Consejo Nacional para la
Igualdad Intergeneracional

ChildFund®

Evaluación de la **Política Pública** por una **internet segura para niños, niñas y adolescentes**

EQUIPO TÉCNICO
Consejo Nacional para la Igualdad Intergeneracional
Arón Sánchez, Secretario Técnico
Leticia Peñafiel, Directora Técnica
Rina Capelo, Analista de Protección Integral 3
Sandra Báez, Analista de Protección Integral 3
Victor Vilaña, Analista de Protección Integral 3

EQUIPO EXTERNO
ChildFund Internacional
María Auxiliadora Villagómez, Directora País
Gabriela Alarcón, Consultora de Incidencia
Grace Vásquez, Especialista de Incidencia y Protección de la Niñez

INFORMACIÓN
Ministerio de Educación
Ministerio de Inclusión Económica y Social
Ministerio de Relaciones Exteriores y Movilidad Humana
Ministerio de Telecomunicaciones y de la Sociedad de la Información
Ministerio de la Mujer y Derechos Humanos
Consejo Nacional para la Igualdad Intergeneracional
Instituto Nacional de Estadística y Censos
Agencia de Regulación y Control de las Telecomunicaciones
Consejo de la Judicatura
Fiscalía General del Estado
Childfund Ecuador

DISEÑO Y DIAGRAMACIÓN
Sofía Albornoz V.

FOTOGRAFÍAS
ChildFund International USA.
Consejo Nacional para la Igualdad Intergeneracional
Primera Edición, 2025
Consejo Nacional para la Igualdad Intergeneracional
Eloy Alfaro N28-105 y Av. 10 de Agosto
Quito- Ecuador
www.igualdad.gob.ec

Consejo Nacional para la
Igualdad Inter generacional

ChildFund®

Evaluación de la **Política Pública** por una **internet segura para niños, niñas y adolescentes**

DICIEMBRE 2024

Índice

Introducción

La política pública "Por una Internet Segura para Niños, Niñas y Adolescentes" en Ecuador tiene como objetivo principal promover un uso saludable, seguro y constructivo de Internet para la población infantil y juvenil. Esta política se centra en maximizar los beneficios y oportunidades que ofrecen las tecnologías digitales, mientras implementa medidas preventivas y protocolos de atención para proteger a niñas, niños y adolescentes frente a posibles riesgos en el entorno virtual.

El desarrollo de esta política responde a la necesidad de proteger los derechos de los niños, niñas y adolescentes en el contexto digital, promoviendo su integridad física, psicológica, emocional y sexual. La política busca fortalecer las competencias de autoprotección de este grupo poblacional y sensibilizar a padres, cuidadores, educadores y a la sociedad en general sobre la importancia de un acompañamiento adecuado en el uso de Internet.

Esta iniciativa es el resultado de un esfuerzo interinstitucional que involucra a más de 22 entidades públicas y privadas, bajo la coordinación del Consejo Nacional para la Igualdad Intergeneracional (CNII). Con el fin de fomentar una cultura de prevención y protección en el ámbito digital, esta política se ha diseñado para implementar acciones articuladas a nivel nacional que aseguren un ambiente seguro y respetuoso permitiendo que niñas, niños y adolescentes puedan beneficiarse de las tecnologías digitales.

La necesidad de esta política pública surge de la creciente interacción de este grupo etario con el entorno digital. Hoy en día, Internet se ha convertido en una herramienta fundamental en

la vida de las niñas, niños y adolescentes, tanto en el ámbito educativo como en el social. Sin embargo, el acceso constante a internet y a las tecnologías digitales también los expone a riesgos significativos que pueden amenazar su bienestar físico, psicológico y emocional. Problemas como el ciberacoso, la explotación sexual, la exposición a contenidos inapropiados y el acceso a redes de contacto potencialmente peligrosas se han intensificado, afectando a niñas, niños y adolescentes en distintas esferas de sus vidas.

El contexto ecuatoriano evidencia una brecha en la protección de niñas, niños y adolescentes en el entorno digital. La ausencia de un marco normativo y estructural específico para garantizar su seguridad en Internet deja a este grupo vulnerable frente a situaciones que pueden impactar negativamente en su desarrollo. Según diversas investigaciones, niñas, niños y adolescentes en Ecuador están cada vez más expuestos a situaciones de violencia digital, y la falta de habilidades de autoprotección digital, en ellos y sus cuidadores, agrava este problema. Por tanto, la implementación de una política pública que aborde estas amenazas y promueva el uso seguro de Internet se vuelve indispensable.

Además, en un contexto de rápida evolución tecnológica, la educación en competencias digitales es fundamental para que niñas, niños y adolescentes desarrollen una relación saludable con el uso de Internet. La política pública "Por una Internet Segura para Niños, Niñas y Adolescentes" tiene como objetivo no solo la prevención de riesgos, sino también la promoción de una cultura de seguridad y responsabilidad digital. Es necesario que el Estado, en colaboración con entidades educativas, organizaciones civiles y la comunidad en general, establezca directrices que orienten el acceso seguro a Internet, protegiendo así los derechos de niñas, niños y adolescentes en el ámbito digital.

Esta política no solo busca responder a los desafíos presentes, sino también anticiparse a futuros riesgos y cambios en el ecosistema digital. A través de la sensibilización y el fortalecimiento de capacidades en la sociedad, se aspira a crear un entorno en el que las niñas, niños y adolescentes puedan disfrutar de las oportunidades que ofrece Internet de manera segura y positiva. En última instancia, esta política refleja el compromiso de Ecuador por garantizar un espacio seguro y respetuoso, permitiendo que las nuevas generaciones aprovechen al máximo el potencial de las tecnologías, contribuyendo a su desarrollo integral y a la construcción de una sociedad más informada y consciente de los derechos digitales.

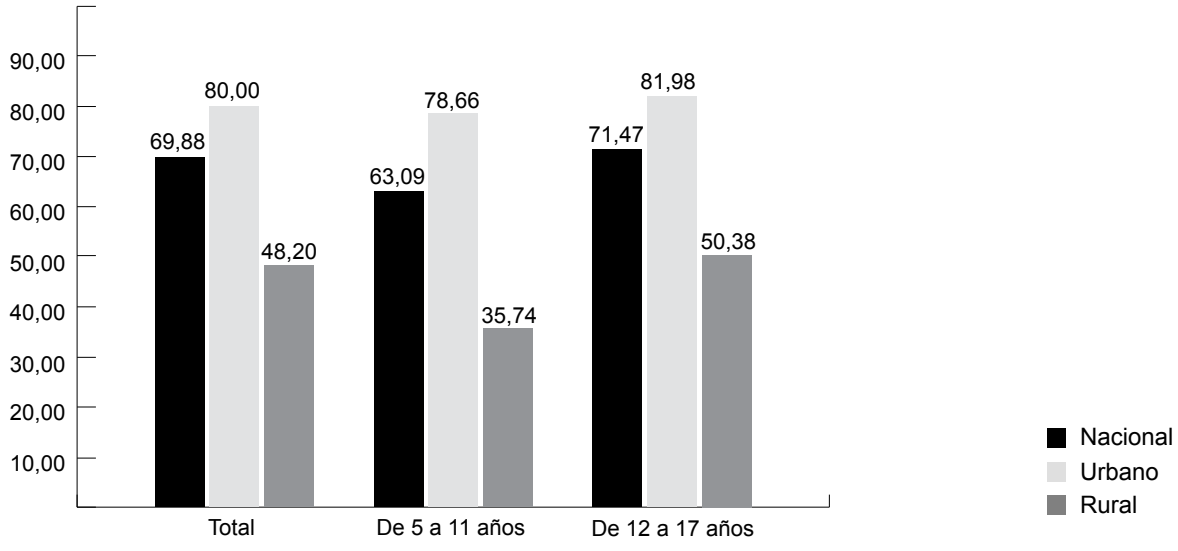
Diagnóstico

El indicador "Personas en hogares con acceso a Internet" evidencia desigualdades significativas en el acceso a internet en Ecuador, tanto por áreas geográficas como por grupos etarios. A nivel nacional, el 69.88% de las personas tienen acceso a internet en sus hogares, con una cobertura considerablemente mayor en áreas urbanas (80%) en comparación con las rurales (48.20%), lo que refleja una marcada brecha digital.

Por edades, los niños de 5 a 11 años tienen el menor acceso (63.09% a nivel nacional y solo 35.74% en zonas rurales), lo que podría limitar su desarrollo educativo y social en entornos digitalizados. En cambio, los adolescentes de 12 a 17 años representan el mayor acceso (71.47% a nivel nacional, 81.98% en áreas urbanas y 50.38% en rurales), posiblemente por la percepción de una mayor necesidad tecnológica en este grupo.

Figura 1

Personas en Hogares con acceso a Internet



Fuente: INEC – ENEMDU, Julio 2024

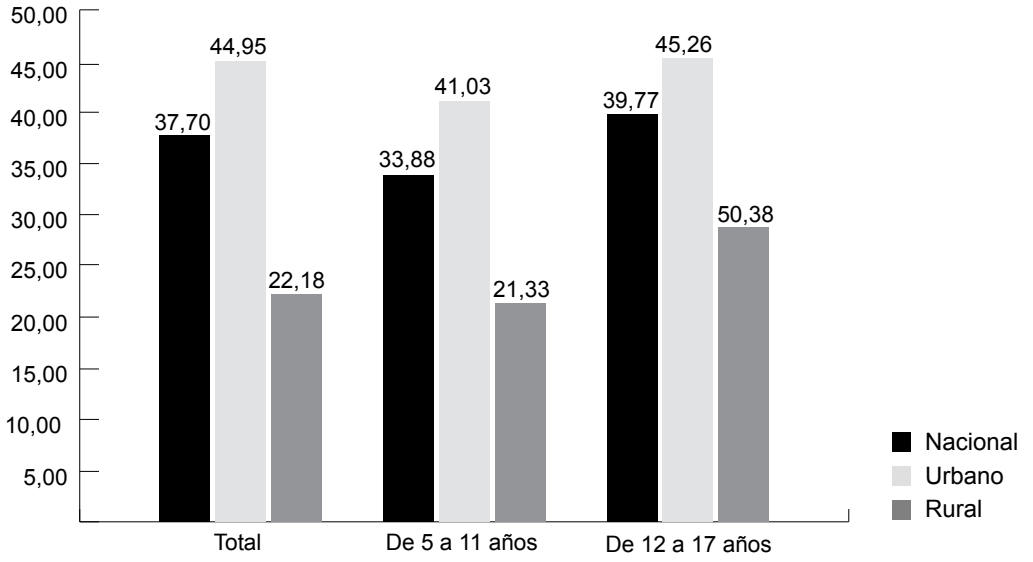
El indicador "Personas en hogares con equipamiento tecnológico" refleja una notable desigualdad en el acceso a dispositivos tecnológicos necesarios para la conectividad y el aprendizaje en Ecuador. A nivel nacional, solo el 37.70% de las personas vive en hogares con equipamiento tecnológico, cifra que aumenta a 44.95% en zonas urbanas, pero desciende drásticamente a 22.18% en áreas rurales, evidenciando una profunda brecha tecnológica entre estas regiones.

Por grupos etarios, los niños de 5 a 11 años tienen el menor acceso a equipamiento (33.88% a nivel nacional, 21.33% en zonas rurales), lo que limita su exposición a recursos educativos digitales en etapas cruciales de desarrollo. Los adolescentes de 12 a 17 años tienen un acceso ligeramente superior (39.77% a nivel nacional, 28.73% en zonas rurales), posiblemente debido a la prioridad que las familias otorgan a este grupo para actividades escolares y sociales.

Estos datos subrayan la urgente necesidad de políticas públicas que promuevan el acceso equitativo a dispositivos tecnológicos, especialmente en áreas rurales, para garantizar la igualdad de oportunidades de desarrollo y aprendizaje en el contexto digital.

Figura 2

Personas en Hogares con Equipamiento Tecnológico



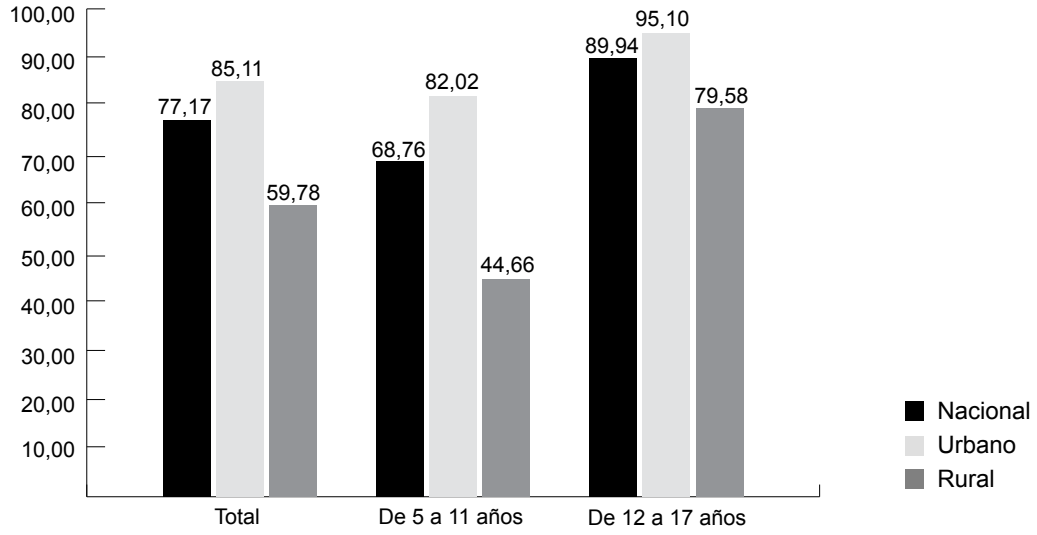
Fuente: INEC – ENEMDU, Julio 2024

El indicador "Personas que utilizan Internet" destaca una realidad marcada por diferencias significativas en el acceso y uso de Internet según el área geográfica y los grupos etarios en Ecuador. A nivel nacional, el 77.17% de las personas utiliza Internet, con una notable diferencia entre las áreas urbanas (85.11%) y rurales (59.78%), lo que refleja una brecha digital persistente entre ambas regiones.

Por edades, los niños de 5 a 11 años tienen el menor nivel de uso (68.76% a nivel nacional, 44.66% en zonas rurales), lo que evidencia limitaciones en el acceso temprano a herramientas digitales fundamentales para su educación y desarrollo. En contraste, los adolescentes de 12 a 17 años registran el mayor uso de Internet (89.94% a nivel nacional, 79.58% en zonas rurales), probablemente impulsado por la necesidad de conectividad para actividades escolares y sociales.

Este análisis subraya la importancia de promover estrategias que cierren la brecha digital en zonas rurales y garanticen un acceso equitativo a Internet desde edades tempranas, facilitando una inclusión tecnológica integral en el país.

Figura 3
Personas que utilizan Internet



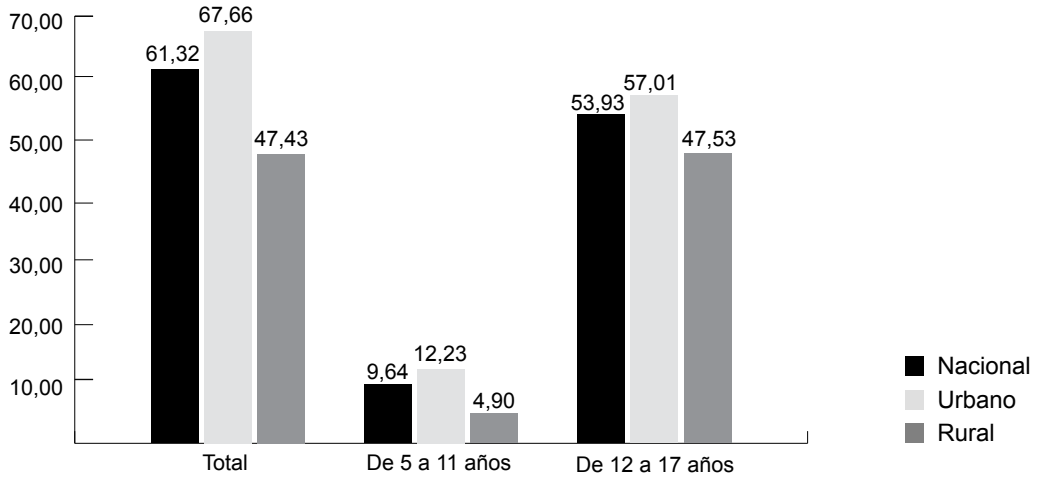
Fuente: INEC – ENEMDU, Julio 2024

El indicador "Personas que tienen teléfono celular activado" muestra una cobertura nacional del 61.32%, con una evidente disparidad entre zonas urbanas (67.66%) y rurales (47.43%), lo que refleja una brecha significativa en el acceso a dispositivos móviles.

Los niños de 5 a 13 años registran un acceso muy bajo (9.64% a nivel nacional, 4.90% en áreas rurales), posiblemente debido a su menor necesidad percibida de uso, pero que también podría limitar su inclusión digital en actividades educativas. En contraste, los adolescentes de 14 a 17 años presentan un mayor acceso (53.93% a nivel nacional, 47.53% en zonas rurales), aunque este nivel aún es insuficiente para garantizar igualdad de oportunidades en términos de conectividad, comunicación y aprendizaje.

Estos datos resaltan la importancia de políticas que faciliten el acceso a dispositivos móviles en las zonas rurales, donde las brechas son más marcadas, y que promuevan un uso adecuado y equitativo de esta tecnología en beneficio del desarrollo de los niños y adolescentes.

Figura 4
Personas con celular activado



Fuente: INEC – ENEMDU, Julio 2024

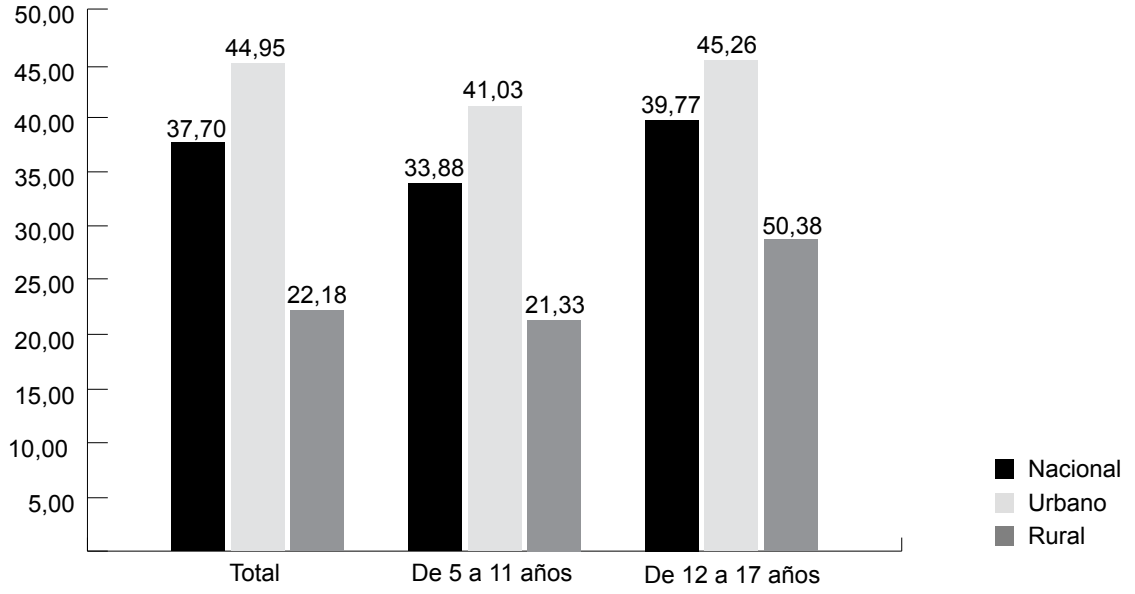
El indicador "Personas que tienen teléfono inteligente" evidencia una cobertura nacional del 57.69%, con una notable diferencia entre zonas urbanas (64.86%) y rurales (41.96%), lo que refleja una marcada brecha en el acceso a dispositivos avanzados clave para la conectividad digital.

En el grupo de 5 a 13 años, el acceso es muy bajo (9.55% a nivel nacional, 4.82% en áreas rurales), limitando significativamente las oportunidades de este grupo para acceder a recursos educativos digitales y actividades que requieren dispositivos modernos. Por otro lado, los adolescentes de 14 a 17 años presentan un acceso considerablemente mayor (53.51% a nivel nacional, 46.72% en zonas rurales), aunque la disparidad rural-urbana persiste.

Estos datos subrayan la necesidad de reducir las barreras económicas y geográficas para el acceso a teléfonos inteligentes, especialmente en áreas rurales, como un paso crucial para cerrar la brecha digital y garantizar que niños y adolescentes puedan aprovechar plenamente las oportunidades que ofrecen las tecnologías modernas.

Figura 5

Personas que tienen teléfono inteligente



Fuente: INEC – ENEMDU, Julio 2024

Los datos sobre las denuncias recibidas por la Fiscalía relacionadas con actos delictivos cometidos mediante medios electrónicos reflejan una preocupante realidad, especialmente en casos de contacto con finalidad sexual con menores de 18 años, que representan la gran mayoría de los casos reportados (898 de 945 casos).

Este delito afecta principalmente a adolescentes de 11 a 14 años (489 casos) y 15 a 17 años (364 casos), lo que evidencia que los adolescentes son el grupo más vulnerable a este tipo de crímenes en línea. En contraste, los niños menores de 10 años reportan un número menor de casos (45 casos), posiblemente debido a una menor exposición o interacción activa en redes sociales y plataformas digitales.

Por otro lado, aunque los casos de oferta de servicios sexuales con menores de 18 años por medios electrónicos son menos frecuentes (47 casos), siguen representando una grave violación a los derechos de los adolescentes, con mayor incidencia en adolescentes de 15 a 17 años (28 casos).

Estos datos resaltan la urgente necesidad de fortalecer las medidas de prevención y educación digital, promover campañas de concienciación dirigida a para padres, cuidadores y educadores, y asegurar que las plataformas digitales implementen herramientas más efectivas para prevenir estos delitos. Además, es crucial que las instituciones gubernamentales refuercen los mecanismos de denuncia y protección para garantizar la seguridad de los menores en los entornos digitales.

Tabla 1
Número de delitos por medios electrónicos.

Tipo de delito	Niños (0 a 10 años)	Adolescentes (11 a 14 años)	Adolescentes (15 a 17 años)	Total
Contacto con finalidad sexual con menores de 18 años por medios electrónicos	45	489	364	**898**
Oferta de servicios sexuales con menores de 18 años por medios electrónicos	2	17	28	**47**
Total	**47**	**506**	**392**	**945**

Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) - ANALÍTICA FGE; Unidad de Análisis: Noticias de delito, víctimas; Fecha de corte: 15/11/24; Periodo de análisis: (10/08/2014 - 31/10/2024)

Los datos sobre el número de denuncias recibidas entre 2014 y 2024 evidencian una tendencia fluctuante, pero alarmante, en los casos de contacto con finalidad sexual con menores de 18 años y oferta de servicios sexuales con menores de 18 años.

El total de denuncias asciende a 676 casos, de los cuales la gran mayoría (635 casos) corresponden a contacto con finalidad sexual, mientras que los casos de oferta de servicios sexuales son significativamente menores (41 casos).

Los años 2021 y 2022 presentan los picos más altos de denuncias con 100 y 93 casos, respectivamente, lo que podría reflejar un aumento en la visibilización de estos delitos o en la disposición de las víctimas para denunciar, posiblemente asociado a una mayor digitalización durante la pandemia. Sin embargo, en 2024 se observa una disminución significativa con solo 48 casos, lo que podría interpretarse de diversas maneras:

- Una reducción real de los delitos.
- Menor disposición a denunciar.
- Cambios en la accesibilidad de los canales de denuncia.

Esta evolución subraya la urgente necesidad de medidas sostenidas para prevenir estos delitos tales como:

- Promoción de campañas educativas.
- Fortalecimiento de la seguridad en plataformas digitales.
- Mejor acceso a mecanismos de denuncia efectivos.

Además, es fundamental realizar estudios adicionales para comprender las causas detrás de las fluctuaciones y garantizar que la reducción de denuncias no sea resultado de barreras estructurales o de una falta de confianza en el sistema judicial.

La continuidad en la vigilancia y protección de los menores en entornos digitales debe ser una prioridad para evitar que estos delitos sigan afectando a las poblaciones más vulnerables.

Tabla 2
Número de delitos por medios electrónicos por año.

Años	Contacto con finalidad sexual con menores de 18 años por medios electrónicos	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	Total
2014	0	0	**0**
2015	15	0	**15**
2016	42	5	**47**
2017	59	4	**63**
2018	82	5	**87**
2019	68	5	**73**
2020	73	2	**75**
2021	94	6	**100**
2022	87	6	**93**
2023	71	4	**75**
2024	44	4	**48**
Total	**635**	**41**	**676**

Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) - ANALÍTICA FGE; Unidad de Análisis: Noticias de delito, víctimas; Fecha de corte: 15/11/24; Periodo de análisis: (10/08/2014 - 31/10/2024)

Marco Normativo

El artículo 17 de la Convención sobre los Derechos del Niño (CDN) reconoce el derecho de niñas, niños y adolescentes a acceder a información, para lo que, los Estados deben promover la elaboración de principios rectores para protegerlos de todo tipo de información o material perjudicial.

En contraposición al reconocimiento de este derecho, el artículo 19 de la misma Convención obliga a los Estados adoptar medidas para proteger a la niñez contra toda forma de violencia, incluyendo la explotación a través de Internet.

En suma, la Convención sobre los Derechos del Niño exige a los Estados parte, la protección de niñas, niños y adolescentes contra la explotación sexual y el abuso en redes de Internet.

Para ayudar a la correcta interpretación de estos derechos, el Comité de los Derechos del Niño elabora documentos periódicos donde aborda aspecto que requieren mayor atención, o que han sido interpretados de manera errónea o insuficiente.
Entre estos documentos, destaca la Observación General No. 25, relativa a los derechos de la niñez en relación con el entorno digital, la cual establece que:

- Los Estados parte deben crear oportunidades para hacer efectivos los derechos de los niños y asegurar su protección en el entorno digital.

- Se requiere que los Estados parte realicen evaluaciones del impacto del entorno digital en los derechos de la niñez, a fin de integrar estos derechos en su legislación, las asignaciones presupuestarias y demás decisiones administrativas.

- Los Estados parte deben garantizar el acceso a la información digital a niñas, niños y adolescentes. Las restricciones solo podrán aplicarse sí están respaldadas por la ley y son necesarias para proteger su reputación y otros derechos.

- Se debe asignar y utilizar recursos para aplicar leyes, políticas y programas que garanticen los derechos digitales de la niñez y mejoren la inclusión digital.

- Los Estados parte están obligados a asegurar mecanismos de reparación judicial y no judicial, adecuados y eficaces, para abordar violaciones a los derechos de la niñez en el entorno digital.

Normativa nacional

El Ecuador es un Estado de derechos y justicia, lo cual implica que la Constitución y otros tratados internacionales de derechos humanos ratificados por el país tienen prevalencia sobre cualquier otra norma jurídica o acto del poder público.

- El artículo 11, numeral 3, y el artículo 424 de la Constitución de la República del Ecuador establecen que, los derechos y garantías reconocidos en la Constitución y los tratados internacionales de derechos humanos son de aplicación directa e inmediata.

- El artículo 44 de la Constitución del Ecuador dispone que el Estado, la sociedad y la familia deben garantizar de manera prioritaria el desarrollo integral de niñas, niños y adolescentes, asegurando el ejercicio pleno de sus derechos y atendiendo su interés superior.

- El artículo 66, numeral 19 reconoce el derecho a la protección de datos personales, incluyendo el acceso, control y resguardo de la información personal. Este derecho se enmarca en el interés superior del niño.

- El Código de la Niñez y Adolescencia, en su artículo 51, literal b) reconoce el derecho a la dignidad, autoestima, honra, reputación e imagen propia de las niñas, niños y adolescentes.

- El artículo 52 del mismo Código prohíbe la publicación o exhibición de noticias, reportajes, crónicas, historias de vida o cualquier otro contenido periodístico que exponga la imagen o el nombre de menores de edad que han sido víctimas de maltrato y abuso.

- La Ley Orgánica de Protección de Datos Personales, en su artículo 21, categoriza los datos de niñas, niños y adolescentes como información especialmente protegida. Su tratamiento solo es permitido con la autorización expresa de sus representantes legales.

- El artículo 24 de la misma ley establece como obligación del Estado, y de los proveedores de servicios digitales brindar información y capacitaciones sobre el uso seguro y responsable, de los datos personales de niñas, niños y adolescentes.

Normativa penal

El Código Orgánico Integral Penal (COIP) sanciona diversos delitos relacionados con la protección de niñez en entornos digitales:

- Artículo 103: Penaliza la pornografía infantil incluyendo su producción, difusión y comercialización en medios digitales y electrónicos.

- Artículo 178: Sanciona la violación de la privacidad, aplicable a casos de ciberacoso e invasión indebida de la privacidad de las personas en plataformas digitales.

- Artículo 173: Tipifica el delito de "grooming" que consiste en el alistamiento de menores de edad a través de medios electrónicos con fines de explotación sexual.

En 2023, el Ministerio de Educación expidió el Acuerdo Ministerial Nro. MINEDUC-MINEDUC-2023-00054-A, que establece el Protocolo de Actuación frente a Situaciones de Violencia Digital detectadas en el Sistema Nacional de Educación:

Este protocolo tiene como objetivo:

Definir los lineamientos de actuación para todas las personas que conforman la comunidad educativa, para garantizar la prevención, detección, intervención, derivación, seguimiento y reparación frente a situaciones de violencia digital detectadas o cometidas en el sistema educativo.

Metodología de la Evaluación

Justificación teórica de la evaluación de la Política Pública

El avance tecnológico ha transformado la vida de niñas, niños y adolescentes, así como de sus familias, quienes utilizan Internet para aprender, socializar y entretenerse. Sin embargo, el entorno digital también conlleva riesgos significativos, como el grooming[1] , el ciberacoso, la explotación sexual en línea y el acceso a contenido inapropiado (Livingstone & Stoilova, 2021).

En este contexto, la Convención sobre los Derechos del Niño (1989) establece que los Estados tienen la responsabilidad de proteger a la niñez y adolescencia frente a cualquier forma de explotación o abuso, incluyendo las amenazas derivadas del entorno digital.

En respuesta a estos desafíos, el Consejo Nacional para la Igualdad Intergeneracional, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, y la Dirección Nacional de Registro de Datos Públicos, con el apoyo de dieciséis instituciones públicas y privadas formularon la Política Pública por una Internet Segura para Niñas, Niños y Adolescentes 2020-2024 (PPIS-NNA):

> El objetivo de esta política es garantizar un entorno digital seguro y protector de los derechos de la niñez y adolescencia, asegurando que el acceso a Internet se realice de manera responsable y en condiciones óptimas para su bienestar.

[1] ***Grooming***: Estrategias que realiza un adulto para ganarse la confianza de un niño, niña y adolescente, a través de Internet, con el propósito de abusarlo o explotarlo sexualmente. Es importante expresar que siempre es un adulto quien ejerce el vgrooming. Existen dos tipos de grooming:
• Cuando no existe la fase previa de relación y generación de confianza, el acosador logra obtener fotos o videos sexuales de las niñas, niños y/o adolescentes, con la intención de extorsionar con difundir dicho material, a cambio de acceder a encuentro personal.
• Cuando existe una fase previa donde el acosador busca generar confianza en la niña, niño o adolescente, logrando que los mismos entreguen material sexual para volverlo objeto de chantaje, valiéndose de distintas herramientas, como hacerse pasar por un chico o chica menor, manipular a través de los gustos y preferencias de la víctima, utilizar el tiempo para fortalecer el vínculo (CNII, 2020).

La PPIS-NNA se fundamenta en la promoción de un uso sano, seguro y constructivo de Internet, centrado en dos ejes fundamentales:

- Potenciar oportunidades y habilidades digitales, promoviendo el uso beneficioso de las TIC dentro de un marco de derechos digitales, dignidad e integridad física, psicológica, emocional y sexual.

- Fomentar conductas protectoras que prevengan factores de riesgo y, en caso de vulneraciones, implementar protocolos de atención, protección y reparación.

Esta política no solo busca mitigar los riesgos del entorno digital, sino también empoderar a niñas, niños y adolescentes en el uso de Internet como una herramienta de desarrollo personal y educativo.

Para evaluar su impacto y eficacia, se propone una metodología de semaforización, que permite medir el cumplimiento de sus acciones, identificar áreas críticas y proponer ajustes necesarios para su actualización e implementación en los próximos años.

La evaluación de políticas públicas es una herramienta esencial para:

- Identificar logros en la implementación de acciones como campañas de sensibilización y creación de marcos regulatorios.

- Detectar áreas con metas incumplidas, como el desarrollo de herramientas de denuncia en línea.

- Actualizar estrategias en función de cambios tecnológicos y nuevos riesgos digitales.

- Fortalecer la transparencia y rendición de cuentas, promoviendo la confianza ciudadana en las instituciones responsables (Van Dooren et al., 2015).

- Garantizar la sostenibilidad de la política pública, asegurando su continuidad frente a cambios políticos y económicos.

Además, esta evaluación permite detectar desigualdades en el acceso digital, evitando que las brechas tecnológicas profundicen desequilibrios en la protección y educación digital de la niñez y adolescencia (UNICEF, 2020).

Evaluar el cumplimiento de esta política no solo analiza los logros alcanzados, sino que también ayuda a reformular estrategias en áreas críticas, como la capacitación docente en alfabetización digital o la garantía de acceso equitativo a tecnología segura (Hatry, 2006).

El entorno digital evoluciona constantemente, introduciendo tanto oportunidades como amenazas. La evaluación de esta política debe anticiparse a nuevos desafíos tecnológicos, como el uso indebido de inteligencia artificial en la explotación infantil o el incremento de delitos cibernéticos (Meadows, 2008).

Por último, la evaluación del cumplimiento de las acciones planificadas garantiza la sostenibilidad de la política pública, incluso ante cambios políticos o económicos. Este enfoque promueve la coordinación intersectorial, involucrando a actores clave en educación, justicia y tecnología, para abordar de manera integral los riesgos y oportunidades del entorno digital (Livingstone et al., 2018).

Metodología de semaforización utilizada para evaluar

La metodología de semaforización es un modelo de evaluación que permite identificar avances, estancamientos y desafíos en la implementación de políticas públicas. En el caso de la Política Pública por un Internet Segura para Niñas, Niños y Adolescentes (2020-20204) PPIS-NNA, este enfoque facilita la proporciona la visualización de su grado de cumplimiento en función de indicadores específicos.

De acuerdo con Hatry (2006), la evaluación de políticas públicas debe ofrecer una estructura clara para:

- Medir el progreso de las acciones ejecutadas.
- Identificar obstáculos en la implementación y proponer soluciones.
- Optimizar el uso de recursos y garantizar la eficiencia de la política.
- Asegurar la sostenibilidad de las iniciativas a lo largo del tiempo.

- Este modelo de semaforización permite categorizar el cumplimiento de las acciones de acuerdo con tres niveles:

🔴 Rojo: Acción no iniciada o con problemas estructurales.
🟡 Amarillo: Acción en proceso con avances parciales.
🟢 Verde: Acción implementada de manera efectiva.

Figura 6
Metodología de semaforización

1. Definición de criterios de evaluación	Basados en los objetivos de la política y las acciones implementadas en cada lineamiento de la política pública.
2. Recolección y análisis de datos	Utilizando un enfoque mixto, combinando análisis documental con entrevistas a actores clave y encuestas a niñas, niños y adolescentes.
3. Integración y presentación de resultados	Los hallazgos se representan mediante tableros visuales y gráficas que codifican el estado de cada acción según el semáforo.

Fuente: Elaboración propia con base en Hatry (2006)

Esta metodología proporciona una visión integral y comparativa del estado de la política pública, permitiendo:

- Evaluar la interdependencia de las acciones, como la educación digital, la regulación tecnológica y la protección legal.
- Clasificar el nivel de cumplimiento de cada eje de intervención.
- Detectar áreas críticas que requieren reformas o refuerzo de acciones.
- La semaforización no solo facilita la identificación de avances y obstáculos, sino que también orienta la toma de decisiones para mejorar la efectividad de la política pública (Hatry, 2006).

Definición de los niveles de evaluación

La PPIS-NNA, tiene 5 ejes de intervención, 10 lineamientos de política y 26 acciones.

Mediante la categorización visual del cumplimiento de las acciones, se pueden detectar rápidamente aspectos como:

- Necesidad de recursos.
- Brechas en la cobertura.
- Riesgos emergentes en la protección digital.

Esta metodología facilita la interpretación de resultados complejos, permitiendo que los responsables de políticas públicas, organizaciones de la sociedad civil, educadores y familias comprendan los avances y desafíos de la política (Van Dooren et al., 2015).

Figura 7
Categorización visual del sistema de semaforización

Cumplimiento alto. Las acciones están implementadas y son efectivas, por ejemplo, reformas normativas que tipifican los delitos relacionados con las violencias sexuales en línea contra niñas, niños y adolescentes, que han incrementado el número de denuncias de incidentes de explotación sexual en línea.

Cumplimiento medio. Acciones en marcha, pero enfrentan limitaciones que reducen su efectividad por ejemplo, articulación de la mesa técnica interinstitucional para realizar el seguimiento, monitoreo y evaluación del Plan de política pública por el uso seguro de internet para niñas, niños y adolescentes.

Cumplimiento bajo o inexistente. Las acciones no se han implementado o muestran avances mínimos, sin evidencia de impacto positivo, por ejemplo, implementar normativas y políticas públicas desde los gobiernos autónomos descentralizados para, en el marco de las autorizaciones a comercios o locales que faciliten el acceso a las tecnologías de la información y comunicación, incluyan regulaciones para la USI).

Fuente: Creación propia con base en Van Dooren et al., 2015

En el contexto de la protección de niñas, niños y adolescentes en línea, los niveles de evaluación del sistema de semáforo se basan en criterios específicos y medibles que reflejan el cumplimiento de las acciones de la política pública.

Establecimiento de criterios e indicadores para la evaluación de las acciones.

Para la evaluación de las acciones de la PPIS-NNA, se establecieron 5 criterios. Para cada uno de los criterios, se definieron dos indicadores específicos que permitieron medir el grado de cumplimiento de las acciones implementadas:

Tabla 3
Criterios e indicadores para la evaluación de las acciones.

Criterio	Indicadores
Criterio 1: La acción está institucionalizada en un documento o plan.	**Indicador 1.1:** Existe un documento oficial o plan que describe las acciones. **Indicador 1.2:** Las acciones están alineadas o respaldadas por leyes, normativas, sentencias o estrategias nacionales/internacionales.
Criterio 2: Una o varias organizaciones tienen competencia o lideran la acción.	**Indicador 2.1:** Se han asignado claramente responsabilidades a una organización u organismo. **Indicador 2.2:** Existen recursos humanos, técnicos y financieros asignados.
Criterio 3: Las acciones se han sostenido en el tiempo.	**Indicador 3.1:** Existe evidencia de continuidad en la ejecución durante un período establecido (por ejemplo, 2-4 años). **Indicador 3.2:** Se han superado cambios de gobierno o presupuestarios sin afectar la acción.

Criterio 4: Las acciones tienen una incidencia directa en la vida y desarrollo de la niñez.	**Indicador 4.1:** Hay datos o informes que evidencian el impacto positivo en la población infantil. **Indicador 4.2:** Las acciones responden a necesidades prioritarias identificadas.
Criterio 5: Participación de la comunidad	**Indicador 5.1:** Se ha involucrado a las comunidades locales, incluyendo a niños, niñas y adolescentes, en el diseño, implementación y evaluación de las acciones. **Indicador 5.2:** Las políticas respondan a las necesidades reales de la población.

Fuente: Creación propia.

La selección de los cinco criterios e indicadores para la evaluación de las acciones de la PPIS-NNA responde a la necesidad de garantizar un análisis integral, objetivo y centrado en el cumplimiento y alcance real de las acciones implementadas. Cada criterio fue diseñado para abordar aspectos clave del diseño, implementación y cumplimiento de la política. Por ejemplo, el criterio de institucionalización asegura que las acciones estén formalmente respaldadas en planes y normativas, lo que es esencial para su legitimidad y sostenibilidad. Asimismo, el criterio de liderazgo organizacional permite verificar que las responsabilidades estén claramente asignadas y cuenten con recursos para su ejecución. La sostenibilidad en el tiempo mide la capacidad de las acciones para superar desafíos políticos o presupuestarios, mientras que el impacto directo en la niñez se enfoca en garantizar que las acciones respondan a necesidades prioritarias y generen beneficios tangibles.

Finalmente, la participación de la comunidad destaca la importancia de involucrar a las niñas, niños, adolescentes y sus entornos en el proceso, asegurando que las políticas sean pertinentes y adaptadas a sus realidades. Estos criterios e indicadores ofrecen una estructura para evaluar tanto los logros como las áreas de mejora, promoviendo la efectividad y sostenibilidad de la política.

Recolección y análisis de datos

Para evaluar el cumplimiento de las acciones de la **PPIS-NNA,** se empleó un enfoque mixto que combina métodos cualitativos y cuantitativos. Este enfoque permitió obtener una visión integral y fundamentada de la implementación de las acciones. La **recolección de datos** incluyó las siguientes estrategias:

Análisis documental: Revisión de normativas, reportes y documentos oficiales relacionados con la política pública, con el objetivo de verificar la existencia y alineación de las acciones con los marcos legales y estratégicos establecidos.

Encuestas a niñas, niños y adolescentes: Aplicación de encuesta diseñada para evaluar el conocimiento de las acciones en la población objetivo. Estas encuestas se centraron en temas como el acceso a tecnologías seguras, la percepción de seguridad en línea y el nivel de conocimiento sobre riesgos digitales.

El análisis de estos datos permitió identificar patrones, áreas de cumplimiento, barreras y oportunidades de mejora en la política pública.

Integración y presentación de resultados.

La integración y presentación de los resultados siguieron un enfoque lógico y estructurado, orientado a garantizar una interpretación clara y accionable que inició con la evaluación de cada acción de la política pública con base en los criterios e indicadores previamente definidos. Este proceso incluyó los siguientes pasos:

Este enfoque permitió evaluar el estado actual de cumplimiento de la política pública y generar recomendaciones prácticas y específicas que contribuyan a su mejora continua. La metodología asegura que los resultados de la evaluación sean útiles tanto para ajustar las acciones existentes como para planificar futuras fases de implementación.

Figura 8

Pasos para la integración y presentación de resultados.

1. Aplicación de la evaluación	2. Representación visual de los resultados	3. Proponer acciones de mejora
• Asignación de puntajes o etiquetas (verde, amarillo o rojo) a cada indicador basado en evidencia. • Los puntajes individuales de los indicadores se promediaron para obtener un color general que representara el estado del cumplimiento de cada criterio : • Verde: Cumplimiento alto. • Amarillo: Cumplimiento medio. • Rojo: Cumplimiento bajo o inexistente.	• Los resultados se visualizaron en una matriz de semáforo donde cada columna representa el promedio de los criterios e indicadores evaluados. • La información analizada se complementa con gráficos o reportes que expliquen los resultados.	• Con base en los resultados obtenidos, se proponen recomendaciones diferenciadas según el nivel cumplimiento de las acciones: • Rojo: Identificar las barreras y proponer acciones concretas superar los desafíos. • Amarillo: Monitorear el avance de las acciones parcialmente implementadas y proponer estrategias para continuar su implementación. • Verde: Fortalecer las acciones exitosas, asegurando su sostenibilidad.

Fuente: Elaboración propia.

Resultados de la Evaluación

Resultados de las respuestas institucionales

La matriz de semaforización permite visualizar el grado de cumplimiento de las acciones establecidas en la **PPIS-NNA**. Cada columna de la matriz representa el promedio de los criterios e indicadores evaluados, ofreciendo una visión global y estructurada sobre el nivel de implementación y efectividad de las acciones.

Los resultados se calcularon y representaron con un código de colores, que muestran el nivel de cumplimiento de la política:

Figura 9
Código de semaforización.

	Cumplimiento alto. Las acciones están implementadas y son efectivas.
	Cumplimiento medio. Acciones en marcha, pero enfrentan limitaciones que reducen su efectividad.
	Cumplimiento bajo o inexistente. Las acciones no se han implementado o muestran avances mínimos, sin evidencia de impacto positivo.

Fuente: Elaboración propia.

A continuación, se presenta una matriz resumen semaforizada que muestra los resultados de la evaluación de la Política Pública de Internet Segura para Niñas, Niños y Adolescentes. En el Anexo 1, se encuentra la matriz detallada con la evidencia proporcionada por las instituciones públicas y privadas.

Eje 1: Medidas Legales **Objetivo 1: Desarrollar normativa que promueva los derechos digitales y la dignidad e integridad física, psicológica, emocional y sexual de niñas, niños y adolescentes, estableciendo los mecanismos para el aprovechamiento de los beneficios de las Tecnologías de la Información y Comunicación (TIC) y atienda y mitigue los riesgos y delitos que pueden cometerse a través de ellas.**		
LINEAMIENTO DE LA POLÍTICA PÚBLICA 1	Garantizar los derechos digitales, la ciudadanía digital y las capacidades informacionales de niñas, niños y adolescentes para una Internet segura.	
ACCIÓN 1	Proponer en la reforma al Código Orgánico de Niñez y Adolescencia la inclusión de los derechos digitales, la ciudadanía digital, las capacidades informacionales, las medidas de protección y reparación, y la tipificación y sanciones frente a las transgresiones y delitos cometidos contra de niñas, niños y adolescentes en entornos virtuales.	
ACCIÓN 2	Proponer reformas al Código Orgánico Integral Penal sobre delitos informáticos y transgresiones en contra de niñas, niños y adolescentes en entornos virtuales.	
ACCIÓN 3	Normar a los proveedores de servicios de telecomunicaciones para que brinden herramientas que permitan un acceso sano, seguro y constructivo para niñas, niños y adolescentes a las tecnologías de la información y la comunicación.	
ACCIÓN 4	Proponer normativa que regule el funcionamiento de los centros de acceso a la Internet, con enfoque de protección a la niñez y adolescencia	
ACCIÓN 5	Generar procesos de interoperabilidad de datos entre las instituciones de la Función Judicial para la producción de estadísticas jurimétricas de ingresos de causas de delitos cibernéticos contra niñas, niños y adolescentes generando bases de datos anonimizadas que aporten al portal de estadística judicial en delitos cibernéticos.	
ACCIÓN 6	Incidir en la Asamblea Nacional respecto del proyecto de protección de datos personales y la promoción de derechos digitales.	

Eje 2: Medidas Técnicas y Procedimentales **Objetivo 2: Promover el acceso, uso e interacción adecuada, responsable, sana, segura y constructiva de las tecnologías de la información y la comunicación que impulse el desarrollo integral y el pleno ejercicio de los derechos de niñas, niños y adolescentes.**	
LINEAMIENTO DE LA POLÍTICA PÚBLICA 2	Promover un acceso sano, seguro y constructivo a las tecnologías de la información y la comunicación para proteger los derechos digitales y la integridad y dignidad de niñas, niños y adolescentes frente a los contenidos nocivos, transgresiones y delitos cometidos a través de medios digitales, con la implementación de políticas públicas, lineamientos técnicos, regulaciones, códigos de conducta, recomendaciones, estándares, metodologías, procedimientos, entre otros

ACCIÓN 7	Diseñar e implementar el plan de políticas públicas para una internet segura desde las instituciones estatales con el fin de garantizar un acceso y uso sano, seguro y constructivo a las tecnologías de la información y la comunicación por parte de niñas, niños y adolescentes.	
ACCIÓN 8	Implementar normativas y políticas públicas desde los gobiernos autónomos descentralizados para, en el marco de las autorizaciones a comercios o locales que faciliten el acceso a las tecnologías de la información y comunicación, conforme sus competencias constitucionales y legales, garantizar un acceso y uso sano, seguro y constructivo a las tecnologías de la información y la comunicación, por parte de niños, niñas y adolescentes.	
ACCIÓN 9	Desarrollar e implementar mecanismos, lineamientos y medidas técnicas para la regulación y control del acceso a contenidos nocivos, transgresiones y posibles delitos en los servicios del régimen general de telecomunicaciones (TIC) y las empresas proveedoras de internet y mecanismos de prevención, protección, restitución y reparación de derechos para niñas, niños y adolescentes.	
ACCIÓN 10	Establecer el funcionamiento de una línea de denuncia de contenidos ilegales y atentatorios a los derechos de los niños, niñas y adolescentes, tales como la pornografía infantil en internet, entre otras, bloquear esos contenidos; rastrearlos al país de origen e impulsar todas las acciones pertinentes para sancionar a los responsables.	
ACCIÓN 11	Diagnosticar y evaluar la factibilidad de una línea de denuncia de contenidos ilegales y atentatorios a los derechos de los niños, niñas y adolescentes, tales como la pornografía infantil en internet, entre otras, bloquear esos contenidos; rastrearlos al país de origen e impulsar todas las acciones pertinentes para sancionar a los responsables.	
ACCIÓN 12	Elaborar directrices contra la violencia digital con base en los protocolos generados por el Sistema Nacional de Prevención y Erradicación de la Violencia de Género, así como del ente encargado de la política pública de protección y en consecuencia generar rutas para la denuncia, atención, y protección de niñas, niños y adolescentes contra las transgresiones y delitos realizados mediante medios virtuales.	
LINEAMIENTO DE LA POLÍTICA PÚBLICA 3	Aumentar las capacidades de las instituciones públicas, privadas y comunitarias para la prevención, atención y protección de las niñas, niños y adolescentes frente a los contenidos nocivos, vulneraciones y los delitos perpetrados mediante medios virtuales.	
ACCIÓN 13	Elaborar protocolos contra la violencia digital y rutas para la denuncia, atención y protección de niñas, niños y adolescentes contra las transgresiones y delitos realizados mediante medios virtuales	
ACCIÓN 14	Implementar un sitio web que cuente con herramientas informativas, recursos y medidas que promuevan el desarrollo integral de niñas, niños y adolescentes a través del uso seguro de las tecnologías de la información y la comunicación	
ACCIÓN 15	Promover la participación de niñas, niños y adolescentes en la implementación, seguimiento y evaluación de la política pública uso seguro de internet y asegurar la intergeneracionalidad en las distintas etapas de este.	

Eje 3: Construcción de estructuras organizacionales de seguimiento y control / Cooperación Internacional

Objetivo 3: Coordinar, dar seguimiento, monitorear y evaluar el cumplimiento de lo estipulado en el Plan de política pública por el uso seguro de internet.
Objetivo 4: Establecer acuerdos, tratados o convenios internacionales multilaterales jurídicamente vinculantes u oficiosos de cooperación técnica y económica en materia de ciberdelincuencia y ciberseguridad enfocados en niñez y adolescencia.

LINEAMIENTO DE LA POLÍTICA PÚBLICA 4	Impulsar la articulación y coordinación institucional para la implementación, seguimiento y evaluación del plan de política pública por el uso seguro de internet para niñas, niños y adolescentes.	
ACCIÓN 16	Articular la mesa técnica interinstitucional para realizar el seguimiento, monitoreo y evaluación del Plan de política pública por el uso seguro de internet para niñas, niños y adolescentes.	
ACCIÓN 17	Informar a las entidades estatales de todos los niveles de gobierno, sociedad civil, organismos territoriales y organismos internacionales los avances del Plan de política pública por el uso seguro de internet impulsada por el Estado.	
LINEAMIENTO DE LA POLÍTICA PÚBLICA 5	Promover un proceso regional de protección de las niñas, niños y adolescentes frente a los riesgos y delitos cometidos por medios digitales.	
ACCIÓN 18	Construir en articulación con instancias regionales, la política pública y el desarrollo de la normativa que promueva los derechos digitales, la ciudadanía digital, las capacidades informacionales, las medidas de protección y reparación, y la tipificación y sanción frente a las transgresiones y delitos cometidos contra de niñas, niños y adolescentes en entornos virtuales.	
LINEAMIENTO DE LA POLÍTICA PÚBLICA 6	Fomentar y fortalecer los acuerdos, tratados y convenios internacionales, multilaterales jurídicamente vinculantes u oficiosos de cooperación técnica y económica para atender los casos de ciberdelincuencia y ciberseguridad enfocados en niñez y adolescencia.	
ACCIÓN 19	Gestionar la adhesión del Estado ecuatoriano al "Convenio sobre la ciberdelincuencia" (Convenio de Budapest)	
ACCIÓN 20	Coordinar acuerdos o tratados internacionales multilaterales jurídicamente vinculantes u oficiosos de cooperación para el intercambio de información, tecnología, conocimiento de expertos y diversos recursos para atender los casos de ciberdelincuencia y ciberseguridad enfocados en niñez y adolescencia.	
ACCIÓN 21	Gestionar la obtención de recursos para financiar políticas, planes, proyectos y líneas de acción que implementen medidas para garantizar los derechos de niñas, niños y adolescentes en relación al acceso, uso e interacción con tecnologías de la información y comunicación.	

Eje 4: Fortalecimiento de capacidades **Objetivo 5: Promover una cultura preventiva para el uso seguro de internet y tecnologías digitales que oriente a los miembros de la comunidad educativa acerca de los beneficios y riesgos, así como desarrolle competencias y habilidades digitales básicas que contribuyen a su desarrollo humano.**		
LINEAMIENTO DE LA POLÍTICA PÚBLICA 7	Generar y socializar en la comunidad educativa conocimientos sobre los derechos de los niños niñas y adolescentes, a la autodeterminación informativa, identidad y reputación digital y responsabilidad de uso de redes sociales, como una estrategia para garantizar una Internet sana, segura y constructiva.	
ACCIÓN 22	Desarrollar una campaña de educomunicación a través de Educa Contigo y otros medios de comunicación públicos y privados sobre el uso seguro de la internet.	
ACCIÓN 23	Coordinar campañas y procesos de difusión y concientización sobre ciberseguridad y manejo seguro de tecnologías digitales con los actores del sistema educativo, el espacio público y la sociedad en general.	

Eje 5: Estrategia comunicacional **Objetivo 6: Desarrollar una estrategia comunicacional para promover los derechos digitales y un uso seguro de la internet por parte de niñas, niños y adolescentes.**		
LINEAMIENTO DE LA POLÍTICA PÚBLICA 8	Activar las redes sociales institucionales con campañas informativas, posicionamiento y mantenimiento del uso seguro de la Internet para niñas, niños y adolescentes.	
ACCIÓN 24	Difundir temas relativos al uso seguro de internet en los medios de comunicación públicos, privados y digitales. Estandarizar los contenidos para difundirlos en medios de comunicación.	
LINEAMIENTO DE LA POLÍTICA PÚBLICA 9	Erradicar los mensajes y contenidos violentos y discriminatorios en contra niñas, niños y adolescentes que se difunden a través de medios virtuales.	
ACCIÓN 25	Coordinar campañas y procesos de difusión y concientización sobre: datos personales, derechos digitales, uso de una internet segura, seguridad en redes dirigidas a los usuarios de los servicios públicos; funcionarios públicos, en especial a Policía Nacional, Fiscalía, Función Judicial, Corte Constitucional; proveedores de servicios de telecomunicaciones; público en general.	
LINEAMIENTO DE LA POLÍTICA PÚBLICA 10	Analizar el impacto de los mensajes difundidos en medios públicos, privados y digitales, además de redes sociales.	
ACCIÓN 26	Monitoreo de noticias en medios: prensa, radio, televisión, digitales. Redes sociales (Facebook, Twitter. YouTube).	

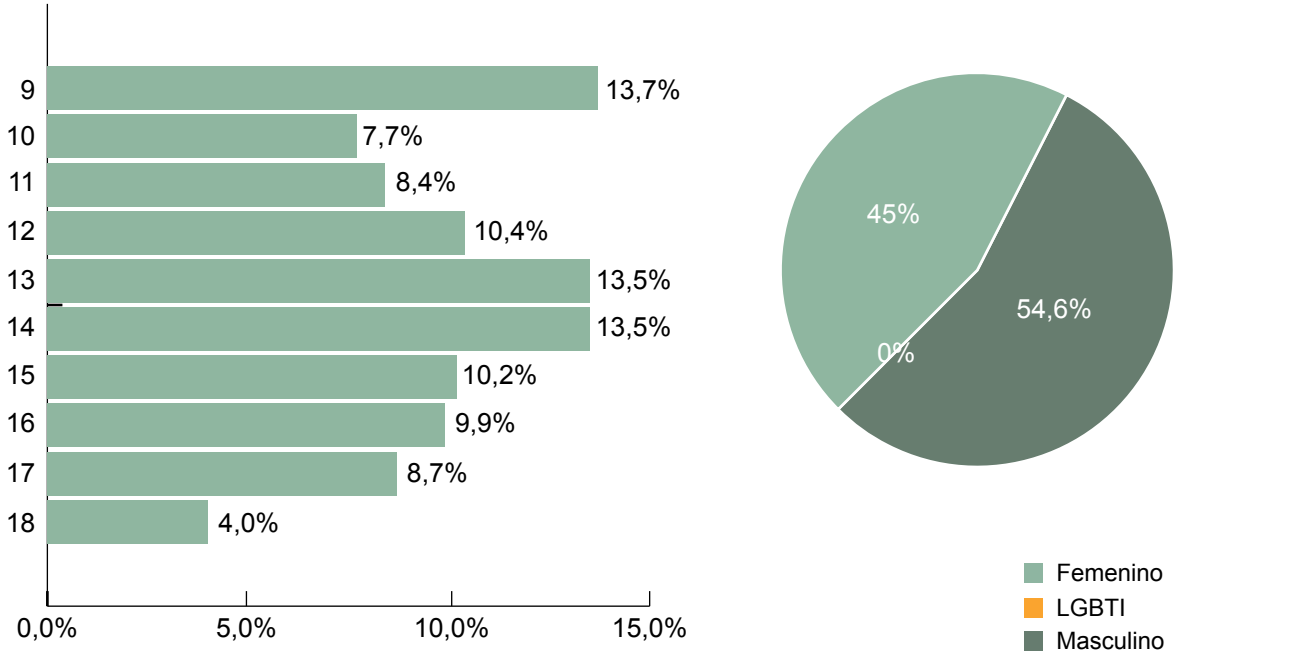
Fuente: Elaboración propia.

Resultados de la encuesta

La encuesta fue completada por un total de 3,673 niñas, niños y adolescentes provenientes de las 23 provincias del Ecuador continental, con edades comprendidas entre los 9 y 18 años. La muestra reflejó una distribución de género donde el 54,6% de los participantes fueron mujeres, el 45.0% hombres, y el restante se autoidentificó como parte de la comunidad LGBTI. Esta representatividad demográfica y de género brinda una visión inclusiva y diversa de la población encuestada, asegurando que las perspectivas y necesidades de diferentes grupos sean tomadas en cuenta en el análisis y diseño de estrategias relacionadas con el acceso y uso de internet en este grupo etario.

Figura 10

Caracterización de la población encuestada

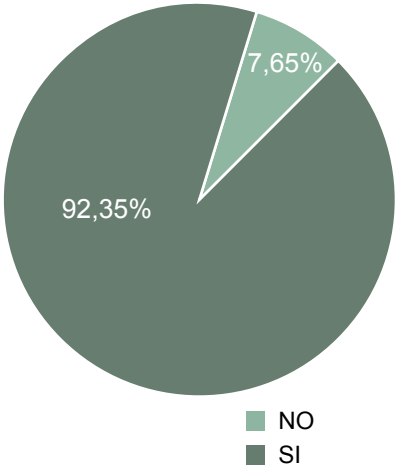


Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los resultados indican que un 92.35% de los encuestados tiene acceso a internet, lo que refleja un alto nivel de conectividad entre niñas, niños y adolescentes en las 23 provincias del Ecuador continental. Sin embargo, el 7.65% restante que no cuenta con acceso evidencia una brecha digital que aún persiste y que podría limitar las oportunidades de este grupo para participar en actividades educativas, sociales y de desarrollo personal en un entorno digital. Estos datos resaltan la importancia de diseñar estrategias inclusivas que garanticen acceso equitativo a internet para toda la población joven.

Figura 11

Porcentaje de niñas, niños y adolescentes que tienen acceso a Internet



Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos sobre el dispositivo a través del cual se conectan al internet reflejan que el 56.7% de los encuestados utiliza un teléfono celular propio como su principal dispositivo para acceder a internet, destacando la prevalencia de los teléfonos móviles en la conectividad de niñas, niños y adolescentes. En contraste, solo el 25.3% dispone de una computadora o tablet propia, lo que sugiere una menor disponibilidad de dispositivos más versátiles para actividades educativas o académicas. Además, el 26.7% accede a una computadora o tablet que pertenece a sus padres, hermanos o cuidadores, lo que indica una dependencia significativa de los recursos familiares para acceder a herramientas tecnológicas avanzadas.

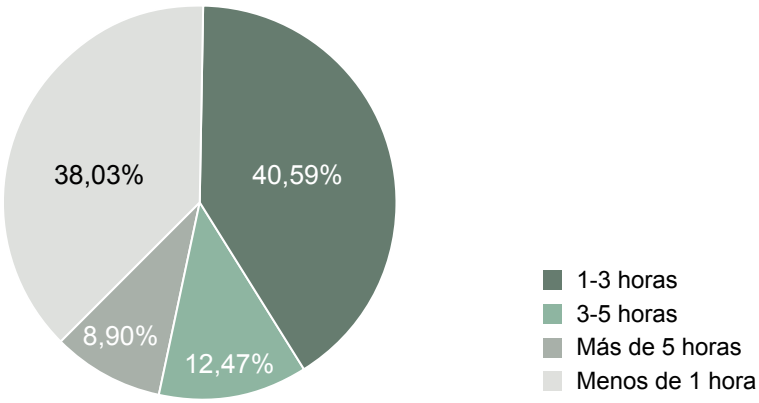
Tabla 4
Dispositivo a través del cual se conectan a internet.

Dispositivo o medio	Porcentaje
Teléfono celular propio	56,7%
Computadora o Tablet propia	25,3%
Computadora o Tablet de mis padres, hermanos/as o cuidadores	26,7%

Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Sobre el tiempo diario de conexión a internet por niñas, niños y adolescentes revelan efectos variados en su vida cotidiana. El 40.6% que se conecta entre 1 y 3 horas parece mantener un uso equilibrado, posiblemente relacionado con actividades educativas, sociales o recreativas moderadas. Sin embargo, el 12.5% que navega entre 3 y 5 horas y el 8.9% que supera las 5 horas diarias podrían estar en riesgo de efectos negativos como distracción, disminución de la actividad física o exposición prolongada a riesgos digitales. Por otro lado, el 38.0% que utiliza internet menos de una hora al día puede estar experimentando una participación limitada en oportunidades educativas y sociales digitales, posiblemente debido a restricciones en el acceso o falta de recursos. Estos patrones reflejan la necesidad de fomentar un uso responsable y balanceado del internet, garantizando que se maximicen sus beneficios mientras se minimizan los riesgos asociados.

Figura 12
Frecuencia de conexión a internet en un día típico



Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Sobre las actividades más frecuentes que niñas, niños y adolescentes realizan en línea muestran que el 92.5% utiliza internet para estudiar o hacer tareas, lo que destaca su papel clave como herramienta educativa. Sin embargo, actividades recreativas como ver videos (80.5%), usar redes

sociales (51.1%) y jugar videojuegos (46.6%) también ocupan una parte significativa de su tiempo en línea, evidenciando el equilibrio entre entretenimiento y aprendizaje. Además, el 68.8% utiliza internet para comunicarse con amigos/as, lo que resalta la importancia del entorno digital en sus interacciones sociales. Por otro lado, actividades como navegar por páginas web (30.8%) y otros usos variados (36.4%) sugieren una exploración más limitada o específica de internet. Estos patrones reflejan cómo el internet se convierte en un espacio multifuncional para las niñas, niños y adolescentes, con un impacto positivo en la educación y las relaciones sociales, pero que también requiere orientación para evitar riesgos asociados al uso recreativo excesivo o inadecuado.

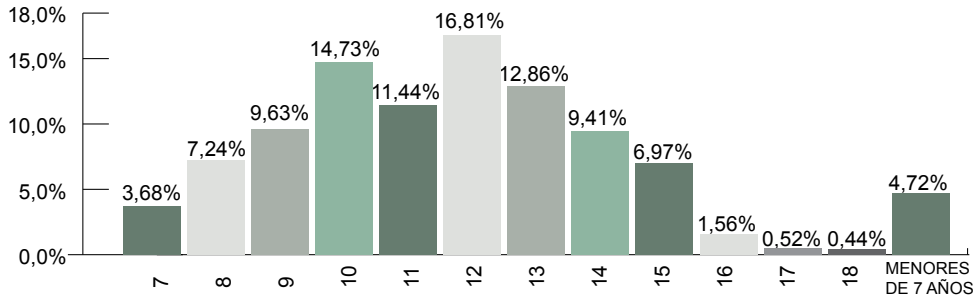
Tabla 5
Actividades más frecuentes que realizan en línea

Actividad	Porcentaje
Jugar videojuegos	46,6%
Usar redes sociales	51,1%
Ver videos	80,5%
Estudiar o hacer tareas	92,5%
Navegar por páginas web	30,80%
Comunicarte con tus amigos/as	68,8%
Otro	36,4%

Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Sobre la edad a la que niñas, niños y adolescentes comenzaron a usar redes sociales evidencian que un porcentaje significativo accede a estas plataformas a edades tempranas, con un 4.7% iniciando antes de los 7 años y un 14.7% a los 10 años. Esto refleja una introducción precoz al mundo digital, lo que puede implicar una exposición prematura a riesgos como el ciberacoso, contenido inapropiado o influencias negativas en el desarrollo emocional y social. Aunque el mayor porcentaje comienza a usar redes sociales entre los 12 y 13 años (16.8% y 12.9%, respectivamente), lo cual está alineado con las restricciones de edad de muchas plataformas, la alta proporción de niñas, niños y adolescentes iniciándose antes de esta edad indica la falta de control o supervisión por parte de adultos responsables. Este escenario resalta la necesidad de fortalecer la educación digital y la alfabetización mediática desde etapas tempranas, así como establecer límites claros y supervisión activa por parte de cuidadores para minimizar los riesgos y promover un uso seguro y saludable de las redes sociales.

Figura 13
Edad a la que empezaron a usar redes sociales



Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

El análisis de las redes sociales más utilizadas por niñas, niños y adolescentes en Ecuador revela una clara preferencia por WhatsApp (74.27%) y TikTok (70.79%), lo que destaca el uso predominante de estas plataformas para comunicación y entretenimiento. Facebook (48.30%) e Instagram (34.60%) también tienen una presencia significativa, aunque con una popularidad menor entre este grupo, posiblemente debido a una percepción más adulta o profesional de estas plataformas. En contraste, redes como Twitter/X (5.20%), Skype (3.48%), y Twitch (6.78%) tienen una adopción marginal, lo que refleja su menor relevancia en las dinámicas sociales y recreativas de esta población. La diversidad de usos queda patente con un 27.09% que reporta utilizar otras plataformas, lo que indica preferencias personales o nichos específicos. Este panorama resalta la necesidad de fomentar la educación digital enfocada en estas plataformas predominantes, promoviendo un uso responsable, consciente y seguro frente a los riesgos asociados a la exposición en redes sociales.

Tabla 6

Redes sociales utilizadas con más frecuencia por niñas, niños y adolescentes.

Red social	Porcentaje
Facebook	48,30%
TikTok	70,79%
Instagram	34,60%
WhatsApp	74,27%
Twitter / X	5,20%
Skype	3,48%
Snapchat	17,12%
Twitch	6,78%
Otro	27,09%

Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Sobre la comodidad de niñas, niños y adolescentes al compartir fotos o videos propios en redes sociales reflejan una actitud cautelosa hacia la autopresentación digital. Aunque un 45.3% señala que "a veces" se siente cómodo compartiendo contenido personal, lo que sugiere que la decisión depende del contexto o de la plataforma, un significativo 43.8% afirma que "nunca" lo hace, lo que podría indicar una percepción de riesgo o una educación preventiva adecuada. Sin embargo, el 10.9% que responde "sí, siempre" plantea preocupaciones importantes, ya que podría reflejar una falta de conciencia sobre los riesgos asociados a compartir contenido personal en internet, como el ciberacoso o el uso indebido de imágenes. Estos resultados resaltan la necesidad de fortalecer la educación digital en temas de privacidad, seguridad y gestión de la identidad digital, para que niñas, niños y adolescentes puedan tomar decisiones informadas y proteger su integridad en las redes sociales.

Figura 14

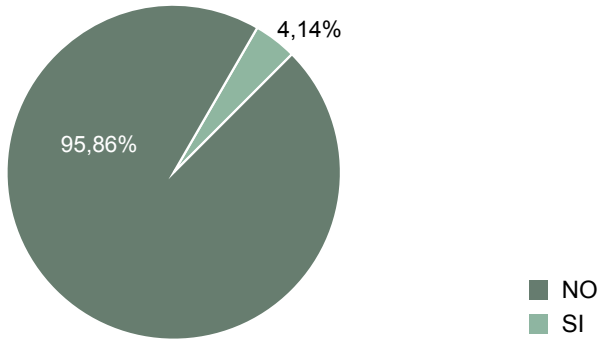
Percepción de comodidad compartiendo fotos o videos de ellos mismo en redes sociales

Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos reflejan que un 95.9% de las niñas, niños y adolescentes encuestados asegura no haber compartido información personal como su dirección o número de teléfono con desconocidos, lo cual es un indicador positivo de concienciación sobre la privacidad y los riesgos en internet. Sin embargo, el 4.1% que reconoce haberlo hecho plantea una preocupación crítica, ya que incluso un porcentaje relativamente bajo implica que un número significativo de niñas, niños y adolescentes está expuesto a situaciones de riesgo potencial, como el ciberacoso, estafas o explotación. Este hallazgo subraya la necesidad de reforzar la educación en seguridad digital desde edades tempranas, no solo enfocándose en los peligros de compartir datos sensibles, sino también promoviendo estrategias prácticas para identificar y evitar interacciones riesgosas en línea. La supervisión activa de padres, cuidadores y educadores es fundamental para mitigar este riesgo y garantizar la protección de los niñas, niños y adolescentes en el entorno digital.

Figura 15

Porcentaje de niñas, niños y adolescentes que han compartido información personal (como dirección o número de teléfono) con un desconocido, en alguna ocasión.



Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos reflejan que niñas, niños y adolescentes tienen un nivel significativo de conocimiento sobre los riesgos asociados al uso de internet y redes sociales, destacándose la suplantación de identidad (76.10%) como el más reconocido. Otros riesgos, como el ciberacoso (67.38%), las noticias falsas (68.31%), y los retos virales (64.20%), también tienen un alto nivel de reconocimiento, lo que evidencia una sensibilización creciente sobre los peligros en línea. Sin embargo, riesgos graves como la sextorsión (62.40%) y el grooming (59.32%), aunque conocidos por una mayoría, muestran un margen preocupante de desconocimiento que podría dejar a un porcentaje considerable de niñas, niños y adolescentes vulnerables a estas prácticas. La diversidad de respuestas en la categoría "Otro (45.44%)" indica que aún existen áreas de riesgo menos exploradas o comprendidas. Este

panorama subraya la importancia de reforzar la educación digital, abordando de manera integral y específica todos estos riesgos, para garantizar que niñas, niños y adolescentes estén plenamente equipados para protegerse en entornos digitales. Además, resalta la necesidad de estrategias preventivas que involucren tanto a familias como a instituciones educativas para mitigar la exposición a estos peligros.

Tabla 7

Los riesgos más reconocidos por las niñas, niños y adolescentes al usar Internet y redes sociales.

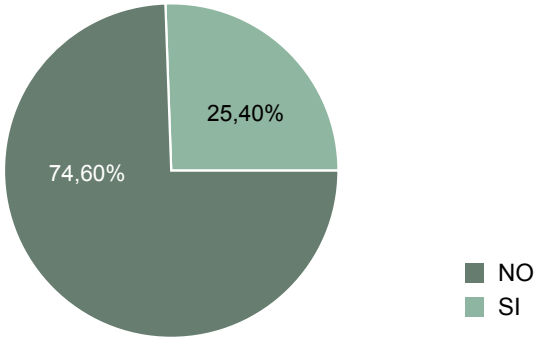
Tipo de riesgo	Porcentaje
Suplantación de identidad	76,10%
Ciberacoso	67,38%
Sextorsión	62,40%
Grooming	59,32%
Mensajes que incitan al odio	61,58%
Noticias falsas	68,31%
Retos virales	64,20%
Otro	45,44%

Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos indican que el 74.6% de niñas, niños y adolescentes ha tomado medidas para protegerse en línea y mantener un entorno seguro en redes sociales, lo que refleja una concienciación creciente sobre la importancia de la seguridad digital. Sin embargo, el 25.4% que no ha adoptado ninguna medida representa un grupo considerablemente vulnerable a los riesgos en línea, como el ciberacoso, la suplantación de identidad o el acceso no autorizado a su información personal. Este porcentaje pone de manifiesto la necesidad de fortalecer los programas de alfabetización digital, enfocándose en estrategias prácticas de protección, como la configuración de privacidad, el reconocimiento de comportamientos sospechosos y la denuncia de contenido o interacciones inapropiadas. Además, se requiere involucrar a padres, educadores y comunidades para fomentar una cultura de prevención activa que alcance a este segmento de usuarios que aún no toman medidas, reduciendo así su exposición a peligros en el entorno digital.

Figura 16

Porcentaje de niñas, niños y adolescentes que han tomado medidas para protegerse en línea y mantener un entorno seguro en las redes sociales.

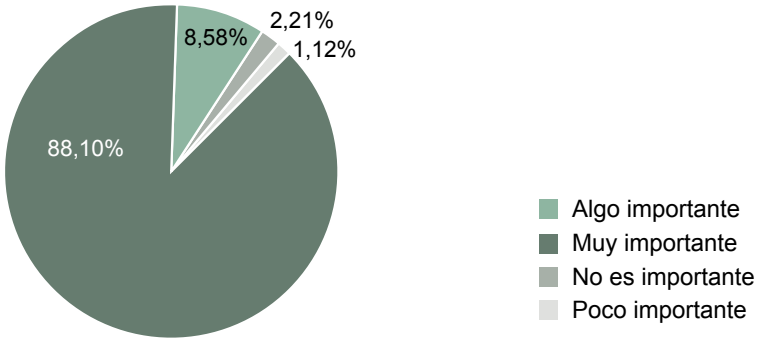


Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos reflejan que la mayoría de las niñas, niños y adolescentes reconoce la relevancia de mantener un comportamiento respetuoso en línea, con un 88.1% que considera este aspecto como "muy importante" y un 8.6% que lo califica como "algo importante". Esto evidencia una conciencia generalizada sobre la necesidad de promover interacciones digitales basadas en el respeto y la empatía, lo cual es esencial para prevenir problemas como el ciberacoso o los mensajes de odio. Sin embargo, aunque minoritario, el 3.3% que considera este comportamiento como "poco" o "no importante" plantea una preocupación, ya que esta perspectiva podría contribuir a la perpetuación de dinámicas negativas en línea. Este análisis subraya la importancia de reforzar programas educativos que fomenten una ciudadanía digital responsable, haciendo énfasis en cómo un comportamiento respetuoso beneficia tanto a las relaciones interpersonales como al bienestar colectivo en los entornos digitales.

Figura 17

Percepción sobre la importancia de mantener un comportamiento respetuoso hacia los demás en línea

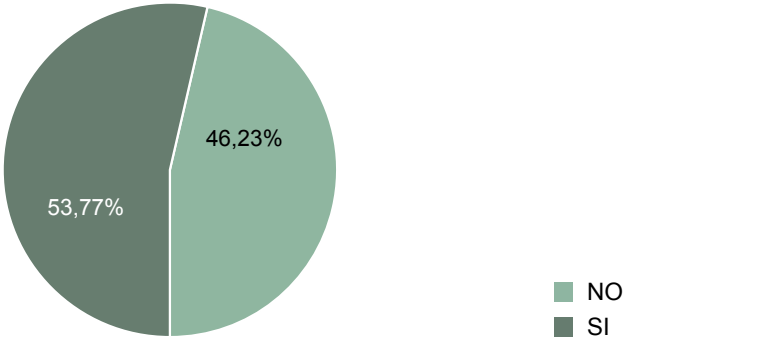


Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos muestran que solo el 53.8% de niñas, niños y adolescentes afirma conocer sus derechos digitales, mientras que un significativo 46.2% no tiene conocimiento al respecto, lo que evidencia una importante brecha en la alfabetización digital en este grupo etario. Este desconocimiento limita la capacidad de las niñas, niños y adolescentes para identificar y ejercer sus derechos en el entorno digital, dejándolos más vulnerables a riesgos como la violación de su privacidad, el ciberacoso y la exposición a contenidos inapropiados. Aunque más de la mitad reconoce tener algún nivel de conocimiento, es crucial garantizar que este porcentaje se eleve mediante programas educativos que incluyan formación específica sobre derechos digitales, como la privacidad, la libertad de expresión y la protección contra abusos en línea. Este análisis resalta la necesidad de incluir la educación sobre derechos digitales en currículos escolares y campañas públicas, para empoderar a las niñas, niños y adolescentes y fomentar una ciudadanía digital consciente y protegida.

Figura 18

Porcentaje de niñas, niños y adolescentes que conocen sus derechos digitales

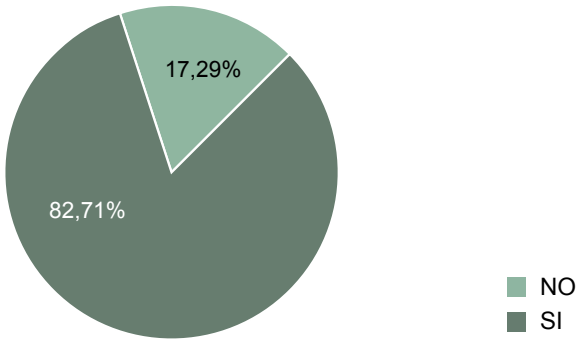


Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos indican que el 82.7% de niñas, niños y adolescentes siente que tiene un adulto de confianza al que puede acudir si enfrenta una situación desagradable, amenaza o daño en internet, lo cual es alentador y sugiere que la mayoría percibe un entorno de apoyo en su círculo cercano. Sin embargo, el 17.3% que no cuenta con este respaldo plantea una preocupación crítica, ya que representa un grupo vulnerable que podría enfrentarse solo a riesgos graves como el ciberacoso, grooming o sextorsión. Este hallazgo resalta la importancia de fomentar espacios de diálogo abiertos y seguros entre las niñas, niños y adolescentes y los adultos, así como de sensibilizar a padres, cuidadores y educadores sobre la importancia de estar disponibles y capacitados para abordar estos temas. Además, subraya la necesidad de fortalecer sistemas de apoyo institucionales y comunitarios que brinden orientación y protección a aquellos que no encuentran en su entorno inmediato un adulto confiable.

Figura 19

Porcentaje de niñas, niños y adolescentes que tienen un adulto de confianza al que puedan acudir si experimentan algo desagradable, reciben una amenaza o sufren algún daño mientras usas internet o redes



Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos muestran que el 94.96% de niñas, niños y adolescentes identifica a sus padres como sus principales adultos de confianza, lo que resalta la importancia del vínculo familiar en la protección y orientación frente a riesgos en internet. Sin embargo, también destaca el papel significativo de otros actores, como hermanos (59.41%), profesores (35.94%) y otros familiares (33.51%), que complementan esta red de apoyo. Aunque en menor medida, la confianza depositada en amigos (22.19%) y cuidadores (9.94%) sugiere que algunas niñas, niños y adolescentes recurren a figuras no familiares, lo que podría indicar la ausencia de relaciones de confianza dentro del hogar o una necesidad de diversificar las fuentes de apoyo. La diversidad de opciones, incluyendo el 18.38% que menciona "otros", evidencia la importancia de ampliar y fortalecer los canales de apoyo, asegurando que todos tengan acceso a adultos preparados para abordar situaciones críticas en el entorno digital, especialmente en casos donde los padres no están disponibles o no son percibidos como figuras de confianza.

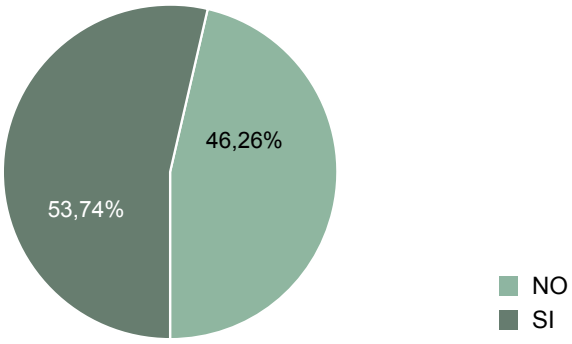
Tabla 8
Adulto de confianza de la niña, niños y adolescentes

Adulto de Confianza	Porcentaje
Madre/padre	94,96%
Hermana/hermano	59,41%
Cuidadora/cuidador	9,94%
Amiga/amigo	22,19%
Profesora/profesor	35,94%
Otros familiares	33,51%
Otros	18,38%

Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos muestran que solo el 53.8% de niñas, niños y adolescentes afirma conocer sus derechos digitales, mientras que un significativo 46.2% no tiene conocimiento al respecto, lo que evidencia una importante brecha en la alfabetización digital en este grupo etario. Este desconocimiento limita la capacidad de las niñas, niños y adolescentes para identificar y ejercer sus derechos en el entorno digital, dejándolos más vulnerables a riesgos como la violación de su privacidad, el ciberacoso y la exposición a contenidos inapropiados. Aunque más de la mitad reconoce tener algún nivel de conocimiento, es crucial garantizar que este porcentaje se eleve mediante programas educativos que incluyan formación específica sobre derechos digitales, como la privacidad, la libertad de expresión y la protección contra abusos en línea. Este análisis resalta la necesidad de incluir la educación sobre derechos digitales en currículos escolares y campañas públicas, para empoderar a las niñas, niños y adolescentes y fomentar una ciudadanía digital consciente y protegida.

Figura 20
Porcentaje de niñas, niños y adolescentes que saben cómo reportar o denunciar un incidente en Línea



Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos revelan que el 62.87% de niñas, niños y adolescentes identificaría al ECU 9-1-1 como la principal entidad para denunciar incidentes en línea, lo que refleja una confianza en esta plataforma como un recurso accesible y visible. Sin embargo, otros organismos clave como la Policía Nacional (47.26%), la Junta Cantonal de Protección de Derechos (36.22%) y la Fiscalía (32.73%) tienen un reconocimiento significativamente menor, lo que podría evidenciar una falta de información sobre su papel en la gestión de incidentes digitales. Además, solo el 27.81% consideraría denunciar ante una autoridad escolar, lo que sugiere una subutilización de estas figuras, a pesar de su

cercanía con las niñas, niños y adolescentes. La baja proporción de respuestas en "otros" (1.82%) podría reflejar una limitada diversificación de opciones percibidas. Estos datos destacan la necesidad de campañas informativas para educar sobre los canales adecuados para denunciar, enfatizando la coordinación entre instituciones y la importancia de las autoridades escolares y comunitarias en la protección integral de los derechos digitales de niñas, niños y adolescentes.

Tabla 9

Lugar de denuncias que conocen las niñas, niños y adolescentes.

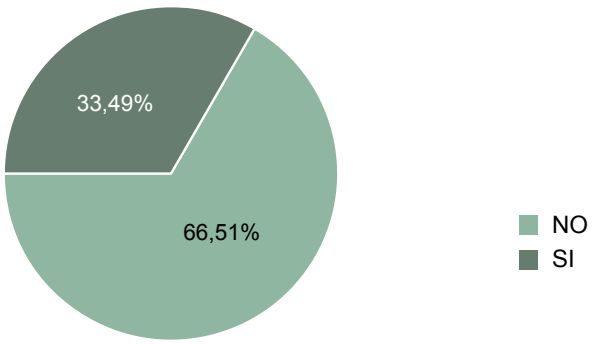
Dónde lo denunciarías	Porcentaje
1. ECU 9-1-1	62,87%
2. Policía Nacional	47,26%
3. Junta Cantonal de Protección de Derechos	36,22%
4. Fiscalía	32,73%
5. Autoridad de la escuela o colegio	27,81%
6. Otros	1,82%

Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos indican que solo el 33.5% de niñas, niños y adolescentes conoce algún sitio web informativo sobre riesgos y peligros en internet, mientras que un alarmante 66.5% desconoce la existencia de estos recursos. Este resultado refleja una brecha crítica en la difusión de información preventiva y la educación digital, lo que limita la capacidad de las niñas, niños y adolescentes para identificar, comprender y enfrentar amenazas en línea de manera proactiva. La falta de conocimiento sobre sitios web confiables para informarse deja a una mayoría de los ellos sin acceso a herramientas esenciales para su autoprotección. Este escenario subraya la necesidad de desarrollar estrategias más efectivas de comunicación y promoción de plataformas informativas sobre seguridad digital, involucrando a escuelas, familias y autoridades en la difusión masiva y accesible de estos recursos, de modo que todos puedan beneficiarse de información clara y relevante para navegar de manera segura en internet.

Figura 21

Porcentaje de niñas, niños y adolescentes que conocen de algún sitio web informativo sobre riesgos/peligros en el internet

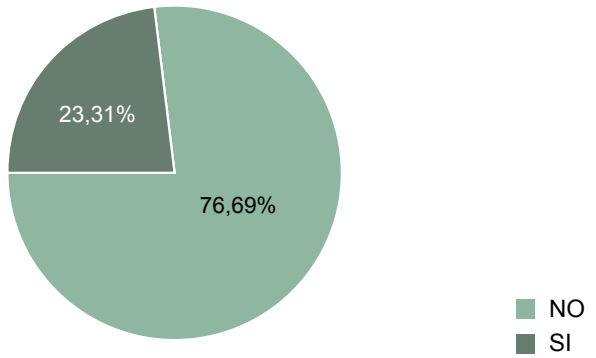


Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos muestran que solo el 23.3% de niñas, niños y adolescentes conoce alguna línea de protección contra peligros en internet a nivel internacional, mientras que una amplia mayoría del 76.7% no tiene conocimiento al respecto. Esto evidencia una preocupante desconexión con los recursos globales de seguridad en línea, los cuales podrían ser fundamentales para acceder a apoyo en situaciones críticas, especialmente en casos de ciberacoso, grooming o explotación en plataformas internacionales. Este desconocimiento limita la capacidad de las niñas, niños y adolescentes para buscar ayuda más allá de las opciones locales, lo que resalta la necesidad de integrar información sobre estas líneas internacionales en programas educativos y campañas de sensibilización. Promover el conocimiento de recursos globales confiables, como los ofrecidos por organismos internacionales especializados en seguridad digital, es crucial para garantizar que estén mejor protegidos en un entorno en línea cada vez más globalizado y conectado.

Figura 22

Porcentaje de niñas, niños y adolescentes que conocen de alguna línea de protección de peligros del internet a nivel internacional



Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos reflejan que la mayoría de las niñas, niños y adolescentes recibe información sobre el uso seguro de internet en el hogar (92.05%) y la escuela (84.15%), destacando estos espacios como los principales referentes en la educación digital. Sin embargo, otras instituciones y contextos comunitarios, como la iglesia (36.54%), municipios (24.31%) y grupos juveniles (21.73%), tienen una participación mucho menor, lo que evidencia un potencial desaprovechado para ampliar el alcance de estas iniciativas. Además, espacios públicos como parques (14.73%) tienen una incidencia marginal, lo que sugiere que la información sobre seguridad en línea aún no se incluye de manera integral en actividades comunitarias. Estos resultados subrayan la importancia de fortalecer la colaboración entre todos los actores sociales, no solo los tradicionales como el hogar y la escuela, sino también organizaciones comunitarias, religiosas y gubernamentales, para garantizar que la educación sobre el uso seguro de internet sea accesible, inclusiva y difundida en diversos entornos. Esto permitiría llegar a sectores de la población que podrían no recibir suficiente orientación en los espacios principales.

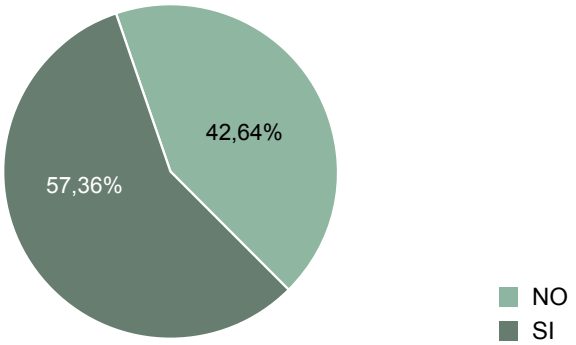
Tabla 10
Espacios en el que, las niñas, niños y adolescentes han recibido información sobre el uso seguro del Internet

Espacio	Porcentaje
Hogar	92,05%
Escuela	84,15%
Iglesia	36,54%
Grupo Juvenil	21,73%
Municipio	24,31%
Parque	14,73%
Otro	26,76%

Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

Los datos muestran que el 57.4% de niñas, niños y adolescentes afirma haber recibido información sobre el uso seguro de internet a través de redes o información pública, lo que indica que más de la mitad ha sido alcanzado por campañas o mensajes preventivos. Sin embargo, el 42.6% que no ha recibido dicha información revela una brecha significativa en la cobertura de estas iniciativas, lo que deja a un porcentaje considerable de niñas, niños y adolescentes sin acceso a orientación crucial para su protección en línea. Este hallazgo destaca la necesidad de mejorar la efectividad y alcance de las estrategias de comunicación, utilizando canales frecuentados por los ellos, como redes sociales y plataformas digitales, para garantizar que los mensajes lleguen a toda la población objetivo. Además, se requiere una evaluación crítica de las campañas existentes para identificar barreras en la difusión y asegurar que la información sea clara, accesible y relevante para diferentes contextos. Fortalecer esta comunicación es clave para una educación digital inclusiva y universal.

Figura 23
Porcentaje de niñas, niños y adolescentes que han recibido información o mensajes sobre el uso seguro de la internet, a través de redes o información pública



Fuente: CNII-Encuesta de evaluación de la política pública de internet segura, 2024

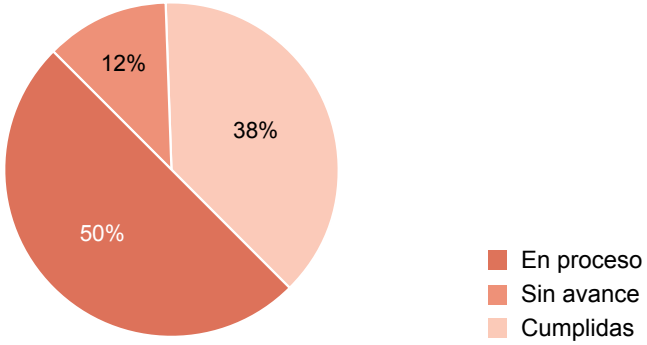
Conclusiones y recomendaciones

Conclusiones Generales

Del total de acciones evaluadas, el **38% (10 acciones)** han sido completamente implementadas, logrando resultados efectivos que contribuyen directamente al cumplimiento de los objetivos de la política pública. **El 50% (13 acciones)** se encuentran en proceso, enfrentando desafíos o limitaciones que dificultan su plena efectividad, lo que requiere ajustes y esfuerzos adicionales para asegurar su implementación total. Finalmente, el 12% (3 acciones) no han sido implementadas o muestran avances mínimos, sin evidencia de impacto positivo, representando áreas críticas que requieren **atención prioritaria** para evitar rezagos en los resultados esperados.

Figura 24

Porcentaje de niñas, niños y adolescentes que han recibido información o mensajes sobre el uso seguro de la internet, a través de redes o información pública



Elaboración propia

- **El Eje 1:** Medidas Legales presenta avances en las acciones relacionadas con la inclusión de derechos digitales en la normativa nacional y la regulación de delitos informáticos. Sin embargo, la falta de implementación en la Acción 4 requiere acciones urgentes y concretas para garantizar un entorno seguro en los centros de acceso a Internet. La continuidad de procesos de interoperabilidad y capacitación fortalecerá los resultados alcanzados hasta la fecha.

- **El Eje 2:** Medidas Técnicas y Procedimentales muestra avances en la implementación de la política pública, especialmente en la participación de NNA y la creación de protocolos. Sin embargo, acciones críticas como el control de contenidos nocivos y la factibilidad de líneas de denuncia requieren atención urgente. Es fundamental articular esfuerzos interinstitucionales y tecnológicos para garantizar un acceso seguro y responsable a las TIC en todo el país.

- **El Eje 3:** Construcción de estructuras organizacionales de seguimiento y control presenta avances s en la coordinación interinstitucional, la cooperación internacional y la adhesión al Convenio de Budapest. No obstante, es necesario reforzar las acciones de financiamiento y ampliar el alcance territorial de programas como FOFOUSI. La reactivación de la mesa técnica interinstitucional y la implementación de mecanismos de monitoreo garantizarán la sostenibilidad de los logros alcanzados.

- **El Eje 4:** Fortalecimiento de capacidades han logrado avances, especialmente en la creación de materiales educativos y en campañas de sensibilización. No obstante, persisten desafíos en el alcance geográfico, la evaluación del impacto y la continuidad de las campañas. Se recomienda fortalecer la cobertura en zonas rurales, monitorear los resultados obtenidos y diversificar los formatos de difusión para asegurar una internet segura y constructiva para niñas, niños y adolescentes en Ecuador.

- **El Eje 5:** Estrategia comunicacional, las acciones muestran avances, especialmente en campañas informativas y materiales educativos desarrollados por las instituciones que son parte de la mesa. Sin embargo, existen desafíos en el monitoreo constante de redes sociales y la falta de una estrategia coordinada entre instituciones. Se recomienda fortalecer la actualización de contenidos, ampliar la difusión en zonas vulnerables y rurales, y garantizar la medición del impacto de las campañas para un uso seguro y responsable de la internet por parte de niñas, niños y adolescentes.

Recomendaciones generales

Dado que se cuenta con un avance del **38% (10 acciones)** que han sido completamente implementadas, logrando resultados efectivos que contribuyen directamente al cumplimiento de los objetivos de la política pública y **el 50% (13 acciones)** se encuentran en proceso, se recomienda **actualizar la Política pública para una Internet segura** dirigida a niñas, niños y adolescentes, para el periodo 2025 – 2029, debido a la pertinencia y relevancia del tema para la prevención y protección de las niñas, niños y adolescentes frente a las violencias digitales y la **evolución constante de las tecnologías y los riesgos digitales emergentes**.

Los avances tecnológicos, el uso creciente de redes sociales y plataformas digitales, así como la sofisticación de amenazas como el *grooming, ciberacoso, sextorsión* y la explotación en línea, requieren que las políticas sean **dinámicas, adaptativas y alineadas** con los nuevos desafíos.

Las estadísticas evidencian la gravedad de la situación: los delitos relacionados con la explotación sexual y otras formas de abuso digital han incrementado alarmantemente, pasando de 11 casos en 2014 a 204 en 2021, y aunque en 2024 se registró una leve disminución a 166 casos, los números siguen siendo preocupantes. El delito más prevalente, el "contacto con finalidad sexual con menores por medios electrónicos", acumula 635 casos, mientras que la pornografía infantil suma 312 casos en el período evaluado. Estos datos evidencian la urgencia de fortalecer las políticas públicas y garantizar su actualización.

Una actualización constante garantiza que las estrategias de prevención, protección y educación

respondan efectivamente a las realidades actuales, promoviendo un entorno digital seguro, inclusivo y constructivo. Además, permite integrar nuevas herramientas tecnológicas, fortalecer la participación activa de niñas, niños y adolescentes y consolidar alianzas intersectoriales para enfrentar estas problemáticas de manera integral y sostenible.

Recomendaciones para la actualización

1. **Establecer una mesa técnica interinstitucional,** liderada por el **Consejo Nacional para la Igualdad Intergeneracional,** con el objetivo de articular el trabajo de las distintas instancias involucradas y dar seguimiento al cumplimiento de las acciones e indicadores de la política pública.

2. Fortalecimiento de capacidades institucionales, en las que se recomienda desarrollar programas de formación continua para servidores públicos, docentes, personal técnico y operadores de justicia, enfocándose en la detección y respuesta a casos de violencia digital (grooming, sexting, ciberacoso); y, manejo de herramientas tecnológicas de monitoreo y denuncia.

3. Establecer unidades de respuesta rápida dentro de instituciones clave como el Ministerio de Educación, Ministerio de Telecomunicaciones y Sociedad de la Información, Fiscalía General del Ecuador y el Consejo de la Judicatura para abordar problemas relacionados con contenidos nocivos y violencia en línea.

4. 4. Diseño e implementación de campañas de prevención permanentes en medios de comunicación tradicionales y digitales sobre el uso seguro y responsable de internet. Promover materiales adaptados a diferentes edades: videos animados, infografías, juegos interactivos y cómics.

5. Inclusión de la ciudadanía digital en el currículo educativo.
   - ¿Incorporar la ciudadanía digital como un eje transversal en el currículo escolar desde la educación inicial hasta el bachillerato.

   - Desarrollar módulos específicos sobre seguridad en línea, protección de datos personales, uso ético de redes sociales y prevención de riesgos digitales.

   - Crear programas de formación para padres, madres y cuidadores con énfasis en el acompañamiento digital y estrategias para identificar riesgos en línea.

   - Crear plataformas de aprendizaje y recursos interactivos adaptados a las edades y necesidades de niñas, niños y adolescentes.

6. Fortalecimiento de mecanismos de denuncia y atención
   - Implementar líneas de denuncia para casos de violencia digital con opciones de atención por chat, teléfono y aplicaciones móviles.

   - Asegurar la confidencialidad y la protección de las víctimas.

   - Mejorar la coordinación interinstitucional entre la policía, fiscalía y organismos de protección para garantizar un manejo oportuno de denuncias y sanciones efectivas a los responsables.

7. Creación de un sistema de monitoreo y evaluación continua.

   - Implementar un Observatorio de Seguridad Digital de la Niñez y Adolescencia interinstitucional encargado de recopilar, analizar y reportar datos sobre el uso seguro de internet y los riesgos digitales que enfrentan niñas, niños y adolescentes. Desde el observatorio se pueden generar informes semestrales y evaluaciones anuales para identificar brechas y áreas de

mejora en la implementación del plan, y monitorear indicadores clave como:

- Número de denuncias atendidas y resueltas.
- o Alcance de capacitaciones y campañas preventivas.
- o Incidencia de riesgos digitales (grooming, ciberacoso, sexting).

- La evaluación anual interinstitucional debe involucrar:
  - Instituciones estatales (MINTEL, Ministerio de Educación, Consejo de la Judicatura, FGE y otros).
  - Organizaciones civiles y especializadas (ChildFund, UNICEF).
  - La participación activa de niñas, niños y adolescentes a través de consultas informadas.

8. Fortalecimiento de la participación de niñas, niños y adolescentes (NNA) con consultas periódicas con niñas, niños y adolescentes. Realizar encuestas y grupos focales anuales con niñas, niños y adolescentes para conocer:

   - Sus experiencias, riesgos y necesidades en el entorno digital.
   - Evaluaciones sobre el impacto de las políticas y campañas implementadas.
   - Formar un consejo integrado por niñas, niños y adolescentes que contribuya a la actualización del plan con propuestas y retroalimentación directa. Este consejo participaría en la revisión y validación de materiales y campañas.

9. Fortalecimiento de alianzas con el sector privado y ONG para desarrollar campañas preventivas innovadoras y herramientas de monitoreo y control parental.

10. Integrar al país en redes globales de monitoreo de violencia digital, como la UIT, UNICEF e INTERPOL, para actualizar las políticas con base en experiencias y estándares internacionales.

11. Creación de un sistema de alerta temprana para monitorear proactivamente los riesgos digitales. Implementar tecnologías de inteligencia artificial y análisis de datos para detectar y alertar sobre patrones de violencia digital, contenidos inapropiados y ciberacoso.

12. Publicación de reportes de avance anuales sobre la implementación y resultados del plan, incluyendo estadísticas, casos de éxito y áreas por mejorar.

Recomendaciones diferenciadas según el nivel de cumplimiento:

Eje 1: Medidas Legales **Objetivo 1: Desarrollar normativa que promueva los derechos digitales y la dignidad e integridad física, psicológica, emocional y sexual de niñas, niños y adolescentes, estableciendo los mecanismos para el aprovechamiento de los beneficios de las Tecnologías de la Información y Comunicación (TIC) y atienda y mitigue los riesgos y delitos que pueden cometerse a través de ellas.**		
LINEAMIENTO DE LA POLÍTICA PÚBLICA 1	Garantizar los derechos digitales, la ciudadanía digital y las capacidades informacionales de niñas, niños y adolescentes para una Internet segura.	
ACCIÓN 1	Proponer en la reforma al Código Orgánico de Niñez y Adolescencia la inclusión de los derechos digitales, la ciudadanía digital, las capacidades informacionales, las medidas de protección y reparación, y la tipificación y sanciones frente a las transgresiones y delitos cometidos contra de niñas, niños y adolescentes en entornos virtuales.	

Avances:

- Inclusión de derechos digitales en la reforma del COPINNA, alineados con estándares internacionales.
- Participación de actores clave como UNICEF, la Comisión Especializada y ChildFund International en la formulación de contenidos.
- Incorporación de medidas específicas para la prevención, protección y reparación frente a la violencia digital.

Recomendaciones:

- Fortalecer la difusión de los derechos digitales entre niñas, niños y adolescentes, familias y comunidades educativas.
- Implementar programas de sensibilización y formación sobre el uso seguro del Internet y los riesgos en línea, articulados con las reformas del COPINNA.
- Apoyar la aprobación final de la reforma en el pleno de la Asamblea Nacional con un proceso de incidencia política continuo.

ACCIÓN 2	Proponer reformas al Código Orgánico Integral Penal sobre delitos informáticos y transgresiones en contra de niñas, niños y adolescentes en entornos virtuales.	

Fortalezas::

- Tipificación de delitos clave como el grooming, ciberacoso y explotación sexual en línea.
- Sanciones agravadas cuando las víctimas son niñas, niños y adolescentes.

Recomendaciones:

- Promover la capacitación especializada a operadores de justicia y personal policial para la correcta aplicación de las disposiciones del COIP.
- Fortalecer los mecanismos de denuncia y acompañamiento legal a víctimas de delitos digitales.

ACCIÓN 3	Normar a los proveedores de servicios de telecomunicaciones para que brinden herramientas que permitan un acceso sano, seguro y constructivo para niñas, niños y adolescentes a las tecnologías de la información y la comunicación.	

Fortalezas::

- Implementación de herramientas de control parental y medidas de protección infantil por parte de los PST.
- Socialización de buenas prácticas y capacitación a proveedores de servicios.

Recomendaciones:

- Fortalecer los controles periódicos para garantizar el cumplimiento de las obligaciones de los PST.
- Ampliar las campañas informativas dirigidas a padres y cuidadores sobre el uso de herramientas de control parental.
- Promover alianzas estratégicas con proveedores de servicios para el desarrollo de tecnologías innovadoras que refuercen la seguridad digital.

ACCIÓN 4	Proponer normativa que regule el funcionamiento de los centros de acceso a la Internet, con enfoque de protección a la niñez y adolescencia	

Barreras identificadas:

- Ausencia de evidencias que respalden avances concretos en la normativa propuesta.
- Falta de un proceso claro de articulación con actores clave (sector público y privado) para el desarrollo de esta regulación.

Recomendaciones:

- Realizar un diagnóstico inicial sobre el funcionamiento de los centros de acceso a Internet (públicos y privados) para identificar brechas en términos de protección digital a NNA.
- Promover la creación de mesas técnicas interinstitucionales con participación del sector educativo, de telecomunicaciones y organismos de protección de derechos.
- Proponer un borrador de normativa técnica que incluya estándares mínimos de seguridad, control parental y monitoreo de contenidos en centros de acceso.

ACCIÓN 5	Generar procesos de interoperabilidad de datos entre las instituciones de la Función Judicial para la producción de estadísticas jurimétricas de ingresos de causas de delitos cibernéticos contra niñas, niños y adolescentes generando bases de datos anonimizadas que aporten al portal de estadística judicial en delitos cibernéticos.	

Avances:

- Implementación del Modelo de Justicia Abierta y publicación de boletines estadísticos sobre delitos cibernéticos.
- Uso de tecnologías para el anonimizado de datos y su publicación en el portal judicial.

Desafíos:

- Limitaciones en el acceso y actualización periódica de los datos anonimizados.
- Necesidad de fortalecer la articulación interinstitucional para garantizar el flujo de información.

Recomendaciones:

- Implementar un cronograma de interoperabilidad de datos entre las instituciones de la Función Judicial con plazos claros para la actualización de información.
- Garantizar el acceso público y transparente a los boletines, promoviendo su uso en la formulación de políticas públicas.
- Realizar capacitaciones técnicas al personal encargado del manejo de datos en cada institución.

ACCIÓN 6	Incidir en la Asamblea Nacional respecto del proyecto de protección de datos personales y la promoción de derechos digitales.	

Fortalezas::

- La Ley Orgánica de Protección de Datos Personales fue aprobada y publicada, marcando un avance significativo en materia de protección de datos y derechos digitales en Ecuador.

Recomendaciones:

- Realizar talleres dirigidos a padres, tutores y docentes para concientizar sobre los riesgos y la importancia del consentimiento informado en el manejo de datos niñas, niños y adolescentes.
- Generar materiales accesibles (guías, infografías, videos) adaptados a diferentes edades y contextos, explicando conceptos clave como “consentimiento informado”, “derecho al olvido” y “protección de la privacidad en línea”.
- Colaborar con instituciones educativas para incluir temas de derechos digitales y protección de datos en la malla curricular.
- Desarrollar protocolos adicionales para proteger los datos personales de niñas, niños y adolescentes en plataformas educativas, redes sociales y otros entornos digitales.
- Incorporar la voz de niñas, niños y adolescentes en foros y espacios de consulta para mejorar la implementación de la ley desde una perspectiva intergeneracional.

Eje 2: Medidas Técnicas y Procedimentales

Objetivo 2: Promover el acceso, uso e interacción adecuada, responsable, sana, segura y constructiva de las tecnologías de la información y la comunicación que impulse el desarrollo integral y el pleno ejercicio de los derechos de niñas, niños y adolescentes.

LINEAMIENTO DE LA POLÍTICA PÚBLICA 2	Promover un acceso sano, seguro y constructivo a las tecnologías de la información y la comunicación para proteger los derechos digitales y la integridad y dignidad de niñas, niños y adolescentes frente a los contenidos nocivos, transgresiones y delitos cometidos a través de medios digitales, con la implementación de políticas públicas, lineamientos técnicos, regulaciones, códigos de conducta, recomendaciones, estándares, metodologías, procedimientos, entre otros

ACCIÓN 7	Diseñar e implementar el plan de políticas públicas para una internet segura desde las instituciones estatales con el fin de garantizar un acceso y uso sano, seguro y constructivo a las tecnologías de la información y la comunicación por parte de niñas, niños y adolescentes.	

Avances:

- Coordinación interinstitucional exitosa con participación de 19 entidades.
- Creación de la política con enfoques intergeneracionales y regionales.
- Implementación de la página web y estrategias de difusión como #InternetSeguraEC.

Recomendaciones:

- Realizar un monitoreo anual para evaluar el impacto de la política y ajustar acciones.

ACCIÓN 8	Implementar normativas y políticas públicas desde los gobiernos autónomos descentralizados para, en el marco de las autorizaciones a comercios o locales que faciliten el acceso a las tecnologías de la información y comunicación, conforme sus competencias constitucionales y legales, garantizar un acceso y uso sano, seguro y constructivo a las tecnologías de la información y la comunicación, por parte de niños, niñas y adolescentes.	

Avances:

- Ejemplo de la Ordenanza Municipal de San Miguel de los Bancos como una buena práctica regulatoria.

Desafíos:

- Limitada réplica de ordenanzas similares en otros cantones.
- Escasa capacitación y monitoreo del cumplimiento de las normas en establecimientos locales.

Recomendaciones:

- Diseñar una **plantilla de ordenanza municipal** a nivel nacional, que los GAD puedan adaptar según sus contextos locales.
- Incluir **requisitos mínimos** como capacitación obligatoria, implementación de software de seguridad y control de horarios.
- Promover programas de **capacitación para autoridades locales** sobre la importancia de estas regulaciones y su impacto en la protección de NNA.
- Brindar asistencia técnica a los GAD a través de entidades como el **Consejo Nacional para la Igualdad Intergeneracional (CNII)** y la **Asociación de Municipalidades del Ecuador (AME).**
- Crear un **reconocimiento anual nacional** para los GAD que implementen ordenanzas efectivas, similar al **Sello de Garantía** local.
- Establecer **fondos de cofinanciamiento** para apoyar a municipios en la adopción de estas normativas.
- **Crear una mesa de trabajo interinstitucional** que articule el apoyo de entidades como **DINAPEN, CNII y AME** a nivel local.

ACCIÓN 9	Desarrollar e implementar mecanismos, lineamientos y medidas técnicas para la regulación y control del acceso a contenidos nocivos, transgresiones y posibles delitos en los servicios del régimen general de telecomunicaciones (TIC) y las empresas proveedoras de internet y mecanismos de prevención, protección, restitución y reparación de derechos para niñas, niños y adolescentes.	

Barreras identificadas:

- Falta de información concreta sobre avances en esta acción.
- Escasa articulación con proveedores de servicios de telecomunicaciones (PST) y TIC para garantizar mecanismos efectivos.
- Limitación en la infraestructura técnica y tecnológica.

Recomendaciones:

- Establecer mesas técnicas interinstitucionales con proveedores de internet y expertos en ciberseguridad para diseñar medidas de regulación y control.
- Desarrollar un plan piloto que implemente software de bloqueo y monitoreo en plataformas locales y públicas.
- Crear un protocolo interinstitucional para el seguimiento y sanción de contenidos nocivos, con participación de entidades regulatorias y judiciales.

ACCIÓN 10	Establecer el funcionamiento de una línea de denuncia de contenidos ilegales y atentatorios a los derechos de los niños, niñas y adolescentes, tales como la pornografía infantil en internet, entre otras, bloquear esos contenidos; rastrearlos al país de origen e impulsar todas las acciones pertinentes para sancionar a los responsables.	

Avances:

- Creación del canal de denuncia en línea por parte de la Fiscalía General del Estado.
- Implementación de la Unidad Nacional Especializada en Investigación de Ciberdelito.

Recomendaciones:

- Ampliar la difusión del canal de denuncia a nivel nacional, especialmente en zonas rurales.
- Asegurar la articulación interinstitucional para la atención oportuna de denuncias.
- Desarrollar campañas educativas para informar a la ciudadanía sobre el uso de la línea.

ACCIÓN 11	Diagnosticar y evaluar la factibilidad de una línea de denuncia de contenidos ilegales y atentatorios a los derechos de los niños, niñas y adolescentes, tales como la pornografía infantil en internet, entre otras, bloquear esos contenidos; rastrearlos al país de origen e impulsar todas las acciones pertinentes para sancionar a los responsables.	

Avances:

- Consultas iniciales con organismos especializados.

Desafíos:

- Ausencia de infraestructura tecnológica adecuada.
- Falta de claridad normativa que permita crear una línea específica.

Recomendaciones:

- Elaborar un diagnóstico técnico y financiero para la implementación de la línea.
- Coordinar con organismos internacionales para identificar mejores prácticas en el rastreo y bloqueo de contenidos ilícitos.
- Alinear los avances con la Unidad Nacional Especializada en Investigación de Ciberdelito de la Fiscalía General del Estado.

ACCIÓN 12	Elaborar directrices contra la violencia digital con base en los protocolos generados por el Sistema Nacional de Prevención y Erradicación de la Violencia de Género, así como del ente encargado de la política pública de protección y en consecuencia generar rutas para la denuncia, atención, y protección de niñas, niños y adolescentes contra las transgresiones y delitos realizados mediante medios virtuales.	

Avances:

- Creación de protocolos y directrices desde el Ministerio de Educación y la Fiscalía.
- Integración del enfoque restaurativo en la ruta de actuación.

Recomendaciones:

- Socializar ampliamente los protocolos a través de campañas informativas y formativas.
- Monitorear el cumplimiento en las instituciones educativas, evaluando su aplicación efectiva.
- Asegurar la capacitación continua a docentes, autoridades y DECE para implementar los lineamientos.
- Desarrollar con el ente rector directrices contra la violencia digital con base en los protocolos generados por el Sistema Nacional de Prevención y Erradicación de la Violencia de Género.

LINEAMIENTO DE LA POLÍTICA PÚBLICA 3	Aumentar las capacidades de las instituciones públicas, privadas y comunitarias para la prevención, atención y protección de las niñas, niños y adolescentes frente a los contenidos nocivos, vulneraciones y los delitos perpetrados mediante medios virtuales.

ACCIÓN 13	Elaborar protocolos contra la violencia digital y rutas para la denuncia, atención y protección de niñas, niños y adolescentes contra las transgresiones y delitos realizados mediante medios virtuales	

Recomendaciones:

- Implementar talleres periódicos para docentes, consejeros DECE, personal administrativo y operadores de justicia sobre la aplicación de los protocolos y la identificación temprana de riesgos digitales.
- Garantizar presupuesto plurianual para la implementación, evaluación y actualización de los protocolos y rutas de denuncia.
- Crear líneas específicas de atención en temas de violencia digital, con personal especializado.
- Implementar una aplicación móvil que facilite denuncias rápidas, seguras y confidenciales.
- Promover que líderes juveniles capacitados difundan el protocolo entre sus pares mediante metodologías participativas en instituciones educativas.
- Incorporar contenidos sobre seguridad digital y uso responsable de internet en asignaturas de educación básica y bachillerato.
- Extender el acceso al curso MOOC a todos los niveles educativos y a familias.
- Ampliar la implementación de la estrategia lúdica a más instituciones educativas a nivel rural y urbano, con un enfoque inclusivo.

ACCIÓN 14	Implementar un sitio web que cuente con herramientas informativas, recursos y medidas que promuevan el desarrollo integral de niñas, niños y adolescentes a través del uso seguro de las tecnologías de la información y la comunicación	

Recomendaciones:

- Mejorar la accesibilidad del portal https://internetsegura.gob.ec/ con funcionalidades inclusivas como navegación adaptada para personas con discapacidades visuales y auditivas.
- Incorporar módulos interactivos y gamificados dirigidos a niñas, niños y adolescentes sobre seguridad digital. Incluir secciones específicas para padres y cuidadores, con herramientas y consejos prácticos para acompañar a las niñas, niños y adolescentes en su uso seguro de las TIC. Generar una biblioteca de recursos descargables con manuales, videos y actividades prácticas sobre riesgos y buenas prácticas digitales.
- Implementar en los Puntos Digitales Gratuitos talleres presenciales y virtuales que aborden temas clave como grooming, ciberacoso, sexting y protección de datos personales.
- Extender la capacitación del programa Americas Girls Can Code a más provincias y fortalecer alianzas con universidades y empresas privadas. Crear versiones del programa enfocadas en niños y adolescentes varones para asegurar un enfoque inclusivo y equitativo.
- Desarrollar campañas de alfabetización digital con materiales didácticos adaptados para diferentes grupos etarios (cómics, videos animados, guías interactivas).
- Implementar jornadas de sensibilización comunitaria en coordinación con escuelas y organizaciones locales.
- Integrar un grupo de niñas, niños y adolescentes que retroalimenten y propongan mejoras a las iniciativas y contenidos del sitio web.
- Implementar concursos, desafíos tecnológicos y proyectos escolares que fomenten el uso seguro y creativo de las tecnologías.

ACCIÓN 15	Promover la participación de niñas, niños y adolescentes en la implementación, seguimiento y evaluación de la política pública uso seguro de internet y asegurar la intergeneracionalidad en las distintas etapas de este.	

Fortalezas:

- Consultas participativas con más de 3.600 NNA a nivel nacional.
- Integración de propuestas concretas en la evaluación de la política pública.

Recomendaciones:

- Mantener espacios periódicos de consulta con NNA para evaluar la implementación de políticas.
- Fortalecer la retroalimentación con resultados concretos para demostrar el impacto de su participación.
- Crear una plataforma virtual interactiva donde los NNA puedan continuar aportando en el seguimiento.

Eje 3: Construcción de estructuras organizacionales de seguimiento y control / Cooperación Internacional

Objetivo 3: Coordinar, dar seguimiento, monitorear y evaluar el cumplimiento de lo estipulado en el Plan de política pública por el uso seguro de internet.
Objetivo 4: Establecer acuerdos, tratados o convenios internacionales multilaterales jurídicamente vinculantes u oficiosos de cooperación técnica y económica en materia de ciberdelincuencia y ciberseguridad enfocados en niñez y adolescencia.

LINEAMIENTO DE LA POLÍTICA PÚBLICA 4	Impulsar la articulación y coordinación institucional para la implementación, seguimiento y evaluación del plan de política pública por el uso seguro de internet para niñas, niños y adolescentes.	
ACCIÓN 16	Articular la mesa técnica interinstitucional para realizar el seguimiento, monitoreo y evaluación del Plan de política pública por el uso seguro de internet para niñas, niños y adolescentes.	

Avances:

- Creación de la mesa técnica interinstitucional liderada por el CNII, con participación de 19 instituciones.
- Integración inicial de acciones en planes operativos institucionales.

Desafíos:

- Falta de continuidad en el seguimiento desde mayo de 2021.
- Escasa articulación entre las instituciones y limitados mecanismos de reporte de avances.

Recomendaciones:

- Reactivar la mesa técnica con un cronograma definido y la participación activa de todas las instituciones.
- Implementar un sistema de monitoreo y reporte periódico para evaluar los resultados y ajustar las estrategias.
- Designar puntos focales institucionales responsables del cumplimiento y seguimiento de los objetivos.

ACCIÓN 17	Informar a las entidades estatales de todos los niveles de gobierno, sociedad civil, organismos territoriales y organismos internacionales los avances del Plan de política pública por el uso seguro de internet impulsada por el Estado.	

Avances:

- Creación de la página web https://internetsegura.gob.ec como plataforma informativa y de seguimiento.
- Participación activa en los Conversatorios de Políticas Públicas a nivel regional.
- Elaboración de propuestas de implementación de la Observación General No. 25.

Recomendaciones:

- Mantener la actualización periódica de la página web con indicadores, estadísticas y resultados de las acciones implementadas.
- Ampliar la difusión de los avances del Plan en foros nacionales e internacionales para fortalecer el posicionamiento del país.
- Publicar informes anuales de avance que incluyan metas cumplidas, desafíos y próximos pasos.

LINEAMIENTO DE LA POLÍTICA PÚBLICA 5	Promover un proceso regional de protección de las niñas, niños y adolescentes frente a los riesgos y delitos cometidos por medios digitales.

ACCIÓN 18	Construir en articulación con instancias regionales, la política pública y el desarrollo de la normativa que promueva los derechos digitales, la ciudadanía digital, las capacidades informacionales, las medidas de protección y reparación, y la tipificación y sanción frente a las transgresiones y delitos cometidos contra de niñas, niños y adolescentes en entornos virtuales.	

Avances:

- Implementación exitosa de la FOFOUSI (Formación de formadores en uso seguro de Internet).
- Participación activa en la construcción del Decálogo para el uso seguro de Internet y la Caja de Herramientas.

Desafíos:

- Necesidad de ampliar la implementación de FOFOUSI a nivel territorial.
- Limitada replicabilidad de buenas prácticas regionales en Ecuador.

Recomendaciones:

- Ampliar la formación FOFOUSI a más territorios y sectores vulnerables, garantizando el acceso en zonas rurales.
- Fortalecer la sostenibilidad de la Red Intergeneracional de Agentes Multiplicadores (RIAMUSI) mediante capacitación continua
- Promover la implementación de la Caja de Herramientas en escuelas y comunidades a través de programas piloto.
- Fortalecer la cooperación técnica con países de la región para intercambiar experiencias y adaptar políticas efectivas.

LINEAMIENTO DE LA POLÍTICA PÚBLICA 6	Fomentar y fortalecer los acuerdos, tratados y convenios internacionales, multilaterales jurídicamente vinculantes u oficiosos de cooperación técnica y económica para atender los casos de ciberdelincuencia y ciberseguridad enfocados en niñez y adolescencia.	
ACCIÓN 19	Gestionar la adhesión del Estado ecuatoriano al "Convenio sobre la ciberdelincuencia" (Convenio de Budapest)	

Fortalezas:

- Aprobación de la adhesión al Convenio por la Asamblea Nacional.
- Ratificación del Convenio por parte del Ejecutivo mediante Decreto 332.

Recomendaciones:

- Capacitar a funcionarios judiciales, fiscales y policiales en el uso del marco legal y herramientas del Convenio.
- Desarrollar un plan de acción interinstitucional para implementar las disposiciones del Convenio de manera efectiva.

ACCIÓN 20	Coordinar acuerdos o tratados internacionales multilaterales jurídicamente vinculantes u oficiosos de cooperación para el intercambio de información, tecnología, conocimiento de expertos y diversos recursos para atender los casos de ciberdelincuencia y ciberseguridad enfocados en niñez y adolescencia.	

Avances:

- Avances en la implementación de la Carta de Principios y Derechos en los Entornos Digitales.
- Firmas de Memorandos de Entendimiento con Chile y Estonia.
- Integración de Ecuador al Foro Global sobre Experiencias Cibernéticas y al Proyecto Glacy-e.

Recomendaciones:

- Fortalecer la implementación de acuerdos a través de mesas de trabajo técnico con organismos internacionales.
- Fomentar la capacitación permanente en ciberseguridad para actores clave como Policía, Fiscalía y operadores de justicia.
- Promover la creación de centros especializados en ciberseguridad con apoyo técnico y financiero de socios internacionales.

ACCIÓN 21	Gestionar la obtención de recursos para financiar políticas, planes, proyectos y líneas de acción que implementen medidas para garantizar los derechos de niñas, niños y adolescentes en relación al acceso, uso e interacción con tecnologías de la información y comunicación.	

Barreras identificadas:

- Falta de mecanismos claros para acceder a financiamiento sostenible.
- Dependencia de cooperación internacional sin estrategias concretas de gestión a largo plazo.
- Escasa visibilidad sobre los avances de la propuesta de la Unión Internacional de Telecomunicaciones (UIT).

Recomendaciones:

- Fortalecer la implementación de acuerdos a través de mesas de trabajo técnico con organismos internacionales.
- Fomentar la capacitación permanente en ciberseguridad para actores clave como Policía, Fiscalía y operadores de justicia.
- Promover la creación de centros especializados en ciberseguridad con apoyo técnico y financiero de socios internacionales.
- Priorizar la elaboración de proyectos con impacto medible y enfocados en zonas rurales y urbano-marginales.

Eje 4: Fortalecimiento de capacidades

Objetivo 5: Promover una cultura preventiva para el uso seguro de internet y tecnologías digitales que oriente a los miembros de la comunidad educativa acerca de los beneficios y riesgos, así como desarrolle competencias y habilidades digitales básicas que contribuyen a su desarrollo humano.

LINEAMIENTO DE LA POLÍTICA PÚBLICA 7	Generar y socializar en la comunidad educativa conocimientos sobre los derechos de los niños niñas y adolescentes, a la autodeterminación informativa, identidad y reputación digital y responsabilidad de uso de redes sociales, como una estrategia para garantizar una Internet sana, segura y constructiva.	
ACCIÓN 22	Desarrollar una campaña de educomunicación a través de Educa Contigo y otros medios de comunicación públicos y privados sobre el uso seguro de la internet.	

Fortalezas:

- Producción de recursos educativos innovadores (juegos interactivos, cómics, videos y guías didácticas) con un alto potencial de impacto en la comunidad educativa.
- Implementación de cursos MOOC con resultados positivos en la capacitación de docentes y estudiantes.
- Ejecución de campañas efectivas como “Cada clic cuenta” y “Escaleras y Resbaladeras”, adaptadas a diferentes grupos etarios.

Recomendaciones:

- Fortalecer la distribución y uso de recursos pedagógicos mediante plataformas educativas y materiales impresos en escuelas rurales.
- Promover la replicación del juego interactivo y de los cursos MOOC en todas las zonas educativas priorizadas.
- Asegurar la actualización constante de contenidos educomunicacionales en temas emergentes como inteligencia artificial, deepfakes y discursos de odio en línea.
- Consolidar alianzas con organismos internacionales y sector privado para garantizar la sostenibilidad de estas acciones y ampliar su impacto.
- Ampliar la cobertura geográfica de las campañas educomunicacionales, con énfasis en comunidades rurales y de difícil acceso.
- Incorporar indicadores de monitoreo y evaluación para medir el impacto de las acciones en los conocimientos y prácticas de uso seguro de internet.
- Diversificar formatos de difusión, desarrollando materiales físicos y radiales para comunidades con limitado acceso digital.
- Fomentar alianzas con medios comunitarios y locales para adaptar los contenidos a las realidades de las distintas regiones.

ACCIÓN 23	Coordinar campañas y procesos de difusión y concientización sobre ciberseguridad y manejo seguro de tecnologías digitales con los actores del sistema educativo, el espacio público y la sociedad en general.	

Recomendaciones:

- Promover la participación de actores clave (familias, docentes y estudiantes) en zonas rurales.
- Fortalecer la coordinación interinstitucional para maximizar los recursos y evitar duplicación de esfuerzos.
- Monitorear el impacto de las campañas mediante encuestas a familias, estudiantes y docentes sobre cambios en conocimientos y prácticas digitales.
- Promover la articulación de actores públicos y privados en mesas técnicas que definan acciones coordinadas de sensibilización.
- Ampliar la frecuencia y continuidad de las campañas, asegurando su sostenibilidad más allá de fechas conmemorativas.
- Incentivar la participación de la sociedad civil y comunidades educativas a través de metodologías participativas como talleres, foros y concursos.

Eje 5: Estrategia comunicacional

Objetivo 6: Desarrollar una estrategia comunicacional para promover los derechos digitales y un uso seguro de la internet por parte de niñas, niños y adolescentes.

LINEAMIENTO DE LA POLÍTICA PÚBLICA 8	Activar las redes sociales institucionales con campañas informativas, posicionamiento y mantenimiento del uso seguro de la Internet para niñas, niños y adolescentes.	
ACCIÓN 24	Difundir temas relativos al uso seguro de internet en los medios de comunicación públicos, privados y digitales. Estandarizar los contenidos para difundirlos en medios de comunicación.	

Recomendaciones:

- Ampliar el alcance de las campañas utilizando radios comunitarias, televisión y recursos físicos para sectores con baja conectividad.
- Establecer indicadores de impacto que permitan evaluar los cambios en percepción y prácticas seguras en internet.
- Continuar con la producción de recursos innovadores como cómics, videos educativos y webinars.

LINEAMIENTO DE LA POLÍTICA PÚBLICA 9	Erradicar los mensajes y contenidos violentos y discriminatorios en contra niñas, niños y adolescentes que se difunden a través de medios virtuales.	
ACCIÓN 25	Coordinar campañas y procesos de difusión y concientización sobre: datos personales, derechos digitales, uso de una internet segura, seguridad en redes dirigidas a los usuarios de los servicios públicos; funcionarios públicos, en especial a Policía Nacional, Fiscalía, Función Judicial, Corte Constitucional; proveedores de servicios de telecomunicaciones; público en general.`	

Fortalezas:

- Ejecución exitosa de campañas anuales por ChildFund International para prevenir riesgos digitales y fomentar el uso seguro y positivo de tecnologías.
- Diversificación de materiales (cómics, guías, videos y webinars) con enfoques específicos para diferentes públicos.
- Participación activa en eventos internacionales como el Día Internacional de la Internet Segura y campañas locales como “Conexiones Digitales” y “Guardianes Digitales”.
- La Fiscalía mantiene una comunicación constante a través de su sala de prensa online y chat con medios de comunicación.

Recomendaciones:

- Fortalecer alianzas interinstitucionales con actores nacionales e internacionales para garantizar la sostenibilidad de las campañas.
- Continuar desarrollando materiales innovadores y adaptados a los nuevos desafíos digitales como inteligencia artificial, deepfakes y sextorsión.
- Asegurar que las campañas se mantengan actualizadas, utilizando tendencias de comunicación digital y redes sociales emergentes como TikTok.
- Promover una evaluación participativa que incorpore las voces de niñas, niños y adolescentes en el diseño de futuras estrategias comunicacionales.

LINEAMIENTO DE LA POLÍTICA PÚBLICA 10	Analizar el impacto de los mensajes difundidos en medios públicos, privados y digitales, además de redes sociales.
ACCIÓN 26	Monitoreo de noticias en medios: prensa, radio, televisión, digitales. Redes sociales (Facebook, Twitter. YouTube).

Barreras identificadas:

- Desactualización de cuentas de redes sociales: Las cuentas en plataformas como Facebook, X y YouTube no reciben actualizaciones constantes.
- Falta de una estrategia coordinada entre instituciones responsables del manejo de redes sociales.
- Limitaciones en la socialización del Plan de Política Pública y la falta de claridad sobre responsables de su ejecución.

Recomendaciones:

- Diseñar e implementar un Plan de Gestión de Redes Sociales con actualizaciones periódicas de contenidos enfocados en la seguridad digital.
- Establecer responsabilidades claras entre las instituciones responsables del manejo de redes y asegurar que las claves de acceso sean controladas.
- Ampliar el monitoreo de mensajes y noticias digitales, usando herramientas de análisis para medir el impacto y alcance de las campañas.
- Realizar capacitaciones interinstitucionales en manejo de redes sociales y comunicación efectiva para temas de protección digital.

Anexos

ANEXO 1: Matriz de semaforización CON EVIDENCIA del cumplimiento de las acciones del Eje 1: Medidas Legales.

Eje 1: Medidas Legales **Objetivo 1: Desarrollar normativa que promueva los derechos digitales y la dignidad e integridad física, psicológica, emocional y sexual de niñas, niños y adolescentes, estableciendo los mecanismos para el aprovechamiento de los beneficios de las Tecnologías de la Información y Comunicación (TIC) y atienda y mitigue los riesgos y delitos que pueden cometerse a través de ellas.**		
LINEAMIENTO DE LA POLÍTICA PÚBLICA 1	Garantizar los derechos digitales, la ciudadanía digital y las capacidades informacionales de niñas, niños y adolescentes para una Internet segura.	
ACCIÓN 1	Proponer en la reforma al Código Orgánico de Niñez y Adolescencia la inclusión de los derechos digitales, la ciudadanía digital, las capacidades informacionales, las medidas de protección y reparación, y la tipificación y sanciones frente a las transgresiones y delitos cometidos contra de niñas, niños y adolescentes en entornos virtuales.	

Inclusión de derechos digitales en el Código Orgánico de Protección Integral a la Niñez y Adolescencia.
En la propuesta de reforma al Código Orgánico de Protección Integral a la Niñez y Adolescencia (COPINNA) se incorporaron los derechos digitales de niñas, niños y adolescentes, incluyendo conceptos como la ciudadanía digital, las capacidades informacionales, las medidas de protección y reparación, así como la tipificación y sanción de delitos cometidos en entornos virtuales contra esta población. Este enfoque responde a la necesidad de actualizar el marco normativo en consonancia con los desafíos del entorno digital y los estándares internacionales, como los establecidos en la Observación General N.º 25 del Comité de Derechos del Niño sobre los derechos de los niños en el entorno digital.

En este proceso, varias organizaciones contribuyeron mediante la provisión de información y la revisión de los contenidos del Libro 1 y el Libro 3 del COPINNA, en mesas técnicas organizadas por la Comisión Especializada Permanente de Protección Integral a Niñas, Niños y Adolescentes y por UNICEF. Como resultado, los derechos digitales fueron transversalizados en toda la legislación y abordados de manera específica en varios artículos, destacando los siguientes aspectos clave:
Derechos digitales incorporados en el COPINNA:

- Derecho a la información: Niñas, niños y adolescentes tienen derecho a buscar, recibir y elegir información adecuada a su edad y desarrollo. Este derecho incluye orientación sobre el uso seguro de Internet y la protección frente a contenido perjudicial, particularmente en plataformas digitales.
- Acceso y protección en el entorno digital: El Estado debe garantizar el acceso seguro a Internet para niñas, niños y adolescentes, desarrollando medidas de seguridad y protocolos específicos tanto en áreas urbanas como rurales. Este derecho abarca el acceso a infraestructura adecuada, información confiable para el desarrollo de capacidades digitales, así como la protección de la privacidad y dignidad en línea. Los niños están protegidos contra diversas formas de violencia digital, incluyendo ciberacoso, sextorsión, explotación sexual, y el acceso a contenido dañino.
- Prevención y protección frente a riesgos y violencia digital: Se incluyen medidas para identificar riesgos y prevenir el acceso a contenidos o comportamientos nocivos en línea. El marco normativo contempla recursos legales y administrativos para denunciar violaciones a los derechos digitales y abordar la violencia digital de manera preventiva y efectiva.
- Educación y participación digital: Padres y cuidadores tienen un rol fundamental en la educación digital y en la protección de los niños en el entorno en línea. Niñas, niños y adolescentes tienen derecho a participar en el diseño e implementación de estrategias para combatir la violencia digital, garantizando un enfoque colaborativo con las familias, las escuelas y las comunidades.
- Derecho a la participación y recreación digital: Los niños tienen derecho a expresar sus opiniones en redes sociales, a ser escuchados y a participar en actividades recreativas en línea, sin discriminación ni vulneración de su seguridad.

Alcances de la reforma
La inclusión de estos derechos digitales en el COPINNA responde a una visión integral y preventiva que busca garantizar el bienestar de niñas, niños y adolescentes en el entorno digital. Este enfoque no solo protege a la población infantil de los riesgos asociados a la tecnología, sino que también promueve el desarrollo de capacidades digitales, fortaleciendo su rol como ciudadanos digitales responsables. Además, las reformas establecen

mecanismos claros para la protección frente a la violencia digital y la reparación en caso de vulneraciones, promoviendo un entorno seguro, inclusivo y respetuoso de sus derechos. En noviembre de 2024 la Comisión Especializada Permanente para la Protección Integral de la Niñez, aprobó el segundo informe del COPINNA y en los siguientes meses se enviará al pleno para su aprobación.
Referencia: ChildFund International. Propuesta para la inclusión de derechos digitales en el Código Orgánico de Protección Integral a la Niñez y Adolescencia.

ACCIÓN 2	Proponer reformas al Código Orgánico Integral Penal sobre delitos informáticos y transgresiones en contra de niñas, niños y adolescentes en entornos virtuales.	

Reformas al Código Orgánico Integral Penal (COIP) sobre delitos informáticos y transgresiones en entornos virtuales contra niñas, niños y adolescentes
El Código Orgánico Integral Penal (COIP) del Ecuador ha incorporado, como resultado de diversas acciones de incidencia, artículos específicos que abordan los delitos informáticos y transgresiones cometidas contra niñas, niños y adolescentes en entornos digitales. Estas reformas buscan fortalecer la protección de esta población frente a los riesgos asociados a la tecnología y los entornos virtuales, estableciendo sanciones severas para quienes vulneren sus derechos. A continuación, se destacan los aspectos más relevantes:

1. Delitos informáticos. El COIP tipifica y sanciona una amplia gama de delitos informáticos, tales como:
   - Acceso no autorizado a sistemas informáticos.
   - Interceptación de datos sin autorización.
   - Alteración de la integridad de datos o programas.
   - Uso indebido de tecnologías de la información.

   En los casos en que estos delitos afecten directa o indirectamente a niñas, niños o adolescentes, las sanciones son más severas, reconociendo su condición de sujetos de especial protección.

2. Delitos sexuales y explotación en línea. El COIP establece disposiciones específicas para combatir los delitos sexuales en entornos digitales, incluyendo:
   - Producción, distribución, posesión y comercialización de material de abuso sexual infantil: Estas conductas están penalizadas con sanciones graves, en concordancia con estándares internacionales.
   - Explotación sexual en línea: Se penaliza cualquier forma de explotación sexual que involucre a niñas, niños y adolescentes mediante el uso de herramientas digitales.

3. Penalización del grooming. El Código prevé sanciones específicas para la captación de niñas, niños y adolescentes a través de medios digitales con fines sexuales, conocida como grooming. Esta conducta incluye la utilización de plataformas en línea para establecer contacto con niñas, niños y adolescentes, con el objetivo de facilitar su abuso o explotación sexual.

4. Protección contra la violencia digital. El COIP también aborda la violencia en línea que afecta la dignidad, integridad física, psicológica y sexual de niñas, niños y adolescentes. Entre las conductas sancionadas se incluyen:
   - Ciberacoso: Persecución persistente o intimidación a través de plataformas digitales.
   - Difusión de contenido perjudicial: Penalización del uso de Internet para compartir material que incite al odio, autolesiones o consumo de sustancias nocivas.

   Estas disposiciones buscan garantizar un entorno digital seguro y proteger a las niñas, niños y adolescentes de diversas formas de violencia y manipulación en línea.

5. Sanciones agravadas. El COIP contempla penas agravadas para delitos informáticos, sexuales o de violencia digital cuando las víctimas son niñas, niños y adolescentes. Esto refuerza su condición de sujetos de especial protección, tal como lo establece la Constitución del Ecuador y tratados internacionales en materia de derechos humanos.

Impacto de las reformas
Estas disposiciones se encuentran vigentes y fortalecen el marco jurídico ecuatoriano para combatir los delitos digitales y proteger a niñas, niños y adolescentes en entornos virtuales. Al reconocer los riesgos emergentes asociados al uso de la tecnología, estas reformas no solo sancionan conductas nocivas, sino que también buscan prevenirlas mediante un enfoque integral de protección, alineado con los estándares internacionales.
Referencia: ChildFund International. Reformas al Código Orgánico Integral Penal sobre delitos informáticos y violencia digital.

ACCIÓN 3	Normar a los proveedores de servicios de telecomunicaciones para que brinden herramientas que permitan un acceso sano, seguro y constructivo para niñas, niños y adolescentes a las tecnologías de la información y la comunicación.	

Regulación a los proveedores de servicios de telecomunicaciones para garantizar un acceso seguro a las tecnologías de la información y comunicación

Con el objetivo de proteger a niñas, niños y adolescentes en el entorno digital, se han establecido normativas y acciones específicas dirigidas a los Proveedores de Servicios de Telecomunicaciones (PST), orientadas a garantizar un acceso sano, seguro y constructivo a las tecnologías de la información y la comunicación (TIC). Estas medidas buscan fomentar un uso responsable de internet y prevenir riesgos asociados al entorno digital. Entre las principales acciones desarrolladas destacan:

1. Expedición de normativa técnica. Mediante la Resolución Nro. ARCOTEL-2018-0176, emitida el 16 de agosto de 2018, se aprobó 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 el artículo 4, numeral 26 de este instrumento, se establecen las obligaciones de los prestadores de servicios para la protección de niñas, niños y adolescentes, incluyendo:
    - Protección infantil: Implementación de herramientas de control parental para resguardar la seguridad de las niñas, niños y adolescentes.
    - Acuerdos con proveedores de contenidos: Garantizar que los contenidos difundidos sean adecuados y seguros para la población infantil.
    - Acceso y seguridad: Promover la seguridad en el acceso a servicios de telecomunicaciones mediante medidas específicas.

2. Socialización de buenas prácticas. En el marco de la campaña "Por un internet seguro para niñas, niños y adolescentes", el 20 de mayo de 2021 se socializó un documento guía y los criterios para el reconocimiento de buenas prácticas entre los PST. Esta campaña fomentó el compromiso de los proveedores con la implementación de herramientas y medidas para proteger a la población infantil en entornos digitales.

3. Taller de capacitación para PST. El 24 de febrero de 2021, en cumplimiento del artículo 4, numeral 26 de la normativa técnica, se llevó a cabo un taller dirigido a prestadores de servicios de acceso a internet, audio y video por suscripción, entre otros. Este evento contó con la participación de 308 representantes de los PST y se enfocó en fortalecer las capacidades para implementar controles de seguridad y medidas de protección para niñas, niños y adolescentes en sus plataformas.

4. Publicación de recomendaciones para control parental. Se elaboró el documento "Recomendaciones para Configuración del Control Parental", disponible en la página web del EcuCERT (www.ecucert.gob.ec). Este documento proporciona orientaciones prácticas para que padres y cuidadores configuren herramientas de control parental, asegurando un uso seguro y adecuado de internet para niñas, niños y adolescentes.

5. Verificación periódica de acciones de los PST. Desde 2021, la Agencia de Regulación y Control de las Telecomunicaciones, a través de sus coordinaciones zonales, realiza controles periódicos para garantizar que los PST cumplan con las disposiciones establecidas. Entre las verificaciones destacan:
    - Difusión de guías para padres y usuarios en sus sitios web o medios de comunicación sobre el uso responsable de internet.
    - Implementación de medidas de control para limitar el acceso a contenidos inapropiados.

Impacto y relevancia

Estas acciones y normativas representan un avance en la regulación del acceso a las TIC. La colaboración entre instituciones como la Agencia de Regulación y Control de las Telecomunicaciones y los PST garantiza que la protección infantil sea un eje transversal en los servicios de telecomunicaciones, promoviendo la corresponsabilidad entre el sector público, privado y las familias.

Referencia: Agencia de Regulación y Control de las Telecomunicaciones. Normativa y acciones para garantizar un internet seguro para niñas, niños y adolescentes en el Ecuador.

ACCIÓN 4	Proponer normativa que regule el funcionamiento de los centros de acceso a la Internet, con enfoque de protección a la niñez y adolescencia	

No se evidencian actividades

ACCIÓN 5	Generar procesos de interoperabilidad de datos entre las instituciones de la Función Judicial para la producción de estadísticas jurimétricas de ingresos de causas de delitos cibernéticos contra niñas, niños y adolescentes generando bases de datos anonimizadas que aporten al portal de estadística judicial en delitos cibernéticos.	

Interoperabilidad de datos y producción de estadísticas jurimétricas para delitos cibernéticos contra niñas, niños y adolescentes

La reforma al Código Orgánico de la Función Judicial de 2020 establece en su artículo 318 la implementación del Modelo de Justicia Abierta, cuyo objetivo es fortalecer la relación entre la ciudadanía y la Función Judicial mediante la transparencia, participación y colaboración. En este marco, el Consejo de la Judicatura, en coordinación con los órganos de la Función Judicial, tiene la responsabilidad de adoptar políticas y programas de gobierno abierto que permitan la publicación de datos, estadísticas y estudios en formatos abiertos, libres de controles y alineados con estándares internacionales. Esto incluye el uso de tecnologías de la información para garantizar un acceso transparente y sistemático a la información judicial.

En este contexto, uno de los objetivos principales ha sido generar procesos de interoperabilidad de datos entre las instituciones de la Función Judicial para la creación de estadísticas jurimétricas sobre ingresos de causas relacionadas con delitos cibernéticos contra niñas, niños y adolescentes. Estas estadísticas se generan a partir de bases de datos anonimizadas y se integran al portal de estadística judicial en delitos cibernéticos, permitiendo un análisis más preciso y accesible para la toma de decisiones y el diseño de políticas públicas.

Avances y acciones realizadas

- Metodología de justicia abierta: La implementación del Modelo de Justicia Abierta se basa en principios rectores de transparencia, participación y colaboración. Este modelo busca construir un Estado Abierto que impulse una justicia eficaz, fomente la paz y fortalezca la democracia. En el ámbito judicial, esto incluye la participación ciudadana en el seguimiento y control de la información, así como la integración de tecnologías para innovar en la presentación de datos.
- Interoperabilidad y anonimización de datos: A través del uso de herramientas tecnológicas avanzadas, se generan bases de datos anonimizadas que alimentan el portal de estadística judicial en delitos cibernéticos. Este proceso garantiza la confidencialidad de las personas involucradas, respetando estándares internacionales de protección de datos.
- Publicación de boletines y estadísticas: En cumplimiento de esta metodología, el Consejo de la Judicatura publica boletines periódicos e infografías accesibles al público sobre temas relevantes, incluyendo información sobre violencia física, psicológica y sexual, así como delitos sexuales contra niñas, niños y adolescentes.

En relación a las causas judiciales que involucran derechos de niñas, niños y adolescentes, el Consejo de la Judicatura lanzó el 07 de junio de 2024 el "Segundo Boletín Estadístico en Materia de Niñez, Adolescencia y Familia" que presenta datos en materia de niñez, adolescencia y familia a partir de la información estadística que provee el Sistema Automático de Trámite Judicial Ecuatoriano (SATJE), con corte 22 de mayo de 2016 a abril 2024 y contiene información de los siguientes temas:

- Por causal y mutuo consentimiento.
- Tutelas Datos de ingresos de causas judiciales.
- Acciones judiciales con mayor incidencia.
- Divorcios, curadurías y régimen de visitas.
- Patria Potestad.
- Adopción y Aptitud Legal para la Adoptabilidad.
- Medidas de Protección.
- Información judicial sobre derecho de alimentos.
- Personas vinculadas al Sistema Único de Pensión Alimenticia (SUPA).
- Medidas de apremio en procesos judiciales de pensión alimenticia.
- Juezas y jueces con competencia en materia de familia, niñez y adolescencia con datos demográficos.

- Disponibilidad de información pública: Los datos recopilados y analizados están disponibles en el micrositio oficial del Consejo de la Judicatura, fomentando un acceso transparente y permitiendo a la ciudadanía y a los investigadores acceder a estadísticas clave. El boletín puede consultarse en el siguiente enlace: https://fsweb.funcionjudicial.gob.ec/www/pdf/BOLETIN%202%20FAMILIA%20NIN%

Impacto y relevancia

La interoperabilidad de datos y la producción de estadísticas jurimétricas representan un avance para comprender y abordar los delitos cibernéticos contra niñas, niños y adolescentes. Estas acciones permiten:

- Monitorear y analizar tendencias en delitos cibernéticos.
- Informar el diseño de políticas públicas basadas en evidencia.
- Promover una justicia más transparente y eficaz, alineada con las necesidades específicas de la niñez y adolescencia.

Al integrar estos procesos en el Modelo de Justicia Abierta, el Consejo de la Judicatura fortalece el sistema de justicia y refuerza la protección de los derechos de niñas, niños y adolescentes frente a los riesgos digitales.

Referencia: Consejo de la Judicatura. Boletines y estadísticas en materia de niñez, adolescencia y familia. Quito, Ecuador, 2024.

ACCIÓN 6	Incidir en la Asamblea Nacional respecto del proyecto de protección de datos personales y la promoción de derechos digitales.	

Incidencia en la Asamblea Nacional para la aprobación de la Ley Orgánica de Protección de Datos Personales y la promoción de derechos digitales

La Ley Orgánica de Protección de Datos Personales, publicada el 26 de mayo de 2021 en el Registro Oficial Suplemento 459, y su reglamento del 13 de noviembre de 2023, marcan un avance significativo en la regulación del tratamiento de datos personales en Ecuador. Este marco legal fue desarrollado con el objetivo de garantizar la protección, el manejo adecuado de los datos personales y la promoción de los derechos digitales de los ciudadanos, alineándose con estándares internacionales, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

Objetivos y alcances de la ley

La ley busca preservar la privacidad, garantizar el consentimiento informado y fortalecer los derechos digitales en el entorno digital, estableciendo principios fundamentales como:

- Derecho al control de datos: Los ciudadanos tienen la potestad de decidir sobre el uso de su información personal. Las empresas y entidades públicas están obligadas a solicitar consentimiento expreso y utilizar los datos únicamente para fines legítimos.
- Supervisión y cumplimiento: Se crea una autoridad reguladora encargada de supervisar el cumplimiento de la ley, promover una cultura de protección de datos y aplicar sanciones a quienes la incumplan.
- Protección específica para niños, niñas y adolescentes: La ley incluye disposiciones para salvaguardar los datos personales de niñas, niños y adolescentes, enfatizando el consentimiento informado por parte de padres o tutores y garantizando su privacidad en plataformas digitales.

Reconocimiento de derechos digitales

El proyecto de ley contempla una amplia gama de derechos digitales, fundamentales para la protección de los datos personales, entre los que destacan:

- Derecho de acceso: Permite a los ciudadanos conocer qué datos están siendo recopilados y cómo se utilizan.
- Derecho de rectificación: Los ciudadanos pueden corregir información inexacta o incompleta.
- Derecho de cancelación: Se asegura la posibilidad de eliminar datos que no sean necesarios para los fines establecidos.
- Derecho de oposición: Garantiza la opción de rechazar el tratamiento de datos en determinadas circunstancias.
- Derecho a la portabilidad: Facilita la transferencia de datos personales entre plataformas o servicios.
- Derecho al olvido: Otorga la posibilidad de solicitar la eliminación de datos en entornos digitales, especialmente cuando su uso ya no sea necesario o haya afectado derechos fundamentales.

Sanciones y disposiciones especiales

La ley establece un marco sancionador que incluye medidas administrativas y penales para entidades que incumplan con el tratamiento seguro y responsable de los datos personales. Estas sanciones buscan garantizar la protección efectiva de la información personal. En particular, se enfatizan medidas de protección para niñas, niños y adolescentes, incluyendo:

- Requisitos estrictos para el consentimiento informado de padres o tutores antes de la recopilación de datos.
- Regulaciones específicas para garantizar el respeto de la privacidad de niñas, niños y adolescentes en plataformas digitales y redes sociales.

Impacto y relevancia

La aprobación de la Ley Orgánica de Protección de Datos Personales y su reglamento permiten contar con un marco jurídico para la promoción de derechos digitales en Ecuador. Este marco normativo refuerza el compromiso del país con la protección de la privacidad, el fortalecimiento del consentimiento informado y el establecimiento de mecanismos de supervisión y sanción.

Referencia: Dirección Nacional de Registros Públicos y ChildFund International. Promoción de derechos digitales y protección de datos personales en Ecuador. Quito, 2023.

ANEXO 2: Matriz de semaforización CON EVIDENCIA del cumplimiento de las acciones del Eje 2: Medidas Técnicas y Procedimentales.

Eje 2: Medidas Técnicas y Procedimentales **Objetivo 2: Promover el acceso, uso e interacción adecuada, responsable, sana, segura y constructiva de las tecnologías de la información y la comunicación que impulse el desarrollo integral y el pleno ejercicio de los derechos de niñas, niños y adolescentes.**		
LINEAMIENTO DE LA POLÍTICA PÚBLICA 2	Promover un acceso sano, seguro y constructivo a las tecnologías de la información y la comunicación para proteger los derechos digitales y la integridad y dignidad de niñas, niños y adolescentes frente a los contenidos nocivos, transgresiones y delitos cometidos a través de medios digitales, con la implementación de políticas públicas, lineamientos técnicos, regulaciones, códigos de conducta, recomendaciones, estándares, metodologías, procedimientos, entre otros	
ACCIÓN 7	Diseñar e implementar el plan de políticas públicas para una internet segura desde las instituciones estatales con el fin de garantizar un acceso y uso sano, seguro y constructivo a las tecnologías de la información y la comunicación por parte de niñas, niños y adolescentes.	

Implementación de la política pública por una Internet Segura para Niñas, Niños y Adolescentes
Proceso de elaboración de la política pública: La formulación de la política para una Internet segura fue liderada por el Consejo Nacional para la Igualdad Intergeneracional, el Ministerio de Telecomunicaciones y la Dirección Nacional de Registro de Datos Públicos, con el apoyo de 16 instituciones públicas y privadas. Este proceso integró aportes de diversos sectores mediante reuniones, talleres y conferencias intergeneracionales.

- Recuperación de experiencias previas como el "Pacto del Gobierno Nacional con la Niñez y Adolescencia por una Internet Segura" (2018) y el marco del Acuerdo Nacional 2030, eje 7 (erradicación de la violencia).
- Construcción de consensos interinstitucionales e intergeneracionales para proteger a la niñez en entornos digitales.
- Estrategias de capacitación y redes: Entre 2019 y 2020, se desarrollaron programas de formación y creación de redes intergeneracionales:
- Curso de Formación de Agentes Multiplicadores en el uso seguro de Internet, con 25 funcionarios públicos capacitados que liderarán la Red Intergeneracional de Agentes Multiplicadores en el uso seguro de Internet (RIAMUSI).
- Colaboración con el Instituto Interamericano del Niño, Niña y Adolescentes (IIN) y países de la región para compartir buenas prácticas.

Difusión y sensibilización: Se implementaron campañas de sensibilización para el uso seguro de Internet:
- Campañas de difusión con hashtag #InternetSeguraEC, difundiendo mensajes sobre riesgos como grooming, ciberacoso y sextorsión.
- Organización de conferencias virtuales con más de 5,000 participantes y un alcance de 125,229 personas a través de redes sociales.
- Desarrollo de contenidos enfocados en la prevención, mitigación de riesgos y protección de derechos digitales.

Coordinación interinstitucional: Un Comité Técnico Interinstitucional compuesto por 19 instituciones y organizaciones de la sociedad civil, como ChildFund International Ecuador y la Asociación Ecuatoriana de Ciberseguridad, impulsó la política. Acciones clave:
- Construcción de la página web www.internetsegura.gob.ec como recurso central para usuarios y autoridades.
- Implementación de alianzas estratégicas nacionales e internacionales para fortalecer capacidades de protección digital.

Desarrollo de capacidades técnicas: Se fortalecieron las capacidades institucionales mediante:
- Elaboración de un repositorio digital.
- Creación de herramientas para identificar y denunciar delitos en línea.
- Colaboración con el sector educativo para integrar una agenda digital.

Participación regional: La política se diseñó con la cooperación de países como México, Panamá y Perú, articulándose a redes internacionales para compartir experiencias y fortalecer enfoques regionales.
Principales logros:
- Creación de un marco regulatorio para el uso seguro de Internet.
- Establecimiento de campañas de sensibilización y herramientas de autoprotección.

- Construcción de redes interinstitucionales e intergeneracionales para proteger a la niñez.

La Política Pública para la Internet Segura para Niñas, Niños y Adolescentes (PPIS-NNA) se estructura en cinco ejes de intervención, diseñados para garantizar la protección integral de los derechos digitales de esta población. Este marco incluye **10 lineamientos de política pública y 26 acciones estratégicas** que buscan abordar los desafíos del entorno digital, promoviendo un uso sano, seguro y constructivo de las tecnologías de la información y comunicación (TIC).

- **Medidas Legales:** Reformar la legislación para garantizar derechos digitales y sancionar delitos virtuales.
- **Medidas Técnicas y Procedimentales:** Crear lineamientos técnicos, normativas y herramientas de regulación.
- **Seguimiento y Control:** Monitoreo y evaluación de la implementación, articulando esfuerzos interinstitucionales.
- **Construcción de Capacidades:** Fortalecer el sistema educativo y las habilidades digitales de niñas, niños y adolescentes.
- **Estrategia Comunicacional:** Difundir mensajes que promuevan un uso seguro de Internet y derechos digitales.

Cada eje responde a un área prioritaria, incluyendo aspectos legales, técnicos, comunicacionales, educativos y de articulación institucional. Se designaron instituciones líderes y co-responsables encargadas de ejecutar y dar seguimiento a las acciones estratégicas, garantizando el cumplimiento de los objetivos. El diseño e implementación de la política se apoya en una propuesta integral de articulaciones interinstitucionales, necesarias para maximizar los resultados de las acciones.

Logros clave

- **Fortalecimiento institucional:** Capacitación y sensibilización de actores clave sobre riesgos digitales y derechos de la niñez.
- **Avances normativos:** Propuestas legislativas para garantizar los derechos digitales en el marco jurídico nacional.
- **Creación de herramientas digitales:** Implementación de plataformas y recursos informativos para promover un acceso seguro y responsable a las TIC.
- **Difusión y sensibilización:** Desarrollo de campañas de comunicación masiva para posicionar el uso seguro de Internet como una prioridad nacional.

La política pública de Internet Seguro en Ecuador es un esfuerzo interinstitucional e intergeneracional que busca garantizar un entorno digital seguro para niñas, niños y adolescentes. Este marco aborda la prevención de riesgos digitales, la promoción de derechos digitales y la creación de un entorno propicio para el aprendizaje, el desarrollo y la protección integral. Aunque el seguimiento directo del CNII culminó en 2021, el marco estratégico establecido permite a las instituciones continuar implementando acciones alineadas con los objetivos de la PPIS-NNA. Esto asegura la sostenibilidad de las medidas y refuerza la corresponsabilidad interinstitucional e intergeneracional para proteger a niñas, niños y adolescentes en el entorno digital.

Fuente: Consejo Nacional para la Igualdad Intergeneracional.

ACCIÓN 8	Implementar normativas y políticas públicas desde los gobiernos autónomos descentralizados para, en el marco de las autorizaciones a comercios o locales que faciliten el acceso a las tecnologías de la información y comunicación, conforme sus competencias constitucionales y legales, garantizar un acceso y uso sano, seguro y constructivo a las tecnologías de la información y la comunicación, por parte de niños, niñas y adolescentes.	

Ordenanza Municipal 01-CMSMB-2020 de San Miguel de los Bancos sobre la Regulación de Cabinas Públicas de Internet y Salas de Videojuegos

La Ordenanza Municipal 01-CMSMB-2020 del Cantón San Miguel de los Bancos regula el funcionamiento de las cabinas públicas de internet y salas de videojuegos, fue publicada en el Registro Oficial el 23 de septiembre de 2020 y tiene como objetivo proteger a los niños, niñas y adolescentes de la información, los productos nocivos y los riesgos en línea. Se aplica en todos los establecimientos que ofrecen el servicio de internet y en espacios municipales. La normativa se fundamenta en la Convención sobre los Derechos del Niño, la Constitución ecuatoriana, y otras legislaciones nacionales e internacionales.

Regulaciones principales

- **Capacitación obligatoria:** Propietarios y administradores deben recibir formación sobre prevención de violencia digital y protocolos de respuesta.
- **Espacios visibles:** Las instalaciones deben asignar un mínimo del 50% de cabinas exclusivas para NNA, ubicadas en zonas visibles.
- **Mecanismos de seguridad:** Es obligatorio implementar software de bloqueo y registro de acceso para proteger a las niñas, niños y adolescentes.
- **Horario restringido:** El uso de las cabinas está limitado hasta las 20h00 para niños y 21h00 para adolescentes.

- **Control municipal:** Inspecciones periódicas serán realizadas por autoridades locales, incluyendo la DINAPEN y el Consejo Cantonal de Protección de Derechos (CCPD).XX

Infracciones y Sanciones: El incumplimiento de las disposiciones será sancionado con multas progresivas, clausuras temporales y, en casos graves, definitivas. Las sanciones buscan fomentar el cumplimiento de medidas de protección.

Medidas Complementarias

- **Sello de Garantía:** Los establecimientos que cumplan con la normativa recibirán un reconocimiento anual.
- **Difusión y Educación:** Se promoverán campañas de concienciación y capacitación sobre el uso responsable de Internet.
- **Rutas de Denuncia:** Los establecimientos deben exhibir información visible sobre cómo reportar casos de ciberacoso o conductas sospechosas.

Impacto Esperado: La Ordenanza busca fomentar una cultura de protección digital en el cantón, involucrando a las familias, las escuelas y los administradores de cibercafés como actores clave en la prevención de riesgos en línea y la promoción del bienestar integral de los NNA.
Fuente: ChildFund International, Gobierno Autónomo Descentralizado del Cantón San Miguel de los Bancos.

ACCIÓN 9	Desarrollar e implementar mecanismos, lineamientos y medidas técnicas para la regulación y control del acceso a contenidos nocivos, transgresiones y posibles delitos en los servicios del régimen general de telecomunicaciones (TIC) y las empresas proveedoras de internet y mecanismos de prevención, protección, restitución y reparación de derechos para niñas, niños y adolescentes.	

No se cuenta con información de avances en esta acción.

ACCIÓN 10	Establecer el funcionamiento de una línea de denuncia de contenidos ilegales y atentatorios a los derechos de los niños, niñas y adolescentes, tales como la pornografía infantil en internet, entre otras, bloquear esos contenidos; rastrearlos al país de origen e impulsar todas las acciones pertinentes para sancionar a los responsables.	

Implementación de un canal de denuncia en línea:
La Fiscalía General del Estado (FGE) implementó un canal de denuncia en línea, según la Resolución No. 028-FGE-2020, el 18 de abril de 2020. Este canal facilita el registro de posibles hechos de violencia de género e intrafamiliar, y permite denunciar delitos relacionados con la explotación infantil en medios digitales. Entre estos delitos destacan:

- Contacto con menores con fines sexuales por medios electrónicos.
- Pornografía infantil, incluyendo su distribución y comercialización.
- Oferta de servicios sexuales con menores de 18 años a través de plataformas electrónicas.
- Corrupción de niñas, niños y adolescentes.
- El formulario de denuncia está disponible en la plataforma oficial de la Fiscalía en el enlace fiscalia.gob.ec/denuncia-en-linea-de-violencia-basada-en-genero/.

Creación de la Unidad Nacional Especializada en Investigación de Ciberdelito:
Mediante Resolución No. 34-FGE-2022, la Fiscalía General del Estado estableció esta unidad para coordinar, orientar y manejar investigaciones de ciberdelitos, con especial atención en:

- Seguridad de los sistemas de información y comunicación.
- Pornografía infantil y su comercialización en línea.

Esta unidad garantiza una gestión integral en la investigación de delitos cibernéticos, colaborando con organismos internacionales para rastrear contenidos ilegales hasta sus países de origen, bloquearlos, y sancionar a los responsables.
Impacto: Estas acciones refuerzan el compromiso del Estado ecuatoriano con la protección de los derechos digitales de la niñez y adolescencia. Al garantizar canales efectivos para la denuncia y el manejo especializado de estos casos, se contribuye a la prevención de delitos y a la protección integral de las niñas, niños y adolescentes en entornos digitales.
Fuente: Fiscalía General del Estado.

ACCIÓN 11	Diagnosticar y evaluar la factibilidad de una línea de denuncia de contenidos ilegales y atentatorios a los derechos de los niños, niñas y adolescentes, tales como la pornografía infantil en internet, entre otras, bloquear esos contenidos; rastrearlos al país de origen e impulsar todas las acciones pertinentes para sancionar a los responsables.	

Evaluación y consultas realizadas
El establecimiento y funcionamiento de una línea de denuncia para contenidos ilegales y atentatorios a los derechos de niñas, niños y adolescentes, como la pornografía infantil en internet, requiere un diagnóstico profundo y una evaluación integral de su factibilidad. Esta medida busca no solo bloquear y eliminar los contenidos ilícitos, sino también rastrear su origen y promover acciones legales efectivas contra los responsables.

Se realizaron consultas con organismos especializados en la protección de derechos y la persecución de delitos cibernéticos, como la Fiscalía General del Estado y la Policía de Delitos Cibernéticos. Dichas instituciones destacaron limitaciones normativas y operativas que actualmente dificultan la implementación de una línea específica de denuncia de este tipo. Entre las barreras identificadas se encuentran:

- La ausencia de disposiciones legales específicas que habiliten un canal de denuncia exclusivo para contenidos ilícitos relacionados con niñas, niños y adolescentes.
- La falta de infraestructura tecnológica adecuada para rastrear y bloquear contenidos de manera eficiente, especialmente aquellos alojados en servidores internacionales.
- La necesidad de personal capacitado en el manejo de denuncias sensibles, con énfasis en la protección de los denunciantes y el debido seguimiento de los casos.

Fuente: ChildFund International

ACCIÓN 12	Elaborar directrices contra la violencia digital con base en los protocolos generados por el Sistema Nacional de Prevención y Erradicación de la Violencia de Género, así como del ente encargado de la política pública de protección y en consecuencia generar rutas para la denuncia, atención, y protección de niñas, niños y adolescentes contra las transgresiones y delitos realizados mediante medios virtuales.	

Dirección de Protección y Asistencia a Víctimas, Testigos y Otros (SPAVT)
La **Dirección de SPAVT**, está desarrollando el "Protocolo de atención a niños, niñas y adolescentes del sistema nacional de protección y asistencia a víctimas, testigos y otros participantes en el proceso penal -SPAVT", que tiene como objetivo estandarizar el procedimiento de atención a los niños, niñas y adolescentes respecto de los servicios del SPAVT. El documento en mención cuenta con un apartado específico sobre: **"Recomendaciones generales en asistencia y protección en casos de delitos sexuales, trata de personas, pornografía y grooming".** Esta herramienta fortalecerá el abordaje e intervención de los equipos técnicos del SPAVT de Fiscalía General del Estado.

Dirección de Control Jurídico y Evaluación Fiscal

1. Directriz 001-FGE-DCJEAF-2020, de 25 de mayo de 2020 , respecto al procedimiento administrativo para solicitar medidas de protección para víctimas de violencia de género e intrafamiliar con firma electrónica.
2. Directriz 001-FGE-DCJEAF-2021, 06 de mayo de 2021, respecto a el "Procedimiento Unificado especial y expedito de delitos de violencia contra la mujer o miembros del núcleo familiar en las Unidades Especializadas de Flagrancia-Violencia de Género.
3. Directriz 001-FGE-DCJEAF-2023, de 13 de mayo de 2023, respecto al "Ocultamiento de expedientes físicos y digitales de noticias del delito a cargo de las Fiscalías Especializadas de Justicia Juvenil.
4. Disposición a los Fiscales Provinciales, el cumplimiento inmediato y obligatorio de ingreso al Sistema de Protección a Víctimas y Testigos SPAVT de Niñas, Niños y Adolescentes en delitos contra la integridad sexual. (Memorando FGE-CGAJP-DCJEAF-2023-00033-M, de 05 de enero de 2023).
5. Disposición a los Fiscales Provinciales socialicen a los Agentes Fiscales la obligación de receptar las denuncias presentadas por las mujeres, niñas, adolescentes y personas gestantes víctimas de violación, en caso de que hayan decidido interrumpir voluntariamente su embarazo, para su inmediato y obligatorio cumplimiento. (Memorando FGE-CGAJP-DCJEAF-2023-00312-M, de 08 de febrero de 2023).
6. Disposición a los Fiscales Provinciales que toda muerte violenta de una mujer, adolescente o niña, debe registrarse en el Sistema Integrado de Actuaciones Fiscales SIAF, como delito de femicidio, conforme lo establece el Protocolo Nacional para investigar Femicidios y otras Muertes violentas de Mujeres y Niñas. (Memorando FGE-CGAJP-DCJEAF-2023-00651-M, de 15 de marzo de 2023).
7. Disposición a los Fiscales Provinciales, realizar el seguimiento del registro oportuno de partes policiales en el Sistema Integrado de Actuaciones Fiscales SIAF, como noticias del delito o actos administrativos, para que la institución cuente con estadística reales respecto a los casos de femicidios en el país (Memorando

FGE-CGAJP-DCJEAF-2023-00850-M, de 06 de abril de 2023).
8. Participación en la elaboración del "Instructivo del Subproceso Atención Especializada a Niñas, Niños y Adolescentes Víctimas de delitos relativos a su integridad sexual", aprobado el 17 de noviembre de 2023.

Fuente: Fiscalía General del Estado.

LINEAMIENTO DE LA POLÍTICA PÚBLICA 3	Aumentar las capacidades de las instituciones públicas, privadas y comunitarias para la prevención, atención y protección de las niñas, niños y adolescentes frente a los contenidos nocivos, vulneraciones y los delitos perpetrados mediante medios virtuales.	
ACCIÓN 13	Elaborar protocolos contra la violencia digital y rutas para la denuncia, atención y protección de niñas, niños y adolescentes contra las transgresiones y delitos realizados mediante medios virtuales	

El Consejo de la Judicatura, cuenta con mecanismos de seguimiento, participación y control social. Además ha creado canales de alerta y queja sobre la atención en flagrancia en materia de violencia, por medio de una línea permanente de mensajería instantánea, correo electrónico y formulario virtual.

- Mensajería instantánea a través de la línea telefónica N.º 0962128555
- Correo electrónico: quejas.violencia@funcionjudicial.gob.ec
- Formulario de quejas F06 publicada en la página web:
- https://www.funcionjudicial.gob.ec/

Fuente: Consejo de la Judicatura.

El Ministerio de Educación del Ecuador elaboró el Protocolo y Ruta de Actuación y Prevención de los riesgos y vulneraciones a los derechos de niñas, niños y adolescentes por medios virtuales detectados o cometidos en el Sistema Nacional de Educación alineados a los protocolos vigentes, la Ley Orgánica de Interculturalidad Educación (LOEI) y normativa legal vigente.
El “Protocolo de actuación frente a situaciones de violencia digital detectadas en el Sistema Nacional de Educación”, se construye en cumplimiento de la misión y visión del Ministerio de Educación de garantizar una educación integral, inclusiva y de calidad, en entornos libres de violencia; así como en respuesta a la Sentencia No. 456-20-JP/21 de la Corte Constitucional. https://www.corteconstitucional.gob.ec/sentencia-456-20-jp-21/
Este protocolo brinda lineamientos y acciones que deben ser implementadas por las autoridades de la institución educativa, por el equipo de profesionales del Departamento de Consejería Estudiantil (DECE) y por docentes, así como por el personal administrativo y de servicio.
La elaboración de este instrumento se realizó desde un enfoque intergeneracional que incluyó la participación de niñas, niños y adolescentes estudiantes del sistema educativo e integrantes de la Red de Organizaciones por la Defensa de los Derechos de la Niñez y Adolescencia (RODDNA) del Movimiento Por Ser Niña y participantes de los programas de ChildFund International y sus socios locales; docentes, profesionales DECE, funcionarios públicos de la Defensoría del Pueblo, del Consejo Nacional para la Igualdad Intergeneracional y del Instituto Interamericano del Niño, la Niña y Adolescentes (IIN). También se consultó una extensa bibliografía nacional e internacional.
Este documento forma parte de los “Protocolos y rutas de actuación frente a situaciones de violencia detectadas o cometidas en el sistema educativo” e incorpora el enfoque restaurativo en la promoción, protección y reparación en casos de riesgos o vulneraciones de derechos de niños, niñas y adolescentes en entornos digitales.
https://educacion.gob.ec/wp-content/uploads/downloads/2023/09/protocolo_frente_a_violencia_digital.pdf
El Protocolo fue aprobado mediante Acuerdo Ministerial MINEDUC-MINEDUC-2023-00054-A, publicado el 11 de septiembre de 2023
https://educacion.gob.ec/wp-content/uploads/downloads/2023/09/MINEDUC-MINEDUC-2023-00054-A.pdf y socializado mediante Circular Nro. MINEDUC-SIEBV-2023-00016-C, de 15 de septiembre de 2023 a las 9 Coordinaciones Zonales de Educación para su difusión a las Direcciones Distritales de Educación y a las 16.140 instituciones educativas del Sistema Nacional de Educación
El Protocolo de actuación frente a situaciones de violencia digital detectadas en el Sistema Nacional de Educación” es de aplicación obligatoria en todas las instituciones educativas de los sostenimientos fiscal, municipal, fiscomisional y particular, para todos los niveles de Inicial, Básica y Bachillerato (técnico, técnico profesional y complementario en artes) del Sistema Nacional de Educación; y, en todos los programas de educación especializada e inclusiva, para las modalidades presencial, a distancia, semipresencial y escolaridad inconclusa.
También se elaboró la propuesta de socialización de estos instrumentos en el Sistema Educativo. La Estrategia de prevención del uso seguro e identificación de riesgos en la Internet se enfoca en tres ejes para prevenir y educar sobre el uso seguro de la Internet:

1) Informar a docentes, estudiantes, padres y madres, consejeros estudiantiles y personal administrativo de las unidades educativas. El protocolo se difundirá de manera digital y mediante videos explicativos. Se cuentan con las siguientes herramientas:

- Manual de uso de imagen de la estrategia. 72 piezas comunicacionales para redes sociales, con malla de contenidos para 6 meses.
- Cómic del protocolo para niños y niñas de entre 7 y 11 años de edad.
- Cómic del protocolo para adolescentes a partir de los 12 años de edad.
- Video animado del protocolo y de la sentencia 456 JP (caso sexting).

2) Educar a docentes y estudiantes en ciudadanía digital a través de cursos virtuales;
   - Curso MOOC para personal educativo en la plataforma Me Capacito, con una duración de 40 horas. Se incluye una caja de herramientas con recursos educativos digitales y recursos de aprendizaje.
   - Curso MOOC para estudiantes a partir de 12 años, con una duración de 10 horas. Este curso estará disponible en la página de Recursos Educativos.
3) Sensibilizar a la comunidad educativa a través de la metodología y el juego Escaleras y Resbaladeras en instituciones educativas y la utilización de herramientas virtuales.
   - **Primera fase:** Activación (piloto) implementación de la metodología entre pares “Escaleras y resbaladeras” para la prevención de la violencia digital” en Quito y Guayaquil (junio- julio 2024).
   - **Segunda fase:** implementación de la metodología en instituciones educativas de las 9 zonas:
     - Socios locales de ChildFund International en: Carchi, Imbabura, Pichincha, Cotopaxi, Tungurahua (junio - octubre 2024).
     - **3480** Unidades Educativas con un alcance potencial de **1.200.000** estudiantes (2024)

Fuente: Ministerio de Educación del Ecuador.

LINEAMIENTO DE LA POLÍTICA PÚBLICA 3	Aumentar las capacidades de las instituciones públicas, privadas y comunitarias para la prevención, atención y protección de las niñas, niños y adolescentes frente a los contenidos nocivos, vulneraciones y los delitos perpetrados mediante medios virtuales.	
ACCIÓN 14	Elaborar protocolos contra la violencia digital y rutas para la denuncia, atención y protección de niñas, niños y adolescentes contra las transgresiones y delitos realizados mediante medios virtuales	

El Consejo de la Judicatura, cuenta con mecanismos de seguimiento, participación y control social. Además ha creado canales de alerta y queja sobre la atención en flagrancia en materia de violencia, por medio de una línea permanente de mensajería instantánea, correo electrónico y formulario virtual.

- Mensajería instantánea a través de la línea telefónica N.º 0962128555
- Correo electrónico: quejas.violencia@funcionjudicial.gob.ec
- Formulario de quejas F06 publicada en la página web:
- https://www.funcionjudicial.gob.ec/

Fuente: Consejo de la Judicatura.

El Ministerio de Educación del Ecuador elaboró el Protocolo y Ruta de Actuación y Prevención de los riesgos y vulneraciones a los derechos de niñas, niños y adolescentes por medios virtuales detectados o cometidos en el Sistema Nacional de Educación alineados a los protocolos vigentes, la Ley Orgánica de Interculturalidad Educación (LOEI) y normativa legal vigente.
El “Protocolo de actuación frente a situaciones de violencia digital detectadas en el Sistema Nacional de Educación”, se construye en cumplimiento de la misión y visión del Ministerio de Educación de garantizar una educación integral, inclusiva y de calidad, en entornos libres de violencia; así como en respuesta a la Sentencia No. 456-20-JP/21 de la Corte Constitucional. https://www.corteconstitucional.gob.ec/sentencia-456-20-jp-21/
Este protocolo brinda lineamientos y acciones que deben ser implementadas por las autoridades de la institución educativa, por el equipo de profesionales del Departamento de Consejería Estudiantil (DECE) y por docentes, así como por el personal administrativo y de servicio.
La elaboración de este instrumento se realizó desde un enfoque intergeneracional que incluyó la participación de niñas, niños y adolescentes estudiantes del sistema educativo e integrantes de la Red de Organizaciones por la Defensa de los Derechos de la Niñez y Adolescencia (RODDNA) del Movimiento Por Ser Niña y participantes de los programas de ChildFund International y sus socios locales; docentes, profesionales DECE, funcionarios públicos de la Defensoría del Pueblo, del Consejo Nacional para la Igualdad Intergeneracional y del Instituto Interamericano del Niño, la Niña y Adolescentes (IIN). También se consultó una extensa bibliografía nacional e internacional.
Este documento forma parte de los “Protocolos y rutas de actuación frente a situaciones de violencia detectadas o cometidas en el sistema educativo” e incorpora el enfoque restaurativo en la promoción, protección y reparación en casos de riesgos o vulneraciones de derechos de niños, niñas y adolescentes en entornos digitales.
https://educacion.gob.ec/wp-content/uploads/downloads/2023/09/protocolo_frente_a_violencia_digital.pdf
El Protocolo fue aprobado mediante Acuerdo Ministerial MINEDUC-MINEDUC-2023-00054-A, publicado el 11 de septiembre de 2023 https://educacion.gob.ec/wp-content/uploads/downloads/2023/09/MINEDUC-MINEDUC-2023-00054-A.pdf y socializado mediante Circular Nro. MINEDUC-SIEBV-2023-00016-C, de 15 de septiembre de 2023 a las 9

Coordinaciones Zonales de Educación para su difusión a las Direcciones Distritales de Educación y a las 16.140 instituciones educativas del Sistema Nacional de Educación
El Protocolo de actuación frente a situaciones de violencia digital detectadas en el Sistema Nacional de Educación" es de aplicación obligatoria en todas las instituciones educativas de los sostenimientos fiscal, municipal, fiscomisional y particular, para todos los niveles de Inicial, Básica y Bachillerato (técnico, técnico profesional y complementario en artes) del Sistema Nacional de Educación; y, en todos los programas de educación especializada e inclusiva, para las modalidades presencial, a distancia, semipresencial y escolaridad inconclusa.
También se elaboró la propuesta de socialización de estos instrumentos en el Sistema Educativo. La Estrategia de prevención del uso seguro e identificación de riesgos en la Internet se enfoca en tres ejes para prevenir y educar sobre el uso seguro de la Internet:

1) Informar a docentes, estudiantes, padres y madres, consejeros estudiantiles y personal administrativo de las unidades educativas. El protocolo se difundirá de manera digital y mediante videos explicativos. Se cuentan con las siguientes herramientas:
   - Manual de uso de imagen de la estrategia. 72 piezas comunicacionales para redes sociales, con malla de contenidos para 6 meses.
   - Cómic del protocolo para niños y niñas de entre 7 y 11 años de edad.
   - Cómic del protocolo para adolescentes a partir de los 12 años de edad.
   - Video animado del protocolo y de la sentencia 456 JP (caso sexting).
2) Educar a docentes y estudiantes en ciudadanía digital a través de cursos virtuales;
   - Curso MOOC para personal educativo en la plataforma Me Capacito, con una duración de 40 horas. Se incluye una caja de herramientas con recursos educativos digitales y recursos de aprendizaje.
   - Curso MOOC para estudiantes a partir de 12 años, con una duración de 10 horas. Este curso estará disponible en la página de Recursos Educativos.
3) Sensibilizar a la comunidad educativa a través de la metodología y el juego Escaleras y Resbaladeras en instituciones educativas y la utilización de herramientas virtuales.
   - **Primera fase:** Activación (piloto) implementación de la metodología entre pares "Escaleras y resbaladeras" para la prevención de la violencia digital" en Quito y Guayaquil (junio- julio 2024).
   - **Segunda fase:** implementación de la metodología en instituciones educativas de las 9 zonas:
     - Socios locales de ChildFund International en: Carchi, Imbabura, Pichincha, Cotopaxi, Tungurahua (junio - octubre 2024).
     - **3480** Unidades Educativas con un alcance potencial de **1.200.000** estudiantes (2024)

Fuente: Ministerio de Educación del Ecuador.

ACCIÓN 15	Promover la participación de niñas, niños y adolescentes en la implementación, seguimiento y evaluación de la política pública uso seguro de internet y asegurar la intergeneracionalidad en las distintas etapas de este.	

Consultas informadas a las Niñas, Niños y Adolescentes

El Consejo Nacional para la Igualdad Intergeneracional (CNII), en colaboración con organizaciones como ChildFund International, realizó dos procesos de consulta informada con los Consejos Consultivos de niñas, niños y adolescentes y niñas, niños y adolescentes no organizados. Estas consultas tuvieron como objetivo garantizar la participación efectiva de los actores directamente afectados en el diseño, implementación y evaluación de políticas públicas.

La consulta informada para evaluar la política público abordó la necesidad de protección y seguridad en el entorno digital, un espacio donde las niñas, niños y adolescentes son particularmente vulnerables. Problemas como explotación sexual en línea, ciberacoso, contenidos inapropiados y riesgos tecnológicos se analizaron con las contribuciones directas de los NNA. En la consulta participaron: 3,673 niñas, niños y adolescentes provenientes de las 23 provincias del Ecuador continental, con edades comprendidas entre los 9 y 18 años.

Se aplicaron técnicas participativas y adaptadas a la edad, garantizando un ambiente seguro y apropiado para expresar opiniones. Se facilitó el acceso a información clara y comprensible, promoviendo una participación informada y genuina. Las aportaciones de los NNA se integraron en la evaluación de la política.

Las NNA señalaron las áreas críticas relacionadas con el uso seguro de Internet, tales como: Educación sobre seguridad en línea; Prevención del acoso cibernético; Protección contra riesgos digitales como grooming, sexting y difusión no consentida de información personal; Fortalecimiento de mecanismos de protección. Las propuestas de los NNA contribuyeron a la identificación de medidas efectivas para garantizar un entorno digital seguro.

El Consejo Nacional para la Igualdad Intergeneracional, ha sentado un precedente en la formulación de políticas públicas inclusivas, participativas y centradas en la protección de niñas, niños y adolescentes en entornos

digitales. La participación activa de los NNA fortalece el enfoque de derechos y asegura que sus voces sean escuchadas y respetadas.

Fuente: Consejo Nacional para la Igualdad Intergeneracional y ChildFund International.

ANEXO 3: Matriz de semaforización CON EVIDENCIA del cumplimiento de las acciones del Eje 3: Construcción de estructuras organizacionales de seguimiento y control / Cooperación Internacional.

Eje 3: Construcción de estructuras organizacionales de seguimiento y control / Cooperación Internacional **Objetivo 3: Coordinar, dar seguimiento, monitorear y evaluar el cumplimiento de lo estipulado en el Plan de política pública por el uso seguro de internet.** **Objetivo 4: Establecer acuerdos, tratados o convenios internacionales multilaterales jurídicamente vinculantes u oficiosos de cooperación técnica y económica en materia de ciberdelincuencia y ciberseguridad enfocados en niñez y adolescencia.**		
LINEAMIENTO DE LA POLÍTICA PÚBLICA 4	Impulsar la articulación y coordinación institucional para la implementación, seguimiento y evaluación del plan de política pública por el uso seguro de internet para niñas, niños y adolescentes.	
ACCIÓN 16	Articular la mesa técnica interinstitucional para realizar el seguimiento, monitoreo y evaluación del Plan de política pública por el uso seguro de internet para niñas, niños y adolescentes.	

Mecanismo de articulación: Mesa Técnica.
El Consejo Nacional para la Igualdad Intergeneracional (CNII) lideró la conformación de una mesa técnica interinstitucional, que funcionó como el principal espacio de coordinación, seguimiento y evaluación de la política. Este mecanismo permitió el desarrollo de estrategias conjuntas entre instituciones públicas, privadas y de la sociedad civil, promoviendo un enfoque participativo e intergeneracional.
Hasta **mayo de 2021**, el CNII supervisó directamente el cumplimiento de la política pública, asegurando el desarrollo inicial de las acciones estratégicas y el fortalecimiento de las capacidades institucionales. Posteriormente, las instituciones involucradas asumieron la continuidad de las acciones en el marco de sus competencias, integrándolas en sus planes operativos y presupuestarios.
Fuente: Consejo Nacional para la Igualdad Intergeneracional.

ACCIÓN 17	Informar a las entidades estatales de todos los niveles de gobierno, sociedad civil, organismos territoriales y organismos internacionales los avances del Plan de política pública por el uso seguro de internet impulsada por el Estado.	

Ministerio de Inclusión Económica y Social. En abril del año 2020, se elaboró la Propuesta para la Implementación de la Observación General No 25 del Comité de Los Derechos del Niño Sobre los Derechos de los Niños en el Entorno Digital, en Los Servicios de Acogimiento Institucional y Modalidades Alternativas de Cuidado.
Fuente: Ministerio de Inclusión Económica y Social
La Dirección Nacional de Registros Públicos, ha implementado la página web: https://internetsegura.gob.ec/, mediante la cual se informa de avances, indicadores y estadística, sobre temas relacionados a la implementación de la política de internet segura.
Fuente: Dirección Nacional de Registros Públicos
En los Conversatorios de Políticas Públicas para el Uso Seguro de la Internet (CPP) organizados por el Instituto Interamericano del Niño, Niña y Adolescentes, se presentaron los avances de la Política Pública por una Internet Segura para niñas, niños y adolescentes durante los años 2020 y 2021. En los CPP participan varios países de la región.
Fuente: ChildFund International

LINEAMIENTO DE LA POLÍTICA PÚBLICA 5	Promover un proceso regional de protección de las niñas, niños y adolescentes frente a los riesgos y delitos cometidos por medios digitales.	
ACCIÓN 18	Construir en articulación con instancias regionales, la política pública y el desarrollo de la normativa que promueva los derechos digitales, la ciudadanía digital, las capacidades informacionales, las medidas de protección y reparación, y la tipificación y sanción frente a las transgresiones y delitos cometidos contra de niñas, niños y adolescentes en entornos virtuales.	

Implementación de la Formación de formadores en uso seguro de Internet.
El Instituto Interamericano del Niño, la Niña y Adolescentes de la OEA en conjunto con el Consejo Nacional para la Igualdad Intergeneracional de Ecuador, el Ministerio de Educación de Ecuador y ChildFund International, realizó dos proceso de formación de formadores de Uso Seguro de Internet (FOFOUSI)
La Formación de formadores en uso seguro de Internet, llamada también FOFOUSI, está diseñada para aquellos funcionarios que ocupan cargos que deben/pueden tomar decisiones operativas-técnicas, capacitándoles para generar proyectos y enseñar a otros sobre prácticas de seguridad en línea. La edición FOFOUSI Ecuador 2024 se centró específicamente en que los funcionarios egresados tengan las herramientas suficientes para saber cómo instalar una Red Intergeneracional de Agentes Multiplicadores en Uso Seguro de Internet (RIAMUSI) en territorio. FOFOUSI es una propuesta amigable, actualizada y específica, dirigida a capacitar, desarrollar habilidades, contenidos y herramientas, a funcionarios/as y técnicos/as del Ministerio de Educación e instituciones nacionales afines.

La formación de los participantes de la FOFOUSI se realizó a través de la plataforma Moodle del IIN-OEA con la dirección de los técnicos/as del IIN, MINEDUC, CNII y ChildFund International. La acreditación fue otorgada por el IIN-OEA, el Consejo Nacional para la Igualdad Intergeneracional, Ministerio de Educación y ChildFund International, considerando su rol como: Formadores/as en el uso seguro de Internet. La metodología de la FOFOUSI consta de un curso online a través de la plataforma Moodle y un taller presencial de cierre.

La capacitación online de los participantes de la FOFOUSI utilizó la plataforma Moodle del IIN-OEA. La formación se dividió en 11 módulos, cada uno con la duración de 8 días calendario que tuvo una evaluación y que constó de una actividad asincrónica (foro, cuestionario, etcétera).

Una vez finalizada la FOFOUSI, los funcionarios/as, técnicos/as que participaron, están acompañando la implementación de la RIAMUSI en el año 2025.
Fuente: Ministerio de Educación y Ministerio de Relaciones Exteriores y Movilidad Humana.

Decálogo para el uso responsable y seguro de Internet y la Caja de Herramientas
El Consejo Naci onal para la Igualdad Intergeneracional y ChildFund International participaron durante el año 2023 y 2024 en la construcción del Decálogo para el uso responsable y seguro de Internet y la Caja de Herramientas, proceso liderado por el Instituto Interamericano del Niño, Niña y Adolescentes. El Ecuador representado por el CNII también ha participado en los Conversatorios de Política Pública para el Uso Seguro de la Internet.

- **El Decálogo para el uso responsable y seguro de Internet** es un documento que sintetiza los principios y recomendaciones esenciales para fomentar prácticas seguras y responsables en el entorno digital, especialmente dirigidas a niñas, niños, adolescentes, familias y actores educativos.
- **La Caja de Herramientas,** un recurso integral compuesto por materiales pedagógicos, guías y actividades que permiten a las instituciones educativas y comunidades promover el uso seguro y positivo de las tecnologías digitales. Este proceso ha sido liderado por el **Instituto Interamericano del Niño, la Niña y Adolescentes**, con la participación activa de organizaciones aliadas y especialistas en derechos de la niñez.

Los **Conversatorios de Política Pública para el Uso Seguro de Internet** es un espacio de diálogo y reflexión interinstitucional donde se comparten las experiencias, propuestas y buenas prácticas a nivel nacional e internacional. Estos conversatorios han sido una plataforma estratégica para promover la articulación entre el Estado, la sociedad civil y los organismos internacionales, garantizando así un enfoque integral y participativo en la formulación y aplicación de políticas públicas.
Fuente: Consejo Nacional para la Igualdad Intergeneracional| ChildFund International

LINEAMIENTO DE LA POLÍTICA PÚBLICA 6	Fomentar y fortalecer los acuerdos, tratados y convenios internacionales, multilaterales jurídicamente vinculantes u oficiosos de cooperación técnica y económica para atender los casos de ciberdelincuencia y ciberseguridad enfocados en niñez y adolescencia.	
ACCIÓN 19	Gestionar la adhesión del Estado ecuatoriano al "Convenio sobre la ciberdelincuencia" (Convenio de Budapest)	

Ratificación del Convenio de Budapest.
Luego del trámite correspondiente, establecido en el artículo 37 del Tratado, Ecuador fue aceptado como Estado Observador el 31 de marzo de 2022, en la sesión número 1430 del Comité de Ministros del Consejo de Europa y se le otorgó un plazo de hasta cinco años para la armonización legislativa y para finalizar el proceso interno de ratificación del instrumento.

El 4 de julio de 2024, en la sesión No. 941 del Pleno de la Asamblea Nacional, se debatió el informe sobre la adhesión de Ecuador al Convenio de Budapest sobre Cibercriminalidad presentado por la Comisión de Soberanía, Integración y Seguridad Integral. El pleno de la Asamblea aprobó la adhesión al Convenio con 92 votos. ChildFund International realizó acciones de incidencia con los legisladores y realizó una comparecencia en el pleno.

Una vez que se contó con el dictamen de la Corte Constitucional y la aprobación de la Asamblea Nacional, el Presidente de la República mediante Decreto Ejecutivo 332, del 12 de julio de 2024, ratificó el Convenio de Budapest. Por lo que corresponde depositar el instrumento de ratificación ante la Secretaría y luego de tres meses de dicho depósito, entrará en vigencia.
Fuente: Ministerio de Relaciones Exteriores y Movilidad Humana / ChildFund International

ACCIÓN 20	Coordinar acuerdos o tratados internacionales multilaterales jurídicamente vinculantes u oficiosos de cooperación para el intercambio de información, tecnología, conocimiento de expertos y diversos recursos para atender los casos de ciberdelincuencia y ciberseguridad enfocados en niñez y adolescencia.	

Avances de Ecuador en la implementación de la Carta de Principios y Derechos en los Entornos Digitales
En cumplimiento de la **Carta de Principios y Derechos en los Entornos Digitales**, aprobada en la Cumbre Iberoamericana el **25 de marzo de 2023,** donde en su apartado número 5 se resalta la **especial atención a niñas, niños y adolescentes**, Ecuador ha logrado avances en materia de **capacitación digital** y ciberseguridad.

El **Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL)** ha desarrollado **capacitaciones presenciales y virtuales** dirigidas a este grupo etario, a través del **Proyecto Puntos Digitales Gratuitos**. Los contenidos formativos incluyen: Administración de amenazas cibernéticas; Introducción a la ciberseguridad; Seguridad en dispositivos móviles y protección de datos personales; y, Prevención de delitos cibernéticos. Estas acciones fortalecen las competencias digitales de niñas, niños y adolescentes, permitiendo que puedan interactuar en entornos digitales de manera **segura, responsable y constructiva.**

Plataformas de Educación en Línea, gracias a **alianzas estratégicas** con **proveedores de tecnología y contenido educativo**, se han implementado **plataformas de educación en línea** accesibles a la ciudadanía en todo el país. Estas plataformas ofrecen **recursos educativos interactivos** que facilitan el aprendizaje remoto y el desarrollo de habilidades digitales. Entre los socios clave que colaboran con el MINTEL a través de convenios de cooperación interinstitucional se encuentran: **CLARO; TELEFÓNICA; IBM; Unión Internacional de Telecomunicaciones (UIT); Microsoft; Amazon Web Services (AWS); y, ChildFund International,** entre otros.
Estas iniciativas reflejan el compromiso del Ecuador con la democratización del acceso a la infor mación y la promoción de competencias digitales como herramientas fundamentales para el desarrollo integral.
Fuente: Ministerio de Telecomunicaciones y Sociedad de la Información, Dirección Nacional de Registros Públicos

La Dirección de Investigación Civil ha logrado avances significativos en la cooperación internacional y en la lucha contra la ciberdelincuencia, especialmente enfocada en la protección de la niñez y la adolescencia. Sus principales logros incluyen:

- Acceso a plataformas globales como Meta, X (antes Twitter), Apple, TikTok y proveedores de correo electrónico, siguiendo estrictos procedimientos legales para la obtención de información y rastreo de datos.
- Coordinación con empresas de criptomonedas como Binance, y plataformas como Bumble, Discord, Fidelity, Gab, Imgur y Kik para identificar y rastrear transacciones vinculadas a delitos contra menores.

Fuente: Fiscalía General del Estado

En el marco de la cooperación internacional:

- Se suscribió el Memorando de Entendimiento en Ciberseguridad con el Ministerio del Interior y Seguridad Pública de Chile y el MINTEL de Ecuador, vigente desde el 6 de junio de 2019.
- En abril de 2022, se firmó un Memorando de Entendimiento con la Autoridad de Sistemas de Información de Estonia, en el marco del proyecto LAC4 del Centro de Competencia Cibernética de América Latina y el Caribe (EUCyberNet), vigente hasta abril de 2024.
- En febrero de 2024, Ecuador se integró al Foro Global sobre Experiencias Cibernéticas, con la expectativa de involucrarse activamente en iniciativas y proyectos de alto impacto.

Además, Ecuador ha sido reconocido como país prioritario en el proyecto Glacy-e del Consejo de Europa, facilitando la participación de personal de Policía y Fiscalía en formaciones y reuniones orientadas a la lucha contra la ciberdelincuencia.
Fuente: Ministerio de Relaciones Exteriores y Movilidad Humana

ACCIÓN 21	Gestionar la obtención de recursos para financiar políticas, planes, proyectos y líneas de acción que implementen medidas para garantizar los derechos de niñas, niños y adolescentes en relación al acceso, uso e interacción con tecnologías de la información y comunicación.	

La Subsecretaría de Asuntos Económicos y Cooperación Internacional reporta entre los proyectos de cooperación el suscrito entre el Ministerio de Telecomunicaciones de la Sociedad de la Información, en conjunto con la Unión Internacional de Telecomunicaciones (UIT), en agosto de 2024, presentaron un documento de trabajo que tiene como objetivo la elaboración de una propuesta de marco para la construcción de la estrategia nacional de protección de la infancia en línea.

La referida propuesta será realizada bajo la supervisión del Proyecto Mundial de Protección Infantil en Línea de la Oficina de Desarrollo de las Telecomunicaciones (BDT) de la UIT Equipo Directivo, entre otras oficinas de la UIT, junto con los expertos nacionales del Ecuador.

Cabe destacar que, las Naciones Unidas señala que su iniciativa sobre Protección Infantil en línea es una red compuesta por todas las partes interesadas lanzada por la Unión Internacional de Telecomunicaciones (UIT) para concienciar sobre la seguridad infantil en el mundo en línea y desarrollar herramientas para ayudar a los gobiernos, la industria y los educadores. Se puede revisar mayor información sobre el tema en el siguiente enlace web: https://www.un.org/es/global-issues/child-and-youth-safety-online
Fuente: Ministerio de Relaciones Exteriores y Movilidad Humana

ANEXO 4: Matriz de semaforización CON EVIDENCIA del cumplimiento de las acciones del Eje 4: Fortalecimiento de capacidades.

Eje 4: Fortalecimiento de capacidades **Objetivo 5: Promover una cultura preventiva para el uso seguro de internet y tecnologías digitales que oriente a los miembros de la comunidad educativa acerca de los beneficios y riesgos, así como desarrolle competencias y habilidades digitales básicas que contribuyen a su desarrollo humano.**		
LINEAMIENTO DE LA POLÍTICA PÚBLICA 7	Generar y socializar en la comunidad educativa conocimientos sobre los derechos de los niños niñas y adolescentes, a la autodeterminación informativa, identidad y reputación digital y responsabilidad de uso de redes sociales, como una estrategia para garantizar una Internet sana, segura y constructiva.	
ACCIÓN 22	Desarrollar una campaña de educomunicación a través de Educa Contigo y otros medios de comunicación públicos y privados sobre el uso seguro de la internet.	

El Ministerio de Educación generó insumos para la prevención de riesgos en entornos digitales.
El Ministerio de Educación ha desarrollado diversos insumos y recursos para la **prevención de riesgos en**

entornos digitales, en el marco del compromiso con la seguridad en línea de niñas, niños y adolescentes. Los recursos pueden descargarse de: https://educacion.gob.ec/prevencion-de-riesgos-en-entornos-digitales/

Recursos Disponibles

1. **Información y sensibilización**
   - **Videos educativos:** Dos videos que resumen el *Protocolo de Violencia Digital* y el caso relacionado con la sentencia sobre **difusión no consentida de imágenes íntimas**.
   - **Cómics educativos:** Materiales ilustrativos que incluyen recomendaciones prácticas para que docentes trabajen en el aula sobre prevención y uso responsable de Internet. Los recursos están disponibles para su descarga.
   - **Juego interactivo "Escaleras y Resbaladeras" (versión digital):** Desarrollado con apoyo de ChildFund International, este recurso ha sido ajustado y rediseñado con una nueva imagen.
2. **Educación y Formación**
   - **Curso MOOC "Guardianes Digitales en la Educación":** Dirigido a **docentes**, disponible a través del **Centro de Formación Digital Me capacito.** Hasta la fecha, se han realizado dos cortes de formación con éxito.
   - **Curso piloto para estudiantes:** Implementado inicialmente con estudiantes de Guayaquil. A partir de enero, este curso se amplió a nivel **nacional.**
   - **Entrega de materiales impresos:** Se han distribuido **cómics impresos** y versiones físicas del **juego "Escaleras y Resbaladeras"** a **3.460 instituciones educativas priorizadas** en las **9 zonas de educación**.
3. **Productos Educomunicacionales de EDUCA TV**

   La plataforma EDUCA TV ha producido y transmitido 61 contenidos educomunicacionales enfocados en el uso seguro y responsable de Internet. Estos materiales han sido difundidos a través de:
   - **8 canales nacionales**
   - **68 canales regionales**
   - **Plataformas digitales y redes sociales: www.educa.ec.**

Temáticas Abordadas:

- Ciberseguridad y uso seguro de Internet
- Día Internacional de la Internet Segura
- Ciudadanía digital
- Protección de datos personales
- Algoritmos y sus implicaciones
- Discurso de odio y agresión en línea
- Inteligencia artificial
- Sesgos mediáticos y manipulación de la información
- Análisis crítico de la información en línea
- Comportamiento ético en el entorno digital
- Activismo digital

Sitios Oficiales de EDUCA

- Facebook: https://www.facebook.com/EducaTele/
- Instagram: https://www.instagram.com/educatele
- T ikTok: https://www.tiktok.com/@educatele
- X (Twitter): https://x.com/EducaTele
- YouTube: https://youtube.com/@educatele
- Canal en línea: www.educa.ec

Con estas acciones, el Ministerio de Educación refuerza su compromiso con la seguridad digital y la formación integral de niñas, niños y adolescentes, preparando a la comunidad educativa para enfrentar los desafíos del entorno digital.

Fuente: Ministerio de Educación.

ACCIÓN 23	Coordinar campañas y procesos de difusión y concientización sobre ciberseguridad y manejo seguro de tecnologías digitales con los actores del sistema educativo, el espacio público y la sociedad en general.	

Campañas para concienciar

El Ministerio de Educación en conjunto con ChildFund International realizaron dos campañas de difusión en redes sociales institucionales:

- De septiembre a noviembre de 2023 con información permanente sobre las acciones de prevención, la identificación de riegos y difusión del protocolo.
- En el mes de febrero de 2024 se realizó una campaña en el marco del Día de la Internet Segura.
- Para las campañas en redes sociales se generó la marca “Cada clic cuenta” y se desarrollaron los siguientes productos:

- Producto 1: manual de uso de imagen de la estrategia, más 72 piezas comunicacionales para las redes sociales, con mallas de contenidos.
- Producto 2: elaboración del comic “Conexiones digitales” sobre los riesgos que pueden afectar a niñas y niños en la internet.
- Producto 3: elaboración del comic “Guardianes digitales” sobre la difusión no consentida de imágenes íntimas dirigida a adolescentes.
- Producto 4: elaboración de video que resuma el protocolo de violencia digital dirigido a la comunidad educativa.
- Producto 5: video animado que explica la Sentencia Nro. 456-JP y recoge las opiniones de las y los adolescentes frente a la difusión no consentida de imágenes íntimas.

Webinars:

- En febrero de 2024 se realizó un webinar dirigido a las familias a través de Facebook Live del Mineduc contó con la participación de cerca de 4000 personas conectadas; así como la participación en el panel de Buenas Prácticas de USAID.
- Se presentó el protocolo como iniciativas de protección organizado por el Instituto Interamericano del Niño, Niña, Adolescente – OEA en el webinar “Ideas fuerza – conectando visiones” el 15 de febrero de 2024.
- El protocolo se presentó en la Comisión Interamericano de Educación de la Organización de Estados Americanos (OEA), quienes se encuentran en la construcción de un curso hemisférico sobre educación digital y literacidad crítica, en enero de 2024.

Fuente: Ministerio de Educación

Campañas de sensibilización

- Puntos Digitales Gratuitos: En colaboración con empresas tecnológicas (Corporación Nacional de Telecomunicaciones (CNT EP), se han establecido centros comunitarios de capacitación que ofrecen formación en competencias digitales básicas, medias y avanzadas. Estos centros están destinados a diversos grupos, incluyendo niños, jóvenes y adultos, para mejorar sus habilidades digitales y promover la inclusión digital con énfasis en las zonas rurales urbano marginales. Las temáticas principales que se brinda a la ciudadanía son: herramientas TIC, redes sociales para jóvenes con responsabilidad, TIC para niñ@s, programa CREATIC, curso básico de robótica, diseño de páginas web comunitarias, ensamblaje y mantenimiento de computadoras, cómputo básico, entre otras.
- Campañas de Alfabetización Digital: A través de asociaciones con organizaciones privadas y ONG, se han llevado a cabo campañas de alfabetización digital que buscan educar a la población sobre el uso seguro y efectivo de las tecnologías de la información y comunicación una de esas alianzas con ChildFund International Internacional – Ecuador.
- Plataformas de Educación en Línea: Gracias a alianzas con proveedores de tecnología y contenido educativo, se han creado plataformas de educación en línea accesibles para la ciudadanía de todo el país. Estas plataformas ofrecen recursos educativos y herramientas interactivas que facilitan el aprendizaje remoto. Las principales alianzas estratégicas que le MINTEL mantiene a través de convenios de cooperación interinstitucionales son: CLARO, TELEFÓNICA, IBM, Unión Internacional de Telecomunicaciones

Fuente: Dirección Nacional de Registros Públicos

Capacitación y sensibilización en prevención de explotación infantil en línea.

La Dirección de Capacitación y Fortalecimiento Misional conjuntamente con la Embajada Americana, Oficina Homeland Security Investigations – HSI, ha ejecutado capacitaciones sobre “PREVENCIÓN DE EXPLOTACIÓN INFANTIL EN LÍNEA”. La referida dirección ha realizado 5 capacitaciones entre el 22 de abril al 31 de mayo del año en curso, en donde han participado 284 funcionarios de esta dependencia. Estas capacitaciones se realizaron en distintas provincias del Ecuador, bajo la temática "Guardian - Prevención en Crímenes de Abuso Sexual Infantil en Línea".

Fuente: Fiscalía General del Estado

Acciones por el Uso Seguro de la Internet

a. Desarrollo de Recursos Pedagógicos. ChildFund International, en colaboración con el Ministerio de Educación y otras instituciones, ha elaborado y adaptado recursos pedagógicos innovadores para su uso en entornos educativos:
   - Juego i nteractivo “Escaleras y Resbaladeras” (versión digital y física): Herramienta lúdica para trabajar en el aula temas de prevención y ciudadanía digital.
   - Manuales y guías didácticas para docentes, orientados a fortalecer la educación digital en las escuelas.
   - Caja de Herramientas para el Uso Seguro de Internet: Compendio de actividades prácticas, guías metodológicas y recursos para familias, educadores y estudiantes.

b. Formación de Formadores y Actores Clave. ChildFund International ha participado en programas de formación de formadores como el FOFOUSI (Formación de Formadores de Uso Seguro de Internet) en conjunto con el Instituto Interamericano del Niño, la Niña y Adolescentes (IIN) y el Consejo Nacional para la Igualdad Intergeneracional (CNII). Las acciones clave incluyen:

c. Capacitación a docentes y funcionarios públicos sobre prácticas seguras en el uso de Internet. Formación en el uso de metodologías para la educación digital y la prevención de riesgos en línea. Acompañamiento en la implementación de la Red Intergeneracional de Agentes Multiplicadores en Uso Seguro de Internet (RIAMUSI).

d. Campañas de Alfabetización Digital y Ciberseguridad. En colaboración con actores públicos y privados, ChildFund International ha ejecutado campañas de alfabetización digital para fomentar habilidades tecnológicas y digitales:

- Capacitaciones en competencias digitales básicas, medias y avanzadas para niñas, niños, adolescentes y familias.
- Talleres especializados sobre ciberseguridad, enfocándose en temas como:
- Protección de datos personales.
- Seguridad en dispositivos móviles.
- Identificación de amenazas y prevención de delitos cibernéticos.

e. Participación en Conversatorios y Espacios Internacionales. ChildFund International ha participado activamente en foros y conversatorios internacionales relacionados con la protección de NNA en entornos digitales, tales como:
   - Conversatorios de Políticas Públicas para el Uso Seguro de Internet, organizados por el IIN-OEA.
   - Webinars y paneles interinstitucionales para compartir experiencias, buenas prácticas y avances en la promoción de entornos digitales seguros.

Fuente: ChildFund International

ANEXO 5: Matriz de semaforización CON EVIDENCIA del cumplimiento de las acciones del Eje 5: Estrategia comunicacional.

Eje 5: Estrategia comunicacional **Objetivo 6: Desarrollar una estrategia comunicacional para promover los derechos digitales y un uso seguro de la internet por parte de niñas, niños y adolescentes.**		
LINEAMIENTO DE LA POLÍTICA PÚBLICA 8	Activar las redes sociales institucionales con campañas informativas, posicionamiento y mantenimiento del uso seguro de la Internet para niñas, niños y adolescentes.	
ACCIÓN 24	Difundir temas relativos al uso seguro de internet en los medios de comunicación públicos, privados y digitales. Estandarizar los contenidos para difundirlos en medios de comunicación.	

Difusión de campañas informativas

La Fiscalía General del Estado (FGE), a través de su Dirección de Comunicación y Promoción Institucional, implementa de manera continua campañas informativas relacionadas con delitos informáticos, en particular sobre pornografía infantil y la protección de los derechos de niñas, niños y adolescentes (NNA). Las noticias sobre investigaciones y procesos judiciales se difunden a través de:

- Sala de prensa online en el sitio web institucional.
- Distribución directa a medios de comunicación mediante un chat de prensa.
- Como parte de la estrategia de acceso a la justicia, la Fiscalía amplió su formulario de denuncia en línea sobre violencia basada en género. Este formulario ahora permite reportar:
- Contacto con fines sexuales y oferta de servicios sexuales con menores de 18 años.
- Pornografía infantil (producción, difusión y comercialización).
- Difusión de material pornográfico dirigido a NNA.
- Para promover este servicio, la Dirección de Comunicación lanzó una campaña informativa a través de los canales oficiales de la Fiscalía.

La Dirección de Estudios Penales publicó en mayo de 2020 la edición n.º 27 de la Revista Científica de Ciencias Jurídicas, Criminología y Seguridad: Perfil Criminológico, titulada “Child Grooming”. El documento está disponible en el siguiente enlace: Revista Científica - Perfil Criminológico
Fuente: Fiscalía General del Estado

Eventos en medios de comunicación y redes sociales
Año 2021: Se organizaron seis eventos con 1.346 participantes, destacando:

- 09 de febrero: Lanzamiento de la primera campaña institucional "Por un Internet seguro para niños, niñas y adolescentes".
- 18 y 24 de febrero: Webinars “Fomentemos un Internet Seguro desde los prestadores de telecomunicaciones”.
- 08 de marzo: Charla “Fomentemos Internet Seguro desde los colegios”.
- 23 de abril: Charla “Fomentemos Internet Seguro desde el hogar”.
- 18 de octubre: Participación en la Mesa Técnica Intersectorial.

Año 2022: Se llevaron a cabo seis eventos con 1.979 participantes, incluyendo:
- 08 de marzo: Webinar “Fomentemos una Internet Segura desde los colegios”.
- 23 de abril: Día Mundial de las Niñas en las Tics, charla “Internet Segura desde el hogar”.
- •15 de mayo: Charla “Fomentemos una Internet Segura desde el hogar”.
- 07 de junio: Webinar “Internet Segura con prestadores de telecomunicaciones”.
- 08 de julio: Charla “Buenos hábitos de ciberseguridad”.
- 09 de octubre: Webinar “Protección frente a los depares”.

Año 2023: Se realizaron tres eventos con 609 participantes:
- 29 de septiembre: Webinar “Engaños de la red utilizando Inteligencia Artificial (IA)”.
- 01 de octubre: Webinar “Engaños en la red de juegos en línea”.
- 01 de noviembre: Webinar “Alfabetización en nuevos tipos de engaños en ciberseguridad para NNA”.

Año 2024
- 10 de junio: Charla presencial en la Institución Educativa Colegio Luis Napoleón Dillon (Quito), con la participación de 225 estudiantes.

Fuente: Agencia de Regulación y Control de las Telecomunicaciones

Difusión de información sobre las investigaciones y procesos judiciales

Además de las campañas informativas sobre delitos informáticos, el Departamento de Comunicación de la Fiscalía General del Estado (FGE) gestiona de manera continua la difusión de información sobre las investigaciones y procesos judiciales relacionados con delitos de pornografía infantil y la protección de los derechos de niños, niñas y adolescentes (NNA). Estas noticias se publican en la sala de prensa online del sitio web institucional y se distribuyen a los medios de comunicación a través de un chat de prensa.

Con el objetivo de fortalecer el acceso a la justicia para las víctimas, la Fiscalía amplió el catálogo de delitos que pueden ser denunciados a través del formulario de denuncia en línea sobre violencia basada en género. Ahora es posible reportar delitos como: contacto con fines sexuales y oferta de servicios sexuales con menores de 18 años mediante medios electrónicos; pornografía con utilización de niñas, niños y adolescentes (NNA); así como la difusión de material pornográfico a NNA.

La Dirección de Comunicación lanzó una campaña para promover este servicio a toda la ciudadanía a través de sus canales oficiales.

Dirección de Estudios Penales. Se ha elaborado mediante la Dirección de Estudios Penales, la Revista Científica de Ciencias Jurídicas, Criminología y Seguridad: Perfil Criminológico n.° 27, titulada "Child Grooming", en el mes de mayo de 2020.

Se encuentra en el siguiente enlace: https://www.fiscalia.gob.ec/pdf/politica-criminal/revista-Perfil-Criminologico-julio-2020.pdf

Fuente: Fiscalía General del Estado

Campañas comunicacionales por el uso seguro de la Internet.

Desde 2020, ChildFund International ha desempeñado un rol activo y sostenido en la promoción del Uso Seguro de Internet como parte de su compromiso con la protección de los derechos de niñas, niños y adolescentes (NNA), en el marco de la política pública nacional e internacional. Estas acciones han buscado concienciar a la sociedad, fortalecer capacidades y generar entornos digitales seguros para la niñez y adolescencia ecuatoriana.

Principales Acciones Realizadas

a. Campañas Anuales de Sensi bilización. ChildFund International ha desarrollado campañas anuales de difusión y sensibilización para familias, docentes, estudiantes y la comunidad en general sobre la seguridad digital, enfocadas en:
   - Prevención de riesgos digitales como ciberacoso, grooming, sextorsión y exposición a contenidos inapropiados.
   - Uso responsable y positivo de las tecnologías de la información y comunicación (TIC).
   - Promoción de la alfabetización digital y la construcción de habilidades críticas para identificar y prevenir amenazas en línea.
   - Las campañas han utilizado materiales y recursos específicos, tales como:
   - Videos informativos y cápsulas educativas.
   - Cómics digitales e impresos:
   - “Conexiones Digitales”: Dirigido a niñas y niños, aborda riesgos comunes en Internet.
   - “Guardianes Digitales”: Enfocado en adolescentes, trata la difusión no consentida de imágenes íntimas.
   - Infografías y guías con recomendaciones para padres, docentes y adolescentes.
   - Webinars y talleres virtuales realizados en fechas clave como el Día Internacional de la Internet Segura.

Fuente: ChildFund International

Activaciones en redes sociales con materiales, carruseles y baterías de contenidos:
En el eje de la estrategia comunicacional para abordar la política pública por una internet segura, desde el CNII, se han abordado varias campañas, actividades y acciones comunicacionales, que permitieron la difusión de esta política, informaron sobre los avances y logros realizados. Entre algunas acciones de comunicación se destacan:

- Presentación de la política pública sobre internet segura. 24 de septiembre de 2020.
- Campaña sobre internet segura, en el marco de la estrategia comunicacional gubernamental "Quédate en casa". Batería con 7 mensajes explicativos de cuáles son los riesgos para niñas, niños y adolescentes en internet.
- Campaña de difusión de los extractos de la política pública sobre una internet segura. Batería de redes sociales. 22 de octubre de 2020.
- Campaña por el uso del internet seguro para niñas, niños y adolescentes, en el marco del trabajo de Pacto con la niñez y adolescencia que detalló las ventajas de trabajar por una internet segura. 6 de marzo del 2020.
- En el marco del uso del tiempo en el confinamiento, se activó la campaña con todo el Ejecutivo, sobre internet segura para niñas, niños y adolescentes-COVID-19. 28 de marzo de 2020.
- Campañas de segunda activación: 22 de junio 2020 y 7 de agosto 2020.

Cabe destacar que estas campañas fueron activadas desde el Ejecutivo, con todos los sectores, logrando entrar en tendencia de redes sociales, por cinco ocasiones, con el hashtag: #InternetSeguraEc

- Niñez protegida / delitos cometidos en internet. 11 de febrero de 2021
- Internet segura / extractos de la política pública. 3 de junio de 2021

Fuente: Consejo Nacional para la Igualdad Intergeneracional

LINEAMIENTO DE LA POLÍTICA PÚBLICA 9	Erradicar los mensajes y contenidos violentos y discriminatorios en contra niñas, niños y adolescentes que se difunden a través de medios virtuales.	
ACCIÓN 25	Coordinar campañas y procesos de difusión y concientización sobre: datos personales, derechos digitales, uso de una internet segura, seguridad en redes dirigidas a los usuarios de los servicios públicos; funcionarios públicos, en especial a Policía Nacional, Fiscalía, Función Judicial, Corte Constitucional; proveedores de servicios de telecomunicaciones; público en general.	

Puntos Digitales Gratuitos: En colaboración con empresas tecnológicas (Corporación Nacional de Telecomunicaciones (CNT EP), se han establecido centros comunitarios de capacitación que ofrecen formación en competencias digitales básicas, medias y avanzadas. Estos centros están destinados a diversos grupos, incluyendo niños, jóvenes y adultos, para mejorar sus habilidades digitales y promover la inclusión digital con énfasis en las zonas rurales urbano marginales. Las temáticas principales que se brinda a la ciudadanía son: herramientas TIC, redes sociales para jóvenes con responsabilidad, TIC para niñ@s, programa CREATIC, curso básico de robótica, diseño de páginas web comunitarias, ensamblaje y mantenimiento de computadoras, cómputo básico, entre otras.

- Campañas de Alfabetización Digital: A través de asociaciones con organizaciones privadas y ONG, se han llevado a cabo campañas de alfabetización digital que buscan educar a la población sobre el uso seguro y efectivo de las tecnologías de la información y comunicación una de esas alianzas con ChildFund International Internacional – Ecuador.
- Plataformas de Educación en Línea: Gracias a alianzas con proveedores de tecnología y contenido educativo, se han creado plataformas de educación en línea accesibles para la ciudadanía de todo el país. Estas plataformas ofrecen recursos educativos y herramientas interactivas que facilitan el aprendizaje remoto. Las principales alianzas estratégicas que el Ministerio de Telecomunicaciones y Sociedad de la Información mantiene a través de convenios de cooperación interinstitucionales son: CLARO, TELEFÓNICA, IBM, Unión Internacional de Telecomunicaciones (UIT), Microsoft, Amazon Web Service (AWS), ChildFund International, entre otros.

Fuente: Ministerio de Telecomunicaciones y Sociedad de la Información

LINEAMIENTO DE LA POLÍTICA PÚBLICA 10	Analizar el impacto de los mensajes difundidos en medios públicos, privados y digitales, además de redes sociales.	
ACCIÓN 26	Monitoreo de noticias en medios: prensa, radio, televisión, digitales. Redes sociales (Facebook, Twitter. YouTube).	

En 2020, la Dirección Nacional de Registros Públicos fue designada responsable de la creación de la página web https://www.internetsegura.gob.ec
La construcción de la página web se realizó de acuerdo a la plantilla gubernamental; sin embargo, se dejó de usar el azul como predominante, dado que la temática se enfoca en un público más dinámico y menos formal, niños, adolescentes, padres de familias y maestros.

La web contiene videos, reportajes, juegos e ideas para niñas, niños, adolescentes, familias y docentes. Este es un espacio informativo, a través del cual se brindan herramientas lúdicas sobre las oportunidades y riesgos de la red y cómo actuar ante alertas. Además, se destacan proyectos institucionales sobre la temática.

El Consejo Nacional para la Igualdad Intergeneracional era el responsable de recopilar la información y solicitarnos los cambios.

En agosto de 2021, con Oficio Nro. DINARDAP-DINARDAP-2021-0878-OF, la autoridad de la fecha, designó a los funcionarios: María Fernanda Torres (Dirección de Comunicación Social), Darío Torres Bedón (Dirección de Seguridad Informática) y Elita Chico Pico (Dirección de Talento Humano), como delegados para continuidad de la política pública por una internet segura para niños, niñas y adolescentes, en respuesta al Oficio. CNNI-CNNI.2021-0354-OF, 16 de junio de 2021.

Adicionalmente, desde la Dirección Nacional de Registros Públicos conforme los compromisos adquiridos procedieron con la creación de las cuentas en las diferentes redes sociales, mismas que se detallan a continuación:
Web: https://www.internetsegura.gob.ec/

Referencias

Livingstone, S., Carr, J., & Byrne, J. (2018). *Protecting children in the digital world: An international perspective*. Innocenti Research Brief.

Convención sobre los Derechos del Niño. (1989). Asamblea General de las Naciones Unidas.

Van Dooren, W., Bouckaert, G., & Halligan, J. (2015). *Performance Management in the Public Sector.* Routledge.

UNICEF. (2020). *Policy Guidance on Addressing Online Child Exploitation.* UNICEF Publications.

Behn, R. D. (2003). *Why Measure Performance? Different Purposes Require Different Measures*. Public Administration Review, 63(5), 586-606.

Hatry, H. P. (2006). *Performance Measurement: Getting Results*. The Urban Institute.

Livingstone, S., & Stoilova, M. (2021). *Global Kids Online: Children's Online Activities, Risks, and Opportunities*. London School of Economics.

Livingstone, S., Carr, J., & Byrne, J. (2018). *Protecting children in the digital world: An international perspective.* Innocenti Research Brief.

Meadows, D. H. (2008). *Thinking in Systems: A Primer*. Chelsea Green Publishing.

Van Dooren, W., Bouckaert, G., & Halligan, J. (2015). *Performance Management in the Public Sector*. Routledge.

Consejo Nacional para la Igualdad Intergeneracional

@CN_Igualdad
@ecuadorintergeneracional
@cniiecuador

ChildFund

@ChildFundEc
@ChildFundEcuador
@ChildFundEcuador