



Guía para la identificación de riesgos de violencias en entornos digitales con énfasis en Explotación Sexual Comercial de Niñas, Niños y Adolescentes.



#VocesQuePrevienen

En convenio con:



Naciones Unidas
Oficina contra
la Droga y el Delito





UNODC

Representante Regional

Amado Philip de Andrés

Representante Regional Adjunto

Oliver Inizan

Coordinador Regional del Área de Justicia y Prevención de Violencias

Andrés Díaz Mescias

Coordinadora Componente de Estrategias para Sujetos de Especial Protección

Rocío Urón Durán

Asesora Técnica para la Intervención y Prevención de la ESCNNA

Maria Alejandra Calderon Quiroga

Asesor Técnico de Trata de Personas, Tráfico Ilícito de Migrantes y otros delitos conexos

Julián Camilo Quinche Yaya

Jimena Velez - Experto en Ciberdelitos

Instituto Colombiano de Bienestar Familiar

Directora general

Astrid Eliana Cáceres Cárdenas

Subdirectora general

Adriana Velásquez Lasprilla

Directora de Infancia

Beatrice Eugenia López Cabrera

Directora Adolescencia y Juventud

Naya Gutiérrez Pinzón

Subdirectora de Promoción y Fortalecimiento a la Atención de la Infancia

Ángela Fernanda Cabrera Fonseca

Subdirectora de Gestión Técnica para la Adolescencia y la Juventud (E)

Ángela Fernanda Cabrera Fonseca

Jefe Oficina Asesora de Comunicaciones

Betty Leonor Monzón Cifuentes

Equipo Técnico Instituto Colombiano de Bienestar Familiar

Álvaro Vicente Fera Núñez

Daniel Mauricio Sánchez Prado

Fabián Antonio Bolaños Chamorro

Fredy Abelardo Velásquez Montoya

Gemma Judith Ángel Vargas

Concepto y diseño:

CLICK+CLACK - Laboratorio de aprendizaje

Diagramación e impresión:

Corcas Editores SAS

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) e Instituto Colombiano de Bienestar Familiar. Diciembre, 2025. Todos los derechos reservados.

INTRODUCCIÓN

En los últimos años, diversos informes oficiales en Colombia han alertado sobre el aumento de los riesgos que enfrentan niñas, niños y adolescentes en el entorno digital. El Instituto Colombiano de Bienestar Familiar (ICBF), en su Boletín Estadístico de febrero de 2025, reportó que las violencias más notificadas contra la población menor de 18 años continúan siendo la violencia sexual y la negligencia, con miles de casos atendidos en todo el país [ICBF, 2025]. A su vez, el Informe Anual de la Ley 1336 de 2009 ante el Congreso de la República, vigencia 2023 documentó la persistencia de casos de Explotación Sexual Comercial de Niñas, Niños y Adolescentes y la necesidad de fortalecer los mecanismos de prevención y respuesta frente a estas manifestaciones incluyendo los contextos digitales [ICBF, 2024]. De manera complementaria, la Cámara de Representantes de Colombia advirtió en 2024 que siete (7) de cada diez (10) personas menores de 18 años en Colombia han sido víctimas de ciberacoso, lo que refleja la magnitud del fenómeno y sus implicaciones en el bienestar emocional y social de esta población [Cámara de Representantes, 2024]. El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), por su parte, ha identificado al grooming, al sexting y al ciberacoso¹ como temas prioritarios en sus campañas de prevención digital [MinTIC, 2023].

Estos hallazgos se ven reforzados por la Procuraduría General de la Nación, que en 2024 señaló la necesidad de vigilancia especial sobre casos de ciberacoso, grooming y violencia sexual en entornos escolares, dada su creciente recurrencia y complejidad [Procuraduría General de la Nación, 2024]. Todo esto muestra que, si bien Colombia ha avanzado en normativas y políticas para proteger a niñas, niños y adolescentes, persisten desafíos frente a la detección temprana, el subregistro y la capacidad de respuesta frente a riesgos emergentes como la suplantación digital, los deepfakes, la sextorsión y los retos virales peligrosos.

¹ Grooming: es una conducta mediante la cual un adulto establece una relación de confianza con una niña, niño o adolescente a través de internet con el fin de obtener algún tipo de actividad con contenido sexual. Sexting: envío o intercambio de mensajes, fotos o videos de contenido sexual a través de medios digitales. Ciberacoso: hostigamiento, humillación o amenazas que una persona recibe de manera repetida mediante redes sociales, mensajería u otras plataformas en línea.



Frente a este panorama, la presente guía se enmarca en el convenio de cooperación entre el ICBF y la Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], cuyo objeto es “aunar esfuerzos técnicos, administrativos y financieros para el fortalecimiento de la prevención, identificación y atención de violencias que pueden afectar a niñas, niños y adolescentes como las Violencias Basadas en Género (VBG), la Trata de Personas y la Explotación Sexual Comercial de niñas, niños y adolescentes, favoreciendo un abordaje desde la protección integral hacia las niñas, niños, adolescentes y la promoción de entornos protectores en las familias y comunidades”. Este documento busca aportar orientaciones que, en coherencia con los marcos normativos nacionales y estándares internacionales, fortalezcan las capacidades de prevención, identificación y atención de violencias en entornos digitales, promoviendo la garantía del interés superior de los derechos de las niñas, niños y adolescentes.



ALCANCE Y PÚBLICO OBJETIVO

- Instituciones y profesionales que inciden en la prevención, detección y atención de violencias contra niñas, niños y adolescentes.

Enfoques y principios que guían la construcción del presente documento:

Enfoque de derechos de las niñas, niños y adolescentes

Este enfoque posibilita el reconocimiento de las niñas, niños y adolescentes como titulares de derechos y requieren una protección especial sin ningún tipo de discriminación (ya sea por motivos de raza, género, nacionalidad, origen étnico u otros), de acuerdo con lo dispuesto en los tratados y convenios internacionales ratificados por el Estado colombiano y en la legislación nacional vigente. Esto implica que cualquier medida en el ámbito digital debe priorizar la protección, el bienestar y el desarrollo integral de niñas, niños y adolescentes frente a intereses económicos, tecnológicos o institucionales.

Enfoque de curso de vida

Reconoce que el crecimiento y el desarrollo forman parte de un proceso continuo a lo largo de toda la vida humana. Estas etapas no deben entenderse como fases rígidas determinadas únicamente por la edad, sino como resultado de las interacciones que cada persona mantiene con su entorno social, económico, histórico y cultural. Asimismo, se ven influenciadas por los acontecimientos significativos y los contextos en los que se desarrollan, los cuales impactan tanto en la vida de niñas, niños y adolescentes como en las dinámicas de sus familias.

La Ley 1098 de 2006 [Código de Infancia y Adolescencia] reconoce que las necesidades y formas de protección varían según la edad. Así, las estrategias para prevenir violencias digitales deben adaptarse a cada etapa, por ejemplo: en la primera infancia, privilegiar la mediación parental y contenidos apropiados; en la niñez intermedia, fortalecer habilidades



críticas y digitales; y en la adolescencia, promover la autonomía responsable, la participación y la protección frente a riesgos como grooming o sextorsión. Teóricamente, se basa en el modelo de desarrollo humano de Bronfenbrenner y en el enfoque de curso de vida de la CEPAL, que plantean la necesidad de intervenciones diferenciadas según la etapa vital.

Enfoque de género y diversidades - Orientaciones Sexuales e Identidades de Género Diversas- OSIGD

Permite analizar las dinámicas históricas de poder entre hombres y mujeres, en las cuales se privilegia la representación de lo masculino con relación a lo femenino, así como las formas de relación entre distintas identidades de género y orientaciones sexuales. En Colombia, la **Ley 1257 de 2008** reconoce la obligación de prevenir y sancionar todas las formas de violencia contra las mujeres, incluidas aquellas en entornos digitales. Estudios recientes de ONU Mujeres y European Institute for Gender and Equality (EIGE), muestran que las niñas y adolescentes mujeres están más expuestas a ciberacoso sexual, sextorsión y difusión no consentida de imágenes. Asimismo, adolescentes OSIGD enfrentan riesgos agravados de acoso, discriminación y discursos de odio en línea. Este enfoque busca garantizar la igualdad sustantiva, evitar revictimización y reconocer las particularidades de género y diversidad sexual².

Enfoque diferencial étnico y territorial

El artículo 7 de la Constitución reconoce y protege la diversidad étnica y cultural. En territorios indígenas, afrodescendientes y rurales, la conectividad

² Sexo: Esta categoría hace referencia a las características biológicas con las que nace cada persona, de esta manera, contiene los caracteres sexuales de los seres humanos, los cuales hacen referencia en primer lugar al aparato reproductor y los genitales, en segundo lugar, el componente hormonal, el desarrollo muscular, la estructura ósea y la constitución genética. Las subcategorías que lo conforman son: hombre, mujer e intersexual. Cuando se enuncia el sexo de una persona, se hace alusión al Sexo asignado al nacer.

Orientación sexual: Esta categoría hace referencia a la atracción afectiva, emocional y sexual hacia otra persona. En esta se involucra: el deseo, el erotismo, la atracción sexual, el enamoramiento y otros sentimientos. En este sentido las personas pueden tener atracción por una/varias personas del mismo sexo, de otro sexo o pueden no sentir atracción hacia otra persona. Las subcategorías que lo conforman son: Heterosexual, Homosexual, Bisexual,

Pansexual, Asexual.



suele ser más limitada, lo que genera brechas de acceso, pero también riesgos distintos, como menor capacidad institucional de respuesta. **El Auto 251 de 2008 de la Corte Constitucional** y la Ley 21 de 1991 [Convenio 169 de la OIT] obligan a adoptar medidas culturalmente pertinentes. En contextos digitales, esto significa producir materiales en lenguas propias, reconocer saberes comunitarios y adecuar estrategias a realidades territoriales diversas.

INCLUSIÓN Y ACCESIBILIDAD

La Convención sobre los Derechos de las Personas con Discapacidad [ratificada por Colombia con la Ley 1346 de 2009] exige garantizar accesibilidad física, comunicacional y tecnológica. El **Conpes 166 de 2013** y la Ley Estatutaria 1618 de 2013 establecen lineamientos para garantizar derechos de las personas con discapacidad. En entornos digitales, esto se traduce en la obligación de que plataformas, contenidos y protocolos de prevención y atención sean accesibles [ej. subtítulos, lectores de pantalla, interfaces amigables].

De acuerdo con el Instituto Colombiano de Bienestar Familiar [2023], con la Convención Internacional sobre los Derechos de las Personas con Discapacidad [CDPD], la idea de discapacidad cambia desde una perspectiva social, entendiendo que no reside en la persona, sino en las desventajas, obstáculos y desigualdades que impone el entorno en el que vive. De esta manera, la discapacidad surge cuando la persona interactúa con su medio, ya que es allí donde aparecen las barreras que restringen sus oportunidades.

PRINCIPIOS RELEVANTES

Principio del interés superior

El interés superior de la niña, niño o adolescente, entendido como principio implica considerar de manera prioritaria su desarrollo pleno y equilibrado.



Este principio representa una obligación para toda la sociedad de asegurar la satisfacción integral y simultánea de todos los derechos humanos de la infancia y la adolescencia, los cuales son universales, prioritarios e interdependientes. El marco constitucional colombiano [art. 44 de la Constitución Política de 1991] establece que los derechos de las niñas, niños y adolescentes son prevalentes. La Convención sobre los Derechos del Niño [1989], ratificada por Colombia mediante la Ley 12 de 1991, y la **Observación General N.º 25 [Comité de los Derechos del Niño, 2021] sobre los derechos en entornos digitales, señalan que el interés superior del niño, niña y adolescentes debe orientar todas las decisiones, políticas y acciones.**

Presunción de Minoría de Edad:

Cuando exista duda sobre la edad de una persona que podría ser niño, niña o adolescente, se deberá asumir que tiene la edad menor. Este principio, en concordancia con el artículo 149 del Código de Infancia y Adolescencia [Ley 1098 de 2008], establece que mientras la autoridad competente determine la edad exacta, se considerará que la persona es menor de 18 años, presumiéndose siempre la edad inferior.

No discriminación

El principio de no discriminación establece que los derechos humanos son propios de todas las niñas, niños y adolescentes sin excepción alguna, sin importar su raza, color, sexo, idioma, religión, opiniones, origen nacional, étnico o social, situación económica, discapacidad, nacimiento, condición migratoria o cualquier otra circunstancia personal o la de sus padres o representantes legales.

Confidencialidad

Hace referencia al resguardo de la confidencialidad de toda información relacionada con la niña, niño o adolescente, en cumplimiento del deber de garantizar sus derechos, especialmente su derecho a la intimidad.

Acción sin daño:

Toda acción o intervención realizada debe llevarse a cabo evitando causar cualquier daño adicional a la niña, niño o adolescente, garantizando así que no se produzca una revictimización.

ÉTICA DIGITAL Y PROTECCIÓN DE DATOS PERSONALES

La Ley 1581 de 2012 regula la protección de datos personales en Colombia y establece un régimen especial para datos de niñas, niños y adolescentes, reforzando el consentimiento informado y la confidencialidad. Además, la Ley 1266 de 2008 y el Decreto 1377 de 2013 fortalecen las obligaciones de quienes manejan información personal. Teóricamente, este enfoque se soporta en principios de ética digital como transparencia, minimización de datos y "safety by design", recomendados por la UNESCO (2021) y el Consejo de Europa (2018). La protección de datos personales de niñas, niños y adolescentes es clave frente a la economía digital, la publicidad dirigida y la exposición a fraudes o explotación.

DEFINICIONES OPERATIVAS

- **Entornos preventivos:** Son espacios físicos, sociales o digitales que promueven condiciones de bienestar y seguridad, orientados a anticipar y reducir factores de riesgo que puedan afectar a niñas, niños y adolescentes. Estos entornos fortalecen capacidades individuales y colectivas, fomentan prácticas protectoras, facilitan la identificación temprana de señales de alerta y articulan la participación de familias, instituciones y comunidades para evitar la ocurrencia de violencias y vulneraciones de derechos. (UNICEF. 2017)
- **Entornos digitales:** Son los espacios virtuales de interacción mediados por tecnologías de la información y las comunicaciones, que incluyen internet, dispositivos móviles, aplicaciones y plataformas de socialización y aprendizaje. Según la Observación General N.º 25 del Comité de los



Derechos del Niño (2021), los entornos digitales forman parte integral de la vida de niñas, niños y adolescentes, por lo que los Estados deben garantizar el goce pleno de sus derechos también en ellos.

- **Redes sociales:** Plataformas digitales que permiten la creación y el intercambio de contenidos entre usuarios, favoreciendo la interacción, comunicación y conformación de comunidades en línea. De acuerdo con la Ley 1978 de 2019 (art. 2) en Colombia, hacen parte de los servicios de Tecnologías de la Información y las Comunicaciones, sujetos a principios de acceso, protección y uso responsable.
- **Videojuegos en línea:** Aplicaciones digitales de carácter lúdico que permiten la interacción entre usuarios en entornos virtuales, ya sea en tiempo real o de manera asincrónica. El Documento CONPES 3918 de 2018 reconoce el papel de la industria de videojuegos en la economía digital, resaltando la importancia de políticas de uso responsable y protección de usuarios menores de edad.
- **Herramientas de Inteligencia Artificial (IA):** Sistemas digitales que, mediante algoritmos, procesan datos y generan resultados como texto, imágenes, audios o decisiones automatizadas. El UNICEF (2020) – Policy Guidance on AI for Children establece que la IA debe diseñarse y utilizarse con criterios de ética, transparencia y protección reforzada para niñas, niños y adolescentes.
- **Explotación Sexual Comercial de Niñas, niños y Adolescentes- ESCNNA:** La Explotación Sexual Comercial de Niños, Niñas y Adolescentes (ESCNNA), conforme a la definición del Instituto Colombiano de Bienestar Familiar (ICBF), se entiende como una forma de violencia sexual en la que una persona menor de 18 años es utilizada con fines sexuales a cambio de dinero, bienes o cualquier tipo de retribución. En este contexto, la víctima es tratada como un objeto de intercambio o mercancía, siendo vendida o comprada por adultos, lo que constituye una manifestación



contemporánea de esclavitud y una grave vulneración de los derechos humanos de la niñez y la adolescencia [2018].

- **Trata de Personas:** Se entenderá la captación, el transporte, el traslado, la acogida o la recepción de personas, recurriendo a la amenaza o al uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder o de una situación de vulnerabilidad o a la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación [Protocolo de Palermo 2003].

Es importante reconocer que la Trata de Personas con fines de explotación sexual es diferente de la Explotación Sexual Comercial de Niñas, Niños y Adolescentes [ESCNNA], debido a que para que exista la conducta de Trata con fines de explotación sexual de una niña, niño o adolescente, en lugar de cualquier otro de los delitos contemplados como de explotación sexual se requiere del traslado y desarraigo del niño, niña y adolescente víctima de la explotación, rompiendo su red vincular de apoyo y sustrayéndolo de su ambiente social generando una mayor vulnerabilidad de éste para lograr su explotación [ICBF, 2018].

- **Grooming:** Cualquier acción realizada por un adulto a través de medios digitales con el fin de ganarse la confianza de un niño, niña o adolescente para obtener ventajas sexuales. En Colombia, la Ley 1336 de 2009 incorporó el artículo 217-A al Código Penal, tipificado como delito el "grooming" o utilización de medios electrónicos para contactar con personas menores de 18 años de edad con fines sexuales.
- **Ciberbullying:** El hostigamiento virtual se entiende como una forma de acoso entre pares que se expresa mediante conductas repetitivas y deliberadas, realizadas por una persona o grupo con la intención de causar daño a otra, haciendo uso de las tecnologías de la información y las comunicaciones.

- **Material de explotación sexual de niñas, niños y adolescentes (MESNNA):** Toda representación, por cualquier medio, de un menor de 18 años en actividades sexuales explícitas, reales o simuladas, o la utilización de imágenes de niña, niños y adolescentes con fines sexuales. Esta definición corresponde al artículo 218 del Código Penal colombiano [modificado por Ley 1329 de 2009 y Ley 1453 de 2011] y se encuentra en armonía con el Convenio de Budapest sobre Ciberdelincuencia [2001, art. 9] y la Observación General N.º 25 del Comité de los Derechos del Niño y la Niña [2021].
- **Deepfakes:** Contenidos sintéticos [videos, audios o imágenes] creados con inteligencia artificial que manipulan la apariencia o voz de una persona. El Parlamento Europeo [2020] y la UNESCO [2021] han alertado sobre sus riesgos, especialmente cuando se utilizan para la explotación sexual de niñas, niños y adolescentes. En Colombia, si bien no existe una tipificación específica, su uso con fines sexuales o de engaño puede enmarcarse en los delitos de Material de explotación sexual de niñas, niños y adolescentes³, suplantación y fraude informático [Ley 1273 de 2009].
- **Sextorsión:** Forma de extorsión en la que se amenaza a una persona con difundir imágenes íntimas si no se accede a exigencias de índole sexual o económica. La Fiscalía General de la Nación en Colombia lo reconoce como una modalidad del delito de extorsión [art. 244 del Código Penal].
- **Ingeniería social:** Conjunto de técnicas de manipulación psicológica utilizadas para obtener información confidencial, acceso a sistemas o inducir a realizar acciones que comprometen la seguridad. La Ley 1273 de 2009 sanciona el acceso abusivo a sistemas informáticos y el hurto por medios informáticos, dentro de los cuales suelen usarse estas prácticas.

³ Si bien el legislado habla de "pornografía infantil" para la presente guía se hablará de **Material de explotación sexual de niñas, niños y adolescentes**.

- **Phishing:** Modalidad de fraude electrónico en la cual se engaña al usuario para que revele datos personales, contraseñas o información financiera. La Policía Nacional de Colombia – CAI Virtual [2024] lo reconoce como uno de los principales cibercrímenes que afectan a niñas, niños adolescentes y adultos.
- **Doxxing:** Práctica de recopilar y publicar información personal identificable de una persona en internet sin su consentimiento, con el fin de amenazar, acosar o extorsionar. De acuerdo con la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos [2022], constituye una grave violación al derecho a la privacidad y puede derivar en riesgos de violencia digital y física.



MARCO NORMATIVO NACIONAL E INTERNACIONAL

La protección de niñas, niños y adolescentes en entornos digitales se soporta en un conjunto articulado de normas nacionales y compromisos internacionales que obligan al Estado colombiano a garantizar sus derechos en el ámbito virtual.

Normativa nacional

- **Constitución Política de Colombia [art. 44]:** consagra la prevalencia de los derechos de las niñas, niños y adolescentes y establece el deber de la familia, la sociedad y el Estado de protegerlos contra toda forma de violencia, abuso, explotación y trata. Este principio se aplica también a los entornos digitales, donde emergen nuevas formas de vulneración.
- **Ley 1098 de 2006 [Código de Infancia y Adolescencia]:** regula integralmente la protección de los derechos de niñas, niños y adolescentes. El artículo 20 establece la obligación del Estado de proteger a las niñas, niños y adolescentes frente a contenidos nocivos, lo que incluye internet y medios digitales.
- **Ley 679 de 2001 y Ley 1336 de 2009:** conocidas como el "estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores de edad". Estas leyes sancionan la producción, difusión y comercialización de material de explotación sexual infantil en línea, imponiendo además obligaciones a prestadores de servicios de internet.
- **Ley 1329 de 2009 y Ley 1453 de 2011:** fortalecen la protección penal frente a delitos como la pornografía con personas menores de 18 años, el uso de medios tecnológicos para contactar a menores [grooming] y la sextorsión.

- **Ley 1273 de 2009 [delitos informáticos]:** incorpora el Título VII Bis al Código Penal, sancionando conductas como el acceso abusivo a sistemas, la interceptación de datos y el uso de medios digitales para delinquir, fundamentales para enfrentar el cibercrimen contra niñas, niños y adolescentes.
- **Ley 1581 de 2012 [protección de datos personales]:** regula el tratamiento de datos y otorga especial protección a la información de los niñas, niños y adolescentes. Prohíbe el tratamiento de sus datos sin autorización expresa y con fines contrarios a su interés superior.
- **Ley 2489 de 2025 [por la cual se adoptan medidas para entornos digitales seguros]:** refuerza obligaciones de plataformas tecnológicas en materia de verificación de edad, eliminación expedita de contenidos nocivos y cooperación con autoridades en casos de explotación infantil en línea.
- **Lineamientos del Instituto Colombiano de Bienestar Familiar (ICBF), Sistema Nacional de Bienestar Familiar (SNBF), Protocolos de Fiscalía General de la Nación y Policía Nacional:** establecen procedimientos interinstitucionales para la atención de casos de violencia digital, incluyendo la articulación con la línea 141, CAIVAS y CAI Virtual.

NORMATIVA INTERNACIONAL

Colombia ha ratificado instrumentos internacionales que obligan a la protección de niñas, niños y adolescentes frente a las violencias digitales:

- **Convención sobre los Derechos del Niño [1989] – Ley 12 de 1991:** reconoce el derecho de niñas, niños y adolescentes a la protección frente a cualquier forma de explotación y abuso, incluyendo la explotación sexual.
- **Protocolo Facultativo de la Convención sobre la venta de niños, la prostitución infantil y la utilización de niños en pornografía [2000] – Ley 765 de 2002:** obliga a sancionar y prevenir la producción, distribución y



posesión de material de explotación sexual infantil, incluidas las formas digitales.

- **Convenio de Budapest sobre Ciberdelincuencia [2001]:** primer tratado internacional vinculante en materia de delitos informáticos incluye el artículo 9 que tipifica conductas relacionadas con pornografía infantil. Colombia lo aprobó mediante la Ley 1335 de 2009.
- **Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer [Convención de Belém do Pará, 1994]:** obliga a prevenir la violencia contra niñas y adolescentes, aplicable también a la violencia en entornos digitales.
- **Protocolo de la Organización Internacional del Trabajo sobre trabajo forzoso [2014] y Convenio 182 [1999] sobre las peores formas de trabajo infantil:** consideran la explotación sexual infantil, incluida la digital, como una de las peores formas de trabajo infantil, actualmente el desarrollo académico ha realizado análisis al respecto entendiendo la explotación sexual de niñas, niños y adolescentes como una grave vulneración de derechos.
- **Observación General N.º 25 del Comité de los Derechos del Niño y la Niña [2021]:** establece que los derechos de las niñas, niños y adolescentes [educación, privacidad, protección contra violencia, libertad de expresión y asociación] deben garantizarse en entornos digitales.
- **Directrices de UNICEF sobre IA para niñas, niños y adolescentes [2020]:** recomiendan a los Estados y al sector privado asegurar que el desarrollo y uso de IA proteja los derechos de niñas, niños y adolescentes frente a riesgos como los deepfakes o la explotación sexual en línea.

La importancia de la prevención de los riesgos de violencias hacia niñas, niños y adolescentes en contextos digitales:

La rápida evolución de las tecnologías de la información y la comunicación ha redefinido los modos en que las personas interactúan, acceden al conocimiento y participan en dinámicas socioculturales. De igual manera, los entornos digitales han diversificado los factores de riesgo, generando nuevas dinámicas de vulneración de derechos, entre ellas la transformación de delitos como explotación sexual comercial de niñas, niños y adolescentes (ESCENNA) y distintas violencias que se despliegan a través de redes sociales, servicios de mensajería instantánea, plataformas de juego en línea y otros espacios virtuales. Frente a este panorama, la prevención se posiciona como un componente estratégico, orientado no solo a disminuir la exposición a las situaciones de riesgo, sino también a desarrollar capacidades en niñas, niños, adolescentes, familias, actores institucionales y comunidades para la identificación oportuna de indicadores de vulneración y la promoción de entornos digitales preventivos y protectores.

En consecuencia, la implementación de enfoques, como el enfoque de género, en los procesos de prevención de riesgos digitales debe considerar que, de manera particular, para las niñas y adolescentes mujeres, las experiencias como el **body shaming**, el acoso sexual, presión para compartir imágenes íntimas o manipulación afectiva, entre otros, representan puertas de entrada a formas de explotación digital. De manera similar, para niñas, niños y adolescentes con orientaciones sexuales e identidades de género diversas, quienes pueden explorar su identidad en espacios digitales buscando apoyo o confidencialidad; sin embargo, los espacios digitales pueden convertirse en escenarios donde agresores instrumentalizan el miedo al rechazo o la revelación de su identidad y la discriminación colectiva para coaccionar, extorsionar o captar con fines de explotación. Estas vulnerabilidades diferenciadas exigen estrategias preventivas más sensibles, específicas y afirmativas para asegurar que todas las adolescencias puedan desarrollarse en entornos digitales seguros.



Frente a este panorama, la prevención se posiciona como un componente estratégico, orientado no solo a disminuir la exposición a situaciones de riesgo, sino también a desarrollar capacidades en niñas, niños, adolescentes, familias, actores institucionales y comunidades para la identificación oportuna de indicadores de vulneración y la promoción de entornos digitales preventivos y protectores. Impulsar una cultura de prevención en el ámbito digital exige comprender que la seguridad no depende exclusivamente de conductas individuales frente al uso de la tecnología, sino de la corresponsabilidad efectiva entre las familias, Estado, sector privado, las comunidades y la sociedad civil en general.

En esta perspectiva, las acciones preventivas deben garantizar que la niñez y la adolescencia ejerzan sus derechos digitales con autonomía, confianza y condiciones de prevención y protección, reduciendo la probabilidad de ocurrencia de violencias y fortaleciendo el acompañamiento que permita anticipar riesgos, promover prácticas seguras y consolidar entornos digitales protectores para la garantía plena de sus derechos.



PREVENCIÓN DE TIPOLOGÍAS DE RIESGOS EN LÍNEA: MODELO DE LOS 4CS

El análisis de los riesgos digitales que afectan a niñas, niños y adolescentes ha adquirido especial relevancia en los últimos años, conforme el entorno digital se ha integrado de manera natural en la vida cotidiana. Los contextos digitales, aunque representan múltiples oportunidades para el aprendizaje, la comunicación y el desarrollo, también conlleva riesgos que deben ser comprendidos y gestionados de manera informada. En este sentido, la presente guía no pretende restringir el uso de las tecnologías, sino de promover una formación adecuada y orientación permanente por parte de las familias, las instituciones y la sociedad en general, con el objetivo de garantizar mecanismos de prevención, protección integral de los derechos, la dignidad y la integridad de la niñez y la adolescencia.

Los análisis de riesgos digitales contribuyen al propósito de identificar, clasificar y abordar de manera sistemática los diferentes factores de vulnerabilidad presentes en los contextos sociales, económicos, culturales y tecnológicos actuales. En este sentido, el análisis de riesgos digitales en niñas, niños y adolescentes se ha fortalecido en los últimos años gracias a modelos conceptuales que permiten organizar la complejidad de las amenazas en categorías comprensibles y operativas. Uno de los más reconocidos es el modelo de los 4Cs [Contenido, Contacto, Conducta y Contrato/Comercio], propuesto inicialmente en el Byron Review (2008) en el Reino Unido y posteriormente consolidado por la red de investigación EU Kids Online [Livingstone, Haddon & Görzig, 2012; Staksrud & Ólafsson, 2019]. Este enfoque ha sido adoptado por organismos internacionales como UNICEF (2020), UNESCO (2021) y la Comisión Europea [Better Internet for Kids] por su utilidad pedagógica y práctica en la formulación de políticas públicas, programas educativos y estrategias de prevención.

Este enfoque ha sido adoptado por organismos internacionales como UNICEF (2019, 2020), UNESCO (2019, 2021) y la Comisión Europea [Better Internet for Kids], por su utilidad pedagógica y práctica en la formulación de políticas públicas, programas educativos y estrategias de prevención de violencias



en línea. El modelo reconoce que los riesgos digitales no son homogéneos ni lineales: difieren en su origen, en los mecanismos de daño, en los actores implicados y en los tipos de respuesta institucional requeridos.

En esta guía, el modelo de los 4Cs se utiliza como una herramienta operativa para:

- organizar los riesgos de manera accesible para equipos territoriales, instituciones educativas y familias;
- orientar la identificación y valoración de los riesgos;
- definir respuestas diferenciadas y articuladas con las rutas de protección existentes.

A continuación, se describen cada una de las categorías, incorporando ejemplos, referencias normativas e indicadores sugeridos para la identificación de riesgos en territorio.

RIESGOS DE CONTENIDO

Se refieren a la exposición de niñas, niños y adolescentes a materiales nocivos o ilegales que pueden afectar su desarrollo físico, psicológico o moral. Incluyen la pornografía infantil o material de explotación sexual de niñas, niños y adolescentes (MESNNA), la violencia extrema, los discursos de odio, los retos virales peligrosos y la desinformación en temas sensibles como salud sexual o consumo de sustancias. El Código Penal colombiano [art. 218, modificado por la Ley 1329 de 2009] sanciona la producción y difusión de pornografía con personas menores de 18 años, mientras que la Ley 1098 de 2006 [art. 20] establece el deber del Estado de proteger a niñas, niños y adolescentes de contenidos nocivos. A nivel internacional, el Convenio de Budapest sobre Ciberdelincuencia [2001, art. 9] obliga a tipificar y sancionar estas conductas, y la Observación General N.º 25 del Comité de los Derechos del Niño [2021] reconoce que la protección frente a contenidos digitales dañinos es parte del derecho a crecer en entornos seguros.



Investigaciones recientes subrayan que la exposición reiterada a contenidos violentos o sexualizados puede generar procesos de desensibilización, normalización de la violencia y adopción de guiones de comportamiento agresivo o de riesgo [Huesmann, 2007]. Estudios sobre niñas y niños más pequeños destacan, además, el papel de los algoritmos de recomendación en plataformas de vídeo, que pueden prolongar la exposición y llevar progresivamente a contenidos más extremos [Jang & Ko, 2023].

Indicadores sugeridos para la identificación de riesgos de contenido.

Estos indicadores son orientadores y deben adaptarse a la edad, contexto y competencias del equipo territorial:

Señales en el relato de niñas, niños y adolescentes

- Menciones reiteradas a videos de violencia extrema, autolesiones o retos peligrosos.
- Referencias de haber visto “fotos o videos fuertes”, “cosas de sexo”, “cosas que dan miedo” en redes sociales o plataformas de video.
- Uso de lenguaje sexualizado o violento que no corresponde a la etapa de desarrollo.

Cambios de comportamiento asociados al uso de dispositivos

- Aumento brusco del tiempo de conexión a ciertas plataformas.
- Evitación de ver contenidos acompañados de personas adultas, ocultamiento de pantallas, cambio rápido de aplicación.
- Alteraciones del sueño o incremento de miedos después de consumir contenidos digitales.
- La exposición a contenidos sexualizados puede ser utilizada por agresores para evaluar reacciones, vulnerabilidades o intereses, con el fin de iniciar procesos de grooming.
- Las niñas, niños o adolescentes pueden ser inducidos, a través de contenidos, a prácticas sexualizadas, retos o desafíos que luego son

utilizados para sextorsión, por ejemplo: "envía una versión tuya de este reto para entrar a un grupo".

Fuentes de información para el tamizaje

- Reportes de docentes sobre conversaciones, dibujos o juegos que reproducen escenas violentas o sexualizadas.
- Denuncias o alertas de madres, padres o cuidadores sobre contenido al que se ha expuesto el niño o la niña.
- Revisión, con consentimiento y apoyo psicosocial, de historial de navegación o aplicaciones [cuando sea pertinente y respetando el interés superior y la confidencialidad]

Ejemplo operativo

- Un adolescente comienza a recibir videos en TikTok con retos sexualizados a través del algoritmo. Responde a una historia de un perfil desconocido que "invita" a participar en un "concurso para un viaje", lo que desencadena un proceso de captación para ESCNNA o posible traslado para una trata de personas.



RIESGOS DE CONTACTO





Involucran la interacción directa entre niñas, niños adolescentes y actores que buscan aprovecharse de su vulnerabilidad. Ejemplos son el grooming, la sextorsión o el acercamiento por adultos que se hacen pasar por pares. Estos riesgos son altamente relevantes en Colombia: según datos de la Fiscalía General de la Nación [2023], una parte significativa de las investigaciones por explotación sexual en línea inicia con un contacto digital. El artículo 217-A del Código Penal, incorporado por la Ley 1336 de 2009, tipifica el grooming como delito. Internacionalmente, el **Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, prostitución infantil y pornografía infantil** [2000] y el Convenio de Budapest [2001] refuerzan la obligación de los Estados de prevenir y sancionar estas conductas.

La investigación comparada muestra que el tiempo de conexión, la ausencia de mediación adulta y el uso de dispositivos en soledad son factores que incrementan la probabilidad de contactos abusivos [Tintori et al., 2023; Jang & Ko, 2023].

Indicadores sugeridos para la identificación de riesgos de contacto

Señales en el discurso de niñas, niños y adolescentes

- Relatos de “amistades” o “parejas” que solo existen en línea y que no desean presentar a la familia o a la escuela.
- Comentarios sobre personas que piden secretos, fotos, videos o información personal “que nadie más debe saber”. Pueden constituir un riesgo para la ocurrencia de ESCNNA, o posible captación y traslado para explotación en casos de trata de personas.
- Referencias a haber recibido propuestas para enviar imágenes íntimas, participar en retos sexualizados o cambiar fotos por regalos como constitutive de una posible ocurrencia de ESCNNA.
- Conversaciones con desconocidos que piden mantener el contacto en secreto.
- Invitaciones a encuentros fuera del entorno habitual o a cambiar a plataformas cifradas [Telegram, Signal, Whisper].
- Expresiones como “te puedo ayudar a ganar dinero” o “te puedo llevar a otro lugar donde te valoren”.



Evidencia en dispositivos y plataformas (cuando el contexto lo permita bajo la implementación de un enfoque de derechos)

- Mensajes insistentes de perfiles desconocidos o con datos mínimos.
- Solicitudes de cambio de plataforma a aplicaciones más privadas o cifradas.
- Conversaciones que incluyen manipulación emocional, culpabilización o amenazas (por ejemplo, "si no me mandas la foto, se la digo a todos/as").

Señales comportamentales y emocionales

- Aislamiento repentino, irritabilidad o cambios de humor vinculados al uso del celular o del computador.
- Miedo o angustia al recibir mensajes o notificaciones.
- Incremento de conductas evitativas (no querer ir al colegio o a ciertos lugares por temor a que se conozca algo difundido en línea).

Ejemplo operativo

Una niña o niño que juega videojuegos en línea conoce a un adulto que se hace pasar por alguien de su edad. Comienza enviando regalos dentro del juego y luego directamente solicita fotos realizando alguna actividad o fotos íntimas. Posteriormente amenaza con difundirlas para forzar producción de material sexual (MESNNA).

RIESGOS DE CONDUCTA

Son aquellos que derivan de las acciones realizadas por las propias niñas, niños y adolescentes en línea, a menudo sin plena conciencia de sus consecuencias. Ejemplos incluyen el sexting, el ciberacoso, la difusión de imágenes íntimas de terceros o la participación en retos virales peligrosos. Aunque estas conductas pueden parecer voluntarias, muchas veces son resultado de presión de pares o manipulación externa. En Colombia, la



Ley 1620 de 2013 sobre convivencia escolar incluye la responsabilidad de atender casos de ciberacoso en el ámbito educativo, mientras que la Ley 1273 de 2009 sanciona la difusión no consentida de información íntima. Investigaciones de EU Kids Online (2020) muestran que este tipo de riesgos aumenta con la edad, cuando los adolescentes adquieren mayor autonomía digital pero aún carecen de herramientas plenas para evaluar riesgos.

Indicadores sugeridos para la identificación de riesgos de conducta

Señales en el clima escolar y comunitario

- Casos reportados de humillaciones, insultos o burlas en grupos de chat, redes sociales o foros.
- Existencia de "memes", montajes o videos que ridiculizan a una compañera o compañero.
- Comentarios reiterados sobre "reenviar nudes", "compartir packs" "pasar fotos" de pares.

Autorreporte de niñas, niños y adolescentes

- Reconocimiento de haber enviado imágenes íntimas a alguien (pareja, amistades, personas desconocidas).
- Participación en grupos donde se comparten contenidos de odio, violencia o discriminación. Participación en retos virales que implican daño físico, humillación exposición de la vida privada.

Indicadores emocionales y relacionales

- Aumento de conflictos con pares vinculados a publicaciones, estados, historias o comentarios en redes.
- Retroceso escolar, ansiedad, evitación del uso de tecnologías o, al contrario, hiperconectividad asociada a conflictos en línea.

EJEMPLO OPERATIVO

Un adolescente comienza a participar activamente en grupos de chat donde circulan "packs" o imágenes de pares, motivado por presión social o búsqueda de validación. En un intento por integrarse al grupo y ser divertido, decide enviar una fotografía íntima propia. Días después, esa imagen empieza a circular entre otros contactos, lo que genera burlas, chantajes y amenazas para que envíe dinero a sus compañeros para que no siga circulando la foto.

Riesgos de Contrato/Comercio

Se relacionan con la explotación económica y comercial de niñas, niños y adolescentes en entornos digitales, incluyendo fraudes electrónicos, publicidad engañosa, apuestas en línea, uso indebido de datos personales, microtransacciones abusivas en videojuegos o monetización de la interacción infantil. Estos riesgos han sido señalados por la OECD (2022) y la UNCTAD (2021) como crecientes en economías digitales emergentes. En Colombia, la Ley 1480 de 2011 [Estatuto del Consumidor] protege frente a la publicidad engañosa, y reconoce derechos especiales para consumidores en situación de vulnerabilidad. La Ley 1581 de 2012 regula el uso de datos personales, incluyendo disposiciones específicas para la información de niñas, niños y adolescentes. A nivel internacional, la Convención sobre los Derechos del Niño (art. 32) obliga a protegerlos de toda forma de explotación económica, lo cual incluye las dinámicas digitales actuales.

Indicadores sugeridos para la identificación de riesgos de contrato/comercio

Señales económicas y de consumo

- Compras no autorizadas desde dispositivos utilizados por niñas, niños o adolescentes (aplicaciones, juegos, plataformas de streaming).
- Aumento inusual de gastos en microtransacciones o servicios digitales vinculados a cuentas familiares.

- Uso frecuente de aplicaciones o juegos que promueven cajas de botín, apuestas o transacciones con dinero real.

Indicadores de exposición a prácticas comerciales agresivas

- Niñas, niños o adolescentes que reportan recibir anuncios insistentes, presiones para comprar mensajes que vinculan la compra con popularidad, belleza, éxito o aceptación social.
- Participación en sorteos, concursos o "regalos" que exigen compartir datos personales, subir fotos o etiquetar a otras personas.

Riesgos asociados a datos personales y privacidad

- Creación de múltiples cuentas sin supervisión adulta, aceptación de términos y condiciones sin lectura ni comprensión.
- Uso de redes sociales o plataformas que recopilan datos de geolocalización, contactos o comportamiento sin que niñas, niños, adolescentes y familias comprendan el alcance.
- Publicación reiterada de información personal (dirección, colegio, rutinas, ubicación en tiempo real) sin medidas de protección que genera un alto riesgo para captación en delitos asociados a ESCNNA o trata de personas.

EJEMPLO OPERATIVO

Un adolescente empieza a jugar en una plataforma que ofrece incentivos económicos por generar contenido y atraer seguidores. Motivado por la posibilidad de obtener ingresos rápidos, acepta participar en transmisiones en vivo donde usuarios anónimos le piden que realice acciones cada vez más explícitas a cambio de "propinas" virtuales. La plataforma no verifica la edad ni los límites del contenido, y las sesiones son grabadas y revendidas por terceros sin su consentimiento.

USO DE LA TIPOLOGÍA DE LOS 4CS EN LA PREVENCIÓN E IDENTIFICACIÓN Y GESTIÓN DE RIESGOS

La tipología de los 4Cs [contenido, contacto, conducta y contrato/comercio] no se presenta aquí únicamente como una clasificación conceptual, sino como una herramienta operativa para orientar la identificación, valoración y respuesta frente a riesgos digitales que afectan a niñas, niños y adolescentes. Su adopción responde a las recomendaciones de la red EU Kids Online, la UNESCO [2021] y la Observación General N.º 25 del Comité de los Derechos del Niño y la Niña [2021], las cuales destacan la necesidad de marcos claros que faciliten la protección integral de niñas, niños y adolescentes en entornos digitales.

En esta guía, el modelo se utiliza con tres propósitos principales:

1. Clasificar los casos identificados: Cada situación de riesgo detectada en los territorios se ubica en una o más de las categorías del modelo. Esto permite determinar con rapidez:

- El tipo de amenaza [contenido, contacto, conducta, contrato/comercio];
- La forma en que se manifiesta;
- Los actores que deben intervenir [familia, escuela, salud, justicia, TIC, protección al consumidor, entre otros].

2. Ejemplarización operativa

- Un adolescente contactado por un adulto a través de videojuegos para pedirle fotos íntimas → riesgo de contacto, con posible articulación con riesgo de conducta si ya envió imágenes → se activan rutas judiciales [Fiscalía, Policía] y de protección [ICBF, comisarías de familia, equipos psicosociales].

- Una niña expuesta a videos con retos de autolesión en redes sociales → riesgo de contenido, con posible impacto en salud mental → se activan medidas escolares, familiares y de salud [orientación escolar, atención psicosocial, servicios de salud mental].

3. Valorar la gravedad del riesgo: La tipología permite elaborar instrumentos de tamizaje que combinan, al menos, dos variables:

- Probabilidad de ocurrencia o repetición [baja, media, alta].
- Impacto sobre el bienestar y la seguridad de la niña, niño o adolescente [leve, moderado, grave⁴].

EJEMPLOS:

- Exposición ocasional a publicidad engañosa [contrato/comercio], sin impacto evidente en la economía familiar o en la salud mental → riesgo **bajo/medio**.
- Sextorsión con amenaza de difusión masiva de imágenes íntimas [contacto y conducta], con afectación emocional significativa → riesgo **alto** que exige respuesta urgente.

Esta valoración alimenta la priorización de recursos, la definición de tiempos de respuesta y la decisión sobre escalamiento a instancias de protección o justicia.

4. Orientar respuestas diferenciadas y sectorizadas: Cada categoría de riesgo activa mecanismos específicos:

- **Contenido:**
 - herramientas tecnológicas [filtros, controles parentales];
 - alfabetización mediática e informacional para prevenir riesgos;
 - acompañamiento adulto en el consumo de contenidos.

⁴ En este punto para los casos de ESCNNA y/o Trata de Personas, las afectaciones siempre serán de gravedad

- **Contacto:**

- detección temprana de contactos sospechosos;
- denuncia penal y preservación de evidencia digital;
- acompañamiento psicosocial especializado;
- articulación con sistemas de protección.

- **Conducta:**

- educación socioemocional y ciudadanía digital;
- trabajo grupal en escuelas y comunidades para transformar normas de pares;
- intervención restaurativa en casos de ciberacoso;
- fortalecimiento de habilidades de autocuidado digital.

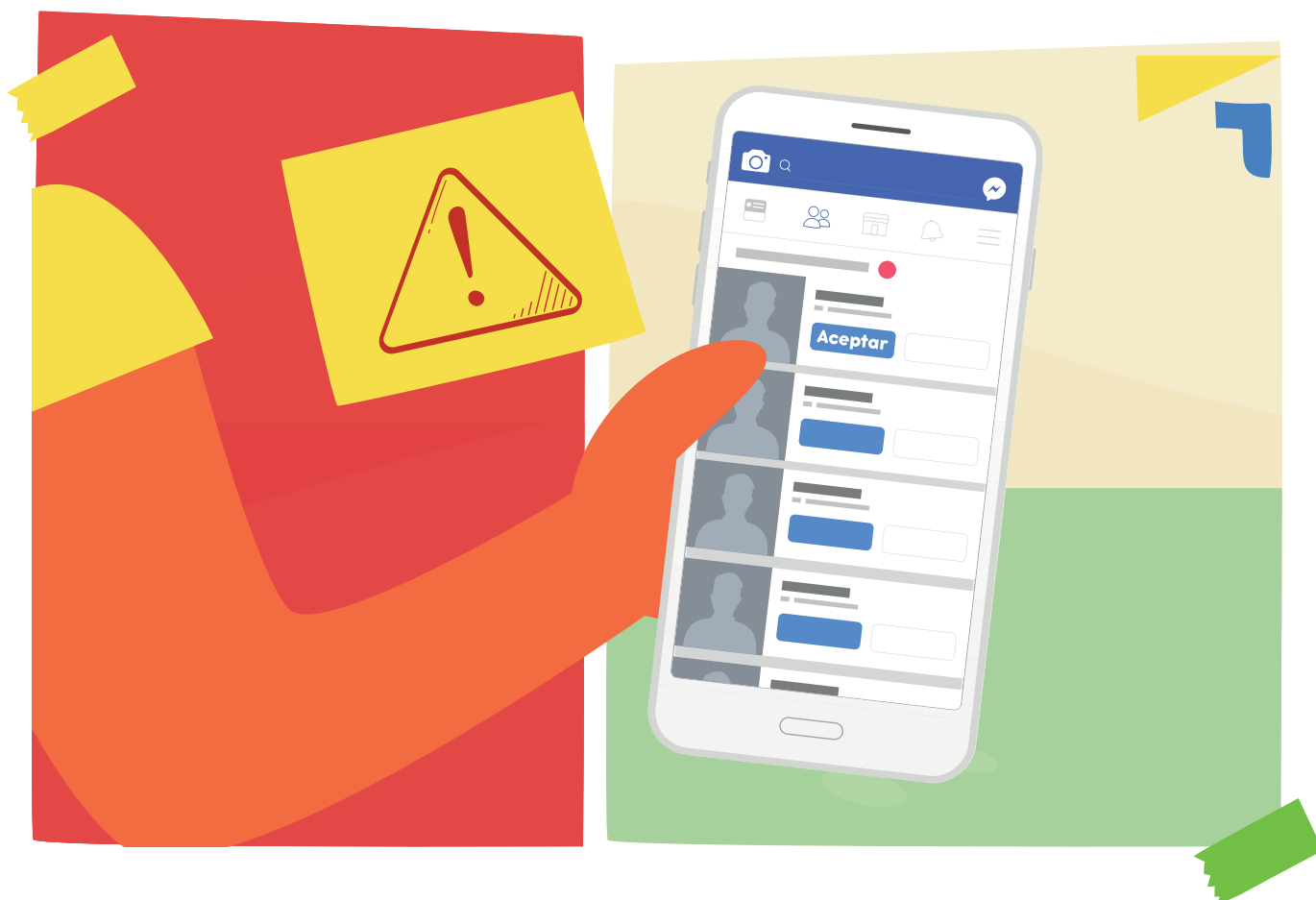
5. Contrato/Comercio:

- regulación y supervisión de prácticas comerciales;
- protección de datos personales y promoción de "data literacy" en niñas, niños, adolescentes y familias;
- articulación con autoridades de protección al consumidor y autoridades TIC.

6. Articular la acción interinstitucional El uso de esta tipología permite que entidades con mandatos diferentes —educación, justicia, salud, TIC, protección al consumidor— hablen un lenguaje común. Esto favorece la coordinación en la respuesta, evita duplicidad y asegura que cada sector asuma el rol que le corresponde.

7. Fortalecer la prevención y la capacitación Al ser un modelo comprensible y ampliamente difundido, el de los 4Cs facilita la creación de materiales pedagógicos, guías para familias y docentes, y campañas de sensibilización. De esta manera, se traduce en una herramienta práctica de comunicación pública.

RUTA BÁSICA PARA PREVENIR E IDENTIFICAR RIESGOS DIGITALES (PASO A PASO)



Para que la guía cumpla una función operativa en territorio, se propone una **ruta básica para la prevención e identificación** y basada en el modelo de los 4Cs:

Paso 1. Recoger información inicial [detección o tamizaje]

- Escuchar el relato de niñas, niños, adolescentes, familias y actores comunitarios.
- Identificar en qué plataformas ocurre la situación [red social, videojuego, aplicación de mensajería, etc.].
- Registrar brevemente qué está ocurriendo, desde cuándo y con qué frecuencia.

Paso 2. Clasificar el riesgo en una o más "C"

- Preguntas orientadoras:
- ¿El problema principal es lo que se ve o consume en línea? → **Contenido**.
- ¿El problema principal es con quién se relaciona o quién le escribe? → **Contacto**.
- ¿El problema principal es lo que el propio niño, niña o adolescente hace en línea (frente a sí o frente a otras personas)? → **Conducta**.
- ¿El problema principal es lo que se compra, se apuesta, se paga o el uso de sus datos personales? → **Contrato/Comercio**.

La situación puede abarcar varias categorías a la vez; en ese caso, se registra la principal y las secundarias.

Paso 3. Valorar el nivel de riesgo

Se puede utilizar una escala simple:

- **Riesgo bajo:**
- Evento aislado, sin daño evidente, que puede abordarse con información, orientación y ajustes de uso.
- **Riesgo medio:**
- Situación repetida o con indicios de afectación emocional o social, que requiere acompañamiento psicosocial y seguimiento.
- **Riesgo alto:**
- Indicios de delito [grooming, explotación sexual comercial, sextorsión, trata de personas⁵];
- afectación grave de la salud mental [ideas de autolesión, intentos de suicidio];
- impacto económico significativo o coacción.

Paso 4. Activar la respuesta correspondiente

De acuerdo con la categoría principal y el nivel de riesgo:

- Documentar la situación en los formatos institucionales vigentes.
- Activar rutas de protección [ICBF, comisaría de familia, defensoría de familia, Fiscalía, Policía] cuando corresponda por ejemplo línea gratuitas como la 141 del ICBF y la línea 123 de la Policía Nacional.

⁵ En caso de ocurrencia de los delitos de trata de personas y/o ESCNNA, se requiere estimar las afectaciones en salud física

- Coordinar con la institución educativa, los servicios de salud y otros actores relevantes.
- Acordar acciones de seguimiento con la familia.

Paso 5. Registrar indicadores clave

En cada caso, se recomienda registrar como mínimo

- tipo de riesgo (C principal y C secundarias);
- edad y género de la niña, niño o adolescente;
- plataforma o entorno digital implicado;
- nivel de riesgo (bajo/medio/alto);
- acciones activadas (orientación, acompañamiento, denuncia, remisión).
- Esto permitirá, a mediano plazo, contar con información agregada para ajustar estrategias de prevención, formación y articulación interinstitucional.

RIESGOS DIGITALES EN LA NIÑEZ Y ADOLESCENCIA - MODELOS EMERGENTES

En el escenario digital actual, las experiencias de niñas, niños y adolescentes ya no dependen únicamente de la interacción entre personas a través de la tecnología, sino también de sistemas automatizados que influyen, diseñan y condicionan su comportamiento y recorrido en línea. La protección integral de la población infantil y juvenil requiere, por tanto, vigilar no sólo los contenidos y conductas individuales, sino también las arquitecturas algorítmicas que operan de manera oculta, los mecanismos de captación de la atención digital y las dinámicas de circulación de datos que sustentan estos entornos. A continuación, se exponen algunos riesgos relevantes:

1. Diseño algorítmico y riesgos sistémicos:

Las recomendaciones de la UNESCO enfatizan que las plataformas digitales deben aplicar procedimientos de debida diligencia en materia de derechos humanos, y que tanto la forma en que están diseñados sus sistemas como los procesos de moderación y selección de contenidos deben ajustarse a las normas internacionales [UNESCO, 2023]¹. Asimismo, la Organisation



for Economic Co-operation and Development [OECD] advierte que los algoritmos⁶ y las herramientas que personalizan contenidos y crean perfiles digitales pueden generar mayores riesgos para la salud, la privacidad y la igualdad de niñas, niños y adolescentes [OECD, 2025]².

A continuación, se señalan algunas maneras en que los algoritmos influyen en las experiencias y derechos de niñas, niños y adolescentes. [UNICEF,2021]:

- **Bienestar:** Como estas tecnologías están diseñadas para mantener a los usuarios(as) conectados(as) el mayor tiempo posible, pueden promover contenidos adictivos, violentos o perjudiciales para la salud emocional y física de niñas, niños y adolescentes.
- **Privacidad:** Para personalizar la información que muestran, las plataformas recopilan datos personales (como lo que buscan, observan, comentan o incluso su ubicación) lo que puede resultar en una exposición indebida de su información y generar riesgos para su seguridad.
- **Desigualdad:** Los sistemas algorítmicos no tratan a todos las niñas, niños y adolescentes por igual; pueden ofrecer contenidos educativos o beneficiosos a unos y limitar esa exposición para otros, contribuyendo a reproducir brechas y desigualdades.

Frente a lo anterior, es necesario adoptar un enfoque de prevención que vaya más allá de controlar los contenidos y conductas, por lo que se requiere que también incluya:

- **Transparencia respecto al funcionamiento de los algoritmos:** Que las plataformas digitales expliquen de forma clara cómo deciden qué mostrar a niñas, niños y adolescentes.
- **Evaluaciones previas sobre el impacto en los derechos de niñas, niños y adolescentes:** Revisar previamente si una app o página web puede afectar la seguridad, privacidad o bienestar de las personas antes de ponerla en uso

6

Los algoritmos son programas que deciden qué contenidos mostramos a cada persona en internet.

- **Diseño de productos centrado en la infancia y adolescencia:** Crear plataformas y aplicaciones considerando desde el principio las necesidades y protección de niñas, niños y adolescentes, evitando la acción con daño y no adaptarlas después de una posible exposición al riesgo.

Por otra parte, distintas investigaciones han mostrado que las tecnologías inmersivas —especialmente la realidad virtual— introducen formas particulares de riesgo para niñas, niños y adolescentes. Diversos análisis internacionales, entre ellos los realizados por la OCDE [2025], señalan que la fuerte sensación de presencia y la estimulación multisensorial que caracterizan a estos entornos pueden intensificar el efecto emocional de situaciones como el acoso, el contacto inapropiado o la invasión del espacio personal. Estos impactos resultan especialmente relevantes en edades tempranas, cuando la diferenciación entre experiencias reales y simuladas aún se encuentra en desarrollo.

De igual forma, los estándares de seguridad desarrollados por la Extended Reality Safety Initiative [XRSI, 2024] identifican riesgos adicionales asociados al anonimato de los avatares, la posibilidad de tocamientos virtuales no deseados, la limitada capacidad de moderación en tiempo real y la exposición prolongada en espacios inmersivos que suelen percibirse como seguros o privados. En conjunto, estos hallazgos subrayan la urgencia de incorporar criterios de protección específicos para las tecnologías de realidades inmersivas [Extended Reality- XR] y anticipar los desafíos emergentes que plantean para el bienestar y la seguridad de la niñez y la adolescencia.

En este contexto, las estrategias de prevención, regulación y diseño de plataformas deben integrar una mirada prospectiva sobre el desarrollo y uso de realidades inmersivas, de modo que la identificación de riesgos no se limite exclusivamente a los entornos digitales tradicionales. La rápida expansión de estas tecnologías exige avanzar hacia marcos de gobernanza que contemplen evaluaciones de impacto específicas, mecanismos robustos de supervisión y protocolos de protección adaptados a la interacción corporal y sensorial propia de los entornos XR.

2. Ciclo dinámico de vulnerabilidad digital (análisis complementario)

Con base en la evolución de riesgos documentados por la OECD [que distingue riesgos de contenido, conducta, contacto y consumo]³, este esquema analítico se propone como herramienta estratégica para comprensión y acción:

Fase	Descripción	Ejemplo	¿Qué hacer?
Captación	Es el primer contacto. La niña, niño o adolescente se expone a algo que puede aprovechar de sus emociones, su necesidad de pertenecer o simplemente su curiosidad.	Juegos virales, Micro segmentación publicitaria, Primeros contactos en redes.	Educación a adultos respecto de riesgos Enseñarles a niñas, niños y adolescentes a reconocer riesgos digitales Alertas y campañas de autoridades y escuelas Filtros y herramientas de protección en plataformas

Vinculación	Consolidación de la interacción o dependencia digital. Aquí ya existe una relación o hábito fuerte: la niña, niño o adolescente empieza a depender o a confiar en lo que encontró.	Grooming, uso compulsivo de redes, comunidades de alto riesgo. Adicción a redes o juegos Grupos peligrosos o dañinos	Monitoreo activo por parte de adultos Educación socio-emocional, - Intervención temprana si se detecta algún riesgo.
Explotación	Uso de la dependencia para obtener beneficio sexual, económico o simbólico, por ejemplo: obtención de información, imágenes, dinero, control emocional.	Sextorsión Explotación sexual online Extracción de datos personales.	Denunciar y activar rutas de atención interinstitucional Atención y restablecimiento de derechos de las niñas, niños y adolescentes. Usar las herramientas para rastrear y probar delitos.



Normalización / Diseminación	Es la Integración de la conducta en dinámicas culturales o de consumo que perpetúan el riesgo.	Reenvío de material sexualizado. Gamificación de violencia. Mensajes o discursos de odio que se viralizan.	Campañas públicas, regulación de plataformas. Responsabilidad corporativa activa. Regulación de redes sociales y digitales
---	--	--	--

3. Gobernanza de datos, Inteligencia Artificial y derechos emergentes

La incorporación de la inteligencia artificial y el análisis de datos genera nuevos desafíos para la protección de los derechos humanos. UNICEF (2021) señala que estas tecnologías deben desarrollarse poniendo en el centro a niñas, niños y adolescentes, considerando su etapa de desarrollo, así como la importancia de incorporar criterios de inclusión, equidad, privacidad y seguridad en el desarrollo de plataformas web.

De manera complementaria, la OECD (2025) plantea que las regulaciones no solo deben enfocarse en prevenir daños, sino también en fortalecer la participación infantil, promover la alfabetización digital y asegurar la supervisión adecuada de los productos tecnológicos, anticipando y evitando riesgos emergentes.

En este sentido, se recomienda que los Estados implementen:

- Sistemas de evaluación y control transparente de algoritmos.
- Protocolos de diseño que prioricen la seguridad y la protección de datos desde el inicio.



- Mecanismos que permitan la participación significativa de niñas, niños y adolescentes en la creación de políticas digitales.

4. Bienestar digital y derecho a desconexión

La evidencia actual muestra que la participación digital de niñas, niños y adolescentes debe equilibrarse con espacios de descanso, cuidado de la salud mental y bienestar emocional. Hoy, el bienestar infantil en entornos digitales no depende únicamente del tiempo que pasan en línea, sino también de la calidad de esas experiencias y de la relación que mantienen con adultos, pares y actividades fuera de internet. Este enfoque comprende:

- Reconocimiento del bienestar digital como parte del derecho al desarrollo de la persona menor de 18 años de edad.
- Políticas para uso informado y crítico de la tecnología.
- Promoción de entornos escolares, familiares y comunitarios saludables y corresponsables.

5. Evaluaciones de Impacto de las Tecnologías e Inteligencia Artificial en los Derechos de la Niñez y Adolescencia.

5.1 Fundamentación

Las transformaciones impulsadas por la inteligencia artificial (IA) y la analítica de datos exigen que los Estados y las empresas adopten medidas específicas para garantizar que estas tecnologías no vulneren los derechos de niñas, niños y adolescentes. La Observación General n.º 25 del Comité de los Derechos del Niño y la Niña (2021) y las Directrices de la UNESCO sobre ética en IA (2023) señalan que las decisiones automatizadas deben basarse en la equidad, la transparencia, la responsabilidad y medidas de protección reforzadas. No obstante, la mayoría de las políticas de los Estados aún no cuentan con instrumentos metodológicos que permitan implementar estos principios de manera práctica a lo largo del ciclo de vida de los sistemas de IA.

5.2 Concepto y propósito

La Evaluación de Impacto en Derechos de la Niñez (EIDN) es una herramienta preventiva que permite identificar, medir y mitigar los riesgos que un sistema digital o algorítmico puede generar sobre los derechos de la infancia y adolescencia, incluyendo privacidad, desarrollo, autonomía, igualdad, no discriminación y participación. De acuerdo con la UNICEF [Policy Guidance on AI for Children, 2021] y The Alan Turing Institute [2022], una EIDN debe realizarse antes del diseño, durante el desarrollo y luego del despliegue de cualquier sistema de IA que procese datos de personas menores de 18 años de edad o que pueda influir en sus decisiones, emociones o bienestar.

5.3 Componentes mínimos de una Evaluación de Impacto en Derechos de la Niñez -EIDN

Los estándares internacionales recomiendan que toda evaluación de impacto en infancia contemple, como mínimo:



- **Identificación de la población afectada:** edades, contextos y vulnerabilidades específicas.



- **Evaluación del ciclo de vida del sistema:** fuentes de datos, sesgos en el entrenamiento, mecanismos de supervisión humana y criterios de actualización.



- **Valoración de impacto en derechos clave:** privacidad, no discriminación, libertad de expresión, bienestar digital y protección frente a manipulación o vigilancia.



- **Mecanismos de participación infantil:** consulta adaptada a la edad y el contexto para incluir las percepciones de niñas, niños y adolescentes sobre el uso de la tecnología.



- **Plan de mitigación y monitoreo continuo:** adopción de medidas correctivas y publicación de resultados con transparencia.

5. 4 Relevancia para la política pública y la cooperación internacional

Integrar la EIDN en las políticas nacionales fortalece el principio de protección por diseño y por defecto, previsto en la legislación europea y en la Estrategia Global de IA de la UNESCO. Los países que incorporan este mecanismo —como Irlanda y Finlandia— han iniciado la exigencia de evaluaciones ex ante de impacto sobre la infancia en los proyectos de IA y servicios digitales públicos. En América Latina, la adopción de EIDN permitiría articular los marcos de protección infantil con la Ley 1581 de 2012 sobre protección de datos, la Ley 1098 de 2006 [Código de Infancia y Adolescencia] y la Ley 2489 de 2025 sobre entornos digitales seguros.





ORIENTACIONES PSICOSOCIALES PARA EL ACOMPANIAMIENTO DE CASOS DE RIESGO EN CONTEXTOS DIGITALES





Para la intervención psicosocial en la prevención e identificación de riesgos digitales es fundamental un abordaje basado en el interés superior, la protección integral y el acompañamiento emocional seguro. A continuación, se integran algunas orientaciones:

a. Acompañamiento centrado en la escucha activa

Proporcionar un espacio seguro donde niñas, niños y adolescentes puedan expresar sus experiencias digitales sin temor a sanciones, juicios morales o culpabilización. La escucha respetuosa permite identificar señales de riesgo y comprender la perspectiva del adolescente.

b. Validación emocional y reducción de la culpa

Muchas niñas, niños o adolescentes sienten vergüenza o culpa cuando están involucrados en situaciones de sextorsión, acoso o difusión de imágenes. La intervención debe enfatizar que la responsabilidad recae exclusivamente en el agresor, no en la víctima. Esto disminuye barreras para solicitar ayuda.

c. Recolección de información con enfoque de derechos

Indagar sobre las dinámicas digitales de manera cuidadosa, evitando preguntas que revictimicen. Cuando sea necesario revisar dispositivos, debe hacerse con consentimiento y respeto a la confidencialidad.

d. Orientación para la activación de redes de apoyo

Facilitar la articulación con familia, escuela, equipos territoriales y sistemas de protección, ajustando la intervención a la edad, autonomía progresiva y situación particular del adolescente. En casos de riesgo grave, activar rutas de protección y justicia.

e. Intervención restaurativa cuando sea pertinente

En situaciones de ciberacoso o conflictos entre pares, se pueden aplicar



estrategias restaurativas que promuevan reconocimiento del daño, reparación y transformación de las dinámicas relacionales, siempre garantizando primero la seguridad de la víctima.

CIUDADANÍAS DIGITALES

La ciudadanía digital es un concepto en constante desarrollo que se relaciona con las actitudes, derechos y responsabilidades que las personas asumen en los entornos digitales. Comprende un conjunto de competencias que permiten acceder, comprender, evaluar, crear y compartir información y contenidos en distintos formatos y plataformas, utilizando diversas herramientas de forma crítica, ética y responsable. Su propósito es fomentar una participación activa y consciente en los ámbitos personales, educativos, laborales y sociales dentro del mundo digital (UNESCO Bangkok, 2015).

La UNESCO plantea comprender la ciudadanía digital a partir de tres niveles de participación: **como receptor, como participante y como actor activo**. En cada uno de estos niveles, la persona debe ser capaz de reconocer tanto las oportunidades como los riesgos que surgen en los entornos digitales.

El fortalecimiento de la ciudadanía digital requiere del diseño e implementación de estrategias inclusivas que reconozcan y valoren la diversidad en todas sus formas. Su desarrollo debe abordarse no solo desde el ámbito educativo, sino también desde los espacios públicos, promoviendo la articulación con distintos sectores, organizaciones sociales y medios de comunicación. Impulsar la ciudadanía digital implica generar escenarios permanentes de diálogo y reflexión que trasciendan las herramientas tecnológicas actuales, comprendiendo que este ejercicio también se construye en contextos no digitales (Cobo, 2016).

Ser ciudadano o ciudadana digital significa asumir principios fundamentales como la protección de datos personales, el acceso libre y responsable a la información, la transparencia, la neutralidad en la red, la participación activa, la libertad de expresión con enfoque de derechos, la colaboración y



la defensa de grupos en situación de vulnerabilidad, especialmente niñas, niños y adolescentes. Aunque estos valores exceden lo digital, adquieren especial relevancia en línea; por ello, es indispensable abordar estos temas desde la educación, promoviendo reflexión constante, debate plural y pensamiento crítico. [Cobo, 2016].

El reto actual es avanzar en acciones pedagógicas que formen personas críticas, participativas y conscientes de las oportunidades y riesgos que presentan las tecnologías. Este esfuerzo debe preparar a las nuevas generaciones para involucrarse de manera informada, ética y responsable en la transformación digital.

De igual forma, es necesario dejar atrás estrategias preventivas centradas exclusivamente en generar temor o limitar el uso de las tecnologías. En su lugar, es fundamental fortalecer habilidades socioemocionales que permitan a niñas, niños, adolescentes y personas adultas interactuar con criterio, respeto y empatía en los entornos digitales. Esto implica promover relaciones saludables en línea, acompañar el uso de la tecnología desde el diálogo y la confianza, y fomentar la participación activa en espacios digitales seguros, inclusivos y que favorezcan la convivencia y el ejercicio de derechos [Cobo, 2016].

En la actualidad, ser competente digitalmente implica mucho más que conocer y utilizar dispositivos o plataformas. Supone ejercer un uso responsable y consciente de la tecnología. Esto incluye reconocer y valorar la diversidad, resguardar la información personal y actuar con ética en las interacciones con otras personas. Para ello, es necesario adaptarse continuamente a las normas de convivencia en línea y mantener una postura de cuidado y respeto, especialmente hacia niñas, niños y adolescentes, garantizando su bienestar y el ejercicio pleno de sus derechos en los espacios digitales.

En este sentido, la promoción de la ciudadanía digital debe incorporar una perspectiva de prevención de las violencias hacia niñas, niños y adolescentes, reconociendo que temas como la privacidad, la inclusión, transparencia, participación y la protección son fundamentales para garantizar entornos



digitales seguros y responsables. Es necesario fortalecer desde la formación procesos educativos que fomenten la reflexión crítica, la empatía y el respeto por los demás en los espacios virtuales. De igual manera, se deben impulsar agendas de acción que promuevan el uso responsable y ético de las tecnologías, la denuncia de situaciones de violencia o acoso en línea y la construcción de comunidades digitales protectoras. Estas acciones contribuyen a formar sujetos críticos y comprometidos con la prevención de todo tipo de violencia en el ámbito digital y con la garantía de los derechos de la niñez y la adolescencia (Cobo, 2016).

DERECHOS EN LOS CONTEXTOS DIGITALES:

En 2004, UNICEF promovió una iniciativa internacional enfocada en fomentar el uso seguro y responsable de las tecnologías digitales entre niños, niñas y adolescentes. En ese contexto, se presentó un decálogo que reunió principios esenciales sobre los derechos y deberes de la infancia en el entorno digital. Este documento resaltó la importancia de asegurar el acceso universal a las Tecnologías de la Información y la Comunicación (TIC) con fines educativos, recreativos e informativos, y enfatizó la responsabilidad compartida de familias, gobiernos y actores tecnológicos en la protección de la seguridad digital de la niñez. (UNICEF, 2004)

Se destacan los siguientes derechos en contextos digitales:

- 1. Derecho al acceso a la información:** Sin discriminación por sexo, edad, recursos económicos, nacionalidad, etnia o lugar de residencia. Este derecho se aplicará en especial a los niños, niñas, adolescentes y personas en situación de discapacidad.
- 2. Derecho a la libre expresión y asociación:** Para buscar, recibir y difundir informaciones e ideas de todo tipo por medio de la red. Es importante mencionar que, estos derechos solo se restringirán para garantizar la protección de personas menores de 18 años de edad frente a informaciones perjudiciales para su bienestar, desarrollo e integridad; y para garantizar el cumplimiento de las leyes, la seguridad, los derechos y la reputación de otras personas.

- 
3. **Derecho de los niños, niñas y adolescentes a ser consultados y a dar su opinión:** específicamente cuando se formulen e implementen leyes o normas en la Internet que les afecten.
 4. **Derecho a la protección:** generar acciones contra cualquier forma de explotación o violencias aún en la red.
 5. **Derecho al desarrollo personal y a la educación:** relacionado a todas las oportunidades que las nuevas tecnologías puedan aportar para mejorar su formación y bienestar.
 6. **Derecho a la intimidad en las comunicaciones:** hace mención al derecho a no proporcionar datos personales por Internet, a preservar su identidad y su imagen de posibles usos ilícitos.
 7. **Derecho al esparcimiento, al ocio, a la diversión y al juego:** los juegos y las propuestas de ocio no deben contener violencia, ni mensajes que hagan mención a racismo, sexismo o denigrantes y que respeten los derechos y la imagen de niños, niñas y adolescentes, así como de otras personas.
 8. **Derecho a recibir orientación de padres, madres o cuidadores(as)** para orientar y acordar un uso responsable de las herramientas informáticas.
 9. **Los gobiernos de los países desarrollados deben comprometerse a cooperar con otros países** para facilitar el acceso de estos y sus ciudadanos, y en especial de los niños y niñas, a Internet y otras tecnologías para promover su desarrollo y evitar la creación de una nueva barrera entre los países ricos y los países pobres.
 10. **Derecho a beneficiarse y a utilizar en su favor las nuevas tecnologías** para avanzar hacia un mundo más saludable, pacífico, solidario, justo y respetuoso con el medioambiente, en el que se respeten los derechos de todos las niñas, niños y adolescentes.

Estos derechos constituyen un marco esencial para garantizar que niñas, niños y adolescentes puedan interactuar en el entorno digital de forma plena, equitativa y sobre todo segura. No se trata únicamente de facilitar el acceso a las tecnologías, sino de garantizar que dicho acceso se realice en condiciones de igualdad, respeto, dignidad y protección. El reconocimiento de los derechos digitales refleja una visión integral de la infancia y adolescencia como sujetos activos de derechos, capaces de utilizar las tecnologías para su desarrollo personal, social y educativo.



Por otra parte, garantizar la privacidad y la protección de la identidad digital se convierte en una condición central para prevenir vulneraciones. Es fundamental que niñas, niños y adolescentes aprendan a gestionar su información personal, reconocer qué datos pueden compartir y cuáles deben proteger, identificar señales de contacto inapropiado y comprender el impacto a largo plazo que puede tener la huella digital. Este proceso debe apoyarse en adultos que fomenten el diálogo, establezcan acuerdos de uso responsable, configuren medidas de seguridad adecuadas a la edad y creen un entorno de confianza que permita consultar dudas sin temor a sanciones o reproches.

Asimismo, el fortalecimiento de la participación y de la denuncia segura [o reporte] es clave para la prevención integral en contextos digitales. Tanto adultos(as) como las niñas, niños y adolescentes deben conocer las rutas de orientación y los mecanismos disponibles para solicitar ayuda cuando experimenten situaciones de riesgo, garantizando que sus voces sean escuchadas. La construcción de entornos de confianza favorece que comuniquen inquietudes, reporten contenidos dañinos o alerten sobre interacciones sospechosas, permitiendo activar de manera oportuna medidas de protección psicosocial, educativa o institucional. De este modo, se consolidan prácticas de corresponsabilidad y cuidado mutuo que promueven entornos digitales preventivos, protectores y respetuosos de todos sus derechos.

Es relevante mencionar que la aplicación de estos derechos requiere del compromiso articulado de familias, educadores, instituciones, gobiernos, agentes tecnológicos y sociedad en general, para asumir un rol de corresponsabilidad en la creación de espacios digitales seguros y protectores. Esto implica generar avance en políticas públicas, programas educativos, marcos regulatorios y estrategias de acompañamiento que garanticen el ejercicio efectivo de los derechos digitales de la niñez y la adolescencia.

REFERENCIAS:

Cámara de Representantes. [2024, mayo 30]. Siete de cada diez niños y adolescentes en Colombia han sido víctimas de ciberacoso. Poder Legislativo. <https://poderlegislativo.camara.gov.co/2024/05/30/siete-de-cada-diez-ninos-y-adolescentes-en-colombia-han-sido-victimas-de-ciberacoso/>

Cobo, C. [2016]. La innovación pendiente: Reflexiones [y provocaciones] sobre educación, tecnología y conocimiento. Colección Fundación Ceibal, Debate. Montevideo.

Instituto Colombiano de Bienestar Familiar [ICBF]. [2024, agosto]. Informe Anual Vigencia 2023 ante el Congreso de la República: ESCNIÑAS, NIÑOS Y ADOLESCENTES. https://www.camara.gov.co/sites/default/files/2024-08/Inf_Ley_1336%20de%202009_ESCNIÑAS, NIÑOS Y ADOLESCENTES%202023_FINAL.pdf

- Instituto Colombiano de Bienestar Familiar [ICBF]. [2025, febrero]. Boletín Estadístico. Febrero 2025. <https://www.icbf.gov.co/system/files/boletinestadisticofebrero.pdf>

- Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. [2023, junio 12]. Ciberacoso, ciberdependencia, 'sexting' y 'grooming', los temas del primer Facebook Live del MinTIC. <https://www.mintic.gov.co/portal/715/w3-article-276452.html>

- Procuraduría General de la Nación. [2024, octubre 23]. Violencia sexual, ciberacoso y grooming tendrán vigilancia especial en colegios. <https://www.procuraduria.gov.co/Pages/violencia-sexual-colegios-ciberacoso-grooming-tendran-vigilancia-especial-procuradora.aspx>

UNESCO Bangkok. [2015]. Fostering digital citizenship through safe and responsible use of ICT: A review of current status in Asia and the Pacific as of December 2014. UNESCO Bangkok. http://www.unescobkk.org/fileadmin/user_upload/ict/SRU-ICT/SRU-ICT_mapping_report_2014.pdf

UNICEF España. [2004]. Decálogo de derechos y deberes de los niños en Internet. UNICEF Comité Español.

ANEXO 1.

MATRIZ DE EVALUACIÓN DE RIESGOS DIGITALES - MODELO DE LOS 4Cs

La matriz de evaluación de riesgos se construye a partir del modelo de los 4Cs, desarrollado inicialmente en el Byron Review [2008] y ampliado por EU Kids Online [Livingstone, Haddon & Görzig, 2012; Staksrud & Ólafsson, 2019], UNICEF [2021] y la OCDE [2021].

I. Datos básicos del caso

Nombre [o código]: _____

Edad: _____ Género: _____

Entidad u operador: _____

Fecha de evaluación: ____ / ____ / ____

Evaluador(a): _____

II. Dimensiones de Riesgo [4Cs]

[Marcar, describir y asignar puntaje]

Escala de valoración por indicador

1 = Riesgo leve [evento aislado, sin afectación visible]

2 = Riesgo moderado [repetición, malestar emocional o conductual]

3 = Riesgo alto [delito, coerción, explotación, daño emocional grave]

A. Riesgos de Contenido

Indicador	Descripción breve	Puntaje [1-3]
A1. Exposición a contenido sexual, violento o perturbador.		☐ 1 ☐ 2 ☐ 3

A2. Lenguaje o conductas no acordes a la edad tras consumo digital.		☐ 1 ☐ 2 ☐ 3
A3. Cambios emocionales (miedo, ansiedad, insomnio) asociados a contenidos.		☐ 1 ☐ 2 ☐ 3
A4. Uso de apps/plataformas sin supervisión con alto riesgo algorítmico.		☐ 1 ☐ 2 ☐ 3

Subtotal Contenido [A]: _____ / 12

B. Riesgos de Contacto

Indicador	Descripción breve	Puntaje [1–3]
B1. Contacto con desconocidos (chat, videojuegos, redes).		☐ 1 ☐ 2 ☐ 3
B2. Solicitud de fotos, datos, secretos o videollamadas.		☐ 1 ☐ 2 ☐ 3
B3. Manipulación emocional, presión, chantaje o amenazas.		☐ 1 ☐ 2 ☐ 3
B4. Intentos de encuentro presencial o envío de regalos/dinero.		☐ 1 ☐ 2 ☐ 3

Subtotal Contacto [B]: _____ / 12

C. Riesgos de Conducta

Indicador	Descripción breve	Puntaje [1–3]
C1. Envío de fotos íntimas o sexting no seguro.		☐ 1 ☐ 2 ☐ 3
C2. Ciberacoso (como víctima o agresor/a).		☐ 1 ☐ 2 ☐ 3
C3. Participación en retos peligrosos.		☐ 1 ☐ 2 ☐ 3
C4. Difusión de contenido íntimo de terceros.		☐ 1 ☐ 2 ☐ 3

Subtotal Conducta [C]: _____ / 12

D. Riesgos de Contrato / Comercio

Indicador	Descripción breve	Puntaje [1–3]
D1. Compras no autorizadas, microtransacciones repetidas.		☐ 1 ☐ 2 ☐ 3
D2. Exposición a estafas, apuestas o fraudes.		☐ 1 ☐ 2 ☐ 3
D3. Cesión de datos personales sin comprensión del riesgo.		☐ 1 ☐ 2 ☐ 3
D4. Publicidad agresiva o marketing dirigido con impacto en la conducta.		☐ 1 ☐ 2 ☐ 3

Subtotal Contrato (D): _____ / 12

III. Factores Modulares de Ajuste del Riesgo

[Si aplica, sumar +1 o +2 por factor]

Factor Agravante	+1	+2	Descripción
Historia de violencia previa [familiar, escolar, sexual].	☐	☐	
Vulnerabilidad socioeconómica o barreras de acceso a protección.	☐	☐	
Problemas de salud mental actuales o previos.	☐	☐	
Ausencia total de supervisión adulta en entornos digitales.	☐	☐	
Participación de múltiples agresores o plataformas.	☐	☐	

Total factores de ajuste: _____ / 10 aprox.

IV. Puntuación total

Total = A + B + C + D + Ajustes

Puntaje final: _____ / 58

V. Clasificación del nivel de riesgo

Puntaje total	Nivel	Significado
1-16	Bajo	Situación manejable con orientación preventiva.
17-34	Medio	Riesgo significativo, requiere acompañamiento psicosocial y acciones de escuela o familia.
35-58	Alto	Riesgo grave. Urge activar rutas de protección, justicia o salud mental.

VI. Acciones obligatorias según nivel

Riesgo Bajo

- Orientación a familia y NNA.
- Ajustes de supervisión digital.
- Trabajo educativo en escuela.
- Seguimiento a 30 días.

Riesgo Medio

- Intervención psicosocial.
- Activación de ruta de convivencia escolar [Ley 1620].

- Evaluación emocional/psicológica.
- Remisión a servicios de salud si se observan afectaciones.
- Seguimiento a 15 días.

Riesgo Alto

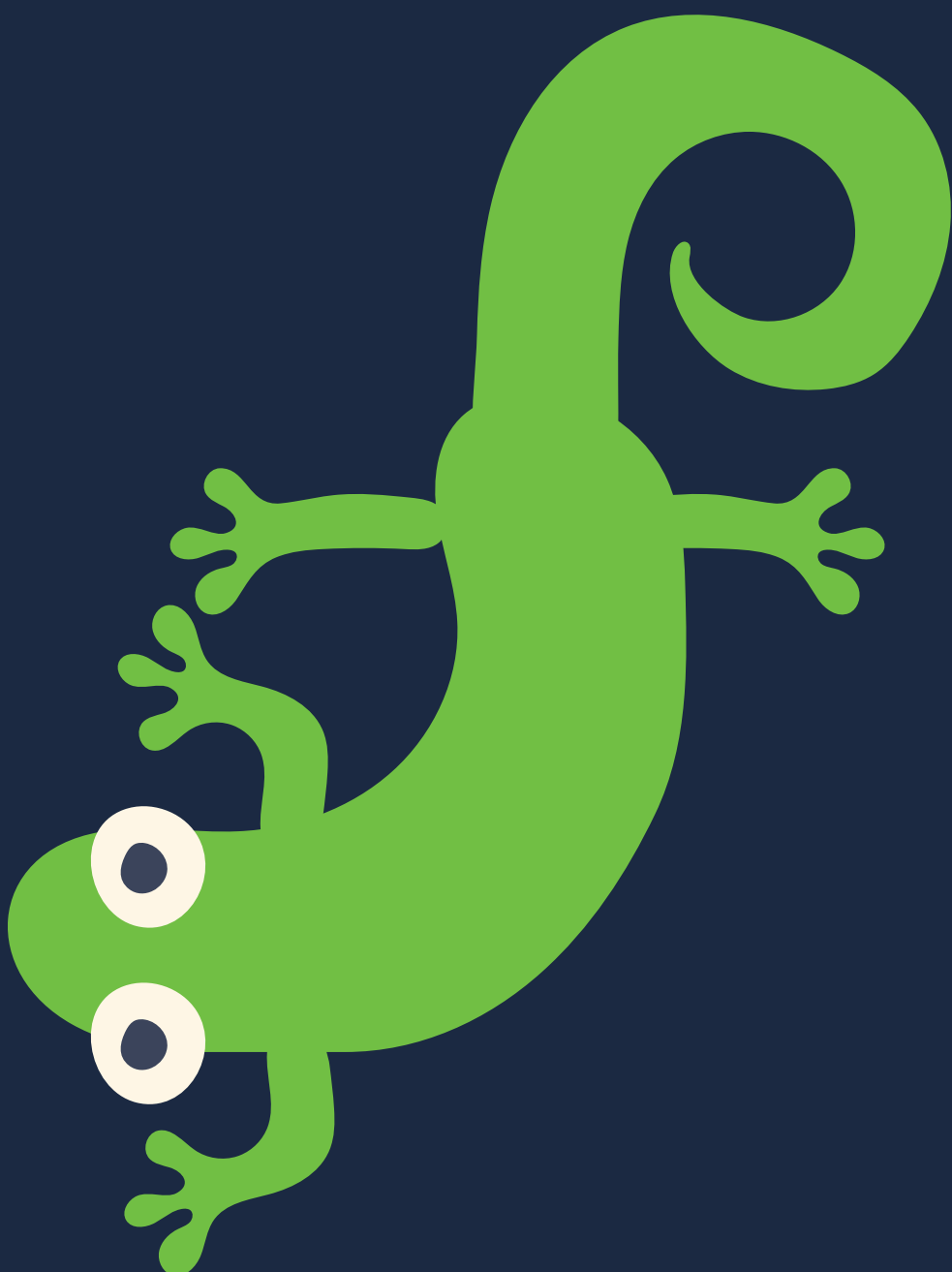
Acciones inmediatas (máximo 24 horas):

- Activar ruta de protección: ICBF / Comisaría.
- Denuncia penal si hay delitos digitales (grooming, explotación, sextorsión).
- Atención en salud mental con prioridad.
- Alertas territoriales si aplica (Secretaría).
- Seguimiento intensivo (48–72 horas + plan de acción).

Vii. Recomendaciones específicas del profesional que realiza la identificación

[Escribir análisis cualitativo brevemente]

Viii. Firma del profesional



CUIDAR, PROTEGER Y ACOMPañAR

#VocesQuePrevienen

Guía para la identificación de riesgos de violencias
en entornos digitales con énfasis en Explotación
Sexual Comercial de Niñas, Niños y Adolescentes.

TE ESCUCHO
#VocesQuePrevienen
las violencias



LÍNEA DE
ATENCIÓN A
NIÑOS, NIÑAS
Y ADOLESCENTES.
PROTECCIÓN EMERGENCIA-ORIENTACIÓN

Línea gratuita nacional ICBF:
01 8000 91 80 80
www.icbf.gov.co

@icbfcolombiaoficial

@ICBFColombia

@icbfcolombiaoficial

ICBFColombia

En convenio con:



Naciones Unidas
Oficina contra
la Droga y el Delito



**BIENESTAR
FAMILIAR**