¹¹¹.
- Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital¹¹².
- Guía para la configuración de privacidad en redes sociales¹¹³.

¹⁰² Disponible para su consulta en: <https://home.inai.org.mx/wp-content/uploads/Recomendaciones-Los-Dispositivos-y-Juguetes-Conectados-a-Internet.png>

¹⁰³ Disponible para su consulta en: <https://home.inai.org.mx/wp-content/uploads/Recomendaciones-a-autoridades-educativas-para-el-tratamiento-seguro-de-imagenes-de-ni%C3%A1as-ni%C3%B1os-y-adolescentes-en-eventos-escolares-1920x1920.jpg>

¹⁰⁴ Disponible para su consulta en: <https://micrositios.inai.org.mx/clic/wp-content/uploads/2020/04/CuidarImagenMenores-Revdgpar-220819-1920x1920.jpg>

¹⁰⁵ Disponible para su consulta en: <https://micrositios.inai.org.mx/clic/wp-content/uploads/2020/04/RecomendacionesPadres-Revdgpar220819-1920x1920.jpg>

¹⁰⁶ Disponible para su consulta en: <https://micrositios.inai.org.mx/clic/wp-content/uploads/2019/10/c3-1.jpg>

¹⁰⁷ Disponible para su consulta en: https://micrositios.inai.org.mx/clic/?page_id=601#&gid=29a38e1f&pid=1

¹⁰⁸ Disponible para su consulta en: <https://micrositios.inai.org.mx/clic/wp-content/uploads/2019/10/c4-1.jpg>

¹⁰⁹ Disponible para su consulta en: <https://micrositios.inai.org.mx/clic/wp-content/uploads/2020/04/Doxing.jpg>

¹¹⁰ Disponible para su consulta en: <https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-055-21.pdf>

¹¹¹ Disponible para su consulta en: <http://home.inai.org.mx/wp-content/documentos/GuiaTitulares/GuiaSupervisionParenta.pdf>

¹¹² Disponible para su consulta en: http://inicio.inai.org.mx/Guias/5RecomendacionesPDP_Web.pdf

¹¹³ Disponible para su consulta en: http://inicio.inai.org.mx/Guias/Guia_Configuracion_RS.PDF



- Guía para prevenir el Robo de Identidad¹¹⁴.
- Guía para madres, padres y cuidadores¹¹⁵.
- Guía para educadores¹¹⁶.
- Comprendiendo qué es tu huella digital: ¿Cómo proteger tus datos personales en Internet? Nivel primaria¹¹⁷.
- Protegiendo tu reputación en línea. Nivel secundaria¹¹⁸.
- Protegiendo tu reputación en línea. Nivel Preparatoria¹¹⁹.

Programas

- Plaza Sésamo: Monstruos en red¹²⁰.
- Aliados INAI: Por una cultura de protección de datos personales.
- TV INAI¹²¹.

Micrositios:

- Micrositio ¡CLIC!¹²²
- Micrositio Aprende y enseña datos personales: Conocimientos y habilidades en protección de datos personales¹²³.
- Micrositio Identidad Segura¹²⁴.

Concursos

- Concurso para ser comisionada y comisionado infantil y formar parte del pleno niñas y niños¹²⁵.
- Concurso Nacional de Cuento Juvenil. Ciberconvivencia responsable¹²⁶.

¹¹⁴ Disponible para su consulta en: http://inicio.inai.org.mx/Guias/Gu%C3%ADa_Prevenir_RI.pdf

¹¹⁵ Disponible para su consulta en: <https://micrositios.inai.org.mx/clic/wp-content/uploads/2019/10/Gu%C3%ADaParaPadresMadres.pdf>

¹¹⁶ Disponible para su consulta en: <https://micrositios.inai.org.mx/clic/wp-content/uploads/2019/10/GuiaEducadores.pdf>

¹¹⁷ Disponible para su consulta en: http://inicio.ifai.org.mx/Guias/Material_Primary_4o_6o.pptx

¹¹⁸ Disponible para su consulta en: http://inicio.ifai.org.mx/Guias/Material_Secundaria.pptx

¹¹⁹ Disponible para su consulta en: http://inicio.ifai.org.mx/Guias/Material_Preparatoria.pptx

¹²⁰ Disponible para su consulta en: <https://sesamo.com/monstruos-en-red/>

¹²¹ Disponible para su consulta en: https://micrositios.inai.org.mx/clic/?page_id=450

¹²² Disponible para su consulta en: <https://micrositios.inai.org.mx/clic/>

¹²³ Disponible para su consulta en: <https://micrositios.inai.org.mx/marcocompetencias/>

¹²⁴ Disponible para su consulta en: <https://micrositios.inai.org.mx/identidadsegura/>

¹²⁵ Disponible para su consulta en: <https://concurso.inai.org.mx/plenoninos/>

¹²⁶ Disponible para su consulta en: http://inicio.inai.org.mx/PublicacionesComiteEditorial/CJ2017_version-elect.pdf



- Concurso Nacional de Trabajo Universitario¹²⁷.
- Concurso “60 segundos para informarme”¹²⁸.
- Concurso Nacional de Spot de Radio en materia de Transparencia, Acceso a la Información y Protección de Datos Personales¹²⁹.
- Concurso de Arte Urbano y Neomuralismo¹³⁰.

Herramientas

- Vulnerómetro. Evita riesgos a tu privacidad¹³¹.
- Cuánto valen tus datos¹³².
- Test: ¿Cómo te proteges en el entorno digital?¹³³
- Memorama de la privacidad¹³⁴.

Publicaciones

- Ina y el Cuervo de Nunca Más¹³⁵.
- Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes. Memorandum de Montevideo¹³⁶.

Protección de la Infancia

La aplicación del principio del interés superior de la niñez sin duda alguna, cobra especial relevancia en materia de protección de datos personales, toda vez que constituyen un sector de la población especialmente vulnerable y expuesto a los riesgos que supone el desarrollo y utilización de las tecnologías de la información y comunicación.

¹²⁷ Disponible para su consulta en: <https://concurso.inai.org.mx/universitario/>

¹²⁸ Disponible para su consulta en: https://concurso.inai.org.mx/snt2021/wp-content/uploads/2021/09/60seg_convocatoria.pdf

¹²⁹ Disponible para su consulta en: <https://concurso.inai.org.mx/spot/>

¹³⁰ Disponible para su consulta en: <http://concurso.inai.org.mx/arturbano/>

¹³¹ Disponible para su consulta en: <https://micrositios.inai.org.mx/vulnerometro/>

¹³² Disponible para su descarga en: <https://play.google.com/store/apps/details?id=com.stick.inaiapp>

¹³³ Disponible para su consulta en:

https://docs.google.com/forms/d/e/1FAIpQLSe39JYTKAMTSLgmO_LrEvvVsuE9zZFeMZZAjosYF09AJIT00A/viewform

¹³⁴ Disponible para su consulta en: [https://ifai-](https://ifai-my.sharepoint.com/personal/erwin_bautista_inai_org_mx/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fferwin%5Fbautista%5Fina%5Fforg%5Ffmx%2Fdocuments%2Fdescargas%20CLIC%20INAI%2FMEMORAMA%20DINAI%2Epdf&parent=%2Fpersonal%2Fferwin%5Fbautista%5Fina%5Fforg%5Ffmx%2Fdocuments%2Fdescargas%20CLIC%20INAI)

[my.sharepoint.com/personal/erwin_bautista_inai_org_mx/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fferwin%5Fbautista%5Fina%5Fforg%5Ffmx%2Fdocuments%2Fdescargas%20CLIC%20INAI%2FMEMORAMA%20DINAI%2Epdf&parent=%2Fpersonal%2Fferwin%5Fbautista%5Fina%5Fforg%5Ffmx%2Fdocuments%2Fdescargas%20CLIC%20INAI](https://ifai-my.sharepoint.com/personal/erwin_bautista_inai_org_mx/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fferwin%5Fbautista%5Fina%5Fforg%5Ffmx%2Fdocuments%2Fdescargas%20CLIC%20INAI%2FMEMORAMA%20DINAI%2Epdf&parent=%2Fpersonal%2Fferwin%5Fbautista%5Fina%5Fforg%5Ffmx%2Fdocuments%2Fdescargas%20CLIC%20INAI)

¹³⁵ Disponible para su consulta en: <http://inicio.inai.org.mx/PublicacionesComiteEditorial/INA.pdf>

¹³⁶ Disponible para su consulta en: <http://inicio.inai.org.mx/Publicaciones/ProteccionRedesSociales.pdf>



En ese sentido, el principio señalado, se constituye tanto en un criterio interpretativo al momento de aplicar la normativa en la materia como en un objetivo claro de política pública que se diseña e implementa desde el ámbito de las atribuciones de este Instituto.

Por tal motivo, el INAI, por conducto de la Secretaría de Protección de Datos Personales, así como de las unidades administrativas adscritas a la misma, atendiendo al ámbito de sus atribuciones, ha implementado distintas acciones destinadas a la protección de los datos personales de este sector de la población, enfocadas en la protección de su privacidad y datos personales para la construcción de un entorno seguro cuando realicen actividades en línea.

Recientemente, una de estas acciones, fue la emisión del Código de buenas prácticas para orientar el tratamiento en línea de datos personales de niñas, niños y adolescentes (Código de buenas prácticas), que toma como referencia la Convención sobre los Derechos del Niño, misma que a nivel internacional reconoce los derechos y libertades que las niñas, niños y adolescentes necesitan en todos los aspectos de su vida para su desarrollo, anteponiendo su interés superior. De igual forma, en el Código se observa lo previsto en el artículo 4, párrafo noveno de la CPEUM, y lo dispuesto en la LGDNNA, en donde se regula lo propio respecto del interés superior de la niñez a nivel nacional.

Asimismo, dicho Código se basa en lo dispuesto en el artículo 16, párrafo segundo de la CPEUM, la LFPDPPP y el RLFPDPPP, la LGPDPSO y sus Lineamientos, en donde se garantiza la protección de los datos personales, integrando los principales estándares que se estima pueden orientar a los responsables, tanto del sector público como del privado, con base en las disposiciones normativas aludidas en el párrafo precedente, respecto de la protección de datos personales de niñas, niños y adolescentes recabados con motivo del diseño, desarrollo y prestación de servicios relacionados con aplicaciones, juegos, juguetes conectados y sitios web a los que es probable que acceda.

Como se ha mencionado anteriormente, el IFT desarrolló el Micrositio de ciberseguridad para usuarios de servicios de telecomunicaciones, el cual contiene un apartado dedicado a madres, padres y personas supervisoras de menores de edad, donde encontrarán datos e información de utilidad para brindar un acompañamiento informado que permita que niñas, niños y adolescentes adopten prácticas seguras en el uso de Internet, servicios, aplicaciones y dispositivos.

Tal es el caso de la sección llamada "*Riesgos en línea*" donde se encuentran diversos materiales que ayudarán a identificar los posibles riesgos que pueden enfrentar los menores de edad cuando realizan actividades en el ciberespacio.



La Guardia Nacional, en la presente administración implementó el “Operativo Salvación”, que consiste en realizar acciones de prevención, capacitación y coordinación entre la Guardia Nacional con la Fiscalía General de la República (FGR) y con las Fiscalías y Procuradurías de las 32 Entidades Federativas, para llevar a cabo la bores de investigación para el combate a la Pornografía Infantil en México y demás conductas antisociales que se cometen a través del Internet, en agravio de niñas, niños y adolescentes, lo que ha permitido la presentación de denuncias ante las autoridades competentes, y en seguimiento a la investigación y a la aportación de la evidencia digital ha permitido la identificación y detención de agresores sexuales y rescate de víctimas menores de edad.

La Guardia Nacional, colabora con diversas agencias policiales internacionales para el intercambio de Información que permite la investigación y prevención de conductas delictivas, por lo que se tiene estrecha colaboración con el Agregaduría de investigaciones de Seguridad interna de Estados Unidos (HSI/ICE), el FBI, INTERPOL, y también se colabora con el Centro Nacional de Niños desaparecidos y Explotados (NCMEC), quien provee información de reportes realizados por las empresas prestadoras de servicios en Internet, sobre usuarios mexicanos que cometen alguna conducta delictiva en línea y que afectan a niñas, niños y adolescentes.

Se tiene colaboración con las empresas prestadoras de servicios y contenidos en Internet, quienes proporcionan información para el seguimiento de los casos de investigación, así mismo se realizan las solicitudes de cancelación o baja de redes sociales, páginas web o plataformas digitales, donde se esté cometiendo la conducta en línea en agravio de niñas, niños y adolescentes.

Sensibilización Nacional

El Instituto, a través de la CGPU, diseña, de manera permanente, diversos mecanismos de información y comunicación, en materia de seguridad en línea para los usuarios de servicios de telecomunicaciones, incluidos niños, niñas y adolescentes y que se han implementado con el objetivo de informar y formar a los usuarios de Internet sobre navegación segura en la red:

Ciber Club IFT

En 2018, el IFT publicó un cómic interactivo, integrado por 6 episodios que tienen como objetivo informar a niños, usuarios de los servicios de telecomunicaciones, sobre diversos conceptos y recomendaciones en materia de ciberseguridad. El cómic está disponible en el microsítio de ciberseguridad para usuarios dentro de la sección Niñas, niños y adolescentes y puede consultarse en video animado, historieta para leer y cuadernillo para colorear.



Conferencias virtuales:

- Conferencia virtual: Mi aventura por el ciberespacio¹³⁷, la cual fue impartida por el joven Mario Ureña García estudiante de nivel bachillerato y asesor en ciberseguridad, quien compartió diversas recomendaciones dirigidas a niñas, niños y adolescentes, mediante una presentación tipo videojuego en la que un personaje llamado Risk se encuentra con algunas dificultades. Esta conferencia fue impartida en el marco de Noviembre Mes de la Usuaría, serie de conferencias web semanales, que se efectuaron en el penúltimo mes del año 2020, con el propósito de presentar información a grupos específicos de usuarios.
- Plática virtual “No te enredes con las redes”¹³⁸ impartida conjuntamente por el IFT y la Policía cibernética de la Secretaría de Seguridad Ciudadana de la Ciudad de México el 29 de abril de 2021. Dicha charla, tuvo como propósito proporcionar información a niñas, niños, adolescentes y sus cuidadores, sobre diversos riesgos que enfrentan los menores de edad en Internet, tales como: *cibergrooming*, *cyberbullying*, *sexting*, entre otros; asimismo se compartió con los asistentes los principios y acciones respecto al uso seguro, responsable de sus dispositivos, servicios y aplicaciones en línea.
- Conferencias de ciberseguridad 2021. El IFT y la Guardia Nacional organizaron esta serie de conferencias virtuales cuyo objetivo fue promover el uso y aprovechamiento de las Tecnologías de la Información y Comunicaciones (TIC) de manera responsable, así como compartir con los usuarios información útil que les permita protegerse ante riesgos, amenazas y ataques cibernéticos. La sesión 2, transmitida el 6 de julio de 2021, estuvo dedicada al tema de ciberseguridad para niñas, niños y adolescentes.¹³⁹

Asimismo, en el portal de Internet del Instituto, se designó una sección especial dentro del rubro de Usuarios y Audiencias, con la finalidad de agrupar la información y materiales didácticos generados en materia de ciberseguridad.

Como actividad continua el Instituto difunde a través de sus redes sociales institucionales, diversos materiales informativos que promueven las recomendaciones de mejores prácticas en materia de ciberseguridad y la protección de información en las redes de telecomunicaciones.

Asimismo, inició dos campañas de difusión “*Ciber Club IFT*” dirigidas a niños y “*Café con @ de Mujer*” dirigida a PyMEs, que tienen como objetivo difundir información focalizada a las necesidades de cada grupo en materia de ciberseguridad.

¹³⁷ Disponible en YouTube: <https://youtu.be/OJNsEQ-Tkm4>

¹³⁸ Disponible en YouTube <https://youtu.be/CikiYxdcH8M>

¹³⁹ Disponible en YouTube <https://youtu.be/nzRP5SnICQI>



Adicionalmente, se han llevado a cabo diversas reuniones de trabajo con instituciones como: Secretaría de Gobernación, Secretaría de Educación Pública, Comisión Nacional para Prevenir y Erradicar la Violencia Contra las Mujeres, Consejo Nacional para Prevenir la Discriminación, Comisión Ejecutiva de Atención a Víctimas, Guardia Nacional, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, SIPINNA, Comisión Nacional de los Derechos Humanos, Secretaría de Comunicaciones y Transportes, Universidad Nacional Autónoma de México, Centro de Investigación especializado en el desarrollo de TIC, entre otras. Lo anterior, con la finalidad de realizar acciones conjuntas para promover la alfabetización de los usuarios y de las organizaciones públicas y privadas, así como fomentar la cultura de la ciberseguridad y el uso seguro del Internet.

Igualmente, el Instituto en colaboración con el Instituto Tecnológico y de Estudios Superiores de Monterrey y la Policía Cibernética de la CDMX, llevó a cabo seminarios y pláticas virtuales que permitieron analizar los retos y oportunidades que la ciberseguridad presenta en el marco de la transformación digital de México y difundir recomendaciones útiles para la ciudadanía.

Por su parte, el INAI, como organismo garante del derecho humano a la protección de datos personales, en el marco de su actuación sobre la promoción y difusión del conocimiento del derecho a la protección de datos personales y su ejercicio entre la sociedad mexicana; actualmente conduce diversos proyectos de sensibilización para las y los titulares de los datos personales, entre ellos la comunidad infantil y adolescentes, con el fin de generar educación cívica en materia de la protección de la información personal desde la corta edad, y contribuir a la formación de una cultura de protección a la privacidad y datos personales entre la población infantil de México. Entre las acciones más relevantes se encuentran: concursos, programas, series, micrositiros informativos e interactivos, cuentos, guías, publicaciones, materiales de apoyo y recomendaciones.

La Guardia Nacional, ofrece oportunidades a los padres y madres de familia, tutores, docentes, cuidadores y a NNA para crear un entorno digital responsable y seguro para su autoprotección. A través de la Jornada de Ciberseguridad “Internet Seguro para Todas y Todos” se impulsan pláticas de sensibilización y concientización, a bordando temas como ciberseguridad para NNA (contenidos nocivos e inapropiados, retos en línea, ciberacoso escolar (cyberbullying), sexting, grooming, pornografía infantil), civismo digital (netiqueta, identidad digital responsable, privacidad en internet y sharenting), ciberseguridad & género (violencia de género y porno venganza); enseñándoles a identificar conductas antisociales e ilícitas, para un uso responsable del Internet; además, involucrando a la ciudadanía en general, dándoles a conocer el rol importante



que juegan en materia de prevención ante amenazas existentes en la red, que ponen en riesgo la integridad de las y los mexicanos, en especial a los NNA.

De forma anual se realiza la Semana Nacional de la Ciberseguridad, en el 2021, se llevó a cabo la 7ma. Edición, en la cual se tiene un día específico con temas de prevención para los NNA, contando con la participación de organismos nacionales e internacionales para el intercambio de conocimientos y estrategias para la protección de la niñez.

El documento denominado “Estrategia IFT 2021- 2025 “Hoja de Ruta”¹⁴⁰ establece en un horizonte de planeación a cinco años, las estrategias y líneas de acción regulatoria (LAR) prioritarias para el IFT, entre las que se encuentran:

- a. Estrategia 3.1 – Promover la seguridad, confianza e innovación para el desarrollo del ecosistema digital;
- b. LAR 3.1.1 - Desarrollar y difundir recomendaciones, lineamientos, disposiciones técnicas y/o buenas prácticas en materia de ciberseguridad;
- c. LAR 3.1.2 - Colaborar con las entidades involucradas en materia de ciberseguridad en el ámbito de las facultades del Instituto, desde una perspectiva colaborativa.

Asimismo, las siguientes acciones también se consideran como prioritarias en la materia:

- Diseño de mecanismos de promoción de cultura de ciberseguridad y alfabetización digital a todos los usuarios, incluidos las niñas, niños y adolescentes.
- Diseñar encuestas en materia de seguridad en línea para conocer de la percepción en materia de ciberseguridad entre usuarios encuestados con dicho propósito.

Como uno de los objetivos del INAI y derechos fundamentales de los cuales se constituye como un organismo garante, se encuentra como prioridad la protección de datos personales de niñas, niños y adolescentes. Para lograr esto, es de suma importancia una adecuada observancia del cumplimiento por parte de los responsables de las obligaciones que derivan de los principios, deberes y derechos rectores de la protección de datos personales, los cuales son: principio de licitud, lealtad, consentimiento, calidad, finalidad, proporcionalidad, responsabilidad e información, así como los deberes de seguridad y confidencialidad, y los derechos de acceso, rectificación, cancelación y oposición.

¹⁴⁰ Disponible para su consulta en: <http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/estrategia20202025acc.pdf>



En el caso particular, considerando que los menores de edad constituyen una población vulnerable, es importante que, como una de las prioridades en el debido cumplimiento de la normatividad en la materia, se destaque lo relativo a la obtención del consentimiento por parte de los responsables para llevar a cabo el tratamiento de datos personales de los titulares, así como apearse a las finalidades para las cuales se recaba dicho consentimiento, máxime cuando el tratamiento que se realice sea en el entorno digital.

Otra de las prioridades a destacar, será la prevención de indebidos tratamientos de datos personales de menores de edad, considerando que se han identificado riesgos relacionados con la protección de sus datos personales en línea, ante el incremento en el uso de Internet, lo que aumenta la posibilidad de ser víctimas de agresiones y ciberacoso.

Datos del 17° Estudio sobre los Hábitos de los Usuarios de Internet en México, de la Asociación de Internet MX 2021, revela que existen 86.8 millones de internautas en México; un 10 por ciento son niñas y niños de entre 6 y 11 años, y un 13.9 por ciento, adolescentes, de 12 a 17 años.

Asimismo, información del Módulo sobre Ciberacoso 2020, publicado por el Instituto Nacional de Geografía y Estadística (INEGI), señala que 21 por ciento de la población usuaria de internet, de 12 años y más, fue víctima de ciberacoso entre octubre de 2019 y noviembre de 2020.

Ante tal escenario, la prevención y la comunicación son herramientas fundamentales para evitar el hostigamiento cibernético y que las niñas, niños y adolescentes conozcan los riesgos que existen en la red si no se utiliza de manera segura cuidando la información personal que proporcionan a los prestadores de dichos servicios.

Finalmente, otra de las prioridades en las que se han enfocado los esfuerzos institucionales, es la creación de una cultura de la protección de datos desde una edad temprana, que permita brindar herramientas para que los menores de edad desarrollen habilidades que les permitan protegerse en línea, por lo que, desde el INAI se han implementado distintas políticas públicas enfocadas en educar en materia de protección de datos personales y sensibilizar a la población objetivo a quien se dirigen para que se salvaguarden sus derechos.

La principal prioridad es la prevención a través de acciones de proximidad social, por lo que la Guardia Nacional promueve una cultura digital responsable en colaboración con aliados estratégicos, entre las que se encuentran las Unidades de Policía Cibernética de las Secretarías de Seguridad Pública y Fiscalías de las entidades federativas, que conforman el Comité de Ciberseguridad de Unidades de Policía Cibernética; también se cuenta con la colaboración de otros aliados de los sectores gubernamentales, privados, académicos y organizaciones nacionales e internacionales.



Dentro de las atribuciones que le son otorgadas al INAI, se encuentran la de elaborar y publicar estudios e investigaciones para difundir y ampliar el conocimiento sobre la materia de protección de datos, así como aquella relativa a proporcionar apoyo técnico a los responsables para el cumplimiento de las obligaciones establecidas en la normatividad respectiva. Lo anterior, ha permitido que se desarrollen herramientas y materiales de facilitación que abarquen diversos enfoques, tales como la protección de los datos de las niñas, niños y adolescentes; la protección de datos personales en línea, así como la sensibilización de los actores involucrados como lo son padres, madres, cuidadores y personal educativo.

Estos materiales y herramientas se desarrollan bajo un esquema didáctico que permite a la sociedad en general una mayor comprensión y entendimiento de los aspectos más relevantes en cuanto a su información personal y la de los menores de edad.

Para muestra de lo anterior, dentro de las distintas actividades realizadas por este Instituto, se puede destacar la emisión del Código de Buenas Prácticas para Orientar el Tratamiento en Línea de Datos Personales de Niñas, Niños y Adolescentes, la cual tiene como objetivo establecer un punto de referencia a través de estándares basados en principios de diseño en tecnología y características prácticas de privacidad, para la protección adecuada de los datos personales de niñas, niños y adolescentes, dirigidos a proveedores de servicios de la sociedad de la información, lo cual comprende servicios en línea. Dicho documento brinda a los proveedores de los servicios de la sociedad de la información, orientación que les permite cumplir y demostrar el debido apego a los principios y deberes relativos a la protección de datos personales previstos en la legislación en materia.

De igual forma, recientemente se puso a disposición de la sociedad el micrositio Aprende y enseña datos personales: Conocimientos y habilidades en protección de datos personales el cual es un recurso para allegarse de información que se requiere para proteger los datos personales y, al mismo tiempo, utilizar con mayor seguridad las tecnologías por parte de las niñas, niños y adolescentes así como cumplir con el objetivo de que profesoras y profesores de educación básica aprendan y transmitan a niñas y niños los conceptos básicos y la normatividad mexicana sobre el derecho a la protección de datos personales y puedan apoyar a crear una cultura sobre este derecho.

Adicionalmente, el INAI ha elaborado distintas herramientas para que los titulares puedan conocer cómo cuidar sus datos personales en el entorno digital como, por ejemplo: Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital, Guía de configuración de privacidad en principales redes sociales y Herramientas o aplicaciones de Supervisión Parental en Internet, las cuales se encuentran disponibles en el portal institucional.



La Guardia Nacional cuenta con la Jornada de Ciberseguridad “Internet Seguro Para Todas y Todos”, donde se crean espacios para la actualización y estudios de la resiliencia de los ciberdelitos, impulsando la promoción de políticas públicas para la protección de los derechos de los NNA en el ciberespacio, obteniendo un impacto favorable en las aplicaciones de las leyes y normas que castigan las conductas antisociales e ilícitas en la red.

Herramientas, Servicios y Ajustes

De acuerdo con una encuesta realizada por la empresa de ciberseguridad Kaspersky en 2020, el 27% de los padres en México rara vez o nunca monitorean lo que hacen los niños en redes sociales, 66% no utiliza el control parental y el 14% ignora si un desconocido ha intentado contactar a los menores a su cargo.

En relación a los esfuerzos emprendidos por el Instituto Federal de Telecomunicaciones y en atención a los mandatos señalados y a las acciones previas que el Instituto ha implementado, el 17 de noviembre de 2021 se publicó el Micrositio de ciberseguridad dirigido a usuarios de servicios de telecomunicaciones, el cual tiene una sección dedicada a padres de familia y personas supervisoras de menores de edad, donde encontrarán datos e información de utilidad para brindar un acompañamiento informado que permita que niñas, niños y adolescentes adopten prácticas seguras en el uso de Internet, servicios, aplicaciones y dispositivos. Las subsecciones que integran este apartado son:

- Riesgos en línea: material destinado a identificar los posibles riesgos que enfrentan los menores de edad en Internet;
- Recomendaciones: en esta sección, los cuidadores de menores de edad podrán encontrar recomendaciones ante las dudas o incidentes que enfrenten niñas, niños y adolescentes en Internet;
- Sitios e información de interés: apartado que presenta contenido informativo sobre seguridad digital para padres y cuidadores, elaboradas por otras instituciones especializadas en el tema;
- Apps y software: subsección que presenta contenido informativo y diversas herramientas de supervisión parental útiles en aplicaciones y servicios digitales, elaboradas por otras instituciones especializadas en el tema.

Adicionalmente, el IFT brinda al público en general diversos materiales para sensibilizar a la población en temas de riesgos en línea, como son los siguientes:



- Sección InF@nTics¹⁴¹. El 28 de abril de 2021, dentro del portal web del Instituto Federal de Telecomunicaciones se publicó la sección InF@nTics, un espacio con contenidos digitales dirigidos al público infantil sobre diversos temas relacionados con las telecomunicaciones y radiodifusión, las tecnologías, la ciberseguridad, así como los derechos que tienen como audiencias y usuarios de telecomunicaciones. Mediante juegos, actividades y materiales informativos se abordan temas de seguridad en el ecosistema digital. Entre los materiales se encuentran la adaptación de cuatro cuentos clásicos de literatura infantil: El Patito feo, Los tres cochinitos, Hansel y Gretel y Caperucita Roja, en los que se desarrollan temas como el ciberbullying o acoso en línea y el grooming o ciberacoso sexual infantil en línea. Con el objetivo de informar sobre la prevención de los riesgos en Internet y generar interés del público en temas relacionados con los sectores regulados y el ecosistema digital.
- Semana de conferencias de Ciberseguridad 2021¹⁴². Del 5 al 9 de julio de 2021, el IFT y la Guardia Nacional llevaron a cabo la semana de conferencias de Ciberseguridad 2021 cuyo objetivo fue brindar al público información útil, consejos y recomendaciones con miras a promover una cultura de ciberseguridad, confianza en uso de plataformas digitales, servicios financieros y el uso seguro y responsable del acceso a Internet, y la confianza en el ecosistema digital. En estas conferencias se abordaron temáticas como: privacidad y protección de datos personales en Internet, ciberseguridad para niñas, niños y adolescentes, y prevención de fraudes en Internet.

El INAI considera fundamental promover desde la infancia el derecho a la protección de los datos personales, sobre todo en el uso de las TIC y las nuevas tecnologías que van surgiendo con el paso del tiempo en donde los menores interactúan con el apoyo de sus madres, padres, educadores y cuidadores.

Para que los individuos puedan ejercer y gozar de su derecho a la protección de su información personal, es necesario que conozcan, primero, sobre la existencia de este derecho y, segundo, sus alcances y contenidos. Además, se requiere que los individuos den valor e importancia a sus datos personales y, en ese sentido, los cuiden y exijan su protección y debido tratamiento por parte de los terceros que los poseen.

En ese sentido, se hace indispensable la actuación de la autoridad garante de este derecho para impulsar el conocimiento del mismo entre la sociedad mexicana y promover su ejercicio, a través del desarrollo de materiales educativos y de fácil acceso, en particular con contenidos didácticos

¹⁴¹ Disponible para su consulta en: <http://www.ift.org.mx/comunicacion-y-medios/infantics>

¹⁴² Disponible para su consulta en: <https://www.gob.mx/gncertmx/articulos/110597>



e interactivos relacionados con el derecho a la protección de datos personales y privacidad, dirigido a la población infantil.

Ante ello, crear un entorno digital seguro para niñas y niños es una responsabilidad compartida, por lo cual, el Instituto continuamente realiza materiales dirigidos al público en general, entre los cuales hay madres y padres de familia, así como educadores y cuidadores, cuyo objetivo es generar conciencia y conocimiento con el fin de educar a la sociedad acerca de la importancia de la protección de datos personales de los menores en línea que constituyen una sinergia para disminuir y prevenir los riesgos que pudieran surgir debido a la inmersión a ciertas tecnologías sin una educación pertinente para hacerlo.

Como ejemplo, el INAI ofrece a madres, padres, cuidadores y personas educadoras las siguientes recomendaciones para evitar el ciberacoso de menores:

- **Supervisión parental.** Involucrarse en el uso que hacen niñas, niños y adolescentes de las redes sociales como una medida de prevención, con respeto a la privacidad y al interés superior del menor.
- **El poder de la red.** Informar a personas menores de edad que la información que se publica en internet se propaga velozmente; por ello, es importante establecer configuraciones de privacidad a fin de controlar quien tiene acceso a su información personal.
- **Límites claros.** La interacción, a través de redes sociales, debe ser con personas conocidas; evitando aceptar como amigos a quienes no se conoce en persona.
- **Cuidar su privacidad.** Fomentar el uso de cuentas privadas en redes sociales. Es importante que no compartan información sensible (imágenes íntimas o comprometedoras, contraseñas, geolocalización, mensajes que pudieran perjudicarles, etcétera).
- **Proteger su dispositivo electrónico.** Fijar una contraseña segura o método de desbloqueo de la pantalla, y establecer configuraciones seguras para aumentar la protección de los menores.
- **Educación digital.** Localizar y analizar recursos existentes como películas, notas informativas, casos reales en los medios de comunicación, que ayuden a orientarles sobre los riesgos que corren en internet, cuando no se toman medidas de seguridad. Los padres, madres y personas educadoras deben estar informados y empoderados para apoyarlos en la protección de sus derechos, respetando sus mejores intereses.



- **Cambios de conducta.** Vigilar cualquier cambio de conducta repentino que no sea común en las y los menores. Muchas de las veces estos cambios pueden estar relacionados en la etapa de la adolescencia; sin embargo, hay que estar alerta de conductas inusuales.
- **Consentimiento.** Consentir el uso de redes sociales y el acceso plataformas de Internet, de acuerdo con su edad y nivel de madurez.
- **Confianza.** Generar espacios que fortalezcan la comunicación entre menores y adultos para facilitar, en su caso, la detección de algún problema.

Acciones como éstas, ayudarán a que niñas, niños y adolescentes estén mejor informados y detecten con mayor facilidad cualquier ataque o acoso en la red.

Asimismo, en razón de que se ha advertido que la situación de vulnerabilidad y necesidades especiales de los menores exige políticas públicas específicas para la protección de su información personal, tanto para fomentar una cultura en la materia, como para reducir los riesgos de un mal uso de sus datos el INAI ha creado el Proyecto “Plaza Sésamo: Monstruos en red”, programa el cual constituye un auxiliar en la formación de buenos hábitos de uso y aprovechamiento de las TIC en donde a través de cápsulas en las que aparecen los personajes de Plaza Sésamo, se busca que las niñas y niños entiendan y hablen de temas como seguridad y autocontrol, para que desde una corta edad tengan esa capacidad crítica, la protección y conceptos básicos para utilizar las tecnologías de la información. Es importante señalar que, como parte de este proyecto existen dos guías que es importante destacar las cuales se dirigen a madres, padres y cuidadores y una específica para educadores.

De manera adicional, se creó el micrositio “Aprende y enseña datos personales: Conocimientos y habilidades en protección de datos personales”, el cual busca reducir la brecha digital, entendido como falta de competencias que permitan obtener un beneficio de las tecnologías, ofreciendo los primeros pasos para que las niñas y niños adquieran habilidades que promueven su uso seguro y provechoso en el entendido de que la educación sobre la seguridad digital fortalece la protección de la infancia.

Además de lo anterior, el INAI ha creado una serie de documentos de facilitación y guías para contribuir a este objetivo, entre las cuales destacan el “Código de Buenas Prácticas para orientar el tratamiento en Línea de Datos Personales de Niñas, Niños y Adolescentes”, “Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital”, “Herramientas o aplicaciones de Supervisión Parental en Internet” y el Micrositio ¡CLIC!, micrositio que busca promover la importancia de la privacidad y la protección de datos personales entre las niñas, niños y adolescentes para que las y los educadores transmitan la información a sus



alumnas y alumnos, con el fin de que se adquieran las habilidades necesarias para ejercer su derecho a la protección de datos personales y, al mismo tiempo, eviten colocarse en una situación, dentro del entorno digital, que pueda comprometer su información personal y ponerlos en riesgo, mismo material que se encuentra a disposición del público en el sitio oficial del INAI.

Asimismo, el Instituto, emitió "Recomendaciones para proteger los datos personales de los menores de edad en las preinscripciones del ciclo escolar 2020-2021" que se realicen a través de Internet, sugiriendo a madres, padres y tutores llevar a cabo las siguientes acciones para proteger los datos de los menores de edad:

- Comprobar que la página web para realizar las preinscripciones comience con <https://> e incluya un candado cerrado en la barra de estado del navegador. Se sugiere teclear la dirección proporcionada por la institución educativa directamente en el navegador.
- Evitar ingresar a sitios web a través de enlaces que se reciben por correo electrónico, aplicaciones de mensajería instantánea o publicaciones en redes sociales. Se sugiere teclear la dirección proporcionada por la institución educativa directamente en el navegador.
- Verificar que los datos personales, especialmente de niñas, niños y adolescentes, compartidos al momento de realizar las preinscripciones sean estrictamente los necesarios para cumplir con la finalidad correspondiente. Además, los datos personales deben estar actualizados y correctos.
- Evitar proporcionar información personal de las niñas, niños y adolescentes a través de redes sociales.
- Revisar la existencia y contenido del Aviso de Privacidad que debe estar disponible en el sitio web de la institución educativa, así como en el portal específico para realizar las preinscripciones.
- Reportar ante el INAI cualquier tratamiento indebido de los datos personales del que se tenga conocimiento.
- Seguir estas recomendaciones evitará que los datos personales de las niñas, niños y adolescentes sean objeto de tratamientos indebidos.

Herramientas o aplicaciones interactivas:

- **Herramientas o aplicaciones de Supervisión Parental en Internet.** Dirigidas a padres y madres de familia, con la finalidad de supervisar y/o limitar el acceso a contenidos de



Internet que sus hijos tienen desde sus dispositivos móviles. dirigidas a padres y madres de familia, con la finalidad de supervisar y/o limitar el acceso a contenidos de Internet que sus hijos tienen desde sus dispositivos móviles. Con estas herramientas los adultos pueden involucrarse de forma positiva en la experiencia y uso de Internet por parte de las y los menores, a través de una supervisión respetuosa de los sitios que visitan y actividades que realizan, a fin de protegerlos y evitar la exposición de sus datos personales.

Disponible para su consulta en: https://home.inai.org.mx/?page_id=3402

- **TEST: ¿Cómo te proteges en el entorno digital?** Es un test interactivo que facilita a los titulares de datos personales identificar los principales riesgos a los que se encuentran expuestos sus datos personales en el entorno digital; casos como alteración, modificación, robo y divulgación no autorizada. Asimismo, permite que identifiquen el nivel de protección que le dan a su información al realizar distintas actividades que involucren el uso de dispositivos electrónicos e Internet. Después de haber contestado el test, en caso de que se identifique la ausencia de medidas de seguridad, se le indica al usuario una recomendación específica sobre lo que puede hacer para proteger sus datos personales.

Disponible para su consulta en:

https://docs.google.com/forms/d/e/1FAIpQLSe39JYTKAMTSLgmO_LrEvvVsuE9zZFeMZ ZAj0sYF09AJIT00A/viewform

- **Vulnerómetro.** Consiste en un cuestionario de veintiocho preguntas, entre las que figuran: ¿olvidas cambiar periódicamente tus contraseñas?; ¿mantienes información personal en tu computadora sin medidas de seguridad para su acceso?; ¿utilizas una conexión inalámbrica sin protección de una contraseña para acceder a internet?; ¿utilizas computadoras de café internet o públicas?, al concluir el cuestionario, la plataforma indica que tan vulnerables son las medidas de la persona para proteger su privacidad.

Disponible para su consulta en: <https://micrositios.inai.org.mx/vulnerometro/>

La Guardia Nacional a través de sus atribuciones conferidas, se realizan acciones de prevención e investigación, como la Jornada de Ciberseguridad “Internet Seguro Para Todas y Todos”, donde se crean espacios para la actualización y estudios de la resiliencia de los Cibercriminales, impulsando la promoción de políticas públicas para la protección de los derechos de los NNA en el ciberespacio, obteniendo un impacto favorable en las aplicaciones de las leyes y normas que castigan las conductas antisociales e ilícitas en la red.



Además, la Guardia Nacional participa en estudios para compartir y reunir datos para análisis en materia de ciberseguridad, como el Estudio de Ciberseguridad AIMX 2021, sobre ciberseguridad en empresas, usuarios de internet y padres de familia en México 2021, publicado en la página de la Asociación de Internet MX.

En materia de capacitación, se generan talleres y cursos como "Formación de Replicadores en Ciberseguridad", "Prevención y Combate de Delitos Cibernéticos" dirigidos a servidores públicos, docentes y público en general; además, se da capacitación a Ministerios Públicos, Magistrados, Peritos, Jueces para que la aplicación de la ley sea pronta y expedita ante los Ciberdelitos.

El "Operativo Salvación", consiste en realizar acciones de prevención, capacitación y coordinación entre la Guardia Nacional con la Fiscalía General de la República (FGR) y con las Fiscalías y Procuradurías de las 32 Entidades Federativas, para llevar a cabo labores de investigación para el combate a la Pornografía Infantil en México, en virtud de sus resultados, fue bien recibido por la comunidad de Interpol, por lo que, en la reunión de la Subcomisión Técnica de Investigación Contra el Ciberdelito celebrada en septiembre de 2021, sus integrantes reconocieron el "Operativo Salvación" como una de las mejores prácticas en Latinoamérica.

Medidas de Accesibilidad

El INAI forma parte del SNT que, con fundamento en el artículo 14, fracción XIII de la LGPDPPSO; tiene la función de promover e implementar acciones para garantizar condiciones de accesibilidad para que los grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.

En la segunda Sesión Ordinaria, celebrada el 13 de abril de 2016 del Consejo Nacional del SNT, se aprobaron los "Criterios para que los sujetos obligados garanticen condiciones de accesibilidad que permitan el ejercicio de los derechos humanos de acceso a la información y protección de datos personales a grupos vulnerables" (en adelante Criterios) que se publicaron en el Diario Oficial de la Federación el 4 de mayo del mismo año.

Los Criterios tienen por objeto establecer los elementos que permitan a los sujetos obligados identificar, implementar y promover acciones para que garanticen la participación e inclusión plena, en equidad e igualdad de condiciones y sin discriminación alguna, en el goce y ejercicio del derecho humano a la protección de los datos personales a los grupos en situación de vulnerabilidad.

Dicha normatividad es obligatoria para el INAI y en ese sentido, se deben implementar las acciones siguientes:



- Asegurar que en la Unidad de Transparencia y en el CAS, donde se asesora el ejercicio del derecho a la protección de datos personales, se cuenten con instalaciones, espacios y mobiliario ideal para que las personas con algún tipo de limitación motriz puedan abrir y cerrar puertas, levantarse y sentarse, asimismo la permanencia y el libre desplazamiento se realicen en condiciones dignas y seguras de las personas con discapacidad.
- Fomentar los procedimientos y requisitos para el ejercicio de la protección de datos personales a través de folletos, trípticos, carteles, audiolibros y otros materiales de divulgación en formatos accesibles.
- Contar con personal capacitado y sensibilizado para orientar a personas que no sepan leer ni escribir, y hablen otra lengua indígena; o contratar con servicios de intérpretes o traductores para facilitar, de manera oportuna, la información solicitada por las y los titulares de los datos personales.
- Realizar adaptaciones en un Portal Web Accesible, que facilite a todas las personas el acceso y el uso de información, bienes y servicios disponibles, independientemente de las limitaciones que tengan quienes accedan a éstas o de las limitaciones derivadas de su entorno, sean físicas, educativas o socioeconómicas, que deberá contener las características siguientes:
 - 1 Que se incorporen lectores de pantalla.
 - 2 Que se cuente con amplificadores de imágenes y lenguaje de señas.
 - 3 Que se utilice contraste de color.
 - 4 Que se proporcione información de contexto y orientación.
 - 5 Que los documentos sean claros y simples.
 - 6 Que se identifique el idioma usado.
 - 7 Que se utilice la navegación guiada por voz.
 - 8 Que se incluya la posibilidad de detener y ocultar las animaciones, lo que representa un apoyo importante también para quienes tienen trastorno de déficit de atención, así como epilepsia u otras discapacidades psíquicas.
 - 9 Que los menús o apartados dinámicos cuenten con suficiente tiempo de traslado, lo que permitirá a cualquier persona con algún tipo de discapacidad encontrar la opción de su preferencia, sin que se oculten las ventanas de opciones por demora en la selección.
 - 10 Que se utilice un lenguaje incluyente en la información y orientación que se difunde.



11 Que se proporcione información desagregada por sexo, edad, situación de vulnerabilidad, grupo y lengua indígena.

Aunado a lo anterior, de acuerdo con el artículo 89 de la LGPDPPSO, el INAI debe garantizar, condiciones de accesibilidad a los titulares que pertenecen a grupos vulnerables para combatir prácticas discriminatorias y que puedan ejercer, en igualdad de circunstancias, su derecho a la protección de dato.

Por lo que, el INAI se encuentra en constante implementación de elementos que permitan garantizar el ejercicio de datos personales a las personas de grupos vulnerables entre los que se encuentran niños que pertenezcan a algún grupo vulnerable o con capacidades diferentes.

Con relación a las medidas de accesibilidad para madres, padres, educadores y cuidadores que pertenezcan a algún grupo vulnerable o con capacidades diferentes, toda vez que la normatividad que ha sido referida resulta aplicable a cualquier persona, por lo que, el Instituto cuenta con la previsión de medidas específicas para titulares que pertenecen a grupos vulnerables que permiten combatir prácticas discriminatorias y que los titulares de los datos puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.

Línea de ayuda

El INAI cuenta con el CAS, cuya función es recibir y responder las consultas que formulen las personas al Instituto, así como también brindar orientación para que la ciudadanía ejerza su derecho a la protección de datos personales, facilitándoles la captura y formulación de las solicitudes para ejercer sus derechos de acceso, rectificación, cancelación u oposición, bien para la interposición de recursos de revisión y/o denuncias en los casos que se considere que sus datos personales fueron vulnerados o utilizados inadecuadamente por parte de responsables del sector público y privado en un ámbito físico o en línea.

La asesoría se brinda por diversos canales de comunicación, ya sea telefónica, presencial, vía correo electrónico o vía correo postal, a través de las siguientes opciones:

- IFAI-Prodatos: <https://www.datospersonales.org.mx/>
- Mediante el número, 800 835 4324 gratuito.
- CAS en la siguiente dirección: Av. Insurgentes Sur 3211, Col. Insurgentes Cuicuilco, Coyoacán, C.P. 04530, Ciudad de México.
- Vía correo electrónico: atencion@inai.org.mx
- 1 Sector privado: verificación@inai.org.mx



2 Sector público: investigayverifica@inai.org.mx

Cuando una institución pública estatal realice un tratamiento indebido de tus datos personales se deberá acudir al Órgano Garante local.

La Guardia Nacional brinda orientación técnica y legal para presentar denuncias ante el Ministerio Público ante un delito cibernético. Se cuentan con los correos electrónicos: cnac@gn.gob.mx, guardia.nacional@gn.gob.mx, para el contacto con la ciudadanía, así como el acercamiento en redes sociales oficiales institucionales y con el número 088 del Centro Nacional de Atención Ciudadana de la Guardia Nacional.

El Centro de Respuesta a Incidentes Cibernéticos (CERT-MX) de la Guardia Nacional impulsa el sitio web <https://www.gob.mx/gncertmx>, con el objetivo de brindar recomendaciones de ciberseguridad, eventos próximos y anteriores, guías de ciberseguridad, alertas de seguridad informática y boletines de vulnerabilidades, también cuenta con un apartado que promueve la denuncia ciudadana de Ciberdelitos e informa los datos de contacto ciudadano de la Guardia Nacional.

Se generan recomendaciones preventivas en materia de ciberseguridad, impulsadas con el hashtag [#InternetSeguroParaTodasYTodos](#), las cuales son difundidas en las redes sociales oficiales de la Guardia Nacional, en el micrositio del CERT-MX y micrositios de aliados estratégicos como el Instituto Federal de Telecomunicaciones (IFT) <https://ciberseguridad.ift.org.mx/>, así como su difusión a través de la Red Interinstitucional de la Guardia Nacional: Vinculación y Proximidad Social para la Prevención en Ciberseguridad.

Adhesión al Convenio de Budapest

México es solo observador del convenio de Budapest, pero aún no ha firmado dicho pacto internacional.

Cabe mencionar que el micrositio de ciberseguridad para usuarios cuenta con un apartado denominado Reporte Ciudadano en el que los usuarios pueden acceder a un directorio con los contactos de las policías cibernéticas adscritas a los Estados de la República Mexicana, y con ello, recibir asesoría o reportar los incidentes cibernéticos que presenten durante su navegación en internet.

La Guardia Nacional y las Unidades de Policía Cibernética del país, atienden este tipo de situaciones.



PARAGUAY

Índice de siglas del capítulo

BID	Banco Interamericano de Desarrollo
CODENI	Consejerías Municipales por los Derechos del Niño, la Niña y el Adolescente
CONATEL	Comisión Nacional de Telecomunicaciones
ISP	Proveedor de Servicios de Internet
MINNA	Ministerio de la Niñez y la Adolescencia
MITIC	Ministerio de Tecnología de la Información y las Comunicaciones
ONAI	Observatorio Nacional para la Protección de los Derechos de Niños, Niñas y Adolescentes en Internet
POLNA	Política Nacional
SNNA	Secretaría Nacional de la Niñez y la Adolescencia
SNPP	Sistema de Protección y Promoción Integral de los Derechos del Niño, la Niña y el Adolescente
TICs	Tecnologías de la Información y Comunicación



Política Nacional Digital

El Gobierno Nacional tiene como eje prioritario el impulso del Plan Nacional de Tecnologías de Información y Comunicación, como estrategia de transformación digital y modernización del Estado en beneficio de toda la sociedad.

La Agenda Digital es, por tanto, el **Plan de Acción de la Estrategia de Transformación Digital**.

De la misma participan instituciones públicas y sectores (empresarial, academia, sociedad civil) y está articulada con diferentes planes y programas, entre ellos, el Programa de Apoyo a la Agenda Digital.

El Programa de Apoyo a la Agenda Digital, es una iniciativa llevada adelante por el Ministerio de Tecnologías de la Información y Comunicación, con préstamo del BID.

Este Programa apoyará las transformaciones sustanciales de los ejes priorizados en la estrategia nacional.

El Programa de Agenda Digital¹⁴³ nos permitirá dar grandes saltos en la ruta hacia la Transformación Digital de Paraguay, pues impulsará:

- Un Gobierno cercano, abierto, transparente, que centra sus servicios en las personas; La economía digital con la adopción de tecnologías en las empresas;
- El fomento de emprendimientos digitales y la formación de trabajadores con conocimientos tecnológicos;
- La conectividad de todos y todas a redes de alta velocidad y asegurando la prestación de servicios de telecomunicación de calidad y accesibles a la población, que nos permita reducir la brecha digital;
- El fortalecimiento del marco de gestión y la capacidad de operación de las instituciones del Estado con la incorporación y aprovechamiento de tecnologías de información y comunicación.

“*Plan de Acción País 2017 — 2021*”, que incorpora la temática del fortalecimiento del marco jurídico en materia de acoso en línea y determina responsabilidades por medio de la gestión del Ministerio Público para la investigación de casos y del Ministerio de Salud Pública y Bienestar Social en la atención a las víctimas, con el apoyo del Ministerio de la Niñez y la Adolescencia.

¹⁴³ Agenda digital <https://www.mitic.gov.py/agenda-digital/que-es>



Asimismo, dicho Plan establece un compromiso multisectorial, que incluye a la industria, implementado para la colaboración en la alerta, bloqueo, remoción y denuncia de contenidos existentes en internet de explotación y abuso sexual de niñas, niños y adolescentes¹⁴⁴.

Se tiene previsto desarrollar un GOBIERNO DIGITAL, que permita ser más eficientes en la atención al ciudadano, ahorrando tiempo y dinero, tanto del Estado como de las personas. Gracias a la conexión entre instituciones, habrá una base de datos única de los ciudadanos, que disminuirá la burocracia.

Se desarrollarán nuevas normativas a través del análisis de los trámites más demandados por los ciudadanos, para digitalizarlos y simplificarlos. La digitalización de trámites implicará que los ciudadanos realicen sus trámites a tiempo convenientes, teniendo a su disposición más de 100 trámites digitales sin necesidad de trasladarse y desde cualquier dispositivo. Esto ayudará a aumentar la transparencia en la gestión de las instituciones del Estado y generará importantes ahorros de tiempo y dinero para el Estado y los ciudadanos.

Por otro lado, mencionamos que las políticas nacionales digitales sobre TIC se hallan dentro de la órbita de competencia del Ministerio de Tecnología de la Información y las Comunicaciones (MITIC), por tanto, se sugiere requerir el apoyo de dicha cartera de Estado para evacuar este punto.

En lo que se ha podido visualizar del marco normativo y las políticas de tecnología de la información y la comunicación disponible en la página web del MITIC no se verifica que exista un enfoque específico de protección enfocado en los derechos del niño. Sin embargo, se sugiere requerir información a este respecto al MITIC. En caso de no contemplarse el enfoque de protección especial de los derechos del Niño, se sugiere iniciar acciones con miras a dicho propósito con el MITIC.

Marco Normativo/Marco Reglamentario

La Constitución Nacional en su artículo 54 De los Derechos del niño, encomienda a la familia, a la sociedad y al Estado, el deber de garantizar a1 niño su desarrollo armónico e integral, así como la obligación de protegerlo contra la violencia, el abuso, el tráfico y la explotación, determinando que en caso de conflicto los derechos del niño tienen carácter prevaleciente.

¹⁴⁴ Paraguay y la protección de la niñez contra el abuso y todas formas de violencia:
https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/regions/paraguay_global_partnership_-_plan_pais_imprimir.pdf



De igual modo el Artículo 27 de la carta magna contempla lo referido a los medios de comunicación masiva, determinando que la ley regulará la publicidad a los efectos de la mejor protección del niño, del analfabeto, del consumidor y de la mujer.

Resulta conveniente referirse asimismo a la Convención sobre los Derechos del Niño, aprobada por Ley N° 57/90, la cual incorpora el principio del interés superior del Niño por el cual las autoridades estatales que intervengan en asuntos relacionados con los niños deben adoptar las medidas más adecuadas que garanticen su bienestar general, estableciendo así mismo el compromiso de los Estados de respetar y promover el derecho a la vida, la supervivencia, el desarrollo integral y la protección contra la violencia, incluida la intervención judicial según corresponda.

Como es sabido, tanto la ley fundamental de la Nación como la Convención sobre los Derechos del Niño, entraron en vigencia con anterioridad al desarrollo y utilización extendida de las tecnologías de la información y las comunicaciones, sobre todo del uso masivo de internet, por tanto, no determinan regulaciones específicas sobre la materia abordada; sirviendo sin embargo como un marco jurídico general y conceptual de relevancia sustantiva para resaltar el carácter primordial que la sociedad jurídicamente organizada confiere a los derechos del niño, por lo que sus preceptos — aunque generales — imponen el deber de protección estatal y respeto de la sociedad toda.

El uso extendido de internet, ha facilitado el acceso a información, posibilitando una multiplicidad de aplicaciones de maneras insospechadas, sin embargo el contacto de esta herramienta digital con los niños, niñas y adolescentes puede constituirse en un factor de riesgo que merece la atención de los Estados, los cuales se ven en la necesidad de incorporar nuevas legislaciones con la finalidad de protegerlos de peligros tales como el ser contactados o abordados por adultos con fines extorsivos y para la comisión de hechos punibles contra su integridad física, psíquica y moral, el uso de la imagen de los niños como material pornográfico, así como el acceso de los niños a contenido potencialmente perjudicial para su desarrollo integral entre otros.

En este aspecto cabe señalar la vigencia de la Ley N° 6002/2017 “QUE MODIFICA EL ARTÍCULO 135 DE LA LEY N° 1160/97 “CÓDIGO PENAL”, MODIFICADO POR EL ARTÍCULO 1º DE LA LEY N° 3440/08 “QUE MODIFICA VARIAS DISPOSICIONES DE

LA LEY N° 1160/97 “CÓDIGO PENAL”, y que en su parte pertinente establece: Art. 135 b) Abuso por medios tecnológicos:

“El que por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, solicite o exija de cualquier modo a un niño o niña que



realice actos sexuales o que le envíe imágenes de sí misma con contenido sexual, será castigado con pena privativa de libertad de hasta tres años. Será castigada también la tentativa”.

Asimismo, por Ley Nº 5653/2016 de “PROTECCIÓN DE NIÑOS, NIÑAS Y ADOLESCENTES CONTRA CONTENIDOS NOCIVOS DE INTERNET”, se puso en vigencia una normativa dirigida a proteger de una manera integral al niño, niña y adolescente frente, a los efectos que pudieran generar en ellos los contenidos nocivos a que tengan acceso o se encuentren en internet.

La norma prevé la obligación a los proveedores de servicios de internet de suministrar en forma gratuita a todos sus clientes un software de protección con un manual de instrucciones sobre su instalación.

La Ley N° 5653/2016, establece asimismo mecanismos de fiscalización y aplicación de sanciones por su incumplimiento, además de crear un cuerpo colegiado intersectorial denominado Observatorio Nacional para la Protección de los Derechos de Niños, Niñas y Adolescentes en Internet (ONAI), integrado por organismos y entidades estatales y con la participación de la sociedad civil. Las funciones principales del ONAI son: monitorear los contenidos que circulan en Internet y realizar informes públicos sobre el cumplimiento de la presente Ley; elaborar y actualizar permanentemente el Banco Digital de Sitios y Contenidos Impropios para la Niñez y la Adolescencia, para la consulta de prestadores de servicios de internet (ISP) y público en general; recibir denuncias sobre prestadores de servicios de internet (ISP) y establecimientos o instituciones de todo tipo que no cumplan con lo dispuesto en la presente Ley y remitir las mismas a las autoridades de aplicación competentes; y asesorar a otras instancias del Estado o de la sociedad civil o sector privado en materia de protección y promoción de contenidos para niños, niñas y adolescentes en internet, entre otras.

La citada ley, en su artículo 6, designa a la Comisión Nacional de Telecomunicaciones (CONATEL) como autoridad de aplicación competente para controlar el cumplimiento de las obligaciones establecidas en la ley por parte de las empresas proveedoras de internet.

Por tanto, la normativa actualmente vigente, en materia de protección infantil en línea cubre los aspectos de la sanción penal contra quienes realicen actos impropios contra niños, niñas y adolescentes por medios telemáticos y la protección de niños, niñas y adolescentes ante los contenidos nocivos para su desarrollo integral a los que pudieran tener acceso por medio de internet.

El Código de la Niñez y la Adolescencia, aprobado por la Ley N° 1.680/2001 es la norma con rango de ley, específica que aborda los derechos del niño, además de crear el Sistema de



Protección y Promoción Integral de los Derechos del Niño, la Niña y el Adolescente (SNPPI), correspondiente al ámbito administrativo y el Sistema de Administración de Justicia Especializado relativo a los órganos jurisdiccionales competentes en materia de Niñez y Adolescencia.

Seguidamente se citan a modo de ejemplo, otras normas de rango legal con enfoque específico en los derechos del niño.

- Ley N° 983/96 Que ratifica el Convenio de la Haya sobre Aspectos Civiles de la Sustracción Internacional de menores.
- Ley N° 1062/1997 Que aprueba la Convención Interamericana sobre tráfico internacional de menores.
- Ley N° 1377/1999 Que dispone la expedición gratuita del certificado de nacimiento y de la cédula de identidad.
- Ley Nº 3977/2010 Que aprueba la Convención Internacional para la Protección de todas las personas contra las Desapariciones Forzosas.
- Ley N° 1657/01 Aprueba el Convenio N° 182 y la Recomendación sobre las peores formas de trabajo infantil.
- Ley N° 2332/03 Que aprueba el Convenio N° 138 de la OIT sobre la edad mínima de admisión a1 empleo.
- Ley Nº 2169/03 Que establece la mayoría de edad.
- Ley N° 2134/2003 Aprueba el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de Niños en la Pornografía”.
- Ley N° 2718/2005 Que prohíbe la venta, suministro y/o distribución de productos que contengan solventes orgánicos a menores de edad.
- Ley Nº 2861/2006 Que reprime el comercio y la difusión comercial o no comercial de material pornográfico, utilizando la imagen u otra representación de menores o incapaces.
- Ley Nº 4788/2012 Integral contra la trata de personas.
- Ley Nº 4698/2012 De Garantía Nutricional en la Primera Infancia.
- Ley N° 4633/2012 Contra el acoso escolar en instituciones educativas Públicas, Privadas o Privadas Subvencionadas.
- Ley N° 5508/15 Promoción, Protección de la Maternidad y Apoyo a la Lactancia Materna.



- Ley N° 6174/2018 Que eleva al rango de Ministerio, a la Secretaría Nacional de la Niñez y la Adolescencia (SNNA) y pasa a denominarse Ministerio de la Niñez y la Adolescencia (MINNA).
- Ley N° 6486/2020 De Promoción y Protección del Derecho de Niños, niñas y adolescentes a vivir en familia, que regula las medidas de cuidados alternativos y la Adopción.
- Ley N° 6572/20 20 Que crea el Registro Nacional de Agresores Sexuales de Niños, Niñas y Adolescentes y el Banco Genético.
- Ley N° 6068/18 Que aprueba el Convenio de la Haya, del 19 de octubre de 1996, relativo a la competencia, la ley aplicable, el reconocimiento, la ejecución y la cooperación en materia de responsabilidad parental y de medidas de protección de los niños.

Según ha sido posible verificar desde la Dirección General de Asesoría Jurídica, la Ley N° 5653/2016 de “PROTECCIÓN DE NIÑOS, NIÑAS Y ADOLESCENTES CONTRA CONTENIDOS NOCIVOS DE INTERNET”, es actualmente la norma más importante que expresa la voluntad política de dar prioridad a la protección infantil en línea en la República del Paraguay.

Notificaciones-contenido ilícito / Notificaciones-preocupaciones de los usuarios

Actualmente se cuenta con una Línea de Atención Telefónica Gratuita denominada **FONOAYUDA 147** que se encuentra disponible para que los niños, niñas y adolescentes, sus padres, encargados de su cuidado y educación requieran orientación sobre el modo de proceder ante casos que pudieran significar la violación de derechos de niños, niñas y adolescentes, incluidas aquellas vulneraciones perpetradas por medios telemáticos. En ocasiones y según corresponda esta línea de atención se constituye en boca de entrada de denuncias, las cuales son derivadas a la institución competente (CODENI/Sistema de Administración de Justicia Especializada/Ministerio Público etc.), conforme a la situación denunciada.

Del mismo modo, se prevé habilitar en la Página Web del Ministerio de la Niñez y la Adolescencia una ventana de recepción de denuncias sobre incumplimiento de la Ley N° 5356/16 atribuible a Proveedoras de Servicios de Internet y propietarios o encargados de espacios públicos que se encuentran obligados a poner a disposición del público, softwares de protección, en el marco de dicha norma.

Actores y partes interesadas

El Ministerio de la Niñez y la Adolescencia es el ente rector de políticas públicas destinadas a la promoción y protección de los derechos de la Niñez y la Adolescencia, conforme a la Ley N° 6174/2018. Esta cartera de Estado en coordinación con los organismos que conforman el Sistema



Nacional de protección y Promoción Integral de Derechos de la Niñez y la Adolescencia (SNPPI) ejercen las funciones de protección por medio de campañas de concienciación tendientes a la prevención de situaciones de vulneración de derechos. Estas acciones son desarrolladas en articulación con otras instituciones estatales como el Ministerio de Educación y Ciencias, el Ministerio de Tecnologías de la Información y la Comunicación — MITIC, las Consejerías Municipales por los Derechos de los Niños, Niñas y Adolescentes — CODENI y organizaciones de la sociedad civil que trabajan la temática, entre otras.

Es parte importante de las campañas de concienciación la difusión acerca de la denuncia oportuna ante las autoridades competentes que son aquellas señaladas en el artículo 5º de la Ley N° 1680/2001 “Código de la Niñez y la Adolescencia, modificada por la Ley 6486/2020.

El Observatorio Nacional para la Protección de los Derechos de Niños, Niñas y Adolescentes en Internet (ONAI), creado por la Ley N° 5356/16, tiene asimismo designadas, facultades para recibir denuncias de transgresiones a la normativa que exige el filtrado de internet destinado a niños, niñas y adolescentes y poner a conocimiento de las autoridades competentes, según dicha norma.

En tanto, la comisión de hechos punibles contra niños, niñas y adolescentes cometidos por medio de herramientas digitales da lugar a la intervención de instituciones del sistema de administración de justicia y sus auxiliares (Ministerio Público a través de la Unidad Especializada en delitos informáticos y Unidad de Trata de Personas, Juzgados Penales, Juzgados de la Niñez y la Adolescencia, Ministerio de la Defensa Pública y Policía Nacional), tanto en lo concerniente a la investigación y sanción a los responsables como en relación a las medidas de protección que resulten necesarias para asegurar el bienestar del niño.

Como otras organizaciones de protección de la infancia en línea se identifican:

- Fundación On Line
- Paraguay Ciber Seguro

Alianzas Nacionales e Internacionales (sector público y sector privado)

Por medio de la participación en espacios de trabajo sobre la materia y la articulación intersectorial con miras al cumplimiento de la Ley N° 5356/16 y otras normas y políticas públicas sobre la materia.



Investigación

El Observatorio TICs del Ministerio de Tecnologías de la Información y Comunicación¹⁴⁵, tiene diversas publicaciones basadas en encuestas e investigaciones sobre conectividad, uso de TIC de adolescentes, entre otras.

Educación en Materia de alfabetización y competencias digitales

Si la alfabetización digital (el aprendizaje de las herramientas digitales) ya era importante, se volvió urgente con la pandemia de COVID-19. La migración de las actividades de la modalidad presencial a la virtual ha acelerado la necesidad de acceder y manejar correctamente las tecnologías de la información y comunicación (TIC).

Como una respuesta a esa necesidad nació *EmpoderaTECH*¹⁴⁶, una guía para el empoderamiento digital de mujeres adultas que se replicará en talleres sobre el uso de las tecnologías requeridas hoy para la comunicación con otras personas y con organizaciones, así como para la gestión de datos personales y el acceso a herramientas tecnológicas.

EmpoderaTECH se convierte en una herramienta clave para la inclusión social y es el resultado de un trabajo mancomunado, impulsado por el Ministerio de la Mujer a través del Programa Ciudad Mujer, con el apoyo del Banco Interamericano de Desarrollo (BID), e implementado por Paraguay Educa.

Recursos educativos

El Ministerio de Tecnologías de la Información y Comunicación (MITIC) ofrece mensualmente de manera gratuita una serie de cursos presenciales y en línea que apuntan a desarrollar la economía digital.

Se busca aumentar el conocimiento sobre temáticas clave, siendo un punto de contacto e intercambio en el cual adquirir y compartir experiencias, recursos, capacitación y soporte para la implementación de iniciativas y proyectos en entornos digitales (catálogo nacional decursos en línea gratuitos)¹⁴⁷.

Protección de la Infancia

En materia de políticas públicas aprobadas por el Consejo Nacional de Niñez y Adolescente POLNA que aborda los asuntos propios de la infancia desde la perspectiva de la doctrina de la

¹⁴⁵ Observatorio TICs del Ministerio de Tecnologías de la Información <https://www.senatics.gov.py/observatorio/publicaciones>

¹⁴⁶ Guía de alfabetización digital EmpoderaTECH: <https://www.mtess.gov.py/noticias/guia-de-alfabetizacion-digital-empoderatech-abre-opportunidades-mujeres-adultas>

¹⁴⁷ Catálogo nacional decursos en línea gratuitos: <https://www.cursos.gov.py/portada>



protección integral, con líneas de acción que siguen especialmente los principios del interés superior del Niño; el de igualdad y no discriminación; supervivencia y desarrollo y el de la participación, con énfasis en el acceso a la identidad, la salud, la educación y la protección contra actividades peligrosas. No se verifica aún en este instrumento referencia directa a la seguridad en línea.

En cambio, el Plan de Acción País 2017 — 2021 ya incorpora la temática del fortalecimiento del marco jurídico en materia de acoso en línea y determina responsabilidades por medio de la gestión del Ministerio Público para la investigación de casos y del Ministerio de Salud Pública y Bienestar Social en la atención a las víctimas, con el apoyo del Ministerio de la Niñez y la Adolescencia.

En igual sentido este Plan establece acciones a ser desarrolladas por el Ministerio de la Niñez y la Adolescencia, con apoyo del Ministerio de Educación y Ciencias, las Gobernaciones y Municipalidades consistentes en capacitación a niñas, niños y adolescentes, familias, recursos humanos de instituciones integrantes del Sistema Nacional de protección, organizaciones de la sociedad civil, organizaciones basadas en la fe, formadores de opinión (periodistas y comunicadores) y el sector privado sobre prevención e identificación de situaciones de acoso escolar, ciber acoso y violencia.

Este documento también prevé además acciones para obtener el compromiso multisectorial para la colaboración en la alerta, bloqueo, remoción y denuncia de contenidos existentes en internet de explotación y abuso sexual de niñas, niños y adolescentes.

Estos datos podrían ser completados con información disponible en el Viceministerio de Planificación, Planes y Programas del Ministerio de la Niñez y la Adolescencia, respecto al Plan Nacional de Niñez y Adolescencia, el cual se halla en construcción y el modo en que este instrumento incorpora la temática de la seguridad en línea para niños, niñas y adolescentes.

En materia de protección contra contenidos nocivos considera prioridades actualmente los siguientes:

- Conseguir en la brevedad el dictado del Decreto del Poder Ejecutivo que reglamente la Ley N° 5356/2016, sobre todo para hacer efectivo el filtrado de contenidos.
- Crear el Banco Digital de Sitios y Contenidos impropios para la Niñez y la Adolescencia por medio del Observatorio Nacional para la Protección de los Derechos de la Niñez y la Adolescencia en Internet - ONAI.



- Realizar campañas de concientización sobre el uso adecuado de las herramientas digitales y la seguridad en línea.

La manera de apoyar la seguridad en línea es a través de la participación en adolescencia en Internet — ONAI y en la redacción de las propuestas de reglamentación en esta materia.

Sensibilización Nacional

En los últimos años han sido desarrolladas campañas comunicacionales sobre seguridad en línea por parte del Ministerio de la Niñez y la Adolescencia con la colaboración de otros organismos del Estado y de la sociedad civil, la educación en este aspecto aún se percibe como insuficiente. En ese sentido, la concreción de la reglamentación de la Ley N° 5356/2016 y la correspondiente difusión de la disponibilidad del uso de softwares de protección en línea se presenta como una magnífica oportunidad para ampliar el conocimiento de las personas sobre el uso seguro de internet con miras a la mejor protección de los niños, niñas y adolescentes.

Herramientas, Servicios y Ajustes

El proceso de reglamentación de la Ley N° 5356/16 “DE PROTECCIÓN DE NIÑOS, NIÑAS Y ADOLESCENTES CONTRA LOS CONTENIDOS NOCIVOS DE INTERNET, se halla en estado avanzado de concreción, lo que permitirá que los operadores suministren herramientas de detección y filtrado de contenidos nocivos a los padres o encargados de niños, niñas y adolescentes.

Se cuenta con un marco normativo, la mencionada Ley N° 5356/16, que establece competencias a diversas entidades estatales para la protección de niños ante los contenidos en línea y crea un organismo intersectorial constituido por instituciones públicas, con posibilidad de incluir al sector privado para el abordaje de este tema.

Medidas de Accesibilidad

No se tiene información de la que se advierte que cuentan con dichas medidas.

Línea de ayuda

Fono Ayuda 147 ¿Qué es Fono Ayuda? Es un servicio de atención y orientación telefónica para situaciones que involucren a niñas, niños y adolescentes, especializado en brindar orientación psicológica, social y legal en casos que se presenten vulneraciones de derechos tales como: maltrato, abuso sexual, explotación sexual, negligencia, entre otras, además de responder a temas de intereses genuinos de las niñas, niños y adolescentes. Actualmente el servicio Fono Ayuda cuenta con otras herramientas para reportes tales como una aplicación para celulares con



sistema operativo Android “Fono Ayuda”, de descarga gratuita a través de la aplicación Play Store y una Fan Page en la red social Facebook con el nombre “Fono Ayuda línea 147¹⁴⁸”.

Los funcionarios del Servicio de Atención Telefónica 147 FONOAYUDA se hallan preparados para orientar al público sobre las diversas vulneraciones a los derechos de los niños, niñas y adolescentes, incluido aquellas que se realizan por internet.

Adhesión al Convenio de Budapest

El 20 de diciembre del 2017, a través de la Ley 5994/17, el **Paraguay** se adhirió oficialmente al **Convenio** sobre Ciberdelito del Consejo de Europa.

Conforme a las disposiciones del Código de la Niñez y la Adolescencia y la Ley N° 6174/2018, el Ministerio de la Niñez y la Adolescencia no tiene establecidas competencias para atención de víctimas ningún tipo de vulneración, siendo tal función competencia del Ministerio de Salud Pública y Bienestar Social, en cumplimiento de órdenes emanadas del Sistema de Administración de Justicia Especializado.

¹⁴⁸ <https://www.paraguay.gov.py/oe/minna/491>



PERÚ

Índice de siglas del capítulo

CAD	Centros de Acceso Digital
DIVINDAT	Dirección de Delitos Informáticos
INEI	Instituto Nacional de Estadística e Informática
INICTEL-UNI	Instituto Nacional de Investigación y Capacitación de Telecomunicaciones de la Universidad Nacional de Ingeniería
MIMP	Ministerio de la Mujer y Poblaciones Vulnerables
MINEDU	Ministerio de Educación
MININTER	Ministerio del Interior
MTC	Ministerio de Transportes y Comunicaciones
ODS	Objetivos de Desarrollo Sostenible
OIT	Organización Internacional del Trabajo
OSIPTEL	Organismo Supervisor de Inversión Privada en Telecomunicaciones
PNAIA	Plan Nacional de Acción por la Infancia y la Adolescencia
RCPI	Red Peruana contra la Pornografía Infantil
TIC	Tecnologías de la Información y Comunicación



Política Nacional Digital

Perú no cuenta con una estrategia digital nacional; sin embargo, actualmente se encuentra en proceso de elaboración la Política Nacional de Transformación digital a cargo de la Secretaria de Gobierno y Transformación Digital y la Política Nacional de Telecomunicaciones con enfoque en Internet de Banda Ancha a cargo del Ministerio de Transportes y Comunicaciones.

No obstante, lo anterior, el Perú, dentro de las políticas de Estado del Acuerdo Nacional, contempla un conjunto de medidas elaboradas y aprobadas sobre la base del diálogo y la construcción de consensos, con el fin de definir un rumbo para el desarrollo sostenible del país.

Las políticas de Estado están agrupadas en cuatro grandes objetivos:

- 1 Fortalecimiento de la: Democracia y Estado de Derecho.
- 2 Desarrollo con: Equidad y Justicia Social.
- 3 Promoción de la: Competitividad del país.
- 4 Afirmación de un: Estado eficiente, Transparente y Descentralizado.

En este último objetivo, se contempla la Política N°35 denominada Sociedad de la información y sociedad del conocimiento, aprobada el 16 de agosto del 2017, en la cual se indica:

“Nos comprometemos a impulsar una sociedad de la información hacia una sociedad del conocimiento orientada al desarrollo humano integral y sostenible, en base al ejercicio pleno de las libertades y derechos de las personas, y capaz de identificar, producir, transformar, utilizar y difundir información en todas las dimensiones humanas incluyendo la dimensión ambiental”¹⁴⁹.

En el marco de políticas de TIC, no se advierte que el Perú cuente con un enfoque específico en los derechos del niño y ciberseguridad; sin embargo, se ha desarrollado un marco normativo orientado a la protección del menor en línea y un código del niño y el adolescente que vela por sus derechos, es decir, que si se cuenta con un conjunto de normativas dispersas relacionadas al tema.

Marco Normativo/Marco Reglamentario

Respecto al marco normativo se ha desarrollado la siguiente regulación:

¹⁴⁹ <https://www.acuerdonacional.pe/politicas-de-estado-del-acuerdo-nacional/politicas-de-estado%e2%80%8b/politicas-de-estado-castellano/iv-estado-eficiente-transparente-y-descentralizado/35-sociedad-de-la-informacion-y-sociedad-del-conocimiento/>



- La Ley N° 30096 “Ley de delitos informáticos”, modificada por la Ley N° 30171, sanciona las *“proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos”*¹⁵⁰.
- Ley de delitos informáticos que incluye y establece penas sobre Delitos contra la indemnidad y libertad sexual en relación con Propositiones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.
- Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niñas y Adolescentes y su reglamento.

Asimismo, Perú es parte del Convenio sobre Ciberdelincuencia (Budapest) que fue ratificado mediante D. S N° 010 – 2019 – RE. Que cuenta con el título 3 y Artículo 9 sobre Delitos relacionados con la pornografía infantil.

En materia de protección infantil en línea, no se ha emitido una norma específica; existen normas generales sobre entorno digital, como es el caso del Decreto Supremo 018-2018-PCM, el cual define a la Seguridad Digital como el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno.

- La Ley N° 30096 – Ley de delitos informáticos, ha contemplado la figura de las proposiciones por medios tecnológicos:

“Artículo 5.- Propositiones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal”.

¹⁵⁰ Pautas para una investigación fiscal especializada

<https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf>



Entre las principales normas relacionadas con los derechos del niño se encuentran:

1. LEY N° 27337 que aprueba el Código del niño y del adolescente, en concordancia con la Convención sobre los Derechos del Niño. (No incluye aspectos normativos respecto a la Protección Infantil en Línea).
2. Política Nacional Multisectorial para las Niñas, Niños y Adolescentes al 2030.
3. Plan Nacional de Acción por la Infancia y la Adolescencia 2012-2021.
4. La Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niñas y Adolescentes y su reglamento.

Asimismo, se estipula el acceso universal al conocimiento a través de las Tecnologías de la Información y Comunicación (TIC), acompañado de la generación de contenidos, servicios y bienes digitales, así como del desarrollo de capacidades para que todos los peruanos puedan desempeñarse plenamente y de manera segura en el entorno digital. De igual manera, también se promueve mecanismos que fortalezcan el acceso, conectividad y su uso en las regiones del país.

Con este objetivo el Estado, entre otros puntos, busca fomentar el pleno ejercicio y respeto de los Derechos Humanos en todo entorno digital y diseñar las políticas y la regulación en materia de sociedad de la información y del conocimiento teniendo como base los principios de internet libre, abierto, neutro y para todos, así como el adecuado resguardo de la seguridad de la información, entre otros aspectos.

De manera oficial no hay una Estrategia Nacional de Seguridad Digital. Sin embargo, durante el 2018, el Congreso de la República trabajó un proyecto de Ley de Ciberseguridad donde se define la seguridad digital y los derechos ciudadanos en el ejercicio de este campo, comunicación de incidentes, gestión de la ciberseguridad en el sector público y privado y el fomento de la cultura de la ciberseguridad, entre los puntos resaltantes del citado proyecto.

En septiembre del 2019, esta propuesta fue observada por el Ejecutivo y organizaciones civiles, tanto en la forma como en algunos temas de fondo. Por este motivo volvió al Congreso para su revisión. Cabe precisar que, en forma paralela, se presentó un proyecto de Ley de Ciberdefensa, la cual fue promulgada como Ley 309999¹⁵¹, la cual es aplicable a las fuerzas armadas peruanas y otorga una ejecución autónoma, sin considerar otras normas aplicables para el resto de la población.

¹⁵¹ <https://busquedas.elperuano.pe/normaslegales/ley-de-ciberdefensa-ley-n-309999-1801519-5/>



Ninguna de las 2 leyes tiene especificado prioridades relativas a la seguridad en línea ni delitos informáticos.

Notificaciones-contenido ilícito/Notificaciones-preocupaciones de los usuarios

En el Perú no se cuenta con la posibilidad de notificar preocupaciones o problemas de seguridad en línea propiamente dicho, sin embargo, Telefónica del Perú ha desarrollado en conjunto con la Red Peruana contra la Pornografía Infantil el portal web “Seguros en internet”, el cual permite la recepción de casos de violencia contra niños en entornos virtuales.

No obstante, una limitante es hacer seguimiento a los casos recibidos. La Red Peruana contra la Pornografía Infantil deriva los casos a las autoridades para la investigación correspondiente, pero no se tiene un registro de cuántas y cuáles denuncias concluyeron en una sentencia. Por el lado estatal existe el portal del Ministerio de Educación, denominado “SISEVE” para los casos de ciberacoso en el entorno educativo, sin embargo, carece de técnicas apropiadas de recojo de información referido a diversas modalidades de violencia en línea hacia los niños.

Mediante Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes, se tiene por objetivo promover el uso seguro y responsable de las tecnologías de la información y comunicaciones (TIC) por niños, niñas y adolescentes para protegerlos de los peligros del mal uso del acceso al Internet.

En este sentido, se considera constituir la Comisión Especial encargada de proponer y definir lineamientos para promover el uso seguro y responsable de las TIC en el país, en especial las medidas que permitan a los niños, niñas y adolescentes utilizar de manera segura y responsable las herramientas educativas vinculadas al uso de la tecnología, el Internet y promover la comunicación fluida entre los operadores, usuarios y los tres niveles de gobierno para el planeamiento y ejecución de campañas educativas y herramientas tecnológicas que puedan contribuir a la protección de los niños, niñas y adolescentes.

Asimismo, el Decreto Supremo N° 093-2019-PCM, del Reglamento de la Ley N° 30254, ha desarrollado la conformación y funciones de esta Comisión.

A nivel institucional no se tiene implementado buenas prácticas en materia de identificación del abuso de menores. A nivel país, en el ámbito estatal no existen políticas concretas o programas de sensibilización implementados. Sólo se han desarrollado reglamentos con futuras acciones para el 2023, como es el caso del Gobierno Digital en conjunto con el Ministerio de la Mujer y Poblaciones Vulnerables para el proyecto de Observatorio Nacional de Población y desarrollo.



Actores y partes interesadas

De acuerdo con la Ley N° 30254, se cuenta con una comisión para abordar el tema y está integrado por:

- Secretaria de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros
- Ministerio de la Mujer y Poblaciones Vulnerables
- Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL)
- Ministerio de Educación
- Ministerio del Interior

El Ministerio de Transportes y Comunicaciones (MTC) a través del Programa Nacional de Telecomunicaciones es responsable de llevar conectividad a zonas rurales y zonas de preferente interés social donde no hay inversión en los servicios de telecomunicaciones por parte de las empresas operadoras. Asimismo, es responsable de la Implementación y operación de los Centros de Acceso Digital (CAD). Es en este sentido, que la responsabilidad está vinculada con los temas de promoción y desarrollo de contenidos en los Centros de Acceso Digital incluido los temas de seguridad en línea.

La Universidad Nacional de Ingeniería (UNI) ejecuta sus políticas de responsabilidad social a través del Centro de Extensión y Proyección Social, con un nuevo enfoque que enriquece la labor de formación de profesionales y contribuye con el desarrollo sostenible de la sociedad¹⁵².

La Autoridad Nacional de Protección de Datos Personales como organismo adscrito al Ministerio de Justicia y Derechos Humanos del Perú, a quien le corresponde el desarrollo de la ley de datos personales y su reglamento, mientras que el siguiente el marco normativo¹⁵³ es el desarrollado por la Secretaría de Gobierno y Transformación Digital (SGTD):

- Decreto Supremo N° 0029-2021-PCM (16 marzo 2021); Reglamento Ley de Gobierno Digital.
- Resolución Directoral N° 02-2020-JU/DGTAIPD (14 febrero 2020); Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia.
- Decreto de Urgencia N° 007-2020 (15 de enero 2020); Marco de Confianza Digital y dispone medidas para su fortalecimiento.

¹⁵² <https://www.rsu.uni.edu.pe/nosotros/normas-rsu/>

¹⁵³ <https://www.gob.pe/anpd>



- Ley N° 29733-2011 (22 de marzo de 2013); Reglamento Ley de Protección de Datos Personales aprobado a través del Decreto Supremo N° 003-2013-JUS.

El Instituto Nacional de Investigación y Capacitación de Telecomunicaciones (INICTEL-UNI) de la Universidad Nacional de Ingeniería, en el marco de la Gobernanza Digital y Gestión de Datos del Estado Peruano y en virtud del principio de valoración de datos, del Reglamento de la Ley de Gobierno Digital aprobado por el Decreto Supremo N° 029-2021-PCM, ha reconocido, en el ámbito institucional, a los datos gubernamentales como un activo estratégico para la toma efectiva de decisiones, para la atención oportuna de solicitudes de información y para una oportuna y mejor prestación de servicios.

Por lo tanto, el INICTEL-UNI considera incorporar roles, de manera interna, para la gobernanza y gestión de datos, entre los que se encuentran:

- El Comité de Gobierno Digital como responsable de la gobernanza y uso estratégico de los datos en la entidad.
- Oficial de Gobierno de Datos como responsable de asegurar el uso ético de las tecnologías digitales y datos, proponer iniciativas de innovación basadas en datos, entre otros.
- El Oficial de Datos Personales como responsable de velar por el cumplimiento de las normas en materia de protección de datos personales en su entidad pública.

Se han realizado planes muy básicos en lo que respecta a la Ley N° 30254, Ley de Promoción del Uso Seguro y responsable de las Tecnologías de la Información y la Comunicación para los Niños, Niñas y Adolescentes, y su Reglamento. Fuera de estas acciones que exige la Ley, no se observa la implementación de políticas, planes, programas o acciones específicas de parte de los organismos públicos y privados del Perú, frente a la violencia sexual contra niños, niñas y adolescentes en entornos virtuales.

También se cuenta con organizaciones no gubernamentales dedicadas a la protección de la infancia en línea, y que son:

- Plan Internacional – Perú
- Capital Humano y social CHS alternativo
- Red Peruana contra la Pornografía Infantil



La organización *Hiperderecho*¹⁵⁴ es una organización civil peruana sin fines de lucro que investiga y promueve el respeto de derechos en entornos digitales. No está dedicada exclusivamente a la niñez o adolescencia, pero atiende casos sobre estos asuntos.

Alianzas Nacionales e Internacionales (sector público y sector privado)

A nivel institucional, no se tiene asignada esta función por la falta de un desarrollo integral de protección de menores, de factores negativos en internet, que debería partir de las oficinas ejecutivas que tienen relación enteramente con esta problemática.

No obstante, a nivel nacional, de manera no masiva y aislada se cuenta con el apoyo de algunas empresas privadas como es Telefónica del Perú con su estrategia “Alto al ciberacoso”, implementada de forma conjunta con la organización CHS-Alternativo, a través de la cual se ofrece un curso virtual gratuito.

Implementación en el desarrollo de los Centros de Acceso Digital (CAD).

A nivel Perú, desde el ámbito privado se han creado pequeños programas y cursos como los desarrollados por Telefónica del Perú, Entel Perú, América Móvil y Bitel, entidades que ofrecen servicios de control parental.

Considerando que los CADs están en desarrollo, sería posible que en un futuro se concrete un acercamiento con el sector privado para promover la seguridad en línea favoreciendo principalmente a los niños y adolescentes.

Si bien varias de las empresas de TIC han suscrito acuerdos internacionales tales como el Pacto Global de Naciones Unidas, los Objetivos de Desarrollo Sostenible - ODS, los Principios Rectores de Empresas y Derechos Humanos, no se evidencia conocimiento de los Derechos del Niño y Principios Empresariales, la cual es una herramienta fundamental para desarrollar plataformas virtuales seguras para los niños, niñas y adolescentes. En el ámbito estatal, pasa exactamente lo mismo, no hay alianzas sólidas con empresas privadas a fin de empoderar a su población, pues ni siquiera se tiene una base de datos que determine experiencias en línea más seguras y positivas.

Conforme al artículo N° 9 del reglamento de la ley N° 30254, son **obligaciones de las empresas operadoras del servicio de Internet:**

Artículo 9.- Obligación de información sobre filtros

¹⁵⁴ <https://hiperderecho.org/nosotros/>



- 1 Las empresas operadoras del servicio de Internet están obligadas a informar a sus potenciales abonados, antes de establecer la relación contractual, sobre la posibilidad de establecer filtros gratuitos u onerosos que bloqueen el acceso a contenidos violentos y pornográficos, corresponde a la empresa operadora del servicio de Internet la carga de la prueba de haber informado a los potenciales abonados sobre la posibilidad de contar con filtros gratuitos u onerosos. Las empresas operadoras del servicio de Internet deben informar el o los dispositivos digitales en los que pueden ser utilizados dichos filtros, los cuales serán de elección del abonado conforme a sus necesidades.
- 2 Las empresas operadoras del servicio de Internet están obligadas a informar a los abonados, en cualquier momento que le sea solicitado, acerca de la posibilidad de establecer filtros gratuitos u onerosos para el bloqueo de páginas de contenido pornográfico o violento.
- 3 Las instituciones educativas públicas a nivel nacional solicitan de manera obligatoria filtros gratuitos u onerosos a sus empresas operadoras del servicio de Internet. Las instituciones educativas privadas, que participan de manera voluntaria, deben adoptar medidas efectivas para el uso seguro y responsable de las TIC.
- 4 Las empresas operadoras del servicio de Internet deben difundir a través de sus principales canales de comunicación la posibilidad que tienen los usuarios de establecer filtros gratuitos u onerosos para bloquear contenidos violentos y pornográficos.
- 5 En los contratos entre las empresas operadoras del servicio de Internet y los usuarios, se debe posibilitar el uso de los filtros gratuitos u onerosos para el bloqueo de páginas de contenido pornográfico o violento, antes, durante o después de la suscripción de los mismos.

La mayoría de grandes operadores de redes de telecomunicaciones ofrecen los servicios de detección, bloqueo y filtro de tráfico de contenido ilícito en internet. En su mayoría, estos servicios se ofrecen para el mundo corporativo. Los servicios ofrecidos para los usuarios residenciales varían de operador en operador, pero en general ofrecen algunas facilidades para administrar el acceso de menores.

Lo que todos ofrecen son recomendaciones y en muchos casos también cursos cortos y herramientas de uso libre para el control por parte de los padres. Como ejemplo se puede citar a *Norton Family*¹⁵⁵.

¹⁵⁵ <https://www.claro.com.pe/personas/beneficios/movil/control-parental/>



A pesar de lo anterior, aún no se cuenta con convenios de colaboración con operadores, del sector público o sector privado, para la retirada de contenidos en línea.

Investigación

En el Perú, de acuerdo con el Instituto Nacional de Estadística e Informática - INEI (en su informe **“Estadísticas de las Tecnologías de Información y Comunicación en los Hogares”**¹⁵⁶, el 92,9%, 93,6% y 85,8% de la población de 12 a 18 años, de 19 a 24 años y de 25 a 40 años de edad, respectivamente, son los mayores usuarios de Internet. Entre los niños de 6 a 11 años acceden el 82,2%. En la población de 60 y más años de edad solo usa Internet el 34,2%.

Por grupos de edad, la información obtenida a través de la ENAHO da cuenta que el 97,1% de la población usuaria de Internet de 25 a 40 años de edad accede a través de teléfonos móviles, el 97,0% de los que tienen entre 41 a 59 años, el 95,5% de los adultos mayores de 60 y más años y el 94,0% del grupo de 19 a 24 años de edad. En menor proporción, el 78,9% de los adolescentes de 12 a 18 años y el 48,4% de los niños de 6 a 11 años también acceden a Internet a través de teléfonos celulares.

El uso de la telefonía móvil muestra diferencia por grupos de edad. Los grupos de edad entre 12 a 59 años usan en mayor proporción la telefonía móvil (más del 90%) que los adultos mayores de 60 y más años (79,9%) y los niños de 6 a 11 años (77,7%).

Al comparar los resultados respecto a similar trimestre del año anterior se aprecia incrementos entre los niños de 6 a 11 años (4,1 puntos porcentuales); mientras que, se registran disminuciones entre la población adulta mayor de 60 y más años, los de 41 a 59 años y los de 25 a 40 años, en 5,2, 2,0 y 0,7 puntos porcentuales, respectivamente. Entre la población de 12 a 24 años, no se aprecian cambios importantes.

Perú no cuenta con indicadores oficiales de protección de la infancia en línea, sin embargo, a través del Ministerio de la Mujer y Poblaciones Vulnerables se computa con indicadores contra la pornografía, más precisamente indicadores de vulnerabilidad en la explotación sexual de niñas, niños y adolescentes. Parte de estos indicadores, con los que el ministerio trabaja, tienen como fuente la Organización Internacional del Trabajo (OIT).

El citado ministerio, a través de un informe presentado en 2021, muestra indicadores de vulnerabilidad. Por ejemplo, los factores de riesgo de explotación sexual de niñas, niños y adolescentes son:

¹⁵⁶ <https://www.inei.gob.pe/media/MenuRecursivo/boletines/04-informe-tecnico-tic-iii-trimestre2020.pdf>



- a. Características personales (entre los subindicadores está: Recibe llamadas frecuentes a su celular y sale de casa sin justificación, tras esas llamadas).
- b. Situación económica.
- c. Sexualidad.
- d. Desempeño escolar.
- e. Lugares que frecuenta.
- f. Personas que frecuenta.

Educación en Materia de alfabetización y competencias digitales

En el Perú hacen falta protocolos de intervención, colaboración y actuación que incorporen a las empresas de TIC para trabajar de manera conjunta con el Estado y la sociedad civil en la prevención y combate de la violencia sexual contra niños en entornos virtuales. Cabe destacar que es una responsabilidad compartida con el gobierno del Perú.

Por el momento no se poseen guías, protocolos de respuesta ante riesgos de la infancia en línea.

La defensoría del Pueblo del Perú en junio de 2020 hizo un llamamiento a adoptar políticas de Estado para dar mayor énfasis en la protección de los niños, sobre todo porque debido a la pandemia, los niños están más cercanos a entornos virtuales para poder estudiar, comunicarse, etc., de manera que no se tienen signos concretos que en un futuro próximo se dé la implementación de soportes formativos para prevenir a los niños de elementos dañinos en línea.

- Promoción y educación a través de los Centros de Acceso Digital (CAD).

A nivel institucional, no se tiene asignada esta función por la falta de un desarrollo integral de protección de menores, de factores negativos en internet, que debería partir de las oficinas ejecutivas que tienen relación enteramente con esta problemática.

Además, Telefónica del Perú cuenta con dos portales web donde brinda información y consejos prácticos para el abordaje de los riesgos en el uso del Internet. Estos portales se denominan EDUCARED¹⁵⁷ y DIALOGANDO¹⁵⁸.

Dichas páginas poseen también cursos para los maestros, sin embargo, no se observa actualmente ningún curso específico enfocado en la prevención y el abordaje de los riesgos en el uso del internet para los niños.

¹⁵⁷ <https://educared.fundaciontelefonica.com.pe/>

¹⁵⁸ <https://dialogando.com.pe/>



También en el ámbito privado, la empresa Entel Perú ha realizado acciones aisladas y sólo en Lima, dirigidas a informar a los niños, niñas y adolescentes sobre un uso seguro y responsable de las TIC. Entre estas acciones cabe destacar eventos con youtubers (muy populares entre los niños) quienes les brindan consejos sobre el buen uso de internet. En lo que respecta a América Móvil-Claro y Bitel, ambas ofrecen a sus clientes servicios de control parental para evitar contenidos no apropiados para los menores.

Recursos educativos

Se encuentran diversos materiales enfocados a riesgos en internet y ciberacoso, entre otros, en el sitio de SíSeVe Contra la Violencia Escolar, que depende del Ministerio de Educación del Perú¹⁵⁹.

Protección de la Infancia

No se cuenta con un programa / proyecto / política específica para la protección infantil en línea. Sin embargo, hay distintas iniciativas o campañas que buscan brindar información sobre los riesgos en línea para niños y adolescentes, a manera de ejemplo se citan:

- Durante el 2020, el Ministerio de Educación presentó un programa contra el acoso y seguridad en internet¹⁶⁰, en el marco del programa Aprendo en casa.
- En el 2021, el Ministerio de la Mujer y Poblaciones Vulnerables, en colaboración con el Colectivo *Child Rights Now*, inició la campaña “Conéctate sin riesgos”, dirigido a adolescentes. (<https://chsalternativo.org/2021/05/mimp-inicia-campana-conectate-sin-riesgos-para-proteger-a-adolescentes-en-entornos-virtuales/>).

Sensibilización Nacional

El MTC forma parte de la Comisión Multisectorial del PNAIA y se coordina acciones en materia de la Infancia y la adolescencia de responsabilidad de los distintos sectores.

El Lineamiento N° 5 del PNAIA indica:

“Las estrategias y campañas de comunicación emplean medios y espacios nacionales, regionales, y locales a favor de los Derechos de las niñas, niños y adolescentes, con el apoyo de instituciones y medios de comunicación que incorporen el uso responsable de las modernas tecnologías de la comunicación.”

¹⁵⁹ <http://www.siseve.pe/web/>

¹⁶⁰ <https://www.drec.gob.pe/noticias/minedu-presentara-programas-contra-el-acoso-sexual-y-la-seguridad-en-internet-en-la-vapa/>



El Instituto Nacional de Investigación y Capacitación de Telecomunicaciones de la Universidad Nacional de Ingeniería (INICTEL-UNI) realiza anualmente la actividad “NOSOTRAS Y LA TECNOLOGÍA”, desde el año 2012, con el objetivo de promover en las niñas y jóvenes mujeres del Perú, las carreras profesionales relacionadas con las TIC, como herramienta para formar una perspectiva de igualdad de género y posicionamiento como líderes de las telecomunicaciones¹⁶¹.

A partir del 2020, hasta la actualidad, el eje de protección en ciberseguridad para adolescentes se desarrolla a través de charlas dirigidas a las adolescentes del nivel secundario de las instituciones educativas.

Desde el ámbito estatal, se tendría que tener mayor protagonismo con el fin de incentivar y promover a través de sus propios departamentos ejecutivos como la Presidencia del Consejo de Ministros, Ministerio de la Mujer y Poblaciones Vulnerables (entre otros) y aliados como *Save The Children International*, para reforzar la implementación de programas de promoción del uso seguro y responsable de las TIC.

“Paz Escolar” Estrategia Nacional contra la Violencia Escolar¹⁶².

Proyecto Educativo Nacional (PEN) que se enfoca en prevenir y afrontar los siguientes tipos de agresiones: físicas, psicológicas, sexuales, verbales, virtuales (vía Internet/Celulares), con armas y por robos.

Tuvo como base un diagnóstico de cuatro fuentes de información:

- Dos de investigación: Revisión de la literatura especializada y revisiones sistemáticas de intervenciones efectivas.
- Dos de debate: Reuniones de trabajo con escolares y representantes de más de 30 organizaciones del gobierno, la cooperación internacional y la sociedad civil; y Consultas en foros nacionales e internacionales, donde destacan el III Congreso Nacional de Niños, Niñas y Adolescentes y el V Congreso Iberoamericano en Prevención de Violencia Escolar.

Se señalan como objetivos estratégicos:

1. Reducir las tasas de victimización escolar en primaria y secundaria, a nivel nacional.
2. Mejorar los logros de aprendizaje, tras reducir la violencia en las escuelas.
3. Mejorar la satisfacción con la vida de los y las escolares de primaria y secundaria, a nivel nacional.

¹⁶¹ <https://www.inictel-uni.edu.pe/index.php/2021/04/15/conferencia-virtual-tecnologia-cultura-y-empoderamiento-de-la-mujer-actual/>

¹⁶² <http://www.infanciaymedios.org.pe/documentos/legislacion/Estrategia%20Nacional%20Paz%20Escolar.pdf>



Herramientas, Servicios y Ajustes

No se cuenta con la información.

Medidas de Accesibilidad

Se cuenta con la Ley de promoción de acceso a internet para personas con discapacidad y de adecuación del espacio físico en cabinas públicas de internet¹⁶³.

Línea de Ayuda

El 8 de julio de 1998 se inaugura el Teléfono ANAR de Ayuda a Niños y Adolescentes en Riesgo en Lima. Es una línea telefónica gratuita y confidencial cuyo fin es ofrecer un espacio de escucha y orientación psicológica, ayuda social y asesoría legal a los niños/as y jóvenes de Perú.

Es atendido por un equipo de profesionales (psicólogos, trabajadores sociales, abogados, educadores), siendo muchos de ellos voluntarios. La Fundación ANAR¹⁶⁴, a través de un recurso como es el Teléfono ANAR, es capaz de llegar a poblaciones que, de otra manera, serían inaccesibles. El Teléfono ANAR está ofreciendo ayuda a los niños/as y adolescentes de todas las regiones de Perú.

- 900 20 20 10, telf. para niños/as y adolescentes.
- 600 50 51 52, telf. para familias y centros escolares.

La línea 100¹⁶⁵ es una línea de denuncia de violencia familiar o sexual a cargo del Ministerio de la Mujer y Poblaciones Vulnerables.

Es un servicio telefónico gratuito de información, orientación, consejería y soporte emocional que ayudará a las personas afectadas o involucradas en hechos de violencia familiar o sexual, o bien, si alguien conoce algún caso de maltrato; permite responder interrogantes al denunciante, aclarar dudas y motivar acciones para solucionar el problema.

Línea 100 puede derivar los casos más graves, reportándolos a los Centros de Emergencia Mujer (CEM) o la Línea 100 en Acción, quienes validarán la información con una visita a la o las personas afectadas para insertarlas en los servicios especializados del CEM.

Además, se pueden realizar llamadas de urgencia para coordinar la intervención urgente de la policía ante una situación de maltrato o violencia familiar y/o sexual.

¹⁶³ <https://www.gob.pe/institucion/minedu/normas-legales/118388-28530>

¹⁶⁴ <https://www.anar.org/anar-peru/>

¹⁶⁵ <https://www.gob.pe/481-denunciar-violencia-familiar-y-sexual-linea-100>



Una línea de ayuda es el teléfono **0800-76888** del SíSeVe Contra la Violencia Escolar, que depende del Ministerio de Educación del Perú, y que se encuentra disponible de lunes a viernes de 8:00 a.m. a 8:00 p.m.

Igualmente, es posible descargar la aplicación del SíSeVe y realizar el reporte de un caso de violencia, o bien, a través del portal de internet <http://www.siseve.pe/web/>.

Que tiene como objetivos:

- Contar con datos reales y desagregados sobre los incidentes de violencia escolar, a nivel nacional, regional y local.
- Evitar el aumento de la violencia a través del temprano reporte y atención de casos.
- Evitar la reconstrucción de profesores que hayan sido sancionados judicial o administrativamente, por agresiones a escolares.
- Ofrecer pautas para evitar que dichas agresiones escolares se repitan, además de los detalles sobre saber dónde encontrar apoyo en tu localidad.
- Articular con otros sistemas de protección infantil.

Adhesión al Convenio de Budapest

Perú es adherente del **convenio de Budapest** con la finalidad de combatir el fenómeno de la ciberdelincuencia. En el 2014 se realizó la solicitud de suscripción, pedido que fue aprobado en el 2015 por el Consejo Europeo. Posteriormente, el 12 de febrero del 2019, el Congreso de la República aprobó – con algunas reservas – el Convenio de Budapest, a través de la Resolución Legislativa N° 30913, el cual fue ratificado por el Poder Ejecutivo mediante Decreto Supremo N° 010-2019-RE, el 09 de marzo de 2019; medida que entró en vigor el 01 de diciembre del mismo año.

Los principales desafíos que enfrenta el Perú con relación a estar conectado al mundo en línea se destacan la limitada información y difusión sobre los riesgos del menor en línea, generar un entorno de cuidado en línea y los procesos de coordinación interinstitucionales, los podemos categorizar en:

Brecha de conectividad, hay numerosos informes sobre el despliegue de redes de comunicación en el Perú y también de los esfuerzos del gobierno por desplegar redes de banda ancha en todas las regiones del país. Sin embargo, la brecha o carencia o de conectividad (en especial a redes de banda ancha) persiste y se agrava mayormente en las zonas alejadas o dispersas fuera de las ciudades.



Desconocimiento de la ciberseguridad, si bien en el Perú se ha avanzado algo en mejorar las capacidades de la población, tanto en la prevención de los riesgos como en la mitigación de incidentes, estas acciones no son masivas. La gran mayoría de peruanos desconoce los riesgos a los que está expuesto al estar en línea (y el uso de internet en el Perú se ha extendido sobremanera debido a la pandemia, a manera de ejemplo ver <https://larepublica.pe/nota-de-prensa/2021/10/25/microsoft-brinda-recomendaciones-de-ciberseguridad-a-usuarios/>).

Ausencia de rectoría en el asunto de ciberseguridad, si bien en el Perú, hay varios ministerios que sesgadamente tratan el tema de la seguridad en línea (PCM a través de la SEGDI, el MTC, el MIDIS y el MININTER, MIMP, MINEDU), hay una cierta desconexión entre las acciones que emprenden y ejecutan estos organismos, lo cual confunde a la población y finalmente, el ciudadano de a pie no sabe quién puede solucionar su problema de ataque, *phishing* o acoso, por citar algunos ejemplos. En especial, los temas relacionados a COP o PIeL.

Las principales oportunidades que tiene el Perú relacionada al mundo en línea son:

- **Negocios globales en línea**, esto implica una forma de comprar e interactuar con los *retail*, o pequeños negocios, incluidos los servicios de *delivery*. También hace que se utilicen intensivamente los servicios de banca en línea. Todo ello mejora el ecosistema económico y permite seguir con el desarrollo del país.
- **Mejora de capacidades en línea**, es posible seguir estudiando (con los ajustes respectivos) desde el hogar y en todos los niveles educativos. Esto trae consigo ventajas y desventajas, el asunto es reducir las desventajas y aumentar las ventajas de la modalidad de aprendizaje en línea.
- **Trámites en línea**, es posible solicitar, hacer seguimiento y obtener resultados de múltiples documentos otorgados por entidades del Estado, en este aspecto, aún hay muchas cosas por mejorar, sin embargo, durante el 2020 y este año 2021, se han simplificado varios trámites que antes se debían hacer de manera presencial.
- Aprovechar la tecnología como un medio para la formación y el desarrollo laboral y personal.
- La comunicación sin fronteras.
- El acceso a servicios digitales y la interacción con las entidades públicas y privadas.

El Ministerio de la Mujer y Poblaciones Vulnerables, la Policía Nacional del Perú a través de la Dirección de Delitos Informáticos (DIVINDAT), atiende víctimas (directas e indirectas) de abuso infantil en línea.



Mediante la Plataforma digital única del Estado peruano se dan recomendaciones para el uso seguro de internet por parte de menores de edad¹⁶⁶. En específico se pueden denunciar los casos a la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía Nacional del Perú, por teléfono o en persona¹⁶⁷.

Además; el Ministerio de la Mujer y Poblaciones Vulnerables tiene, en la Dirección de Protección Especial, unidades especiales para proteger a la niñez y adolescencia, aunque no en forma específica para la seguridad en línea¹⁶⁸.

Asimismo, ha desarrollado un plan de acción por la infancia y adolescencia¹⁶⁹ y la guía para la atención de víctimas de ESNNA entre adolescentes y niños¹⁷⁰ pero en ambos casos no tiene una referencia explícita a la seguridad en línea.

La Defensoría del pueblo¹⁷¹, por su parte, atiende el abuso infantil en general (no específica que sea en línea).

Cabe precisar que no existe una institución específica que atienda las víctimas de abuso infantil en línea.

¹⁶⁶ <https://www.gob.pe/12799-recomendaciones-de-uso-seguro-de-internet-para-menores-de-edad>

¹⁶⁷ <https://www.gob.pe/12801-como-actuar-frente-a-un-caso-de-grooming>

¹⁶⁸ <https://www.mimp.gob.pe/direcciones/dgna/contenidos/articulos.php?codigo=15>

¹⁶⁹ https://www.mimp.gob.pe/webs/mimp/pnaia/pdf/Documento_PNAIA.pdf

¹⁷⁰ <https://www.mimp.gob.pe/webs/mimp/pnaia/pdf/Guia-de-atencion-ESNNA.pdf>

¹⁷¹ https://www.defensoria.gob.pe/grupos_de_proteccion/niñez-adolescencia-y-adultos-mayores/



MATERIALES Y METODOLOGÍA DEL ESTUDIO

El análisis de las políticas de protección y empoderamiento de los niños y jóvenes en línea, es con un enfoque tipo descriptivo, en el que se consideró la participación de seis países de la Región: Colombia, Costa Rica, Ecuador, México, Paraguay y Perú, los cuales respondieron un cuestionario formulado, basado principalmente en la **Observación General No. 25 (2021)** relativa a los **derechos de los niños en relación con el entorno digital**, del Comité Sobre Derechos del Niño de la ONU; la **Ley Orgánica 8/2021 de 04 de junio de 2021, de protección integral a la infancia y la adolescencia frente a la violencia** (España); y por supuesto, en las **directrices sobre protección de la infancia en línea para los encargados de formular políticas**, emitidas por la UIT.

Además de la recopilación de la información aportada gracias a la colaboración de los países participantes, también se llevó a cabo una investigación en línea, a través de sitios web gubernamentales, al igual que de actores y diversos puntos focales, así como de la lectura de diversos artículos y publicaciones en relación con los temas que se abordan en el presente documento.

Análisis comparativo

En este análisis colaboró Colombia, Costa Rica, Ecuador, México, Paraguay y Perú.

De los seis países participantes, podemos observar que en todos ellos se ha impulsado su respectiva estrategia digital nacional, mismas que tienen como objetivos primordiales el fortalecimiento de infraestructura tecnológica, compra de tecnología y capacitación.

La conectividad ha sido una de las preocupaciones de dichos países; sin embargo, durante los últimos tres años, han incorporado la innovación y la ciberseguridad como elementos indispensables en todos los sectores de la sociedad, debido a su impacto en la confianza institucional, al igual que en el ámbito económico y de desarrollo, la educación y la dotación de competencias.

A pesar de dichos avances, es importante considerar que resta mucho aún por hacer en sus estrategias para profundizar sus objetivos hacia la protección de la infancia en línea. Colombia, Costa Rica, Ecuador y Paraguay sí han diseñado políticas públicas y programas con un enfoque específico en niños, niñas y adolescentes.

Colombia: “*En TIC Confío +*” es un programa del Ministerio de Tecnologías de la Información y las Comunicaciones que promueve el desarrollo de las habilidades digitales para enfrentar con seguridad los riesgos asociados al uso de internet y las TIC:



<https://www.enticconfio.gov.co/quienes-somos>).

Costa Rica: "*Estrategia Nacional Prevención y Respuesta a la Explotación y Abuso Sexual De Niños, Niñas y Adolescentes en Línea 2021-2027*", cuyo objetivo general es fortalecer la capacidad país en los entornos digitales mediante la coordinación y articulación interinstitucional e intersectorial para garantizar la protección de la niñez y la adolescencia frente a la explotación y el abuso sexual en línea:

https://www.micitt.go.cr/sites/default/files/estrategia_nacional_easnnal_2021-2027.pdf)

Ecuador: "*Política pública por una internet segura para niños, niñas y adolescentes*", se trata de una política destinada a promover conductas protectoras o preventivas de factores de riesgos que pueden poner en peligro la integridad y dignidad de niñas, niños y adolescentes ante el acceso y uso de internet; y cuando tales vulneraciones han sucedido, promover protocolos adecuados de atención para la protección, atención y reparación.

https://www.igualdad.gob.ec/wp-content/uploads/downloads/2020/09/pol%C3%ADtica_publica_internet_segura.pdf)

Paraguay: "*Plan de Acción País 2017 — 2021*", que incorpora la temática del fortalecimiento del marco jurídico en materia de acoso en línea y determina responsabilidades por medio de la gestión del Ministerio Público para la investigación de casos y del Ministerio de Salud Pública y Bienestar Social en la atención a las víctimas, con el apoyo del Ministerio de la Niñez y la Adolescencia.

Asimismo, dicho Plan establece un compromiso multisectorial, que incluye a la industria, implementado para la colaboración en la alerta, bloqueo, remoción y denuncia de contenidos existentes en Internet de explotación y abuso sexual de niñas, niños y adolescentes.

https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/regions/paraguay_global_partnership_-_plan_pais_imprimir.pdf)

En el caso de México y Perú, no cuentan con una estrategia nacional que atienda de manera específica la protección de la infancia en línea, aunque sí han publicado diversos materiales preventivos, y han impartido cursos a través de diversas instituciones.

En México, se llevó a cabo el "Operativo Salvación", que consiste en realizar acciones de prevención, capacitación y coordinación entre la Guardia Nacional con la Fiscalía General de la República (FGR) y con las Fiscalías y Procuradurías de las 32 Entidades Federativas, para llevar a cabo labores de investigación para el combate a la Pornografía Infantil en México.



También, durante el 2020, el Ministerio de Educación de Perú presentó un programa contra el acoso y seguridad en internet, en el marco del programa Aprendo en casa (<https://www.drec.gob.pe/noticias/minedu-presentara-programas-contra-el-acoso-sexual-y-la-seguridad-en-internet-en-la-yapa/>); y en el 2021, el Ministerio de la Mujer y Poblaciones Vulnerables, en colaboración con el Colectivo Child Rights Now, inició la campaña “Conéctate sin riesgos”, dirigido a adolescentes (<https://chsalternativo.org/2021/05/mimp-inicia-campana-conectate-sin-riesgos-para-proteger-a-adolescentes-en-entornos-virtuales/>).

De todo lo anterior, se observa que si bien no todos los países participantes han tenido la posibilidad de formular una política pública nacional, sí han mostrado interés por ocuparse de la protección de la infancia en Internet a través de diferentes acciones que atiendan de manera específica la problemática que se vive en cada nación, y para efecto de realizar un análisis comparativo de las acciones y actividades llevadas a cabo, resulta pertinente conocer los ámbitos esenciales que se deben tener en cuenta al formular una estrategia nacional de protección de la infancia en línea o COP (Child Online Protection), de acuerdo a las directrices publicadas por la UIT https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/Guidelines/2020-translations/S-GEN-COP.POL_MAKERS-2020-PDF-S.pdf (página 42).

Marco jurídico y reglamentario

Los seis países participantes cuentan con un marco jurídico en el que se reconocen los derechos de los niños, partiendo de sus respectivas Constituciones Nacionales, lo que significa una intención de otorgar un nivel máximo de protección, a lo que se suma que **Costa Rica, México, Paraguay** y **Perú** tienen normatividad reglamentaria, a través de la cual se han creado sistemas nacionales de protección integral a niñas, niños y adolescentes; pero la existencia de la normatividad no es suficiente para que su aplicación sea efectiva, y menos aún, que la misma sea exitosa o de resultados benéficos para la población objetivo: infantes.

Se afirma lo anterior, porque se requiere la existencia de tres elementos fundamentales para que cualquier derecho se pueda hacer efectivo: que esté reconocido en la ley, la existencia de una autoridad encargada de garantizarlo y que estén previstos los procedimientos para hacer valer ese derecho. Elementos que no están satisfechos en cada uno de los países colaboradores.

Colombia, Costa Rica, Paraguay y **Perú**, han elaborado las referidas políticas reglamentarias, como la formulación y publicación de códigos de buenas prácticas o expectativas básicas en materia de seguridad en línea, tanto en relación con la ayuda encaminada a propiciar, coordinar u orquestar y mantener la participación de todos los interesados pertinentes, como en lo relativo a la aceleración del ritmo en que se pueden formular y llevar a la práctica respuestas apropiadas



a los cambios tecnológicos; y por cuanto a **México** y **Ecuador**, han diseñado algunas campañas, pero ninguna estrategia nacional o política pública que tenga como enfoque la protección de la infancia en línea.

Lo anterior es congruente con el resultado obtenido de la comparativa de las actividades llevadas a cabo por los países que han colaborado en el presente análisis comparativo.

De inicio, se desprende que **Colombia** cuenta con normatividad respecto a páginas con contenido material de Explotación Sexual de Niñas, Niños y Adolescentes, pues la ley 679 de 2001, establece que los Proveedores de Redes y Servicios de Telecomunicaciones (PRST), tienen como deber:

- Denunciar ante las autoridades competentes cualquier acto criminal contra menores de edad de que tengan conocimiento, incluso de la difusión de material pornográfico asociado a menores.
- Combatir con todos los medios técnicos a su alcance la difusión de material pornográfico con menores de edad.
- Abstenerse de usar las redes globales de información para divulgación de material ilegal con menores de edad.
- Establecer mecanismos técnicos de bloqueo por medio de los cuales los usuarios se puedan proteger a sí mismos o a sus hijos de material ilegal, ofensivo o indeseable en relación con menores de edad.

También cuenta con normas que establecen las medidas que deben adoptar los PRST, para identificar y bloquear páginas con contenido proscrito, no obstante, cada operador tiene la libertad de implementar los mecanismos tecnológicos que considere necesarios, siempre y cuando den cumplimiento a las medidas técnicas establecidas en la normatividad, así como a los deberes dispuestos en el artículo 8 de la Ley 679 de 2001 y el artículo 2.2.10.2.2 del Decreto 1078 de 2015.

Costa Rica cuenta con un robusto marco normativo y reglamentario que se describe a continuación:

Ley General de las Telecomunicaciones Nº 8642. El objeto principal de esta Ley es establecer el ámbito y los mecanismos de regulación de las telecomunicaciones, que comprende el uso y la explotación de las redes y la prestación de los servicios de telecomunicaciones.



Legislación en vigor la seguridad en línea. En Costa Rica se ha generado una buena base normativa que le permite responder a la violencia virtual contra NNA. Pero ante los avances tecnológicos que pueden conllevar nuevos delitos, las normas existentes no son suficientes y las reformas normativas necesarias no son lo rápidas que se requiere.

- **Código Penal, Ley N° 4573:** En su título III Delitos Sexuales: tipifica los delitos vinculados con la explotación y abuso sexual y otras modalidades de delitos cometidos contra menores de edad, en todas sus modalidades.
- **Ley de Justicia Penal Juvenil, Ley N° 7576:** Se regulan principios, garantías y derechos fundamentales que rigen la materia penal juvenil.
- **Ley Protección de la Persona frente al tratamiento de sus datos personales, Ley N.º 8968** Esta ley tiene como objetivo garantizar, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.
- **Decreto Ejecutivo N° 36274-MICIT,** publicado en el Diario Oficial La Gaceta N° 239 de fecha 09 de diciembre de 2010: Se constituyó la Comisión Nacional de Seguridad en Línea como órgano multidisciplinario e intersectorial, conformado por representantes de distintas instituciones públicas y privadas que tienen ámbitos de competencia especial o desarrollan iniciativas referidas al uso seguro, responsable y significativo de la Internet y las Tecnologías Digitales.
- **Ley N° 10020 Ley para la Prevención del Acoso a Personas Menores de Edad por medios electrónicos o virtuales (grooming) y Reformas al Código Penal.** Esta Ley establece un marco regulatorio procura proteger contra el grooming a menores de edad del acoso cibernético y tiene como fin prevenir, combatir y sancionar la comisión de delitos sexuales a través de medios electrónicos o virtuales. También a través de dicha Ley se crea la Comisión interinstitucional para la protección para la persona menor de edad frente a delitos sexuales cometidos a través de medios electrónicos o virtuales.
- **Ley N° 8148 “Adición de los artículos 196 bis, 217 bis y 229 bis al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos”** del 9 de noviembre del 2001, que introdujo nuevos tipos penales.



- **Ley N° 9048 “Reforma de varios artículos y modificación de la Sección VIII, denominada Delitos Informáticos y Conexos, del Título VII del Código Penal”** de fecha 6 de noviembre del 2012.
- **Ley N° 9135 denominada “Reforma de los artículos 196, 196 bis, 230, 293 y 295 y adición del artículo 167 bis al Código Penal”** del 24 de abril del 2013, que introdujo el artículo 167 bis (Seducción o encuentros con menores por medios electrónicos).
- **Ley N° 7899, “Ley Contra la Explotación Sexual de las Personas Menores de edad”** del 17 de agosto de 1999.
- **Ley N° 8590 “Fortalecimiento de la Lucha Contra La Explotación Sexual de las Personas Menores de Edad mediante la reforma y adición de varios artículos al Código Penal, Ley N° 4573, y reforma de varios artículos del Código Procesal Penal, Ley N° 7594”**

Además, ha signado instrumentos vigentes en materia de protección y garantía de los derechos de los niños y las niñas.

Ecuador tiene su Constitución, aprobada en 2008 refuerza el rol del Estado, la sociedad y la familia como garantes del ejercicio de derechos y con la obligación de brindar protección, apoyo y promover el desarrollo integral de niñas, niños y adolescentes, enmarcado en el principio de interés superior del niño, además, recibirán atención prioritaria y especializada en los ámbitos públicos y privados.

El Ministerio de Educación, al ser el órgano rector de la educación nacional, maneja los protocolos y rutas de actuación frente a situaciones de violencia detectadas o cometidas en el Sistema Educativo, incluyendo las cometidas en entornos virtuales.

Esta normativa define las líneas de acción institucional para la prevención y sanción (administrativa). Además, existe una acción conjunta entre varias instituciones del estado para su sanción legal considerando los cuerpos normativos anteriormente mencionados.

Existen mecanismos legales estipulados en la legislación ecuatoriana que tienen un valor resumido a la seguridad en línea, además cuenta con políticas nacionales digitales, como la ley orgánica de telecomunicaciones y la ley orgánica de protección de datos personales.

La Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), mediante Resolución No. ARCOTEL-2018-0716 de 16 de agosto de 2018, expidió la Norma técnica que regula las condiciones generales de los contratos de adhesión, del contrato negociado con clientes y del empadronamiento de abonados y clientes, en este instrumento entre otros aspectos,



se establecen en el artículo 4, las condiciones generales que deben cumplir los prestadores de servicios, puntualmente en el número 26 que dispone que un apartado de Protección de los niños, niñas, y adolescentes e Inclusión de herramientas para control parental.

México, el 04 de diciembre de 2014, se publicó en el Diario Oficial de la Federación la Ley General de los Derechos de Niñas, Niños y Adolescentes (LGDNNA), la cual tiene como objeto principal el reconocer a las niñas, niños y adolescentes como titulares de derechos, pero también el reconocerles la capacidad de goce de los mismos.

A través de dicha Ley, se busca poder garantizar el pleno ejercicio, respeto, protección y promoción de los derechos humanos que le asisten a las niñas, niños y adolescentes, los cuales se encuentran reconocidos tanto como en la CPEUM, así como en los tratados internacionales de los cuales México forma parte, como en el caso particular lo es la Convención sobre los Derechos del Niño (Convención).

También cuenta con normatividad robusta para sector público y privado en materia de protección de datos personales, como lo son la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como Ley Federal de Protección de Datos Personales en Posesión de los Particulares, respectivamente, así como con un órgano garante a nivel nacional, además de uno en cada entidad federativa.

Igualmente, la Hoja de Ruta 2021-2025 del Instituto Federal de Telecomunicaciones (IFT), contempla la diversificación de usuarios, en la cual se incluye también a los niños. Esta consideración es primordial para garantizar los derechos de todos los usuarios y la calidad de los servicios prestados.

Paraguay, la Constitución Nacional en su artículo 54 De los Derechos del niño, encomienda a la familia, a la sociedad y al Estado, el deber de garantizar al niño su desarrollo armónico e integral, así como la obligación de protegerlo contra la violencia, el abuso, el tráfico y la explotación, determinando que en caso de conflicto los derechos del niño tienen carácter prevaleciente.

Resulta conveniente referirse asimismo a la Convención sobre los Derechos del Niño, aprobada por Ley N° 57/90, la cual incorpora el principio del interés superior del Niño por el cual las autoridades estatales que intervengan en asuntos relacionados con los niños deben adoptar las medidas más adecuadas que garanticen su bienestar general, estableciendo así mismo el compromiso de los Estados de respetar y promover el derecho a la vida, la supervivencia, el desarrollo integral y la protección contra la violencia, incluida la intervención judicial según corresponda.



En este aspecto cabe señalar la vigencia de la Ley N° 6002/2017 “QUE MODIFICA EL ARTÍCULO 135 DE LA LEY N° 1160/97 “CÓDIGO PENAL”, MODIFICADO POR EL ARTÍCULO 1° DE LA LEY N° 3440/08 “QUE MODIFICA VARIAS DISPOSICIONES DE LA LEY N° 1160/97 “CÓDIGO PENAL”, y que en su parte pertinente establece Abuso por medios tecnológicos.

Asimismo, por Ley N° 5653/2016 de “PROTECCIÓN DE NIÑOS, NIÑAS Y ADOLESCENTES CONTRA CONTENIDOS NOCIVOS DE INTERNET”, se puso en vigencia una normativa dirigida a proteger de una manera integral al niño, niña y adolescente frente, a los efectos que pudieran generar en ellos los contenidos nocivos a que tengan acceso o se encuentren en internet.

La Ley N° 5653/2016, establece asimismo mecanismos de fiscalización y aplicación de sanciones por su incumplimiento, además de crear un cuerpo colegiado intersectorial denominado Observatorio Nacional para la Protección de los Derechos de Niños, Niñas y Adolescentes en Internet (ONAI), integrado por organismos y entidades estatales y con la participación de la sociedad civil.

Además de otras normas de rango legal con enfoque específico en los derechos del niño.

Perú, la Ley N° 30096 “Ley de delitos informáticos”, modificada por la Ley N° 30171, sanciona las *“proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos”*¹⁷².

Ley de delitos informáticos que incluye y establece penas sobre Delitos contra la indemnidad y libertad sexual en relación con Propositiones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.

Asimismo, tenemos la Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niñas y Adolescentes y su reglamento.

También, somos parte del Convenio sobre Ciberdelincuencia (Budapest). Ratificado mediante D. S N° 010 – 2019 – RE. Que cuenta con el título 3 y Artículo 9 sobre Delitos relacionados con la pornografía infantil.

En materia de protección infantil en línea, no ha emitido una norma específica.

Existen normas generales sobre entorno digital, como es el caso del Decreto Supremo 018-2018-PCM, el cual define a la Seguridad Digital como el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los

¹⁷² <https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACI%CC%81N%20FISCAL%20ESPECIALIZADA%20-%202015%20FEBRERO%202021.pdf>



riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno.

La Ley N° 30096 – Ley de delitos informáticos, ha contemplado la figura de las proposiciones por medios tecnológicos.

Cada uno de los países participantes ya cuenta con marcos normativos que parecen ser suficientes, pero lo cierto es que en ninguno de ellos tiene una ley especial para la protección de niñas, niños y adolescentes en línea, y la legislación existente está dirigida a la violencia en el ciberespacio, o bien, a delitos de índole sexual; por tanto, hay retos importantes para terminar de construir un andamiaje jurídico especializado, en el que se establezcan roles determinados y consecuencias que no estén enfocadas a la materia penal, pues también existe la necesidad de buscar medios alternativos de solución y mediación de conflictos.

Notificaciones-contenido ilícito / Notificaciones-preocupaciones de los usuarios

Colombia

Las páginas con contenido Material de Explotación Sexual de Niñas, Niños y Adolescentes la ley 679 de 2001, establece que los Proveedores de Redes y Servicios de Telecomunicaciones – PRST, tienen determinadas obligaciones, como la de realizar el bloqueo de las páginas con contenido proscrito, de los listados con URL´s con contenido de pornografía infantil emitidos por la DIJIN y que son publicados en la página WEB del MinTIC.

De los sujetos que vigila el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (PRST), el Artículo 2.2.10.2.2 Decreto 1078 de 2015, establece las medidas técnicas para identificar páginas que contengan Material de Explotación Sexual de Niñas, Niños y Adolescentes.

En TIC Confío + promueve los siguientes canales oficiales de denuncia:

- Línea 141- ICBF: denunciar o pedir orientación sobre casos de maltrato infantil, violencia sexual, acoso escolar, trabajo infantil o consumo de sustancias psicoactivas, entre muchas otras situaciones que amenacen o afecten la vida e integridad de un niño, niña o adolescente.

Canal de denuncia de la Policía Nacional - www.adenunciar.policia.gov.co

Costa Rica sí cuenta con normativa que regula este tipo de contenidos, pues rige al Sector de Telecomunicaciones, en particular, la **Ley General de Telecomunicaciones N° 8642**, desarrolla el régimen de privacidad y de protección de los derechos e intereses de los usuarios finales de los servicios de telecomunicaciones.



Las instituciones MICITT y PANI son responsables de promover el diseño, implementación y ejecución de políticas de protección de la niñez según la legislación. Asimismo, tal como se explicó anteriormente, el ente regulador del sector de telecomunicaciones, la normativa establece que la SUTEL, es la entidad responsable de la ejecución de las disposiciones relativas a la normativa en materia de daños contenidos en Internet y otros medios electrónicos. El Poder Ejecutivo es responsable de coordinar las políticas y asegurar el cumplimiento. Cuando el PANI tenga conocimiento de una situación que vulnere los derechos de uno o más menores, utilizando medios digitales en Internet, debe coordinarse con las instituciones relevantes y remitir asunto a la Corte. Esta entidad se apoya en las disposiciones del Código de la Niñez y la Adolescencia, Artículo 111. (OECD, 2020).

Seguidamente, el país a través de la **Ley N° 8934 para la Protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos**, la cual será aplicable a los locales con acceso al público, destinados al uso público de computadoras conectadas a Internet u otras formas de comunicación en red, sea por medio de computadoras y de cualquier otro medio electrónico, que sean utilizados por personas menores de edad.

Además, en el documento “*Mapeo de la Capacidad institucional en prevención y respuesta a la explotación y abuso sexual en línea, 2018*” se indicó que en relación con los procedimientos de alerta y remoción de contenido local y bloqueo de contenido de Explotación Sexual en Línea es un asunto implica que la Industria de tecnología y telecomunicaciones, incluso por iniciativa propia toma medidas para bloquear información, datos, videos u otros vinculados a esta violencia. En este aspecto la industria no ha enviado registro a las autoridades nacionales (PANIAMOR, 2018).

De igual forma, la FANNA señaló que existe coordinación entre este ente y los operadores mediante los procesos de monitoreo y en coordinación con las instancias judiciales correspondientes.

En ese sentido, según el *Mapeo de la Capacidad Institucional en prevención y respuesta a la explotación y abuso sexual en línea* realizado en 2018, en lo referente a la industria, no hay registro oficial de remoción local y bloqueo de contenido de Explotación Sexual en Línea, por iniciativa propia de los operadores móviles¹⁷³.

Asimismo, se señala que existen protecciones estatutarias que permiten a la industria reportar completa y efectivamente los casos, incluyendo transmisión de contenidos a fuerzas policiales o autoridad competente. Esto se refiere a que es la misma Industria la que denuncia los casos de

¹⁷³https://crianzatecnologica.paniamordigital.org/sites/default/files/recursos_apoyo%20paniamor_preencion_y_respuesta.pdf



Explotación Sexual en Línea, sin embargo, a la fecha, desde el MICITT no se dispone de registro de estas acciones, aunque la legislación nacional lo permite.

Ecuador, no se tiene información de la que se advierta la posibilidad de llevar a cabo dichas notificaciones.

En **México**, el micrositio de Ciberseguridad, cuenta con un apartado denominado “Reporte Ciudadano” en el que los usuarios pueden encontrar los datos de contacto de las policías cibernéticas adscritas a los diferentes estados de la república y, con ello, recibir asesoría o reportar los incidentes cibernéticos que presenten durante su navegación por Internet.

Paraguay, actualmente la institución cuenta con una Línea de Atención Telefónica Gratuita denominada FONOAYUDA 147 que se encuentra disponible para que los niños, niñas y adolescentes, sus padres, encargados de su cuidado y educación requieran orientación sobre el modo de proceder ante casos que pudieran significar la violación de derechos de niños, niñas y adolescentes, incluidas aquellas vulneraciones perpetradas por medios telemáticos. En ocasiones y según corresponda esta línea de atención se constituye en boca de entrada de denuncias, las cuales son derivadas a la institución competente (CODENI/Sistema de Administración de Justicia Especializada/Ministerio Público, etc.), conforme a la situación denunciada.

Del mismo modo, se prevé habilitar en la Página Web del Ministerio de la Niñez y la Adolescencia una ventana de recepción de denuncias sobre incumplimiento de la Ley N° 5356/16 atribuible a Proveedoras de Servicios de Internet y propietarios o encargados de espacios públicos que se encuentran obligados a poner a disposición del público, softwares de protección, en el marco de dicha norma.

El gobierno de **Perú** no se cuenta con la posibilidad de notificar preocupaciones o problemas de seguridad en línea propiamente dicho, sin embargo, Telefónica del Perú ha desarrollado en conjunto con la Red Peruana contra la Pornografía Infantil el portal web “Seguros en internet”, el cual permite la recepción de casos de violencia contra niños en entornos virtuales.

No obstante, una limitante es hacer seguimiento a los casos recibidos. La Red Peruana contra la Pornografía Infantil deriva los casos a las autoridades para la investigación correspondiente, pero no se tiene un registro de cuántas y cuáles denuncias concluyeron en una sentencia. Por el lado estatal existe el portal del Ministerio de Educación, denominado “SISEVE”, sin embargo, carece de técnicas apropiadas de recojo de información referido a diversas modalidades de violencia en línea hacia los niños.



Los países participantes, con excepción de Ecuador, cuentan con mecanismos para la notificación de contenido ilícito de preocupaciones de los usuarios; pero no se advierte con claridad el mecanismo de tales herramientas de comunicación, y tampoco el beneficio para el usuario, lo que hace necesario implementar una evaluación de los procesos que se llevan a cabo, así como la efectividad de dichas notificaciones, es decir, el proceder de la autoridad receptora, los tiempos de respuesta y las consecuencias posibles (denuncia penal, procedimiento administrativo, etc.).

Respecto a los actores y partes interesadas, **Costa Rica** llevó a cabo una labor incluyente, desde las autoridades, organizaciones de la sociedad civil, la academia, y hasta encuestas con menores de diferentes edades y personas encargadas de su cuidado y formación; situación que no ocurrió en Colombia, Ecuador, México, Paraguay y Perú, porque convocaron a algunas instituciones públicas, sector privado y organizaciones de la sociedad civil, incluso en algunos casos como México, también convocó a la academia, pero no a sus principales protagonistas, que son los niños, al igual que todos los que intervienen en su entorno (padres, abuelos, docentes, cuidadores).

La identificación de los puntos focales nacionales e internacionales es de vital importancia en la formulación de la política pública, porque se requiere de su participación para mejorar la calidad de la estrategia, aunado a que deben ser tomados en cuenta en el proceso de evaluación, por ser la población receptora y en su caso, beneficiaria.

Un stakeholder (parte interesada) puede ser cualquier persona, empresa, institución, organización gubernamental o de la sociedad civil; por ello, lograr una convocatoria con esa diversidad de actuación y opinión, permite determinar de la manera más adecuada sus respectivas necesidades y expectativas, que finalmente ayuden a encontrar objetivos comunes para la formulación de la política pública.

La falta de convocatoria de puntos focales también es consecuencia de que no se han realizado **investigaciones** del tema en todos los países que colaboran, ya que de esos esfuerzos se puede descubrir quienes pueden ser considerados como partes interesadas, tal y como lo llevaron a cabo Costa Rica y Ecuador, tanto en el ámbito nacional como en el internacional, en donde se dieron a la tarea de conocer opiniones, experiencias, preocupaciones y oportunidades en relación con la protección de la infancia en línea.

Costa Rica ha implementado desde hace varios años diversos mecanismos de encuesta, sondeo, investigaciones académicas, entre los que se destaca el publicado en febrero de 2020, a través del cual la OCDE oficializó el Informe *Digital Economy Policy in Costa Rica*, elaborado



por la Secretaría de este ente, como un documento de antecedentes para el examen de adhesión de Costa Rica realizado por el Comité de Políticas para la Economía Digital. En el mismo se incluye un apartado de valoración y recomendaciones del Comité relativas a la protección en línea de los niños y niñas [OCDE/LEGAL/0389] (OCDE, 2020).

En dicho documento se refirió que *“El principal objetivo de las políticas de Costa Rica para la protección de los niños y niñas en línea es extender a Internet la protección que se les brinda fuera de línea. Los marcos jurídicos sobre protección infantil y comunicaciones reflejan valores fundamentales e incluyen regulaciones específicas para la protección de las niñas y niños en línea”*. Además, destacó el rol fundamental de las autoridades como el MICITT, MEP y PANI en dichas acciones, asimismo enfatiza la participación activa que han asumido la sociedad civil por medio de la Fundación Paniamor y la FOD, en la implementación de medidas para empoderar y educar a los niños, niñas, personas adolescentes, docentes, madres y padres, para la concienciación de los medios (MICITT, 2021).

Como parte del proceso de construcción de la "Estrategia Nacional para la Prevención y Respuesta a la Explotación y Abuso Sexual de niños, niñas y adolescentes en Línea", se realizó una Consulta Pública no vinculante con personas menores de edad, mediante la aplicación de un formulario en línea llevado a cabo entre el 05 y 25 de mayo del 2021.

Este formulario se distribuyó entre esta población con el apoyo de: Asociación Guías y Scout de Costa Rica, Cruz Roja Costarricense, Redes de Desarrollo Local en Región Caribe del Instituto de Formación y Capacitación Municipal de la Universidad Estatal a Distancia, Fondo de Naciones Unidas para la Infancia (UNICEF) y sus redes de colaboración, así como mediante mensajería de texto.

También, en el 2019 se realizó en Costa Rica, la Encuesta Kids Online, ejecutada por el Instituto de Investigaciones Psicológicas de la Universidad de Costa Rica (IIP-UCR) en conjunto con la Fundación Paniamor cuyo objetivo fue hacer una medición y diagnóstico periódicos de los tipos de usos de la Internet, considerando sus oportunidades, limitaciones riesgos y usos beneficiosos en NNA entre los 9 y los 17 años. La muestra fue de 1.008 personas distribuidos en dos grupos de edad 9 a 12 años y de 13 a 17 años. Además, se incluyó una muestra de 1.008 personas adultas responsables primarias de su cuidado.

Igualmente, en el marco de la construcción del Plan Nacional de Desarrollo de las Telecomunicaciones 2022-2027, la oficina de UNICEF Costa Rica manifestó su interés de contratar una consultoría para realizar un proceso de consulta a población NNA con el fin de



recoger insumos que pudieran ser incorporados en dicha política pública y que a la vez pudieran ser aprovechados por UNICEF.

En **Ecuador**, en febrero de 2018 se publicó el Informe de Impacto DQ en asociación con el Foro Económico Mundial. Ese informe evaluó la seguridad en línea y la ciudadanía digital entre 38 mil niños de 8 a 12 años en 29 países del mundo.

En ese informe se establece que el 56% de niñas, niños y adolescentes estaban expuestos a al menos un riesgo cibernético (incluidos riesgos como el acoso cibernético, el trastorno del juego, las reuniones fuera de línea con extraños y agresiones sexuales en línea).

En los dos años siguientes, febrero de 2020, se amplió la cobertura e indicadores a seis pilares de apoyo para la seguridad en línea. EL Ranking COSI 2020 compara los resultados en 30 países e incluye datos de más de 145 mil niños, así como de otras fuentes externas como la Unión Internacional de Telecomunicaciones (UIT), el Sistema Global para la Asociación de Comunicaciones Móviles (GSMA), la Unidad de Inteligencia Economista y otras instituciones internacionales; según el Ranking COSI, Ecuador ocupa el puesto 14 (de un total de 30 países) con una puntuación total de 43.9.

En **Colombia**, UNICEF y diversas entidades gubernamentales han llevado a cabo investigaciones que han publicado a través de medios digitales, tales como el acceso a las páginas oficiales, así como la lectura de artículos, investigaciones y publicaciones en medios de comunicación.

En **México**, el IFT en su Encuesta Nacional de Consumo de Contenidos Audiovisuales 2019 <https://conectadas.org/encuesta-nacional-de-consumo-de-contenidos-audiovisuales/>;

igualmente, el Instituto Nacional de Estadística y Geografía, en colaboración con la Secretaría de Comunicaciones y Transportes (SCT) y el Instituto Federal de Telecomunicaciones (IFT), publica la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2020 https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH_2020.pdf.

Paraguay tiene diversas publicaciones basadas en encuestas e investigaciones sobre conectividad, uso de TIC de adolescentes, entre otras <https://www.senatics.gov.py/observatorio/publicaciones>

En el **Perú**, de acuerdo con el Instituto Nacional de Estadística e Informática - INEI (en su informe "[Estadísticas de las Tecnologías de Información y Comunicación en los Hogares](#)") que comparó los trimestres del julio, agosto y septiembre del 2019 con los del 2020, se llegó a la conclusión



que la población de niñas, niños y adolescentes es la que ha incrementado el uso del Internet. <https://www.unicef.org/peru/comunicados-prensa/preocupaci%C3%B3n-bienestar-ninos-ninas-adolescentes-tiemp-frente-pantalla-internet-seguro>

De los esfuerzos llevados a cabo por los países participantes, se observa que solamente Ecuador y Costa Rica realizaron investigaciones con la colaboración de diversas partes interesadas, desde los organismos gubernamentales, así como los responsables de hacer valer la ley, los proveedores de servicios de internet (PSI), los proveedores de redes de telefonía móvil, empresas relacionadas con tecnología, padres, niños y jóvenes, organizaciones dedicadas a la protección de la infancia, organizaciones de sociedad civil, así como la comunidad académica, lo que les ha permitido incorporarlos en la formulación e implementación de las estrategias.

Se ha destacado como relevante para la formulación de las políticas sobre la protección de la infancia en línea, que los países cuenten con una **autoridad nacional en materia de protección de datos personales**, pues les resulta la calidad de parte interesada, en virtud de su naturaleza, atribuciones y competencia.

Con excepción de **Paraguay**, el resto de los países participantes sí tienen una autoridad que garantice la protección de los datos personales, es decir que Colombia, Costa Rica, Ecuador, México y Perú sí cuentan con una autoridad a nivel nacional en esta materia; lo que es muy positivo, debido a la labor que realizan, principalmente con los materiales que elaboran y publican, y los cursos que imparten el objetivo de sensibilizar, concienciar y capacitar a todos los sectores de la sociedad con, ya que la debida gestión de la privacidad y el cuidado en la protección de los datos en línea es indispensable para salvaguardar otros derechos de los infantes.

En **Colombia**, la Autoridad de Protección de Datos encargada de vigilar y garantizar que las entidades públicas y privadas, respeten los principios, derechos y garantías en el tratamiento de los datos personales regulados en la Ley 1266 de 2008 y la Ley 1581 de 2012, es la **Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio**; dicha autoridad emite diversos materiales y guías para todos los sectores de la sociedad, y en materia de protección de la infancia en línea, ha publicado diversos contenidos, como ejemplo de ello, la Guía cuida tu identidad digital y protege tus datos personales: riesgos sobre el tratamiento de datos personales de niños, niñas y adolescentes. https://issuu.com/quioscosic/docs/guia_cuida_tu_identidad_digital_002

En **Costa Rica** mediante la Ley N° 8968, Protección de la Persona frente al Tratamiento de sus Datos Personales publicada en el diario oficial La Gaceta N°170 del 5 de setiembre del 2011, se creó la **Agencia de Protección de Datos de los Habitantes (Prodhab)**, institución de



desconcentración máxima adscrita al Ministerio de Justicia y Paz, con independencia de criterio y personalidad jurídica instrumental propia en el desempeño de las funciones y en la administración de sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones.

Ecuador: La institución que tiene la autoridad en protección de datos personales es la Dirección Nacional de Registro de Datos Públicos (DINARDAP).

México: el INAI¹⁷⁴, por lo que refiere específicamente al derecho humano a la protección de datos personales, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI o Instituto), es el organismo constitucional autónomo garante de este derecho, y es una de las autoridades obligadas a garantizar los derechos de los menores de edad, considerando que un indebido tratamiento de sus datos personales puede afectar severamente a la esfera más íntima de las niñas, niños y adolescentes, lo cual repercutiría en su desarrollo social y en el ejercicio de otros derechos fundamentales.

Perú: La Autoridad Nacional de Protección de Datos Personales¹⁷⁵ como organismo adscrito al Ministerio de Justicia y Derechos Humanos del Perú, y cuenta con su respectivo marco normativo¹⁷⁵.

Educación en materia de alfabetización y competencias digitales

Colombia: En 2021 el Programa en TIC Confío + elaboró 2 guías metodológicas orientadas al fortalecimiento de las habilidades digitales en niños, niñas, adolescentes, jóvenes y adultos. Estas guías constituyen material de trabajo de los Embajadores encargados de desarrollar la estrategia de acompañamiento pedagógico en los territorios.

Así mismo, se diseñaron 7 cursos de refuerzo pedagógico:

- Curso prevención de riesgos ante contenidos inapropiados en Internet
- Curso Estrategias de acompañamiento para adultos en el uso responsable y seguro de las TIC
- Curso Activismo digital para transformar el mundo
- Curso Tras los rastros de la huella positiva digital
- Curso Agencia misterio: protección y manejo ético de datos personales

¹⁷⁴ <https://home.inai.org.mx>

¹⁷⁵ <https://www.gob.pe/anpd>



- Curso Inteligencia artificial: el espejo de nuestras conductas en Internet
- Curso Huella D+: ser buena onda en internet

Por otra parte, el SIC COLOMBIA (autoridad en materia de protección de datos personales cuenta con múltiples publicaciones, y que pueden ser consultables en su sitio web

https://www.sic.gov.co/centro-de-publicaciones?field_global_topic_tid=7037&field_anos_p_value=All

Costa Rica

Actividades que se realizan en Costa Rica para apoyar la seguridad en línea a través del **Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones**, dentro del **Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT) 2015-2021, Costa Rica**, se diseñaron e implementaron actividades para el desarrollo de capacidades, habilidades y destrezas dirigidas a promover el uso seguro, productivo y responsable de Internet por parte de la población. Entre las actividades ejecutadas que se suman a los compromisos asumidos por el MICITT en materia de prevención de la explotación y abuso sexual de la niñez en línea, se listan algunas de ellas:

- Campaña de comunicación sobre el uso seguro, productivo y significativo de Internet, 2020.
- Actividades virtuales para la promoción y prevención de la seguridad en línea, 2020.
- Foro virtual: “Promoción de entornos digitales seguros para las niñas, niños y adolescentes”, Comisión Nacional de Seguridad en Línea, 09 setiembre 2020.

Ecuador: El CNII, junto con instituciones público y privadas, han desarrollado el portal web de Internet Segura¹⁷⁶, mismo que busca fortalecer un vínculo entre padres, docentes y el Estado brindando conocimientos y herramientas que permitan usar la Internet de una manera segura, precautelando siempre la integridad de niñas, niños y adolescentes del país.

México: El Programa para **Promover la Confianza en el Entorno Digital**, trata de un programa de trabajo interinstitucional e intersectorial que se realiza a través de reuniones y mesas de trabajo con diferentes actores, entre ellos, organismos gubernamentales, asociaciones civiles y la iniciativa privada, para que a través de la suma de esfuerzos de los diversos entes que participan en el ecosistema digital, se dialogue, comparta e identifiquen los principales riesgos y amenazas de dicho entorno, y se diseñen acciones a ejecutar desde el ámbito de competencia

¹⁷⁶ Portal web de Internet Segura: <https://internetsegura.gob.ec/>



de cada uno de los actores, con la finalidad de promover confianza en el entorno digital, el uso informado y responsable de Internet.

Micrositio “Aprende y Enseña. Conocimientos y Habilidades en Protección de Datos Personales” tiene como objetivo que profesoras y profesores de educación básica aprendan y transmitan a niñas y niños los conceptos básicos y la normatividad mexicana sobre el derecho a la protección de datos personales; fue puesto a disposición por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) <https://micrositios.inai.org.mx/marcocompetencias/>.

Micrositio de ciberseguridad para usuarios de servicios de telecomunicaciones. Sección: niñas, niños y adolescentes. El material elaborado y elegido para esta sección fue diseñado con el objetivo de brindar recomendaciones amenas y puntuales que contribuyan a que los usuarios de este rango de edad tengan una navegación en línea segura, respetuosa, divertida y agradable.

Ciber Club IFT: cómic interactivo, elaborado por el Instituto, integrado por 6 episodios que tienen como objetivo informar a niños, usuarios de los servicios de telecomunicaciones, sobre diversos conceptos y recomendaciones en materia de ciberseguridad. El comic puede consultarse en video animado, historieta para leer y cuadernillo para colorear.

En **Paraguay** se publicó la Guía de alfabetización digital EmpoderaTECH abre oportunidades a mujeres adultas <https://www.mtess.gov.py/noticias/guia-de-alfabetizacion-digital-empoderatech-abre-oportunidades-mujeres-adultas>

En el **Perú** hacen falta protocolos de intervención, colaboración y actuación que incorporen a las empresas de TIC para trabajar de manera conjunta con el Estado y la sociedad civil en la prevención y combate de la violencia sexual contra niños en entornos virtuales. Cabe destacar que es una responsabilidad compartida con el gobierno del Perú. La defensoría del Pueblo del Perú en junio de 2020 hizo un llamamiento a adoptar políticas de Estado para dar mayor énfasis en la protección de los niños, sobre todo porque debido a la pandemia, los niños están más cercanos a entornos virtuales para poder estudiar, comunicarse, etc., de manera que no se tienen signos concretos que en un futuro próximo se dé la implementación de soportes formativos para prevenir a los niños de elementos dañinos en línea.

La educación en materia de alfabetización y competencias digitales es uno de los grandes retos que tenemos en la Región, en tanto que requiere de la colaboración de las autoridades educativas y el sector privado y académico, pues se necesitan expertos para el diseño de programas educativos que puedan adaptarse a las actuales circunstancias, en atención a las brechas que ya tenemos y que aún deben combatirse.



Recursos educativos

Colombia: La Dirección de apropiación del MinTIC, desde la implementación del Programa En TIC Confío +, promueve acciones de prevención de riesgos y delitos cibernéticos (identificación, prevención y denuncia). <https://www.enticconfio.gov.co/>

Costa Rica: Plan Nacional para el Desarrollo de Estrategias de Prevención y Erradicación de la Violencia Contra Niños, Niñas y Adolescentes, Costa Rica (2017-2019)

Este plan busca delimitar el concepto integral de prevención de la violencia contra las niñas, niños y adolescentes, se han interrelacionado varias fuentes de información, desde la literatura, los talleres participativos y las entrevistas, buscando avanzar a una delimitación concreta y operativa que guiaría el plan de acción (UNICEF, 2017).

Enlace: <https://www.unicef.org/costarica/media/341/file/Plan-nacional-para-desarrollar-estrategias-de-prevencion-y-erradicacion-de-la-violencia.pdf>

Además, en relación con el ICE mencionó que ha emitido los comunicados que han salido sobre los peligros latentes a los que se enfrenta la niñez mediante el uso de Internet. Por parte la Fiscalía de Género y la Fiscalía de Trata de Personas y Tráfico Ilícito de migrantes, así como la Fiscalía Penal Juvenil, han emitido algunas políticas.

Ecuador: El CNII, junto con instituciones público y privadas, han desarrollado el portal web de Internet Segura¹⁷⁷, mismo que busca fortalecer un vínculo entre padres, docentes y el Estado brindando conocimientos y herramientas que permitan usar la Internet de una manera segura, precautelando siempre la integridad de niñas, niños y adolescentes del país.

México: El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), ha elaborado y publicado distintos materiales de concientización respecto a la protección de datos personales de menores en línea, entre las que se encuentran:

Infografías (links en el apartado correspondiente a México)

- Los dispositivos y juguetes conectados a internet.
- Recomendaciones a autoridades educativas para el tratamiento seguro de imágenes de niñas, niños y adolescentes en eventos escolares.
- Recomendaciones para el tratamiento seguro de imágenes de niñas, niños y adolescentes en eventos escolares.

¹⁷⁷ Portal web de Internet Segura: <https://internetsegura.gob.ec/>



- Recomendaciones a padres o tutores para el tratamiento seguro de imágenes de niñas, niños y adolescentes en eventos escolares.
- Derecho a la Intimidad de niñas, niños y adolescentes y el manejo de su imagen.
- Si eres pequeño y navegas en internet. Esto debes saber.
- La intimidad personal y familiar.
- Cuídate del doxing.

Paraguay: El Ministerio de Tecnologías de la Información y Comunicación (MITIC) ofrece mensualmente de manera gratuita una serie de cursos presenciales y en línea que apuntan a desarrollar la economía digital.

Se busca aumentar el conocimiento sobre temáticas clave, siendo un punto de contacto e intercambio en el cual adquirir y compartir experiencias, recursos, capacitación y soporte para la implementación de iniciativas y proyectos en entornos digitales.

Catálogo nacional de cursos en línea gratuitos <https://www.cursos.gov.py/portada>

Perú: Se encuentran diversos materiales enfocados a riesgos en internet y ciberacoso, entre otros, en el sitio de SíSeVe Contra la Violencia Escolar, que depende del Ministerio de Educación del Perú¹⁷⁸.

Todos los países participantes cuentan con material de calidad dirigidos principalmente a los niños, niñas y adolescentes, pero aún falta muchos recursos dirigidos a padres de familia y cuidadores para que logren dar un acompañamiento efectivo a los infantes en su vida digital, e igualmente, para eliminar brechas digitales y generacionales; pero también el sector de profesionales, empresas, y las propias autoridades necesitan de estos materiales para mitigar riesgos en cada uno de los ámbitos de nuestra vida diaria, y así, aprovechar todos los elementos posibles ya existentes, como son los propios expertos.

Protección de la infancia

Velar por que existan mecanismos de protección infantil universales y sistemáticos que obliguen a todas las personas que trabajan con menores (en el ámbito social, sanitario, escolar, etc.) a identificar, tratar y denunciar los incidentes de abuso y daño que se producen en línea.

Colombia: Desde el Programa En TIC Confío + se proponen como desafíos claves:

¹⁷⁸ <http://www.siseve.pe/web/>



- Fortalecer las capacidades de los actores para generar un uso positivo, seguro y responsable de las TIC frente a los riesgos asociados a estas, difundiendo múltiples herramientas para prevenirlos.
- Fortalecer las capacidades de los beneficiarios para usar y apropiarse del Internet como una oportunidad de generar un proyecto de vida, la movilización de causas solidarias y positivas en Internet.
- Contribuir desde la acción directa del Programa a mantener el bienestar y seguridad digital promoviendo oportunidades de crecimiento (proyectos de vida) y participación en el entorno digital.

Costa Rica cuenta con una serie de proyectos, programas y políticas públicas:

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT) 2015-2021: Pilar Inclusión Digital.

De acuerdo con lo establecido en la Ley N°8642, Ley General de Telecomunicaciones que establece que le corresponde al Poder Ejecutivo la definición de metas y prioridades del sector sobre acceso, servicio universal y solidaridad mediante, el “*Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT) 2015-2021: Costa Rica: Una sociedad conectada*”, contempló dentro del Pilar de Inclusión digital una línea de acción enfocada en el empoderamiento de la población en cuanto al uso de las TIC con el fin de incrementar el uso y la apropiación responsable, segura y productiva de las tecnologías digitales de la población en general, de este modo en esta misma línea se han llevado a cabo capacitaciones tanto a personas adultas como actividades dirigidas a personas menores de edad (MICITT, 2021).

Comisión Nacional de Seguridad en Línea

A partir de la apertura del sector de telecomunicaciones, surgieron un conjunto de nuevas necesidades en relación con los procesos de alfabetización los cuales se encaminan hacia el mundo digital, propiciando en el año 2010, la creación de la Comisión Nacional de Seguridad en Línea (CNSL) mediante el Decreto Ejecutivo N° 36274-MICIT, publicado en el Diario Oficial La Gaceta N° 239 de fecha 09 de diciembre de 2010, marcando así el inicio de una serie de acciones que se constituyen en hitos que reflejan los esfuerzos nacionales realizados en materia de seguridad en línea, atención y prevención de la Explotación y Abuso Sexual de Niños, Niñas y Adolescentes en Línea (EASNNAL). La comisión está liderada por el MICITT y la integran además MEP, Ministerio de Cultura y Juventud, PANI, Poder Judicial, SUTEL, Cámara de Tecnologías de Información y Telecomunicaciones, la Fundación Omar Dengo (FOD) y la Fundación Paniamor.



“Costa Rica dice No a la Explotación y el Abuso Sexual en Línea de Niñas, Niños y Adolescentes” (CR-NEXST) La iniciativa Costa Rica dice No a la Explotación y Abuso Sexual en Línea (CR-NEXST), surge en el 2018 a partir de un trabajo impulsado por la Fundación Paniamor, con el apoyo del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) y otras entidades públicas y privadas, el Instituto Mixto de Ayuda Social (IMAS) del Ministerio de Desarrollo Humano e Inclusión Social, el Patronato Nacional de la Infancia (PANI) y el Sistema de Emergencias 9-11 cuya finalidad consiste en promover acciones para la protección de niñas, niños y adolescentes (NNA) frente a la explotación y abuso sexual en línea (MICITT, 2021) y a su vez debido a la necesidad de realizar esfuerzos hacia la democratización de acceso a las tecnologías y la inclusión digital, como supuesto a cumplir para el cierre de brechas socioeconómicas y de conocimiento que limitan el desarrollo sostenible de la nación costarricense (PANIAMOR, 2021).

Estrategia Nacional Prevención y Respuesta a la Explotación y Abuso Sexual de Niños, Niñas y Adolescentes en línea 2021-2027. En el 2021, se emitió la "*Estrategia Nacional Prevención y Respuesta a la Explotación y Abuso Sexual De Niños, Niñas y Adolescentes en Línea 2021-2027*", cuyo objetivo general es fortalecer la capacidad país en los entornos digitales mediante la coordinación y articulación interinstitucional e intersectorial para garantizar la protección de la niñez y la adolescencia frente a la explotación y el abuso sexual en línea.

Proyectos de Ley

De parte de la Fiscalía Adjunta de Atención de Hechos de Violencia en perjuicio de Niñas, Niños y Adolescentes (FANNA) del Ministerio Público de Costa Rica se propuso un proyecto de Ley especial para proteger a las NNA, y se incluyeron nuevas tipologías de esa materia, así mismo en la Política de Persecución Penal.

Ecuador

El CNII, en el marco de las atribuciones contempladas en la Constitución de la República del Ecuador y en la Ley Orgánica de los Consejos Nacionales para la Igualdad, dentro del ciclo de la política pública, nos encontramos en la prioridad de realizar el seguimiento a la Implementación de la “Política Pública por el Uso Seguro de Internet para Niñas, Niños y Adolescentes”.

El Ministerio de Educación prioriza las siguientes acciones:

- Desarrollo de competencias digitales en todos los miembros de la comunidad educativa.
- Protección de la información relacionadas a docentes, estudiantes y familias.



- Conocer, identificar y prevenir los riesgos relacionados al uso de dispositivos tecnológicos y a la navegación en Internet.
- Integración de las tecnologías digitales para el fortalecimiento del proceso de formación.
- Proponer políticas de seguridad en línea más rígidas que se ambienten a la realidad nacional.

El CNII, en el marco de las atribuciones contempladas en la Constitución de la República del Ecuador y en la Ley Orgánica de los Consejos Nacionales para la Igualdad, dentro del ciclo de la política pública, encuentra en la prioridad de realizar el seguimiento a la Implementación de la “Política Pública por el Uso Seguro de Internet para Niñas, Niños y Adolescentes”.

El ministerio implementa las siguientes acciones:

- Campaña permanente “El Mundo Virtual de Eugenia” para conocer, identificar y prevenir riesgos. En este contexto se ha desarrollado un microsítio de consulta con más de 140 recursos educativos (videos, podcast, guías para docentes, entre otros; enlace: <https://recursos2.educacion.gob.ec/euinicio/>).
- Gestión de webinars y talleres nacionales para docentes, estudiantes y familias.
- Definición y socialización de normativa para protección de datos.
- Procesos de formación para docentes de IE de sostenimiento fiscal enfocadas en el desarrollo de competencias digitales.
- Cooperación con otras instituciones (públicas y privadas) para desarrollo de planes y programas complementarios.

ChildFund junto a su socio local FENPIDEC apoyó el proceso de construcción y aprobación de la ordenanza para un internet seguro que norma especialmente los servicios de cybercafés y define espacios de prevención de violencia en Internet. El plan de trabajo a nivel local incluye la réplica de esta iniciativa en los cantones de Pedro Vicente Maldonado y Puerto Quito. Además, en Pedro Vicente Maldonado se trabaja de forma conjunta con el CNII para implementar la metodología FOFOSI.

El Ministerio de Educación maneja el sistema REDEVI para la identificación, prevención y seguimiento de casos de violencia identificados a través del sistema educativo. Actualmente se trabaja en su evaluación técnica para mejorar su alcance y funcionalidad.

En **México**, el IFT desarrolló el Microsítio de ciberseguridad para usuarios de servicios de telecomunicaciones, el cual contiene un apartado dedicado a madres, padres y personas



supervisoras de menores de edad, donde encontrarán datos e información de utilidad para brindar un acompañamiento informado que permita que niñas, niños y adolescentes adopten prácticas seguras en el uso de Internet, servicios, aplicaciones y dispositivos.

Tal es el caso de la sección llamada “*Riesgos en línea*” donde se encuentran diversos materiales que ayudarán a identificar los posibles riesgos que pueden enfrentar los menores de edad cuando realizan actividades en el ciberespacio.

La Guardia Nacional, implementó el “Operativo Salvación”, que consiste en realizar acciones de prevención, capacitación y coordinación entre la Guardia Nacional con la Fiscalía General de la República (FGR) y con las Fiscalías y Procuradurías de las 32 Entidades Federativas, para llevar a cabo labores de investigación para el combate a la Pornografía Infantil en México y demás conductas antisociales que se cometen a través del Internet, en agravio de niñas, niños y adolescentes, lo que ha permitido la presentación de denuncias ante las autoridades competentes, y en seguimiento a la investigación y a la aportación de la evidencia digital ha permitido la identificación y detención de agresores sexuales y rescate de víctimas menores de edad.

En **Paraguay** el Ministerio de Tecnologías de la Información y Comunicación (MITIC) ofrece mensualmente de manera gratuita una serie de cursos presenciales y en línea que apuntan a desarrollar la economía digital.

Se busca aumentar el conocimiento sobre temáticas clave, siendo un punto de contacto e intercambio en el cual adquirir y compartir experiencias, recursos, capacitación y soporte para la implementación de iniciativas y proyectos en entornos digitales.

Catálogo nacional de cursos en línea gratuitos:

<https://www.cursos.gov.py/portada>

En **Perú** no se cuenta con un programa / proyecto / política específica para la protección infantil en línea. Sin embargo, hay distintas iniciativas o campañas que buscan brindar información sobre los riesgos en línea para niños y adolescentes, a manera de ejemplo se citan:

- Durante el 2020, el Ministerio de Educación presentó un programa contra el acoso y seguridad en internet¹⁷⁹, en el marco del programa Aprendo en casa.
- En el 2021, el Ministerio de la Mujer y Poblaciones Vulnerables, en colaboración con el Colectivo *Child Rights Now*, inició la campaña “Conéctate sin riesgos”, dirigido a

¹⁷⁹<https://www.drec.gob.pe/noticias/minedu-presentara-programas-contra-el-acoso-sexual-y-la-seguridad-en-internet-en-la-yapa/>



adolescentes. (<https://chsalternativo.org/2021/05/mimp-inicia-campana-conectate-sin-riesgos-para-proteger-a-adolescentes-en-entornos-virtuales/>).

Sensibilización Nacional

En cuanto a educación sobre los elementos dañinos en línea para los niños/padres/educadores/cuidadores, en el marco de implementación del Programa **En TIC Confío +** de **Colombia** se han definido los alcances, la caracterización y los ejes temáticos sobre los cuales se plantea el abordaje de las estrategias de implementación, los contenidos y los recursos dirigidos a los beneficiarios, particularmente: Niños y niñas (6-11 años), Adolescentes y Jóvenes (12-28 años) y Adultos.

En **Ecuador**, la emergencia sanitaria causada por la Covid-19 provocó que la digitalización sea mucho más acelerada, y con ello el incremento de riesgos en su uso, nuevas formas de amenazas y vulneración de derechos, sobre todo para los niños, niñas y adolescentes¹⁸⁰.

En ocasiones, resulta incontrolable la divulgación de los mensajes y el contacto que extraños pueden tener con niños, niñas y adolescentes. Esta falta de “control” en el uso de internet, hace que atraviesen un doble riesgo y exposición al peligro (ciberacoso, grooming, pornografía infantil, sexting y sextorsión, entre otros); y con ello, la consecuente vulneración de sus derechos (vida, integridad, dignidad, libertad); entonces, la corresponsabilidad de los distintos actores de la sociedad, demanda crear estrategias conjuntas para proteger a ese grupo poblacional.

En **Perú**: El MTC forma parte de la Comisión Multisectorial del PNAIA y se coordina acciones en materia de la Infancia y la adolescencia de responsabilidad de los distintos sectores.

El Lineamiento N° 5 del PNAIA indica:

“Las estrategias y campañas de comunicación emplean medios y espacios nacionales, regionales, y locales a favor de los Derechos de las niñas, niños y adolescentes, con el apoyo de instituciones y medios de comunicación que incorporen el uso responsable de las modernas tecnologías de la comunicación.”

- El Instituto Nacional de Investigación y Capacitación de Telecomunicaciones de la Universidad Nacional de Ingeniería (INICTEL-UNI) realiza anualmente la actividad “NOSOTRAS Y LA TECNOLOGÍA”, desde el año 2012, con el objetivo de promover en las niñas y jóvenes mujeres del Perú, las carreras profesionales relacionadas con las TIC,

¹⁸⁰ <https://www.arcotel.gob.ec/por-un-internet-seguro-para-ninos-ninas-y-adolescentes/>



como herramienta para formar una perspectiva de igualdad de género y posicionamiento como líderes de las telecomunicaciones¹⁸¹.

A partir del 2020, hasta la actualidad, el eje de protección en ciberseguridad para adolescentes se desarrolla a través de charlas dirigidas a las adolescentes del nivel secundario de las instituciones educativas.

Implementación en el desarrollo de los Centros de Acceso Digital (CAD).

El INICTEL-UNI no se ocupa de ese tipo de programas. A nivel Perú, desde el ámbito privado se han creado pequeños programas y cursos como los desarrollados por Telefónica del Perú, Entel Perú, América Móvil y Bitel, entidades que ofrecen servicios de control parental.

Es necesario incentivar, promover y reforzar la implementación de programas de promoción del uso seguro y responsable de las TIC a través de sus propios departamentos ejecutivos como la Presidencia del Consejo de Ministros, Ministerio de la Mujer y Poblaciones Vulnerables (entre otros) y aliados como *Save The Children International*.

“Paz Escolar” Estrategia Nacional contra la Violencia Escolar¹⁸².

Proyecto Educativo Nacional (PEN) que se enfoca en prevenir y afrontar los siguientes tipos de agresiones: físicas, psicológicas, sexuales, verbales, virtuales (vía Internet/Celulares), con armas y por robos.

En **Paraguay**, si bien en los últimos años han sido desarrolladas campañas comunicacionales sobre seguridad en línea por parte del Ministerio de la Niñez y la Adolescencia con la colaboración de otros organismos del Estado y de la sociedad civil, la educación en este aspecto aún se percibe como insuficiente. En ese sentido, la concreción de la reglamentación de la Ley N° 5356/2016 y la correspondiente difusión de la disponibilidad del uso de softwares de protección en línea se presenta como una magnífica oportunidad para ampliar el conocimiento de las personas sobre el uso seguro de internet con miras a la mejor protección de los niños, niñas y adolescentes.

En este rubro en particular, se observa que está pendiente todavía involucrar a todos los que trabajan con menores, pues no es suficiente la existencia de los mecanismos de protección infantil, ya que la implementación de los mismos es lo verdaderamente trascendente, pues se requiere de una capacitación profunda para el conocimiento y aplicación de protocolos, con el objetivo de que tengan la capacidad de identificar, tratar y denunciar los incidentes de abuso y otras conductas que suceden en el ciberespacio; circunstancias que no se advierten de la

¹⁸¹ <https://www.inictel-uni.edu.pe/index.php/2021/04/15/conferencia-virtual-tecnologia-cultura-y-empoderamiento-de-la-mujer-actual/>

¹⁸² <http://www.infanciaymedios.org.pe/documentos/legislacion/Estrategia%20Nacional%20Paz%20Escolar.pdf>



información recopilada y que también debe ser materia de valuación constante para efecto de poder actualizar protocolos de actuación y activar procesos de mejora.

En lo que se refiere a **Herramientas, Servicios y ajustes**, de acuerdo con las directrices de la UIT, hay que tomar en consideración la importancia de los ajustes de los dispositivos, las herramientas técnicas (como los programas de filtrado) y las aplicaciones y los ajustes de protección de la infancia que pueden ser de utilidad. Alentar a los usuarios a que sean responsables con sus dispositivos, fomentando la realización de actualizaciones de los sistemas operativos y la utilización de aplicaciones y programas informáticos de seguridad adecuados.

Colombia: el Programa En TIC Confío + ofrece a sus beneficiarios herramientas que permitan hacer parte activa del entorno digital, usar de manera positiva el internet y promover el autocuidado respecto a los riesgos que allí se presentan, mediante el desarrollo de dos estrategias: Acompañamiento Pedagógico y Encuentro Pedagógico (virtual o presencial).

Costa Rica: cuenta con el **Plan Nacional Desarrollo de las Telecomunicaciones (PNDT) 2015-2021**

Visión 2021: Transformar a Costa Rica en una sociedad conectada, a partir de un enfoque inclusivo del acceso, uso y apropiación de las tecnologías de la información y las comunicaciones, de forma segura, responsable y productiva.

En dicho plan se tiene la Línea de Acción Alfabetización Digital, para fomentar el empoderamiento de las Telecomunicaciones/TIC por parte de la población con la participación interinstitucional.

Ecuador: Telefónica pone a disposición una plataforma con el objetivo de fomentar un entorno seguro en Internet y concientizar a la Sociedad sobre la importancia de aprender a sacar el máximo provecho de estas herramientas en el día a día, desarrollado el portal web Dialogando¹⁸³.

Dialogando es un espacio para debatir sobre todo lo que ocurre alrededor de la Red y los dispositivos conectados. Desde cómo pueden ayudar a los menores a gestionar su identidad digital, hasta cómo debemos gestionar nuestra privacidad. Sobre cómo relacionamos a través de la tecnología, el uso excesivo que hacemos de Internet.

México: De acuerdo con una encuesta realizada por la empresa de ciberseguridad Kaspersky en 2020, el 27% de los padres en México rara vez o nunca monitorean lo que hacen los niños en redes sociales, 66% no utiliza el control parental y el 14% ignora si un desconocido ha intentado contactar a los menores a su cargo.

¹⁸³ <https://www.dialogando.com.ec/guia-de-control-parental/>



En relación a los esfuerzos emprendidos por el Instituto Federal de Telecomunicaciones y en atención a los mandatos señalados y a las acciones previas que el Instituto ha implementado, el 17 de noviembre pasado se publicó el Micrositio de ciberseguridad dirigido a usuarios de servicios de telecomunicaciones, el cual tiene una sección dedicada a padres de familia y personas supervisoras de menores de edad, donde encontrarán datos e información de utilidad para brindar un acompañamiento informado que permita que niñas, niños y adolescentes adopten prácticas seguras en el uso de Internet, servicios, aplicaciones y dispositivos.

Asimismo, con el objetivo de que profesoras y profesores de educación básica aprendan y transmitan a niñas y niños los conceptos básicos y la normatividad mexicana sobre el derecho a la protección de datos personales, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), puso a disposición de la sociedad el micrositio <https://micrositios.inai.org.mx/marcocompetencias/>.

Paraguay: El proceso de reglamentación de la Ley N° 5356/16 “DE PROTECCIÓN DE NIÑOS, NIÑAS Y ADOLESCENTES CONTRA LOS CONTENIDOS NOCIVOS DE INTERNET, se halla en estado avanzado de concreción, lo que permitirá que los operadores suministren herramientas de detección y filtrado de contenidos nocivos a los padres o encargados de niños, niñas y adolescentes.

Se cuenta con un marco normativo, la mencionada Ley N° 5356/16, que establece competencias a diversas entidades estatales para la protección de niños ante los contenidos en línea y crea un organismo intersectorial constituido por instituciones públicas, con posibilidad de incluir al sector privado para el abordaje de este tema.

Perú: No se cuenta con información de este país en este apartado.

Sin duda, Colombia, Costa Rica, México, Paraguay y Perú, han desplegado diversas acciones para poner al alcance de los usuarios diversas herramientas para mitigar riesgos tanto de los menores como de los actores en su entorno formativo y social, que les proporciona mayores elementos para actuar ante algún incidente en el que pueda verse comprometida su privacidad; aunque aquí se debe resaltar que se han creado mejores vínculos a través de los cuales los infantes y quienes participan en su cuidado, al compartir inquietudes y guías en cuanto a su privacidad y ciberseguridad.

Respecto a las **Medidas de Accesibilidad**, Como indica el Comité de los Derechos del Niño en la Observación General número 13, las graves repercusiones de la violencia y los malos tratos sufridos por los niños, niñas y adolescentes son sobradamente conocidas, por ello, se debe destacar que los niños, niñas y adolescentes con discapacidad son sujetos especialmente



sensibles y vulnerables a esta tipología de violencia, expuestos de forma agravada a sus efectos y con mayores dificultades para el acceso, en igualdad de oportunidades, al ejercicio de sus derechos.

Así, en especial atención a la protección del interés superior del menor, debe aplicarse siempre la accesibilidad universal, como medida imprescindible, para hacer efectivos los derechos niños, niñas y adolescentes, sin excepciones; y para el mismo efecto, se deben de observar las medidas de accesibilidad necesarias para que los padres, educadores y cuidadores de los menores que estén esa circunstancia de vulnerabilidad, no coloquen en una situación de desventaja al menor que este a su cuidado, por la falta de acceso a las políticas públicas sobre proyección de la infancia en línea.

Por consiguiente, es importante que los Estados cuenten con medidas de accesibilidad considerando a todos los actores que participen dentro del ecosistema de formación y cuidado de los menores.

El Gobierno Nacional de **Colombia** formuló la Política Nacional de Infancia y Adolescencia la cual tiene como finalidad contribuir al desarrollo integral de las niñas, niños y adolescentes en el territorio nacional y generar las condiciones de bienestar, acceso a oportunidades con equidad e incidencia de las niñas, niños y adolescentes en la transformación del país.

Por para parte, para personas menores de edad como para padres, educadores y cuidadores es importante indicar que **Costa Rica** en materia de accesibilidad a la información y a la comunicación cuenta con la ***Ley 8661, Ratificación de la Convención sobre los derechos de las personas con discapacidad***, desde el 2008 y ***la Ley 7600, Igualdad de oportunidades para las personas con discapacidad, desde el año 1996***. No obstante, en cuanto al tema de accesibilidad web, es hasta la puesta en marcha del Plan Nacional de Desarrollo de las Telecomunicaciones PNDT 2015-2021 que se establece una meta referente al desarrollo de una estrategia para la aplicación de criterios de accesibilidad y diseño universal en las tecnologías de la información y la comunicación, dirigida a las instituciones del Gobierno Central al 2021, de la cual se deriva la ***Directriz 051 MTSS-MICITT Implementación de la accesibilidad de sitios web en el sector público, cuyo objetivo es oficializar la utilización de los criterios de accesibilidad establecidos en la norma WCAG 2.1 "Pautas de Accesibilidad para el Contenido Web"*** y sus posteriores versiones, en las páginas de los sitios web de las instituciones del Estado, facilitando a las personas con discapacidad el acceso a la información y a las Tecnologías de Información y Conocimiento (TIC), de manera oportuna y sin costo adicional al usuario final, en formatos accesibles y con las tecnologías adecuadas a los diferentes tipos de discapacidad, con el objeto de garantizar la igualdad real de oportunidades y trato, evitando así



todo tipo de discriminación. Asimismo, se han desarrollado otras acciones como la generación de 19 normas técnicas complementarias, entre las que se cuenta la tropicalización de la norma WGAC 2.1 y diversas actividades de asesoría y capacitación en el tema.

También, el 13 de diciembre de 2006, la Asamblea General de Naciones Unidas (ONU) adoptó la Convención para promover y proteger los derechos y la dignidad de las personas con discapacidad, **Ecuador**, como Estado Parte, ha ratificado dicha Convención y su Protocolo Facultativo a través de la Asamblea Nacional Constituyente en abril del 2008, a partir de su publicación en el Registro Oficial Nro. 329 del 5 de Mayo del 2008.

En **México**, en la segunda Sesión Ordinaria, celebrada el 13 de abril de 2016 del Consejo Nacional del SNT, se aprobaron los “**Criterios para que los sujetos obligados garanticen condiciones de accesibilidad que permitan el ejercicio de los derechos humanos de acceso a la información y protección de datos personales a grupos vulnerables**” que se publicaron en el Diario Oficial de la Federación el 4 de mayo del mismo año.

Paraguay cuenta con una Guía Básica de Accesibilidad al Medio Físico para las Personas con Discapacidad:

https://www.jica.go.jp/paraguay/espanol/office/others/c8h0vm0000ad5gke-att/publication_01.pdf.

Perú formuló el Plan Nacional de Accesibilidad, que considera el compromiso del estado peruano en la implementación de políticas y acciones para que la infraestructura y equipamiento de las ciudades, reúnan las condiciones adecuadas para el acceso de las personas con discapacidad al entorno físico, al transporte, a la información y a las comunicaciones, en igualdad de condiciones con las demás, estableciéndose la diversidad aplicable a la norma, y no la excepción.
<http://dgadt.vivienda.gob.pe/uploads/PNA.pdf>

Se puede advertir que hay pasos concretos en cada uno de los países participantes, que ponen en evidencia la voluntad del Estado por dotar de mejores condiciones a las personas con capacidades diferentes; sin embargo, **Costa Rica** es el único país que cuenta con un marco normativo y una estrategia de cobertura nacional para garantizar la igualdad de oportunidades entre las personas, a través del acceso y uso de las tecnologías de la información y la comunicación, y con ello, reducir el riesgo de discriminación, así como la generación de diversas brechas en la vida digital.

En cuanto a la **Línea de ayuda**, aunque no es un medio legalmente reconocido en los marcos normativos y que por ende, sea exigible a los gobiernos, cuatro de los seis países participantes tienen un mecanismo para ofrecer de manera gratuita a niños, niñas y adolescentes, ayuda para



el uso seguro y responsable de internet, así como una herramienta de prevención, detección y reacción ante situaciones potenciales de riesgo y emergencia en internet, además de ser canal de denuncia en colaboración con las autoridades competentes.

Colombia, con la Línea de Protección a Niños, Niñas y Adolescentes: 141. Se trata de una línea gratuita nacional para denuncia, emergencia y orientación, disponible las 24 horas de los siete días de la semana, que depende del Ministerio Colombiano de Bienestar Familiar (ICBF). <https://www.icbf.gov.co/linea-de-proteccion-ninos-ninas-y-adolescentes-141>. Igualmente, a través de la red PaPaz (<https://www.redpapaz.org>), Colombia ha logrado implementar recientemente la línea de denuncia “te protejo” cuyo objetivo es el trabajo seguro y eficaz para proteger los derechos de niñas, niños y adolescentes de la región, en especial de la violencia sexual en los entornos digitales <https://teprotejo.org>

En **Costa Rica**, se tienen espacios específicos para que los niños, niñas y adolescentes tengan una participación activa en la garantía y restitución del ejercicio de sus derechos, mediante la línea telefónicas gratuitas 1147 y una línea de atención vía WhatsApp 8989-1147. <https://pani.go.cr/tramites-y-servicios/denuncias-en-linea/>

Perú cuenta con la línea 100 es una línea de denuncia de violencia familiar o sexual a cargo del Ministerio de la Mujer y Poblaciones Vulnerables. <https://www.gob.pe/481-denunciar-violencia-familiar-y-sexual-linea-100>

Paraguay cuenta con una Línea de Atención Telefónica Gratuita de lunes a domingo – 24 horas que ofrece el Ministerio de la Niñez y Adolescencia (MINNA), denominada FONOA YUDA 147 que se encuentra disponible para que los niños, niñas y adolescentes, sus padres, encargados de su cuidado y educación requieran orientación sobre el modo de proceder ante casos que pudieran significar la violación de derechos de niños, niñas y adolescentes, incluidas aquellas vulneraciones perpetradas por medios telemáticos. En ocasiones y según corresponda esta línea de atención se constituye en boca de entrada de denuncias, las cuales son derivadas a la institución competente (CODENI/Sistema de Administración de Justicia Especializada/Ministerio Público etc.), conforme a la situación denunciada. <https://www.paraquay.gov.py/oe/minna/491>

Las líneas de estos cuatro países se encuentran reconocidas en el documento denominado “*Voices of Children and Young People: Global Child Helpline Data for 2020*”, publicado en noviembre de 2021 por la organización internacional Child Helpline International. <https://www.childhelplineinternational.org/data-overview/publications/voices-data2020/>

Mientras que en **México** opera el 088 que atiende la Policía Cibernética, es donde la Guardia Nacional brinda orientación para realizar la denuncia ante el Ministerio Público; y a partir de 2021,



a través de la red PaPaz (<https://www.redpapaz.org>), también logrado implementar la línea de denuncia “te protejo” cuyo objetivo es el trabajo seguro y eficaz para proteger los derechos de niñas, niños y adolescentes de la región, en especial de la violencia sexual en los entornos digitales, y al que se puede acceder en el link: <https://teprotejo.org>, del que se desprende que se trata de un canal de denuncia, en donde se canaliza al denunciante con autoridades y otras organizaciones para que reciba el acompañamiento correspondiente, pero también es importante mencionar que se trata de la única línea virtual cuya finalidad es reportar material de abuso y explotación sexual de niñas, niños y adolescentes en el mundo digital, en la que no se da el mismo acompañamiento en diversas situaciones, como lo son Ciberacoso, Sextorsión, Happy Slapping, Grooming, pues ciertamente constituye un esfuerzo muy importante para contar con una mecanismo de denuncia que genera resultados inminentes como la retirada de contenidos en internet, pero la línea de ayuda también debe proporcionar soluciones inmediatas a menores de edad que necesitan atención o acompañamiento psicológico, técnico y legal.

Ecuador tiene mecanismos de denuncia a través de la línea 1800 335486 y página www.fiscalia.gob.ec, con consejos consultivos ya sea nacional o cantonales; igualmente, cuenta con la entidad denominada Servicio Integrado de Seguridad ECU 911, quien gestiona en todo el territorio ecuatoriano, la atención de las situaciones de emergencia de la ciudadanía, reportadas a través del número 911, mediante el despacho de recursos de respuesta especializados pertenecientes a organismos públicos y privados articulados al sistema, con la finalidad de contribuir, de manera permanente, a la consecución y mantenimiento de la seguridad integral ciudadana; sin embargo, los medios implementados por los dos países mencionados, no pueden ser considerados como un medio de protección para menores en línea, por no ser la función de ese número telefónico, pues constituyen medios de denuncia en diversos temas, como violencia intrafamiliar, o bien, un acompañamiento para llevar a cabo determinados trámites, pero no tienen como objetivo ofrecer ayuda en temáticas determinadas (sexting, grooming, ciberacoso, contenidos perjudiciales, entre otros), con procedimientos establecidos para tal efecto, y con la participación de equipos multidisciplinarios, para brindar asistencia legal, técnica y psicológica.

Como ejemplo de la operatividad, alcances y tiempos de funcionamiento de un canal de ayuda, podemos observar algunos implementados en Europa, como el canal prioritario por parte de la Agencia Española de protección de Datos <https://www.aepd.es/es/documento/infografia-canal-prioritario.pdf>, en el que incluso se solicita la retirada de contenido sensible de menores.

Si tiene conocimiento de que **actualmente** están colgadas en internet determinadas imágenes de **contenido sexual** o que muestran actos de **agresión**, cuya difusión sin el consentimiento de las personas afectadas está poniendo en ALTO RIESGO sus derechos y libertades, y no ha



logrado su retirada a través de los **canales especialmente previstos por el prestador de servicios**, puede presentar una reclamación por medio de dicho canal <https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/eliminar-fotos-y-videos-de-internet>.

Canal prioritario para comunicar la difusión de contenido sensible y solicitar su retirada

La Agencia Española de Protección de Datos dispone de un Canal prioritario para comunicar la difusión ilícita de contenido sensible, un sistema que tiene como objetivo dar una respuesta rápida en situaciones excepcionalmente delicadas, como aquellas que incluyen la difusión de contenido sexual o violento.

¿Qué puedo hacer si se difunden imágenes en las que aparezco?

Con carácter general, los afectados por estas conductas deben dirigirse al prestador de servicios en Internet solicitándole la retirada de imágenes que están siendo difundidas sin su consentimiento. A continuación se detallan los enlaces a algunos de los prestadores de servicios mayoritarios:

- [iRing](#) [iRigga](#) [iRigga.com](#) [iRigga.es](#)
- [iRigga](#) [iRigga.com](#) [iRigga.es](#) [iRigga.com](#)
- [iRigga](#) [iRigga.com](#) [iRigga.es](#) [iRigga.com](#)
- [iRigga](#) [iRigga.com](#) [iRigga.es](#) [iRigga.com](#)

Cuando la solicitud de retirada de las imágenes haya resultado infructuosa, los afectados pueden presentar una reclamación en la Sede electrónica de la Agencia Española de Protección de Datos, acompañando la documentación acreditativa de haber solicitado la supresión en primer término al prestador de servicios online.

¿Y si se trata de imágenes de contenido sensible?

En situaciones excepcionalmente delicadas, cuando las imágenes incluyan contenido sexual o muestren actos de violencia, poniendo en alto riesgo los derechos y libertades de los afectados, especialmente víctimas de violencia de género o menores, los canales ofrecidos por los prestadores de servicios online pueden no resultar lo suficientemente eficaces y rápidos para evitar la difusión continuada de las imágenes.

El objetivo del **Canal prioritario** es hacer frente a estas situaciones, estableciendo una vía en la que las reclamaciones recibidas serán analizadas prioritariamente, permitiendo que la Agencia, como Autoridad independiente, pueda adoptar, si es preciso, medidas urgentes que limiten la continuidad del tratamiento de los datos personales.



¿Cómo puedo comunicar esa difusión de imágenes sensibles?

A través de www.aepd.es

El reclamante debe describir las circunstancias en que se ha producido la difusión no consentida de las imágenes, indicando en particular si la persona afectada es víctima de violencia de género, abuso o agresión sexual o acoso, o si pertenece a cualquier otro colectivo especialmente vulnerable como menores de edad, personas con discapacidad o enfermedad grave o en riesgo de exclusión social, así como especificando la dirección o direcciones web en las que se han publicado.

¿Qué decisión puede tomar la Agencia?

Tras el análisis de la reclamación formulada, la Agencia determinará la posible adopción urgente de **medidas cautelares** para evitar la continuidad del tratamiento de los datos personales. Por otra parte, la Agencia valorará si corresponde la apertura de un procedimiento sancionador contra las personas que hayan difundido ese material.



Finalmente, de los seis países participantes, **Colombia, Costa Rica, Paraguay y Perú** están adheridos al **Convenio de Budapest**, mientras que **México** se encuentra únicamente como observador y **Ecuador** tampoco ha firmado dicho instrumento internacional.

La adhesión a dicho instrumento internacional por parte de los países miembros implica un compromiso nacional respecto a la necesidad de aplicar, con carácter prioritario, una política penal común, con el objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional.

Si bien es cierto que la firma del convenio significa la expresión de la voluntad política para sumarse a la lucha contra la ciberdelincuencia para prevenir los actos que pongan en riesgo la integridad, confidencialidad y disponibilidad de los sistemas, redes y datos informáticos, cualquier mecanismo de colaboración internacional es relevante para lograr esfuerzos más globales que permitan establecer objetivos y alcances de mayor beneficio para la población vulnerables, como lo son los menores de edad.

De lo anterior, se advierte necesario para los países que aún no han firmado dicho convenio, llevar a cabo acciones concretas para adherirse a que muestren su preocupación por los riesgos en el uso de las redes informáticas y la información electrónica, los cuales han ido en aumento,



principalmente, ante la contingencia sanitaria que mundial, que ha provocado la hiperconectividad de las personas y por consecuencia, una mayor exposición a los riesgos en el ciberespacio.

La adhesión a dicho instrumento internacional por parte de los países miembros implica un compromiso nacional respecto a la necesidad de aplicar, con carácter prioritario, una política penal común, con el objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional.

Igualmente, los países que no han suscrito el convenio son los que tienen un avance más lento en la construcción de un ecosistema ciberseguro a nivel nacional, en tanto que no hay impulso en las acciones legislativas en la construcción del marco normativo y en la creación o designación de la autoridad rectora en el tema.

De lo anterior, es necesario para los países que aún no han firmado dicho convenio, lleven a cabo acciones concretas para adherirse a dicho instrumento internacional, o en su caso, que muestren su preocupación por los riesgos en el uso de las redes informáticas y la información electrónica, los cuales han ido en aumento, principalmente, ante la contingencia sanitaria que se padece a nivel mundial, y que ha provocado la hiperconectividad de las personas y por consecuencia, una mayor exposición a los riesgos en el ciberespacio.

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

	Colombia	Costa Rica	Ecuador	México	Paraguay	Perú
Política Nacional Digital						
Marco Jurídico						
Marco Reglamentario						
Notificaciones contenido ilícito						
Notificaciones - preocupaciones de los usuarios						
Actores y partes interesadas						
Investigación						
Educación en materia de alfabetización y competencias digitales						
Recursos Educativos						
Protección de la Infancia						
Sensibilización Nacional						
Herramientas, servicios y ajustes						
Medidas de Accesibilidad						
Línea de Ayuda						
Adhesión al Convenio de Budapest						

Cuenta con ... Sí No Parcialmente



Buenas prácticas

Resulta importante destacar que los países participantes han desplegado múltiples y diversas acciones que en su mayoría no han sido diseñadas para la protección de la infancia en línea, pero en sus objetivos, actividades y alcances, pretenden crear espacios digitales para niños y jóvenes que sean seguros, apropiados para su edad, inclusivos y participativos¹⁸⁴, en los que sí atienden algunas de las principales amenazas en línea para los niños.

Entre las buenas prácticas desplegadas por los países participantes, se advierten las siguientes:

Colaboración internacional

El rol positivo que cumple la colaboración internacional, tanto en el aspecto técnico como financiero, es indiscutible. Y como ejemplo de los buenos resultados de proyectos que se han llevado a cabo a través de dicho mecanismo de participación, tenemos el de la Alianza Global para poner fin a la violencia contra los niños (EVAC¹⁸⁵) que inició un programa en Colombia en agosto de 2021, a través del cual se apoya con una inversión de un millón y medio de dólares a Red PaPaz en Colombia para fortalecer los Centros Nacionales Seguros en Línea, espacios de propiedad y operación nacional para que los países prevengan, detecten y respondan al abuso sexual infantil en línea.

Igualmente, a través de la red PaPaz¹⁸⁶ Colombia y México han logrado implementar recientemente la línea de denuncia “te protejo”¹⁸⁷ cuyo objetivo es el trabajo seguro y eficaz para proteger los derechos de niñas, niños y adolescentes de la región, en especial de la violencia sexual en los entornos digitales.

Por otra parte, desde su lanzamiento en julio de 2016, la Alianza Mundial para Poner Fin a la Violencia contra los Niños ha promovido el concepto de Pathfinding¹⁸⁸, que tiene como objetivo crear conciencia, estimular el compromiso de liderazgo, galvanizar la acción y establecer un estándar de prevención nacional de la violencia en todo el mundo. Hoy en día, 37 países se han unido a la asociación como Pathfinders, extendiendo el alcance de la iniciativa a todos los continentes.

¹⁸⁴ https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/Guidelines/2020-translations/S-GEN-COP.POL_MAKERS-2020-PDF-S.pdf, pag. 6.

¹⁸⁵ [The End Violence Partnership invierte \\$3 millones en dos nuevos proyectos para proteger a los niños en línea en Camboya y Colombia | Poner Fin a la Violencia \(end-violence.org\)](https://www.end-violence.org/)

¹⁸⁶ <https://www.redpapaz.org>

¹⁸⁷ <https://teprotejo.org>

¹⁸⁸ <https://www.end-violence.org/pathfinding-countries>



Los países pioneros utilizan las estrategias INSPIRE Seven¹⁸⁹ para poner fin a la violencia contra los niños para comprender los impulsores de la violencia y construir respuestas integradas que mejoren las vidas de los niños y los jóvenes. Estas estrategias se ven a lo largo del proceso de búsqueda de caminos, incluida, entre otras, la creación del plan de acción nacional de un país para poner fin a la violencia.

Colombia, México, Paraguay y Perú, son de los países pioneros en el marco más amplio de los esfuerzos de protección de la niñez que utilizan [las Siete estrategias de INSPIRE para poner fin a la violencia contra los niños](#) para comprender los impulsores de la violencia y crear respuestas integradas que mejoren la vida de los niños y los jóvenes.

Estas estrategias se ven a lo largo del proceso Pathfinding, que incluye, entre otros, la creación de un plan de acción nacional de un país para poner fin a la violencia.

Otro ejemplo de los resultados de la cooperación internacional, es la Iniciativa “**Costa Rica dice No a la Explotación y el Abuso Sexual en Línea de Niñas, Niños y Adolescentes**” (**CR-NEXST**), que nace del reconocimiento país por realizar esfuerzos hacia la democratización de acceso a las tecnologías y la inclusión digital, como supuesto a cumplir para el cierre de brechas socioeconómicas y de conocimiento que limitan el desarrollo sostenible de la nación costarricense. Sin embargo, pese a lo avanzado, el país aún debe robustecer su capacidad institucional para proteger los derechos de la niñez ante la explotación y el abuso sexual en línea.

CR-NEXST es ejecutada por la **Fundación PANIAMOR**, y es financiada por el Fondo **End Violence Partnership & Fund**, y desde su construcción ha contado con la asesoría técnica de **ECPAT International**, además de tener el respaldo institucional sostenido del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), el Instituto Mixto de Ayuda Social (IMAS) del Ministerio de Desarrollo Humano e Inclusión Social, el Patronato Nacional de la Infancia (PANI) y el Sistema de Emergencias 9-11. También ha trabajado en alianza estratégica con el Fondo de Naciones Unidas para la Infancia (UNICEF-CR).

Igualmente, encontramos los esfuerzos a través de la Red ECPAT en Latinoamérica; **ECPAT** es el acrónimo de End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes (Acabar con la Prostitución Infantil, la Pornografía Infantil y el Tráfico de Niños con fines Sexuales); ECPAT International¹⁹⁰ actualmente consta de 122 miembros de ECPAT en 104 países de todas las regiones, entre ellos:

¹⁸⁹ <https://www.end-violence.org/inspire>

¹⁹⁰ <https://ecpat.org/our-members/>



- ✓ Fundación Panimor-ECPAT **Costa Rica**
- ✓ Fundación Renacer-ECPAT **Colombia**
- ✓ Fundación QuitoRaymi- ECPAT **Ecuador**
- ✓ EDIAC-ECPAT **México**
- ✓ Grupo Luna Nueva- ECPAT **Paraguay**
- ✓ CHS Alternativo- ECPAT **Perú**

ECPAT Colombia:¹⁹¹ trabaja para promover y defender los derechos de los niños, especialmente los niños víctimas de explotación sexual comercial. El grupo ha trabajado en comunidades vulnerables y con instituciones educativas en las ciudades de Barranquilla, Bogotá y Cartagena de Indias, convirtiéndose en un líder en prevención y sensibilización de CSEC para los jóvenes del país. El grupo, con la ayuda de la Fundación Renacer, ha centrado su trabajo en dos áreas: prevención y sensibilización y participación de los jóvenes en las políticas públicas. En el área de prevención y sensibilización, las actividades emprendidas incluyen: la creación de un Grupo Juvenil ECPAT para la prevención de CSEC; la capacitación de niños y jóvenes sobre cuestiones de CSEC; actividades recreativas con niños víctimas como parte de la reintegración social; y talleres de sensibilización para padres en comunidades vulnerables a CSEC.

ECPAT Costa Rica:¹⁹² La Fundación Paniamor trabaja para combatir la CSEC, en particular, la trata de niños y el turismo sexual infantil, creando conciencia, trabajando con los organismos encargados de hacer cumplir la ley y gestionando una base de datos de información sobre la trata. El grupo ha establecido un programa de capacitación sobre el Código de Conducta para empleados de empresas de turismo y viajes.

ECPAT México¹⁹³ trabaja con la Red por los Derechos del Niño, que comprende cuatro organizaciones en México. El grupo ha trabajado en la reforma legal en relación con CSEC y la trata con fines sexuales; ha incorporado CSEC a la agenda pública y ha creado conciencia a través de los medios de comunicación; ha ayudado a aumentar el número de miembros del Comité para la Elaboración de una Ley de Trata, compuesto por representantes del mundo académico, organizaciones internacionales, ONG y agencias gubernamentales; ha realizado un análisis de situación de CSEC en el Estado de Tabasco; ha participado en la capacitación de fiscales de Oaxaca; y ha diseñado y coordinado un foro infantil sobre CSEC.

¹⁹¹ <https://ecpat.org/country/colombia/>

¹⁹² <https://ecpat.org/country/costa-rica/>

¹⁹³ <https://ecpat.org/country/mexico/>



ECPAT Paraguay:¹⁹⁴ Luna Nueva, establecida en Asunción en 1995, trabaja para combatir la violencia contra las mujeres y los niños. Es la única organización en Paraguay que trabaja específicamente en problemas relacionados con la explotación sexual y comercial de los niños. Lleva a cabo este trabajo a través del desarrollo e implementación de programas ofrecidos a los niños explotados y también a los trabajadores sexuales adultos en educación, salud, autoestima, derechos humanos y prevención de la violencia. Luna Nueva realiza visitas diarias a mujeres y niños que viven en la calle y participan en la prostitución, ofreciéndoles información médica, asesoramiento sanitario y apoyo continuo.

Red peruana contra CSEC

CHS Alternativo es una organización especializada con 16 años de trabajo promoviendo la protección de los derechos humanos, en particular de las mujeres, los niños y los adolescentes que se encuentran en una situación de vulnerabilidad debido a la trata de personas, la explotación sexual y el trabajo forzoso.

Red peruana contra CSEC (Tejiendo Sonrisas)

Red peruana contra CSEC (REDES- Huancayo)

<https://ecpat.org/country/peru/>

Investigación diagnóstica previa al diseño e implementación de la política pública

En el Caso de Costa Rica, se llevó a cabo una investigación durante casi dos años, en la cual llevó a cabo una revisión del marco normativo nacional entre diversos actores y puntos focales en su país, como primer paso para el diseño de su política pública, para después implementar encuestas y sondeos respecto a diversos temas y que aplicó a distintos sectores de la sociedad.

Detección e intervención de diversos puntos focales, desde el gobierno, el sector privado, organizaciones no gubernamentales, la academia y la sociedad civil.

En la construcción de la política pública de Costa Rica, se desprende que desde las primeras acciones fueron convocados sector gobierno, sector privado y sociedad civil, lo que sin duda aporta una visión integral desde su análisis diagnóstico, durante su implementación y hasta el punto en el que se evalúe o bien, se implementen procesos o mecanismos de mejora, lo que significa un aumento significativo en la calidad de la política pública.

Campañas permanentes de sensibilización y capacitación, en adición a los materiales educativos y el apoyo en materia de alfabetización digital. Todos los esfuerzos y recursos

¹⁹⁴ <https://ecpat.org/country/paraguay/>



empleados en educación y capacitación es una inversión que se traduce en bienestar para la sociedad, ahora más que nunca se requiere de campañas y programas permanentes que se ocupen dotar de capacidades, habilidades y competencias a todos los ciudadanos, más porque la tecnología es cambiante siempre y de manera vertiginosa.

Lecciones aprendidas

Tener una estrategia digital nacional es importante pero no es suficiente para garantizar la protección de la infancia en línea; contar con marcos reglamentarios es indispensable para hacer valer los derechos de los niños, niñas y adolescentes, al igual que contar con la autoridad facultada para hacer cumplir la legislación y aplicar las medidas necesarias ante su inobservancia.

Contar con autoridad en materia de protección de datos personales. De la información obtenida se pudo observar que la actuación de la autoridad nacional encargada de proteger los datos personales es de gran relevancia para las políticas sobre protección de la infancia en línea, al tratarse de un derecho humano que está estrechamente vinculado, además de la colaboración con instituciones de otros sectores (tecnología, comunicaciones, transformación digital, educación, etc.), con el objetivo de generar e implementar campañas, herramientas y recursos de formación, que tienen un impacto directo en la cultura de la protección a la privacidad y la gestión de la identidad digital de los menores, con el objetivo de proteger a los niños, niñas y adolescentes al navegar en internet.

Stakeholders. Respecto a los actores y partes interesadas, se puede destacar que, con excepción de **Costa Rica**, que sí ha convocado a todas las partes interesadas, como lo son las instituciones de gobierno, asociaciones, academia y sociedad civil, el resto de los países participantes han involucrado solamente a algunas de sus instancias de gobierno, es decir, únicamente autoridades, lo que tiene dos consecuencias inmediatas:

1. La disminución de la interoperabilidad entre entes gubernamentales, que conlleva al desconocimiento de la política pública a implementar; y,
2. La falta de convocatoria a stakeholders o partes interesadas durante todo el proceso de la política pública, que tiene como consecuencia que la política pública sea unilateral y no atienda necesidades de todos los sectores, o incluso, que se inviertan recursos en estrategias existentes.

Evaluación de la política pública. No se advierte que se haya llevado a cabo la evaluación de las estrategias implementadas, de las campañas o programas ejecutados, o bien, de los materiales elaborados y publicados; todo lo cual es necesario para conocer además del número de personas beneficiadas, el impacto de los contenidos proporcionados; y en ese mismo sentido,



saber si se cumplió con los objetivos planteados, para la construcción de un programa de mejora eficaz y eficiente.

Cambio de gobierno. La continuidad de las políticas públicas, con independencia de la etapa en la que se encuentre, resulta esencial. Los países de la Región han padecido por décadas durante el cambio de administración pública, el ignorar el trabajo realizado años atrás, sólo por el hecho de haber sido diseñado o implementado por un gobierno diverso, y con ello, presenciar como muchas estrategias dejan de funcionar; sin embargo, el evaluar estrategias anteriores abonará en su permanencia con posibles procesos de mejora, y que además permitirá un ahorro importante en uso de tecnología y personal que ya venía ejecutando la política pública en tiempos de la administración de gobierno anterior.

Algunas de las páginas consultadas aparecen como inseguras o carecen de certificado de seguridad; lo cual debe ser atendido de manera urgente, porque la autoridad debe ser ejemplo ante todos los sectores de la sociedad en el uso de la tecnología, durante cualquier proceso, programas o política pública. Además de que las buenas prácticas implementadas por el sector gobierno pueden ser sumamente útiles para el diseño de estrategias formativas y planes de respuesta a incidentes de seguridad de la información. La ciberseguridad es responsabilidad de todos.

Medidas de accesibilidad para niños, padres, abuelos y cuidadores. De acuerdo a la Convención Internacional sobre los Derechos de las Personas con Discapacidad, que es un instrumento internacional de derechos humanos de las Naciones Unidas o Derecho internacional de los derechos humanos destinada a proteger los derechos y la dignidad de las personas con discapacidad, se observa que en la actualidad es necesario tener en cuenta que los roles en nuestra sociedad han cambiado en los países de la Región de Latinoamérica, entre ello, el hecho que los abuelos han adquirido el rol de cuidadores de sus nietos, principalmente, en edad escolar, es decir, durante la niñez y la adolescencia.

Asimismo, ante la incorporación de las mujeres en la vida laboral, la contratación de personas para desempeñar actividades relacionada con el cuidado de los hijos/as es cada vez más común.

Por ello, es primordial atender a todos los actores que intervienen de alguna manera en el cuidado de los menores, para que tengan los medios y las herramientas en igualdad de condiciones con los demás menores, sin importar quien tenga capacidades diferentes (el menor o el adulto).

Necesidad de contar con un marco jurídico y autoridad en materia de Ciberseguridad

La tecnología avanza de una manera vertiginosa y por ello se requiere de un andamiaje jurídico con una visión progresista, es decir, que no tenga que reformarse cada vez que se dé un cambio



trascendente en el ciber espacio, y para ello se requiere de una autoridad especializada que aplique dicha norma y tenga capacidad y atribución de interpretación de la ley, con la finalidad de resolver incidencias y problemática en el uso de la tecnología, así como vigilante de que los derechos humanos sean una realidad en la red.

Poca difusión de impartición de justicia respecto a delitos digitales. Faltan recursos para que centros educativos y familias tengan conocimiento respecto a respuesta a incidentes y preservación de evidencia digital.

Reconocimiento de estrategias, hay campañas o programas que sí si bien es cierto no tienen como objetivo principal la protección de la infancia en línea, si se advierte que en su diseño e implementación atienden esta temática, principalmente, las que tienen como objetivo reducir la violencia a través de medios digitales.

Modelo replicable

Tomando como parámetro las nuevas Directrices de 2020 sobre la Protección de la Infancia en Línea (PIeL), emitidas por la Unión Internacional de Telecomunicaciones (UIT), consistente en recomendaciones para los niños, los padres y educadores, la industria y los responsables políticos acerca de la manera de contribuir al desarrollo de un entorno en línea seguro y habilitador para los niños y los jóvenes.

- **IDENTIFICAR ACTORES Y PUNTOS FOCALES O PARTES INTERESADAS.** Las diferentes instituciones gubernamentales tienen acercamiento con organizaciones de la sociedad civil que pueden convocar a colaborar, además del sector científico y la academia, y no dejar de lado al público objetivo, a quienes se puede convocar a través de otros medios como encuestas de acceso público.
- **DIAGNÓSTICO** del marco normativo, autoridades, y de las estrategias o políticas públicas existentes sobre el tema de protección de la infancia en línea, para analizar los avances logrados, los retos pendientes, para entonces poder definir las medidas legislativas y las políticas públicas necesarias.
- **COLABORACIÓN MULTISECTORIAL** indispensable del sector gobierno, sector privado, organizaciones de la sociedad civil, comunidad científica e instituciones académicas, y población objetivo, con el objetivo de mejorar los mecanismos de coordinación.
- **DISEÑO E IMPLEMENTACIÓN** de políticas públicas de impacto nacional (reconocer la diferencia entre una política pública y una campaña o programa).



- **INTERINSTITUCIONALIDAD.** Uno de los mayores obstáculos en las administraciones públicas es la falta de empatía institucional, es decir, cuando las instituciones de un mismo gobierno desconocen la existencia del resto de las dependencias públicas, así como su naturaleza, atribuciones y competencia; esa apatía entre instituciones públicas hace que las estrategias y las políticas públicas no tengan el resultado y los alcances previstos.

- **INCLUSIÓN** en todas las etapas de la política pública. Tener en cuenta a todos los actores no es suficiente, ya que es menester conocer y atender particularidades de los mismos.

La inclusión de las personas con capacidades diferentes no es una práctica proactiva, ya que por un lado responde a estándares internacionales, específicamente, a la convención con personas con discapacidad, y por otra parte, resulta preponderante que tanto los menores, así como los actores que interactúan con ellos, es decir, padres, abuelos, cuidadores, educadores, y todo aquél que intervenga en su educación o formación, y que tengan alguna capacidad diferente, estén en igualdad de condiciones para participar y beneficiarse de cualquier estrategia del Estado, más aún, si están encaminadas a la protección de los derechos humanos, pues solo así podrán desarrollar habilidades para acompañar a los menores que por alguna circunstancia se encuentren bajo su cuidado.

- **DIFUSIÓN.** Entre todas las autoridades de gobierno para su conocimiento, y no solamente entre las encargadas de la implementación de la política pública, ya que, en el presente análisis, se pudo observar que muchas de las autoridades participantes desconocían de la existencia de normatividad, programas e incluso de políticas públicas de observancia nacional, y que incluso ya han sido implementadas.

- **IMPLEMENTACIÓN.** Esta fase en el proceso de una política pública es elemental, porque no sólo debe vigilarse el diseño, sino que debe estructurarse de manera precisa los pasos y actividades que deben ejecutarse al momento de implementar la estrategia, incluso prever la posibilidad de activar algún plan contingente en esa propia etapa para garantizar el cumplimiento de los objetivos propuestos.

- **EVALUACIÓN INTERNA Y DE USUARIOS O RECEPTORES.** Conocer la visión de quienes implementan y quienes son población objeto de la estrategia dará como resultado un ejercicio integral del que se puede derivar una propuesta de mejora mucho más efectiva.

- **PROCESOS DE MEJORA.** Los que se determinen en la evaluación de la política pública bajo estándares de honestidad, transparencia, y con una perspectiva de protección de los derechos humanos.



- **ACTUALIZACIÓN EN LAS ESTRATEGIAS YA IMPLEMENTADAS (TEMAS, AUTORIDADES INVOLUCRADAS, ALCANCES DE LA POLÍTICA PÚBLICA).** Pues los esfuerzos deben avanzar en la misma proporción que la tecnología. Una estrategia que no visualice las actualizaciones respecto a los temas que aborda, las autoridades y puntos focales involucrados en el diseño, implementación, evaluación y procesos de mejora de la estrategia, terminará por ser un esfuerzo parcialmente exitoso.
- **CONTINUIDAD DE CAMBIO DE GOBIERNOS.** Encontrar mecanismos que garanticen la continuidad de las estrategias nacionales no es una tarea fácil, y el cambio de gobierno tiene múltiples implicaciones, entre ellas, el riesgo de desaparición de las políticas públicas, con independencia de su estado (diagnóstico, planeación, ejecución, monitoreo y/o evaluación); sin embargo, es una cuestión que debe abordarse desde el diseño de las mismas, porque la implementación total de cualquier estrategia, que incluya las etapas de evaluación y mejora, ayudará a conocer los resultados de la estrategia, pero también dará la oportunidad de mejorar lo llevado a cabo.
- **ESFUERZOS REGIONALES ENCAMINADOS A LO GLOBAL.** Son urgentes e indispensable para que los países que todavía no cuentan aún con una estrategia digital nacional o normas específicas, estén en posibilidad de actuar conforme al marco de dichos esfuerzos basados en los derechos humanos, y seguir los pasos de los países que ya llevan a cabo su propio proceso, como el caso **Costa Rica**, que muestra ser el que ya cuenta con un nivel de madurez en sus políticas de protección de la infancia en línea, en comparación con las de los seis países participantes en el presente análisis.

Desafíos regionales y posibles soluciones

1. Ausencia de marcos normativos y de autoridad nacional en materia de ciberseguridad.

Ciertamente, todos los países han lanzado su Estrategia Nacional de Ciberseguridad de la mano de la OEA, pero ello no ha sido suficiente para que los países participantes en el presente análisis hayan desplegado las acciones institucionales necesarias para la creación y operatividad de una autoridad rectora en ciberseguridad en cada país, así como la publicación de andamiaje jurídico necesario que también contemple de manera específica la protección de la infancia en línea.

2. Atender brechas digitales o de conectividad¹⁹⁵ que atraviesa toda América Latina, y como ejemplo podemos citar la que actualmente atraviesa Perú, es importante, pues a pesar de los esfuerzos del gobierno por desplegar redes de banda ancha en todas las regiones del país, la

¹⁹⁵ <http://dnconsultores.com/wp-content/uploads/2021/09/210902-Conectividad-digital-Agenda-inicial.pdf> página 7.



brecha o carencia o de conectividad (en especial a redes de banda ancha) persiste y se agrava mayormente en las zonas alejadas o dispersas fuera de las ciudades.

Si consideramos a la población total del país de 32 millones de habitantes y excluimos a la población infantil menor a 6 años de 3 millones, esto significa que 19 millones de peruanos son usuarios de Internet y que otros 10 millones son no usuarios.

3. Desconocimiento de la ciberseguridad. Contribuir desde la acción directa de las estrategias nacionales de cada país de la Región, para mantener el bienestar y seguridad digital, al promover oportunidades de crecimiento (proyectos de vida) y participación en el entorno digital.

Fortalecer el incremento en la designación de recursos humanos y financieros suficientes para atender la explotación sexual en línea de niños y adolescentes, a fin de facilitar más información y empoderar a la población objetivo.

Diseñar estrategias robustas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales en el mundo en internet, así como la seguridad de los datos institucionales.

Continuar con el diseño de mecanismos de promoción de cultura de ciberseguridad y alfabetización digital a todos los usuarios, incluidos las niñas, niños y adolescentes.

Contar con mecanismos regionales de colaboración entre las autoridades y los prestadores de servicios y contenidos en Internet, para reportar y proporcionar información de los usuarios que cometen conductas delictivas a través de Internet, en agravio de niñas, niños y adolescentes.

Capacitar a Jueces, Fiscales, Ministerios públicos, unidades de policía cibernética, policía de investigación y peritos en el proceso de investigación de los delitos y conductas asociales, que se cometen a través del internet, en agravio de niñas, niños y adolescentes.

Mecanismos efectivos de atención víctimas directas e indirectas de delitos o conductas cometidas en agravio de menores a través de medios digitales, en la que se contemple una reparación integral para las víctimas.

4. Repositorio Regional de contenidos y herramientas. De la consulta de los sitios web de las autoridades, asociaciones, instituciones educativas, y todas las citadas en este documento, pertenecientes a los países participantes, así como las de índole internacional, se advierte que hay un gran número de materiales, recursos didácticos, tutoriales, guías, herramientas tecnológicas y aplicaciones, entre muchas otras, que tienen como objetivos comunes, la protección y el empoderamiento de los niños y jóvenes en línea; por consiguiente, contar con una plataforma donde cualquier persona pueda acceder a toda esa información, y además observar los esfuerzos de la propia nación, así como de otros países, sería útil, necesario y de múltiples



beneficios, ya que no sólo representa una ventaja para las personas que tengan la posibilidad de conocer el repositorio, pues las autoridades tendrían una enorme área de oportunidad, al poder replicar esfuerzos realizados por otros países, lo que equivaldría al ahorro de tiempo y recursos económicos, aunado a que sin duda, ayudaría a estandarizar contenidos y hacer propuestas regionales que permitan ejecutar alianzas para evaluar y llevar a cabo procesos de mejora de los contenidos.

Es de suma importancia mencionar que **muchas de las estrategias que se contienen en este informe, no fueron proporcionadas por los países participantes, de lo que puede advertirse un desconocimiento de la totalidad de los trabajos que se ejecutan en materia de protección de los niños en línea**, lo cual impide que se convierta en una política pública que tenga el alcance esperado o incluso uno mayor.

5. Encuentro entre responsables de las políticas respecto a las políticas de protección y empoderamiento de los niños y jóvenes en línea. Conocer los esfuerzos, materiales, lecciones aprendidas y estrategias en diseño e implementación llevadas a cabo por diversos países, puede abonar en gran medida para lograr la homologación de procesos y establecer estándares mínimos de evaluación y resultados, así como mecanismos de mejora; asimismo, podrían colaborar a generar documentos basados en los propios resultados de cada país, para hacer propuestas a diferentes sectores del gobierno, como por ejemplo, para la elaboración y emisión de normatividad especializada, bien, para la capacitación de impartidores de justicia o instituciones educativas, que atiendan los retos que la tecnología y la vida digital imponen día con día.



MATERIAL DE REFERENCIA

Referencias ITU

ITU Global Programme on Child Online Protection: <https://www.itu-cop-guidelines.com/implementation>

Carta de los derechos digitales de los niños, niñas y adolescentes: <https://www.anar.org/wp-content/uploads/2019/07/Carta-Derechos-Digitales.pdf>

Directrices sobre la protección de la infancia en línea para los encargados de formular políticas: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/COP/Guidelines/2020-translations/S-GEN-COP.POL_MAKERS-2020-PDF-S.pdf

Glosario de [las Directrices de la COP en español](#) para los responsables de la formulación de políticas, Anexo 1: Terminología, p 55, disponible en: https://www.itu-cop-guidelines.com/files/uqd/9ad503_ddd11b88e9fb446db04dac88def1428a.pdf

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

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

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

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

<https://www.end-violence.org/inspire>

<https://www.end-violence.org/pathfinding-countries>



Referencia Colombia

<http://www.saludcapital.gov.co/Paginas2/Linea106-Inicio.aspx>

https://caivirtual.policia.gov.co/sites/default/files/riesgos_y_tendencias_en_relacion_con_el_abuso_y_la_explotacion_sexual_de_los_ninos_a.pdf

https://gobiernodigital.mintic.gov.co/692/articles-78126_informe_pol_gob_digital_2020.docx

https://gobiernodigital.mintic.gov.co/692/articles-78126_ppt_resultados_gob_digital_2020.pptx

https://gobiernodigital.mintic.gov.co/692/channels-594_manual_gd.pdf

<https://gobiernodigital.mintic.gov.co/portal/Mediciones/>

https://issuu.com/quioscosic/docs/guia_cuida_tu_identidad_digital_002

<https://teprotejo.org>

<https://www.childhelplineinternational.org/data-overview/publications/voices-data2020/>

<https://www.end-violence.org/articles/end-violence-partnership-invests-3-million-two-new-projects-protect-children-online>

<https://www.enticconfio.gov.co/>

<https://www.icbf.gov.co/linea-de-proteccion-ninos-ninas-y-adolescentes-141>

https://www.mineducacion.gov.co/1759/articles-398739_Guia_006.pdf

<https://www.mintic.gov.co/portal/inicio/>

<https://www.policia.gov.co/proteccion-infancia/proteccion-integral>

https://www.policia.gov.co/sites/default/files/informe_rendicion_de_cuentas-infancia_y_adolescencia.pdf

<https://www.redpapaz.org>

SIC COLOMBIA sitio web https://www.sic.gov.co/centro-de-publicaciones?field_global_topic_tid=7037&field_anos_p_value=All

[The End Violence Partnership invierte \\$3 millones en dos nuevos proyectos para proteger a los niños en línea en Camboya y Colombia | Poner Fin a la Violencia \(end-violence.org\)](https://www.end-violence.org)



Referencia Costa Rica

Agencia de Protección de Datos de los Habitantes (2021) <http://www.prodhab.go.cr/>

Aldeas SOS. Conócenos. <https://www.aldeasinfantiles.or.cr/>

Caja Costarricense de Seguro Social. *Guía de atención integral a niños, niñas y adolescentes víctimas de abuso*. <https://www.binasss.sa.cr/protocolos/victimasabuso.pdf>

Coalición Nacional contra el Tráfico Ilícito de Migrantes y la Trata de Personas (2020). *Política Nacional contra la Trata de Personas*.

<https://www.migracion.go.cr/Documentos%20compartidos/Politic/Politica%20Nacional%20Contra%20la%20Trata%20de%20Personas.pdf>

Consejo Nacional de la Persona con Discapacidad (2011). *Política Nacional de Discapacidad*. http://www.conapdis.go.cr/el_conapdis/marco_legal/documentacion_marco_legal/PONADIS%202011-2030.pdf

Contraloría General de la República (2007). *Normas técnicas para la gestión y el control de las Tecnologías de Información*. https://www.pgr.go.cr/wp-content/uploads/2016/12/Normas_tecnicas_N_2_2007_CO_DFOE_de_la_CGR.pdf

Ministerio de Cultura y Juventud (2020). *Política Pública de la Persona Joven 2020-2024*: <https://www.unicef.org/costarica/media/2631/file/Pol%C3%ADtica%20P%C3%ABblica%20de%20la%20Persona%20Joven%202020-2024.pdf>

Defense for Children International: <https://defenceforchildren.org/es/conocenos-es/>

Decreto Ejecutivo N° 36274-MICIT de 2010. Creación de la Comisión Nacional de Seguridad en Línea 09 de diciembre de 2010. Diario Oficial La Gaceta N° 239

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=69239&nValor3=83075&strTipM=FN

Directriz N° 051-MTSS-MICITT (2019). Implementación de sitios Web accesibles en el sector público costarricense. 25 de junio de 2019. Diario Oficial La Gaceta 118.

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=89061&nValor3=116705¶m2=1&strTipM=TC&Resultado=1&strSim=simp

Instituto Nacional de las Mujeres. (2018). *Política Nacional para la Igualdad Efectiva entre Mujeres y Hombres en Costa Rica 2018-2030*.



<https://www.inamu.go.cr/documents/10179/401246/INAMU+PIEG+2018-2030+NEW.pdf/f8333d70-df04-417e-bbe9-c48c412a3cfb>

Fondo de las Naciones Unidas para la Infancia (10 de setiembre de 2021). Firmada Ley para la Prevención del Acoso a Personas Menores de Edad por medios electrónicos. Comunicado de prensa. <https://www.unicef.org/costarica/comunicados-prensa/firmada-ley-para-la-prevencion-del-acoso-personas-menores-de-edad-por-medios>

Fundación Omar Dengo. ¿Quiénes somos? <https://fod.ac.cr/>

Fundación Paniamor. *Iniciativa Código e-mentores.*

<https://paniamor.org/Project/detail/37/iniciativa-codigo-ementores>

Fundación Quirós Tanzi, (2020). *Conectándonos en línea*

<https://sites.google.com/fundacionqt.org/recursos-fqt/p%C3%A1gina-principal>

Ley N° 8148 de 2001. Adición de los artículos 196 bis, 217 bis y 229 bis al Código Penal, Ley N° 4573 para reprimir y sancionar los delitos informáticos. 9 de noviembre de 2001. Alcance 81 del Diario Oficial La Gaceta N° 216.

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=47430&nValor3=50318&strTipM=FN

Ley N° 9048 de 2012. Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal. 6 de noviembre de 2012. Alcance 172 del Diario Oficial La Gaceta N°214 (versión de la norma al 2015)

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=73583&nValor3=0&strTipM=FN

Ley N° 9145 de 2013. Reforma de los artículos 196, 196 bis, 230, 293 y 295 y adición del artículo 167 bis al Código Penal. 26 de abril de 2013. Alcance 78 Diario Oficial La Gaceta N°80. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=74706&nValor3=92348&strTipM=FN

Ley 8642 de 2008. Ley General de Telecomunicaciones. 30 de junio de 2008. Diario Oficial La Gaceta

N°125. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=63431&nValor3=114006¶m2=1&strTipM=TC&IResultado=5&strSim=simp

Ley 9952 de 2021. Día Nacional de la lucha contra el "Grooming". 6 de marzo de 2021. Diario Oficial La Gaceta N°60.



http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC¶m2=1&nValor1=1&nValor2=93987&nValor3=124933&strTipM=TC&IResultado=1&nValor4=1&strSelect=sel

Ley 7600 de 1996. Ley de Igualdad de Oportunidades para las Personas con Discapacidad. 29 de mayo de 1996. Diario Oficial La Gaceta N°102.

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=23261&nValor3=96047

Ley 8661 de 2008. Aprobación de la convención sobre los derechos de las personas con discapacidad. 29 de setiembre de 2008. Diario Oficial La Gaceta N° 187.

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=64038&nValor3=74042&strTipM=TC

Long, Soraya (2018). Informe sobre estado de situación del país sobre su capacidad para la prevención y respuesta a la explotación y abuso sexual en línea de NNA (EASNNAL) Fundación Paniamor.

Ministerio de Ciencia, Tecnología y Telecomunicaciones (2017). Política Nacional de Sociedad y Economía basadas en el Conocimiento.

https://www.micit.go.cr/sites/default/files/politica_nacional_sociedad_y_economia_en_el_conocimiento-min.pdf

Ministerio de Ciencia, Tecnología y Telecomunicaciones (2015). Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021. <https://www.micit.go.cr/plan-nacional-desarrollo-las-telecomunicaciones>

Ministerio de Ciencia, Tecnología y Telecomunicaciones (2021). *Plan Nacional de Desarrollo de las Telecomunicaciones 2022-2027*. <https://www.micit.go.cr/micitt/publicaciones/construccion-plan-nacional-desarrollo-las-telecomunicaciones-2022-2027>

Ministerio de Ciencia, Tecnología y Telecomunicaciones (2017). *Política nacional para la igualdad entre mujeres y hombres en la formación, el empleo y el disfrute de los productos de la ciencia, la tecnología, las telecomunicaciones y la innovación 2018-2027*.

<https://www.micit.go.cr/sites/default/files/pdf.pdf>

Ministerio de Ciencia, Tecnología y Telecomunicaciones (2018). *Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0 2018-2022*.

<https://www.micit.go.cr/sites/default/files/estrategia-tdhcrb.pdf>



Ministerio de Ciencia, Tecnología y Telecomunicaciones (2020). *Informe técnico MICIT-DEMT-INF-003-2020. Resultados de los compromisos del Ministerio de Ciencia, Tecnología y Telecomunicaciones con el Programa e-mentores 2019*. San José Costa.

Ministerio de Ciencia, Tecnología y Telecomunicaciones (2021). Informe técnico MICITT-DEMT-INF-004-2021 Actividades para la promoción de la seguridad y prevención de riesgos en línea Periodo 2020. San José, Costa Rica.

Ministerio de Ciencia, Tecnología y Telecomunicaciones (2021). Informe técnico MICITT-DEMT-INF-016-2021 Resultados de las actividades en Conmemoración del Día de las Niñas en las TIC, 2021. San José, Costa Rica.

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. Diagnóstico Sector Telecomunicaciones. Plan Nacional de Desarrollo de las Telecomunicaciones 2022-2027. https://www.micit.go.cr/sites/default/files/diagnostico_sector_telecomunicaicones_pndt_2022-2027_version_final.pdf

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (2021). Estrategia Nacional para la Prevención y Respuesta a la Explotación y Abuso Sexual de Niños, Niñas y Adolescentes en Línea 2021-2027. https://www.micit.go.cr/sites/default/files/estrategia_nacional_easnnal_2021-2027.pdf

Fondo de Naciones Unidas para la Infancia (2017). Plan Nacional para el Desarrollo de Estrategias de Prevención y Erradicación de la Violencia Contra Niños, Niñas y Adolescentes, Costa Rica. <https://www.unicef.org/costarica/media/341/file/Plan-nacional-para-desarrollar-estrategias-de-prevencion-y-erradicacion-de-la-violencia.pdf>

Ministerio de Educación Pública (2020) Política en Tecnologías de la Información del Ministerio de Educación Pública 2020. <https://www.mep.go.cr/sites/default/files/politica-tic-mep.pdf>

Ministerio de Educación Pública (2015). Protocolo de actuación en situaciones de violencia física, psicológica, sexual, acoso y hostigamiento sexual. <https://www.mep.go.cr/sites/default/files/protocolo-situaciones-violencia.pdf>

Ministerio de Salud (2010). Política Nacional de sexualidad 2010-2021. I Parte Marco Conceptual y Normativo de la Política. <https://www.ministeriodesalud.go.cr/index.php/biblioteca-de-archivos/sobre-el-ministerio/politcas-y-planes-en-salud/politicas-en-salud/1038-politica-nacional-de-sexualidad-2010-2021-parte-i/file>

Ministerio de Salud (2003). *Legislación relacionada con la promoción, defensa y garantía de los derechos humanos de las niñas, niños y adolescentes en Costa Rica*.



https://www.ministeriodesalud.go.cr/gestores_en_salud/derechos%20humanos/leyes/legisninezadoles.pdf

Ministerio de Planificación Nacional y Política Económica (2021). Modelo de Seguimiento al Cumplimiento del Código de la Niñez y la Adolescencia. <https://www.mideplan.go.cr/node/1100>

Ministerio Público, Poder Judicial (2008). Protocolo de atención legal a víctimas de delitos sexuales y violencia doméstica cometidos por personas menores de edad. [https://sitiooj.poder-judicial.go.cr/images/Documentos/Otras-](https://sitiooj.poder-judicial.go.cr/images/Documentos/Otras-Normativas/Protocolo_de_Atencion_Legal_Victimas_de_Delitos%20Sexuales_Violencia_Dome)

[Normativas/Protocolo de Atencion Legal Victimas de Delitos%20Sexuales Violencia Dome](https://sitiooj.poder-judicial.go.cr/images/Documentos/Otras-Normativas/Protocolo_de_Atencion_Legal_Victimas_de_Delitos%20Sexuales_Violencia_Dome)
[stica cometidos por Menores de Edad.pdf](https://sitiooj.poder-judicial.go.cr/images/Documentos/Otras-Normativas/Protocolo_de_Atencion_Legal_Victimas_de_Delitos%20Sexuales_Violencia_Dome)

Núñez, Andrea (2017). El Sistema Nacional de Protección Integral y los Subsistemas Locales de Protección Infantil en Costa Rica: Un contraste entre lo normativo y lo práctico. *Revista Enfoques: Ciencia Política y Administración Pública XV (26)*.

Organismo de Investigación Judicial (2021). Análisis de la información, seducción o encuentro con personas menores de edad por medios electrónicos 2019-2021. [Archivo PDF]. San José, Costa Rica.

Organización para la Cooperación y el Desarrollo Económicos (2020). Digital economy policy in Costa Rica. <https://www.oecd.org/costarica/digital-economy-policy-in-costa-rica.pdf>

Patronato Nacional de la Infancia (2021). Consejo Nacional de la Niñez y la Adolescencia <https://pani.go.cr/consejo-nacional-de-la-ninez-y-la-adolescencia/>

Patronato Nacional de la Infancia (2009). Política Nacional para la Niñez y Adolescencia de Costa Rica 2009-2021. <https://pani.go.cr/descargas/politicas/216-politicanna-2009/file>

Pueblito CR (2021). Quienes somos. <https://www.pueblitocr.com/quienes-somos>

Reglamento de funcionamiento interno de la Comisión Nacional contra la Explotación Sexual Comercial de Niños, Niñas y Adolescentes N° 37563-MTSS (2013). Comisión Nacional contra la Explotación Sexual Comercial de Niños, Niñas y Adolescentes

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74367&nValor3=91803&strTipM=TC

Rodríguez E. (12 de setiembre de 2021). Inamu y Unicef darán capacitaciones sobre Ciberseguridad y Violencia de Género. *La República*. <https://www.larepublica.net/noticia/inamu-y-unicef-daran-capacitaciones-sobre-ciberseguridad-y-violencia-de-genero>



Tribunal Supremo de Elecciones (03 de agosto de 2021). TSE impulsa formación de ciudadanos responsables en el uso de las redes sociales.

<https://www.tse.go.cr/comunicado710.htm>

World Vision (2021). Quienes somos. <https://www.worldvision.cr/quienes-somos>

<https://www.micit.go.cr/micitt/publicaciones/construccion-plan-nacional-desarrollo-las-telecomunicaciones-2022-2027>

https://crianzatecnologica.paniamordigital.org/sites/default/files/recursos_apoyo%20paniamor_pervencion_y_respuesta.pdf

<http://www.paniamor.org>

<https://es-la.facebook.com/fundacionquirosanzi/>

<https://fod.ac.cr>

<https://www.worldvision.cr/quienes-somos>

<https://www.aldeasinfantiles.or.cr/conocenos>

<https://www.pueblitocr.com/quienes-somos>

<https://www.end-violence.org/members/defensa-de-ninas-y-ninos-internacional-dni-costa-rica>

<http://www.foscr.org/nosotros/>

<https://www.inec.cr>

<https://www.icmec.org>

<https://ifedvirtual.tse.go.cr/>

<https://www.mep.go.cr/protocolos-de-actuacion>



Referencia Ecuador

<https://www.arcotel.gob.ec/por-un-internet-seguro-para-ninos-ninas-y-adolescentes/>

https://www.asambleanacional.gob.ec/sites/default/files/documents/old/constitucion_de_bolsillo.pdf

<https://www.dialogando.com.ec/guia-de-control-parental/>

<https://www.gob.ec/regulaciones/codigo-organico-organizacion-territorialcootad>

<https://www.hallo.ec/uploads/GUIA-CONTROL-PARENTAL- -ARCOTEL.pdf>

<https://www.igualdad.gob.ec/marco-normativo-adolescencia/>

https://www.igualdad.gob.ec/wpcontent/uploads/downloads/2018/05/seminario_legislar_sara_oviedo.pdf

<https://www.registrocivil.gob.ec/wp-content/uploads/downloads/2014/01/este-es-06-CÓDIGODE-LA-NIÑEZ-Y-ADOLESCENCIA-Leyes-conexas.pdf>



Referencia México

Diario Oficial, Órgano del Gobierno Provisional de la República Mexicana, el 05 de febrero de 1917, disponible en el vínculo:

https://www.dof.gob.mx/index_113.php?year=1917&month=02&day=05,

Disponible para su consulta en:

https://docs.google.com/forms/d/e/1FAIpQLSe39JYTKAMTSLqmO_LrEwVsuE9zZFeMZZAjosYF09AJIT00A/viewform

Disponible para su consulta en: <http://inicio.inai.org.mx/PublicacionesComiteEditorial/INA.pdf>

Disponible para su consulta en:

<http://inicio.inai.org.mx/Publicaciones/ProteccionRedesSociales.pdf>

Disponible para su consulta en: <https://home.inai.org.mx/wp-content/documentos/ActasSesionesDelPleno/acta251016.pdf>

Disponible para su consulta en: <https://home.inai.org.mx/wp-content/documentos/AcuerdosDelPleno/ACT-PUB-11-11-2020.08.pdf>

Disponible para su consulta en: <https://ifai->

[my.sharepoint.com/personal/erwin_bautista_inai_org_mx/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Ferwin%5Fbautista%5Finai%5Forg%5Fmx%2FDocuments%2FDescargas%20CLIC%2001NAI%2FMEMORAMA%2DINAI%2Epdf&parent=%2Fpersonal%2Ferwin%5Fbautista%5Finai%5Forg%5Fmx%2FDocuments%2FDescargas%20CLIC%2001NAI](https://ifai-my.sharepoint.com/personal/erwin_bautista_inai_org_mx/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Ferwin%5Fbautista%5Finai%5Forg%5Fmx%2FDocuments%2FDescargas%20CLIC%2001NAI%2FMEMORAMA%2DINAI%2Epdf&parent=%2Fpersonal%2Ferwin%5Fbautista%5Finai%5Forg%5Fmx%2FDocuments%2FDescargas%20CLIC%2001NAI)

Disponible para su consulta en: <https://irp.cdn->

[website.com/81280eda/files/uploaded/17%20Estudio%20sobre%20los%20Hábitos%20de%20os%20Usuarios%20de%20Internet%20en%20México%202021%20v16%20Publica.pdf](https://irp.cdn-website.com/81280eda/files/uploaded/17%20Estudio%20sobre%20los%20Hábitos%20de%20os%20Usuarios%20de%20Internet%20en%20México%202021%20v16%20Publica.pdf)

Disponible para su consulta en: <https://www.inegi.org.mx/programas/mociba/2020/>

Disponible para su consulta en:

<https://www.youtube.com/playlist?list=PLAhw62t2Z4CrPGs5rNHdAiE32oeRgJUqv>

Disponible para su descarga en: <https://play.google.com/store/apps/details?id=com.stick.inaiapp>

http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

http://dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

http://dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

http://dof.gob.mx/nota_detalle.php?codigo=5622965&fecha=05/07/2021



<http://home.inai.org.mx/wp-content/documentos/GuiaTitulares/GuiaSupervisionParenta.pdf>

http://inicio.ifai.org.mx/Guias/Material_Preparatoria.pptx

http://inicio.ifai.org.mx/Guias/Material_Primary_4o_6o.pptx

http://inicio.ifai.org.mx/Guias/Material_Secundaria.pptx

<http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf>

http://inicio.inai.org.mx/Guias/5RecomendacionesPDP_Web.pdf

http://inicio.inai.org.mx/Guias/Gu%C3%ADa_Prevenir_RI.pdf

http://inicio.inai.org.mx/Guias/Guia_Configuracion_RS.PDF

http://www.diputados.gob.mx/LeyesBiblio/pdf/1_280521.pdf

<http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

http://www.diputados.gob.mx/LeyesBiblio/pdf/LGDNNA_110121.pdf

http://www.diputados.gob.mx/LeyesBiblio/pdf/LGDNNA_110121.pdf

<http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>

http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum/CPEUM_orig_05feb1917.pdf

http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum/CPEUM_orig_05feb1917_ima.pdf

http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_251_28may21.pdf

http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

http://www.dof.gob.mx/nota_detalle.php?codigo=5343881&fecha=08/05/2014

http://www.dof.gob.mx/nota_detalle.php?codigo=5436057&fecha=04/05/2016

<http://www.ift.org.mx/comunicacion-y-medios/infantics>

<http://www.ift.org.mx/conocenos/hoja-de-ruta-2021-2025>

<http://www.ift.org.mx/conocenos/programa-anual-de-trabajo>

<http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/estrategia20202025acc.pdf>

<http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/upr-planaccionesiberseguridad.pdf>

<http://www.ift.org.mx/usuarios-y-audiencias/ciber-club-ift>



<http://www.ift.org.mx/usuarios-y-audiencias/ciberseguridad>

<http://www.ift.org.mx/usuarios-y-audiencias/ciberseguridad-para-pymes>

<https://ciberseguridad.ift.org.mx/>

https://ciberseguridad.ift.org.mx/reporte_ciudadano.php

https://ciberseguridad.ift.org.mx/reporte_ciudadano.php

https://ciberseguridad.ift.org.mx/seccion/ninas_ninos_y_adolescentes

https://ciberseguridad.ift.org.mx/seccion/ninas_ninos_y_adolescentes

https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021

<https://home.inai.org.mx>

<https://home.inai.org.mx/wp-content/documentos/AcuerdosDelPleno/ACT-PUB-11-11-2020.05.pdf>

<https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/codigobuenaspracticasnna.pdf>

<https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-055-21.pdf>

<https://home.inai.org.mx/wp-content/uploads/Recomendaciones-a-autoridades-educativas-para-el-tratamiento-seguro-de-im%C3%A1genes-de-ni%C3%B1as-ni%C3%B1os-y-adolescentes-en-eventos-escolares-1920x1920.jpg>

<https://home.inai.org.mx/wp-content/uploads/Recomendaciones-Los-Dispositivos-y-Juquetes-Conectados-a-Internet.png>

<https://micrositios.inai.org.mx/clic/>

https://micrositios.inai.org.mx/clic/?page_id=450

https://micrositios.inai.org.mx/clic/?page_id=601#&gid=29a38e1f&pid=1

<https://micrositios.inai.org.mx/clic/wp-content/uploads/2019/10/c3-1.jpg>

<https://micrositios.inai.org.mx/clic/wp-content/uploads/2019/10/c4-1.jpg>

<https://micrositios.inai.org.mx/clic/wp-content/uploads/2019/10/Gu%C3%ADaParaPadresMadres.pdf>

<https://micrositios.inai.org.mx/clic/wp-content/uploads/2019/10/GuiaEducadores.pdf>



<https://micrositios.inai.org.mx/clic/wp-content/uploads/2020/04/CuidarImagenMenores-Revdgpar-220819-1920x1920.jpg>

<https://micrositios.inai.org.mx/clic/wp-content/uploads/2020/04/Doxing.jpg>

<https://micrositios.inai.org.mx/clic/wp-content/uploads/2020/04/RecomendacionesPadres-Revdgpar220819-1920x1920.jpg>

<https://micrositios.inai.org.mx/identidadsegura/>

<https://micrositios.inai.org.mx/marcocompetencias/>

<https://sesamo.com/monstruos-en-red/>

<https://socialtic.org/>

<https://teprotejo.org>

<https://usuarios.ift.org.mx/Encuesta-2-2018/>

<https://usuarios.ift.org.mx/Encuesta-4-2019/>

<https://www.cndh.org.mx/>

https://www.dof.gob.mx/nota_detalle.php?codigo=5374143&fecha=04/12/2014

https://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018

https://www.dof.gob.mx/nota_detalle.php?codigo=5539474&fecha=28/09/2018

https://www.dof.gob.mx/nota_detalle.php?codigo=5605789&fecha=25/11/2020

<https://www.gob.mx/gncertmx/articulos/110597>

<https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad>

<https://www.gob.mx/segob>

<https://www.gob.mx/sep>

<https://www.gob.mx/sipinna>

<https://www.un.org/es/events/childrenday/pdf/derechos.pdf>

<https://www.womcy.org/es/inicio/>

<https://www.youtube.com/watch?v=C2i0fhxCP5A>

<https://www.youtube.com/watch?v=CjkiYxdcH8M>

<https://youtu.be/CjkiYxdcH8M>



<https://youtu.be/nzRP5SnICQI>

<https://youtu.be/OJNsEQ-Tkm4>

[PyMEs: Pequeñas y medianas empresas](#)

www.dof.gob.mx/2020/INAI/ACT-PUB-11-11-2020-05.pdf



Referencias Paraguay

Guía de alfabetización digital EmpoderaTECH abre oportunidades a mujeres adultas

https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/regions/paraguay_global_partnership_-_plan_pais_imprimir.pdf

<https://www.mitic.gov.py/agenda-digital/que-es>

<https://www.mtess.gov.py/noticias/guia-de-alfabetizacion-digital-empoderatech-abre-oportunidades-mujeres-adultas>

<https://www.paraquay.gov.py/oe/minna/491>

<https://www.senatics.gov.py/observatorio/publicaciones>

PARAGUAY Y LA PROTECCIÓN DE LA NIÑEZ CONTRA EL ABUSO Y TODAS FORMAS DE VIOLENCIA EN LA NUEVA AGENDA PARA EL DESARROLLO SOSTENIBLE 2015-2030

https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/regions/paraguay_global_partnership_-_plan_pais_imprimir.pdf



Referencias Perú

[DIALOGANDO \(https://dialogando.com.pe/\)](https://dialogando.com.pe/)

[EDUCARED \(https://educared.fundaciontelefonica.com.pe/\)](https://educared.fundaciontelefonica.com.pe/)

Fundación ANAR: <https://www.anar.org/anar-peru/>

<https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%202015%20FEBRERO%202021.pdf>

<https://www.acuerdonacional.pe/politicas-de-estado-del-acuerdo-nacional/politicas-de-estado%e2%80%8b/politicas-de-estado-castellano/iv-estado-eficiente-transparente-y-descentralizado/35-sociedad-de-la-informacion-y-sociedad-del-conocimiento/>

<https://www.claro.com.pe/personas/beneficios/movil/control-parental/>

<https://www.drec.gob.pe/noticias/minedu-presentara-programas-contra-el-acoso-sexual-y-la-seguridad-en-internet-en-la-yapa/>

<https://www.gob.pe/anpd>

<https://www.rsu.uni.edu.pe/nosotros/normas-rsu/>

<https://www.unicef.org/peru/comunicados-prensa/preocupaci%C3%B3n-bienestar-ninos-ninas-adolescentes-tiemp-frente-pantalla-internet-seguro>

<https://www.gob.pe/institucion/anpd/campa%C3%B1as/2487-yocuidomisdatospersonales-ii-ee-2019>

<https://www.gob.pe/institucion/anpd/campa%C3%B1as/859-1er-concurso-dibujo-e-historietas-yocuidomisdatospersonales>

<https://www.gob.pe/institucion/anpd/campa%C3%B1as/2973-yocuidomisdatospersonales-ii-ee-2020>