

PROTOCOLO DE ACTUACIÓN FRENTE A
SITUACIONES DE VIOLENCIA DIGITAL
DETECTADAS EN EL SISTEMA NACIONAL DE EDUCACIÓN



EQUIPO TÉCNICO

María Brown Pérez
Diana Castellanos Vela
Lorena Peñaherrera Vaca
Andrea Flores Ruilova
Gloria Vinueza Simbaña
Jennifer Barrera Barrera
Camila Banda Capelo
Ana Navas Cueva
Roxana Loor Feicán
Carolina Velez Estrada

EQUIPO EXTERNO

ChildFund Internacional
Instituto Interamericano del Niño, la
Niña y Adolescentes -OEA
Consejo Nacional para la Igualdad
Intergeneracional
Defensoría del Pueblo
Unicef Ecuador

DISEÑO Y DIAGRAMACIÓN

Carla Jarrín Arboleda

Primera Edición, 2023
© Ministerio de Educación
Av. Amazonas N34-451 y Av. Atahualpa
Quito-Ecuador
www.educacion.gob.ec

La reproducción parcial o total de esta publicación, en cualquier forma y por cualquier medio mecánico o electrónico, está permitida siempre y cuando sea autorizada por los editores y se cite correctamente la fuente.

**DISTRIBUCIÓN GRATUITA
PROHIBIDA SU VENTA**

Ministerio de Educación





Contenido

Introducción.....	7
Ámbito y población objetiva.....	11
Objetivos.....	12
General.....	12
Específicos.....	12
Enfoques del documento.....	13
a. Derechos humanos.....	13
b. Primera Infancia, Niñez y Adolescencia.....	13
c. Género.....	14
d. Movilidad Humana.....	14
e. Intercultural	14
f. Intergeneracional.....	14
g. Discapacidades	14
h. Interseccional.....	14
i. Plurinacionalidad	14
j. Restaurativo	14
Glosario.....	15
Capítulo 1. Marco Legal.....	19
Declaración Universal de Derechos Humanos.....	19
Comité de los Derechos del Niño de las Naciones Unidas - Observación General N°. 25 (2021).....	19
Constitución del Ecuador.....	20
Código Orgánico Integral Penal.....	20
Código de la Niñez y Adolescencia.....	21
Ley Orgánica de Educación Intercultural.....	21
Ley Orgánica de Protección de Datos Personales.....	23
Política pública por una Internet Segura para niñas, niños y adolescentes	24
Capítulo 2. Marco Teórico Referencial.....	25
Alfabetización digital.....	25

Ciudadanía digital.....	25
Competencias digitales.....	26
Uso seguro de la Internet.....	26
Huella digital.....	26
Prácticas online y offline.....	27
Lo íntimo, lo privado y lo público.....	27
Brecha digital.....	28
Nivel de riesgo.....	28
Capítulo 3. Protocolo de actuación frente a situaciones de violencia digital.....	33
Prevencción integral.....	33
Detección.....	39
Intervención-actuación.....	46
Derivación.....	49
Seguimiento.....	51
Reparación.....	53
Rutas frente a casos de violencia digital	55
Anexos.....	59
Referencias.....	62

Introducción

La utilización de tecnologías digitales de parte de las niñas, niños y adolescentes es una fuente importante de información, establecimiento de relaciones y entretenimiento. Sin embargo, es necesario tener en cuenta que estas tecnologías también pueden representar peligros y vulnerar sus derechos. Según estudios de Unicef, más de un tercio de los usuarios de la Internet en todo el mundo son menores de 18 años y el 56% de las niñas, niños y jóvenes entre 15 y 24 años ha experimentado algún tipo de violencia en línea (Unicef, 2019).

La falta de legislación clara en ciberseguridad es un problema mundial. Según un informe de la Unesco y la Unión Internacional de Telecomunicaciones, es crucial modernizar las leyes, ya que solamente el 72% de los países tienen legislación funcional en ciberdelincuencia. Esta falta de definiciones claras y coordinación entre agencias permite que los criminales operen impunemente a nivel global (Unesco, 2019).

En Ecuador, el acceso a la Internet ha aumentado considerablemente, alcanzando el 60,4% de los hogares en el país (INEC, 2021). De este porcentaje, el 73,3% lo utiliza principalmente para actividades comunicacionales y redes sociales. Esta realidad plantea la posibilidad de enfrentar riesgos y situaciones de violencia digital (ChildFund, 2023).

Con el objetivo de obtener una visión más detallada, el Ministerio de Educación, en colaboración con Unicef, realizó una en-

cuesta dirigida a adolescentes y jóvenes a través de la plataforma U-Report. La encuesta estuvo activa desde el 5 al 25 de julio de 2022 y contó con la participación de 26.311 personas. Para el análisis estadístico se consideró como población objeto a las niñas, niños y adolescentes de 12 a 18 años, lo que representa el 77,44% de las personas en este grupo de edad, es decir, 20.376 personas encuestadas.

Además, se desglosaron los datos en dos subgrupos etarios: de 12 a 14 años y de 15 a 18 años, que corresponden al 36,93% y al 40,52% de los encuestados, respectivamente. En cuanto a la distribución de género, el 52,33% de las personas de 12 a 14 años son mujeres, mientras que, en el grupo de 15 a 18 años, el 52,83% son mujeres (Unicef, 2022).

Estos datos permiten tener una mejor comprensión de lo que piensan y comparten las niñas, niños y adolescentes en la Internet, así como identificar los riesgos y desafíos a los que se enfrentan.

En cuanto al uso de redes sociales de parte de las niñas, niños y adolescentes, se observa que tanto en el grupo etario de 12 a 14 años como en el de 15 a 18 años, las plataformas más utilizadas son WhatsApp, Facebook y

TikTok. De la información compartida en las redes sociales, se observa que las y los adolescentes de 15 a 18 años tienden a compartir más memes no ofensivos (35,02%), mientras que las y los adolescentes de 12 a 14 años comparten más información educativa de interés (25,36%). Además, se evidencia que las y los adolescentes de 15 a 18 años comparten más contenidos de opinión social y actividades personales en comparación con los de 12 a 14 años (Unicef, 2022).

Sobre el uso de la Internet y redes sociales, las y los adolescentes de 15 a 18 años utilizan principalmente estas herramientas para comunicarse con amigos y familiares, obtener información personal y entretenerse. Por su parte, las y los adolescentes de 12 a 14 años también las utilizan para comunicarse y entretenerse, pero en menor medida. Además, se destaca que las y los adolescentes de 12 a 14 años hacen un mayor uso de las redes sociales para la investigación y el aprendizaje en comparación con los de 15 a 18 años (Unicef, 2022).

En relación con los riesgos que enfrentan las niñas, niños y adolescentes en la Internet, los resultados de la encuesta revelan que un porcentaje significativo ha experimentado amenazas y contenidos nocivos en línea. **Según los datos, 4 de cada 10 adolescentes han enfrentado riesgos en línea como: ciberacoso, hacking, contenidos nocivos o publicación de información privada.** Se destaca que niñas, niños y adolescentes de 12 a 14 años enfrentan más riesgos de retos virales y grooming, mientras que las y los de 15 a 18 años se ven más afectados por el grooming. Estos hallazgos ponen de manifiesto la importancia de abordar de manera integral los riesgos a los cuales se enfrentan estas poblaciones en el entorno digital.

En cuanto a la búsqueda de ayuda frente a amenazas, se observa que la mayoría de las y los adolescentes de ambos grupos de edad recurren a sus familias. Sin embargo, las y los adolescentes de 15 a 18 años tienden a buscar más ayuda de sus compañeros que de instancias competentes como la Fiscalía; prefieren también buscar ayuda policial en lugar de ayuda de sus docentes, a diferencia de las y los adolescentes de 12 a 14 años quienes sí buscan ayuda en sus docentes. Estos datos resaltan la necesidad de fomentar la confianza y el diálogo entre los adolescentes y las personas adultas, así como fortalecer la capacitación y el apoyo de las instituciones educativas y de las instituciones públicas y privadas.

En relación con las consultas de información o investigación en la Internet, el 34,57% de los adolescentes verifican la información cuando realizan consultas de información o investigaciones en el internet, mientras que el 25,58% la obtienen con la primera opción de búsqueda. Por otro lado, el **6,49% de adolescentes confían en la información del internet sin verificar.**

En relación con la protección de datos o información en los dispositivos electrónicos, el **17,44% no realiza ninguna acción de protección**, como la instalación de antivirus o la realización de copias de seguridad, entre otros. Además, se evidencia que niñas, niños y adolescentes comparten información personal en línea como correos electrónicos, nombres completos e intereses. Estos resultados enfatizan la importancia de promover la alfabetización digital, el manejo de información y la conciencia sobre la privacidad en el uso de la Internet.

Las opiniones de niñas, niños y adolescentes participantes en la encuesta sobre el uso de las redes sociales e Internet alertan sobre la necesidad de trabajar en la autoprotección frente a riesgos o amenazas en entornos digitales; se requiere fortalecer su capacidad crítica para convivir en línea, así como definir una ruta clara de atención frente a la vulneración de sus derechos.



En este contexto, 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 Constitucional².

El protocolo ha sido desarrollado a través de un proceso colectivo que involucra a diversos actores y contó con la participación activa de niños, niñas y adolescentes, quienes han desempeñado un papel fundamental en la identificación de estrategias de prevención y protección. Contó con el apoyo técnico de ChildFund, el Consejo Nacional para la Igualdad Intergeneracional y el Instituto Interamericano del Niño, la Niña y Adolescentes (IIN - OEA).

En la formulación del protocolo se acogieron los aportes de niñas, niños y adolescentes representantes de los Consejos Consultivos, representantes de los Consejos Cantonales de Protección de Derechos, las Juntas Cantonales de Protección de Derechos, la Defensoría del Pueblo, la Fiscalía General del Estado, la Secretaría de Educación Intercultural Bilingüe y Etnoeducación, la comunidad educativa, incluyendo autoridades, docentes, profesionales del Departamento de Consejería Estudiantil (DECE) y familias.

También destacamos los aportes realizados desde las y los adolescentes y jóvenes que forman parte de Unicef; desde el Movimiento Por Ser Niña y desde la Red de Organizaciones por la Defensa de los Derechos de la Niñez y Adolescencia (RODDNA). Este enfoque participativo ha permitido abordar de manera integral los riesgos en la Internet y establecer lineamientos de actuación para garantizar la protección de los derechos de las niñas, niños y adolescentes en el sistema educativo.

2 Esta sentencia examinó un caso en el que una estudiante compartió fotos íntimas de una compañera, resultando en su sanción con la suspensión y retiro de su dispositivo electrónico. La Corte Constitucional determinó que los procedimientos sancionatorios en el ámbito educativo deben considerar un enfoque restaurativo y el cumplimiento de un debido proceso. Como medida reparatoria, se ordenó la creación de normativa y protocolos que aborden el fenómeno del sexting en el contexto educativo. Esta normativa incluirá orientaciones generales para prevenir y educar a niños, niñas y adolescentes en los riesgos y el uso responsable de las TIC. Las normativas serán elaboradas con la participación activa de niños, niñas y adolescentes, pues involucran sus derechos y obligaciones en el ámbito educativo.

Ámbito y población objetivo

El presente documento es de aplicación obligatoria para todas las instituciones educativas de sostenimiento fiscal, municipal, fiscomisional y particular, en todos sus niveles: inicial, básica y bachillerato (técnico, técnico profesional y complementario en artes) del Sistema Nacional de Educación. Asimismo, será aplicable en todos los programas de educación especializada e inclusiva, en las modalidades presencial, a distancia, semipresencial, escolaridad inconclusa y en todos los programas educativos que genere el Ministerio de Educación.

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.

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.

Además, fue emitido mediante Acuerdo Ministerial MINEDUC-MINEDUC-2023-00054-A, publicado el 11 de septiembre de 2023.



Objetivos

General

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

Específicos

- Informar a la comunidad educativa sobre el uso seguro y la identificación de riesgos o vulneraciones de derechos en entornos virtuales, para facilitar procesos adecuados de intervención y/o protección.
- Definir lineamientos de actuación ante situaciones de violencia digital detectadas o cometidas en el ámbito educativo, desde una perspectiva de protección integral.
- Fortalecer la coordinación interinstitucional que facilite la investigación y sanción de hechos de violencia digital en contra de niñas, niños y adolescentes; así como la restitución de sus derechos.

Enfoques del documento

Un enfoque para la aplicación de derechos de niñas, niños y adolescentes es un conjunto de principios, valores y estrategias que se utilizan para garantizar el respeto y la protección de los derechos de la infancia y adolescencia. Los enfoques de protección y derechos están ligados al principio del interés superior del grupo objetivo, que establece que todas las decisiones y acciones relacionadas con niñas, niños y adolescentes deben considerar su bienestar y desarrollo integral.

El entorno digital no fue diseñado, en un principio, para las niñas, niños y adolescentes; sin embargo, desempeña un papel importante en su vida. En este sentido, la Observación General 25 del Comité de los Derechos del Niño manda a los Estados: “a cerciorarse de que, en todas las actuaciones relativas al suministro, la regulación, el diseño, la gestión y la utilización del entorno digital, el interés superior de todos los niños sea una consideración primordial” (ONU, 2021). El presente documento sustenta su abordaje en los siguientes enfoques:

a. Derechos Humanos: pone como centro al ser humano, tanto en su dimensión individual como social. La educación es un derecho que permite desarrollar otros tipos de derechos para alcanzar una vida digna.

b. Primera Infancia, Niñez y Adolescencia: obliga a que las necesidades y los derechos, así como la opinión y la participación de ellas y ellos estén en el centro de todas las actividades financieras, administrativas, pedagógicas, curriculares y extracurriculares, así como las políticas públicas que establezcan las distintas instancias o sujetos de la comunidad educativa en el ámbito de sus competencias, contemplando su interés superior.

c. Género: considera las diferentes oportunidades que tienen las mujeres y los hombres, sin discriminación por razones de orientación sexual o identidad de género, las interrelaciones existentes entre ellas y ellos, los distintos papeles que socialmente se asignan las funciones y responsabilidades distintas a la mujer y al hombre. Esto a su vez determina diversas formas de acceder a los recursos materiales o no materiales.

d. Movilidad Humana: se refiere a las distintas dinámicas de la movilidad humana que incluye el ingreso, la salida, tránsito o permanencia en un lugar diferente al de origen o residencia habitual y retorno, con independencia de su nacionalidad y condición migratoria.

e. Intercultural: supone un respeto por las diferencias, reconoce y respeta el derecho a la diversidad y fomenta la interacción entre culturas y pueblos de una forma equitativa, donde se concibe que ningún grupo cultural se encuentra por encima del otro, reconoce y valora los aportes de todos ellos en la sociedad. Alude al reconocimiento de la diversidad cultural, otorgando legitimidad a las representaciones, concepciones y prácticas culturalmente distintas y promueve el conocimiento y respeto mutuo entre culturas.

f. Intergeneracional: la educación a lo largo de la vida determina la necesidad de establecer un diálogo entre grupos de personas de diferentes edades pero que ejercen roles comunes.

g. Discapacidades: considera a la discapacidad como una circunstancia social que excede las características psico-biológicas de un individuo. Se asume a las personas con discapacidad como sujetos de derechos, que aún deben enfrentar barreras de distinta índole para que su participación en la sociedad suceda en igualdad de condiciones. Cuestiona prácticas asistencialistas o discriminatorias y se otorga legitimidad a las diferencias de cada individuo.

h. Interseccional: plantea que para velar por el ejercicio de los derechos de las niñas, niños y adolescentes es preciso reconocer como diversas categorías como el género, el origen étnico, el origen nacional, las discapacidades, la condición socioeconómica u otras situaciones que confluyen y operan inseparable y simultáneamente.

i. Plurinacionalidad: consiste en el reconocimiento de las formas tradicionales y costumbres de las comunas, comunidades, pueblos y nacionalidades en el Sistema Nacional de Educación.

Adicionalmente, se ha considerado fundamental la inclusión del siguiente enfoque:

j. Restaurativo: busca reparar el daño causado a niñas, niños y adolescentes, involucrando a todas las partes afectadas en el proceso de reparación y responsabilización. Identifica acciones distintas al esquema punitivo y plantea la transformación de los conflictos desde la aceptación de responsabilidades y la reparación del daño. También gestiona las relaciones humanas de manera más horizontal, democrática y participativa.

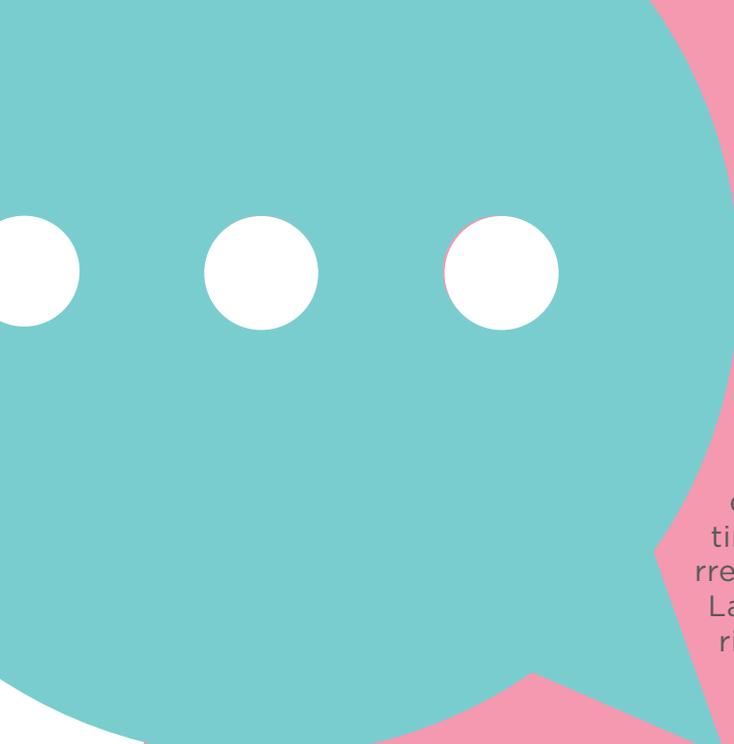
Glosario

Abuso sexual infantil en línea: se presenta de diferentes maneras y niveles de riesgo; niñas, niños y adolescentes pueden ser contactados en línea con el propósito de distribuir imágenes y videos de naturaleza sexual. Además, la comunicación online puede ser la antesala de un futuro abuso y/o explotación sexual en persona, una vez que acceden a encontrarse con alguien tras la comunicación en línea (ECPAT, 2016).

Bloquear: negar el acceso de una persona a publicaciones, chats u otras actividades en línea de la o el usuario. (Ministerio de Educación de Colombia, 2021).

Ciberadicción o abuso del uso de la Internet: el uso abusivo de las Tecnologías de la Información y la Comunicación (TIC) puede degenerar en una adicción con consecuencias físicas y emocionales (Fundación Paniamor, 2017).

Ciberacoso o cyberbullying: sucede cuando alguien es atormentado, amenazado, acosado, humillado o avergonzado por medio de la Internet, medios interactivos, tecnologías digitales o teléfonos móviles. Se desarrolla entre pares (estudiantes) con la intención de hacer daño y de manera repetitiva contra una persona o un grupo de personas. Es una práctica que suele originarse en contextos escolares de manera presencial (acoso escolar) y luego trasciende al entorno digital o viceversa. Este tipo de violencia puede desembocar en situaciones de pérdida de autoestima, ansiedad, soledad, discriminación y, en algunos casos, en el suicidio (Ministerio de Educación de Colombia, 2022).



Difusión no consentida de imágenes: es una situación de violencia que ocurre cuando alguien comparte, reenvía o publica, en entornos digitales, contenido íntimo de otra persona sin su consentimiento. Estas imágenes pueden haber sido recibidas en forma privada (sin permiso para compartirlas) o robadas de dispositivos. También ocurre a través de un grupo de personas amigas. Las principales víctimas son mujeres (Ministerio de Educación Argentina, Argentina, 2021).

Discursos de odio: es la promoción de textos discriminatorios sobre la base de prejuicios y estereotipos, difamando a personas o grupos. Se viraliza en redes sociales, perpetuándose indefinidamente; aísla, margina y excluye a las víctimas, violando valores democráticos y amenazando a la convivencia social (Ministerio de Educación Argentina, Argentina, 2021).

Exclusión digital: sacar a una persona de un chat o grupo al que pertenecía o pretende pertenecer; bloquearla para que no pueda continuar participando (Unesco, 2020).

Explotación sexual de niñas, niños y adolescentes en línea: incluye todos los actos de naturaleza sexual cometidos contra una niña, niño o adolescente, a través de la utilización de la Internet como medio de explotación sexual. (ECPAT, 2016).

Exposición a contenidos nocivos: se refiere al acceso o exposición de niñas, niños y adolescentes a contenido violento, sexualizado o generador de odio, siendo perjudicial para su desarrollo (ECPAT, 2016).

Flaming: son mensajes o publicaciones a través de redes sociales o comunidades virtuales con lenguaje violento, agresivo y/o vulgar, el cual es reiterativo en su intención de humillar e intimidar (Mineduc, 2021).

Grooming: se refiere a la interacción en redes sociales que realizan comúnmente personas adultas con menores de 18 años; se ganan su confianza al hacerse pasar por un niño, niñas o adolescentes con el fin de obtener material íntimo o sexualmente explícito, propiciando situaciones de extorsión, abuso o explotación sexual. Existen dos tipos de grooming: el primero, donde el acosador obtiene material sexual de la víctima sin haber generado una relación previa y lo utiliza para extorsionarla. El segundo, donde el acosador busca generar confianza previamente para que la víctima entregue material sexual que luego utiliza para chantajearla (CNII, 2020).

Haters o bullies: personas que critican o acosan a otros en línea (Ministerio de Educación de Colombia, 2022).

Harassment: se refiere a la denigración, amenaza e insulto constante a alguien a través de correos electrónicos o mensajes de celular, incluyendo la creación de rumores o el enviar fotos humillantes (Mineduc, 2021).

Hipersexualización infantil: es la sexualización de las expresiones, posturas o códigos de vestimenta considerados como demasiado precoces (Methaodos, 2018).

Lolicon/Shotacon: relaciones sentimentales y/o sexuales entre preadolescentes y personas mayores de edad a través de la red (Mineduc, 2021).

Meme: se refiere a una imagen, video o pieza de contenido que se utiliza ampliamente en línea y se comparte a través de las redes sociales (Ministerio de Educación de Colombia, 2022).

Netiqueta: es un conjunto de normas de comportamiento en línea para comunicarse de manera respetuosa y efectiva en entornos digitales. Se enfoca en el respeto hacia los demás, claridad en la comunicación, privacidad y seguridad de la información (Ministerio de Educación de Colombia, 2022).

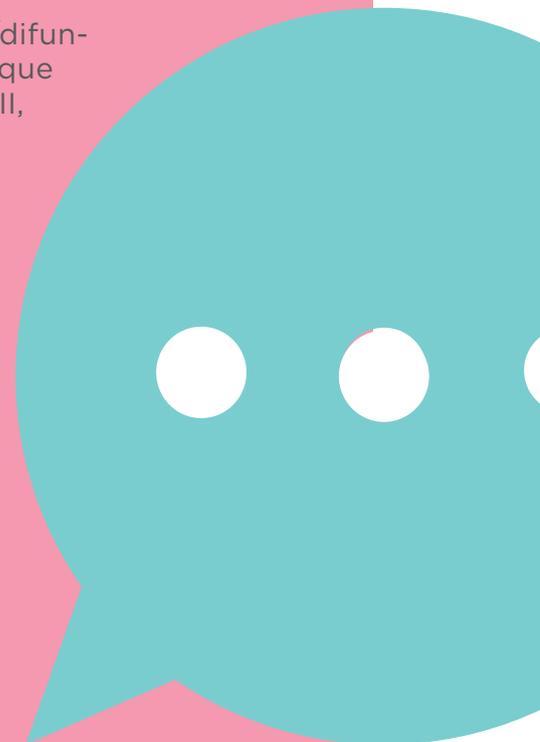
Nomofobia: miedo irracional a no estar cerca del teléfono móvil (Ramos, 2017).

Noticias falsas/fake news: son contenidos engañosos, creados con la intención de perjudicar a personas o grupos, generalmente por motivos políticos o económicos. Estas noticias se difunden rápidamente en el espacio virtual y son difíciles de eliminar, ya que suelen ser anónimas. Su alcance es ilimitado y perduran en el tiempo (Federación Internacional de Periodistas, 2021).

Outing: forma de ciberbullying que consiste en publicar/difundir imágenes, mensajes o correos íntimos, sexuales o que podrían avergonzar a una niña, niño o adolescente (CNII, 2020).

Pack: es un conjunto de imágenes o videos íntimos compartidos a través de plataformas o redes sociales (CNII, 2020).

Paliza feliz/happy slapping: ocurre cuando una persona o grupo golpea a otro, mientras el hecho es grabado en dispositivos móviles para difundirlo en las redes sociales, con la intención de burlarse o ridiculizar a la víctima (Mineduc, 2021).



Phishing: es una suplantación de identidad. Se trata de un modelo de abuso o delito informático (ECPAT, 2016).

Pornografía infantil: explotación y utilización de una niña, niño o adolescente para la creación de material pornográfico (ECPAT, 2016).

Pornovenganza: es la difusión no consensuada de contenido sexual explícito con el objetivo de vengarse o humillar (Ministerio de Educación de Ecuador, 2020).

Portalitis: molestias y dolores musculares producidos por el uso excesivo del teléfono móvil (Ministerio de Educación de Ecuador, 2020).

Sexting/sexteo: se refiere al envío voluntario de fotografías o videos sexualmente explícitos, a través de dispositivos móviles. Es una práctica común entre personas de un abanico de edades cada vez más amplio de la que, en ocasiones, se desprenden situaciones de riesgo para la persona que la realiza, pues su intimidad puede verse vulnerada cuando el receptor del material lo comparte con otras personas (Ministerio de Educación de Colombia, 2022).

Sextorsión: es una forma de chantaje en la que una persona amenaza con difundir imágenes o información sexualmente explícita de otra persona a menos que se cumplan ciertas demandas (CNII, 2020).

Stalking: la práctica de acechar a alguien, observar su comportamiento o actividades sin su conocimiento o consentimiento (Mineduc, 2021).

Troll: es una persona que publica mensajes provocativos u ofensivos en línea con el fin de generar respuestas emocionales en otros usuarios (Ministerio de Educación de Colombia, 2021).

Virus: programa introducido subrepticamente en la memoria de una computadora que, al activarse, afecta su funcionamiento, destruyendo total o parcialmente la información almacenada (Real Academia de la Lengua, 2023) .

Violencia digital: es aquella violencia que se comete y expande a través de medios digitales como redes sociales, correo electrónico, aplicaciones de mensajería móvil, entre otros, que casusa daños a la dignidad, a la propia imagen, a la integridad, privacidad y a la seguridad de las víctimas (ONU Mujeres, 2020).



Capítulo 1. Marco Legal



La Convención sobre los Derechos del Niño establece en su artículo 11 que los Estados deben adoptar medidas para prevenir la victimización y la explotación de niñas, niños y adolescentes, incluyendo aquellas que se produzcan en el ámbito virtual. En su artículo 39 señala que los Estados adoptarán medidas apropiadas para promover la recuperación física y psicológica y la reintegración social de toda niña, niño y adolescente víctima de cualquier forma de abandono, explotación o abuso, tortura u otra forma de trato o castigo cruel, inhumano o degradante o víctima de conflictos armados (ONU, 1989).

El Comité de los Derechos del Niño de las Naciones Unidas emitió la Observación General Nro. 25 (2021), en relación con la protección de los derechos de la niñez en los espacios virtuales y señala que los Estados deben vigilar que niñas y niños tengan acceso igual y efectivo al entorno digital en lo que sea importante y beneficioso para ellos y ellas. Los Estados también deben tomar todas las medidas necesarias para que ningún niño o niña sufra exclusión; para que tengan acceso gratuito y seguro, así como el tomar medidas eficaces para prevenir la discriminación (por sexo, raza, religión, nacionalidad, idioma o cualquier otro motivo) y las comunicaciones que transmitan odio o un trato injusto cuando utilizan esas tecnologías (ONU, 2021).

El Comité de los Derechos del Niño también exhorta a los Estados a velar por que en toda acción realizada en los medios digitales siempre se tenga en cuenta el interés y los derechos de niñas, niños y adolescentes, incluidos sus derechos a buscar, recibir y difundir información, a ser protegidos de todo daño y a que sus opiniones sean tomadas en cuenta. Además, el Comité señala que los Estados deben vigilar el uso de los dispositivos digitales de manera que no sustituyan el contacto entre niños-niñas y padres o tutores, que es esencial para su crecimiento. Adicionalmente, se exhorta el fomentar que niños, niñas y adolescentes participen de los asuntos que los afectan y que conozcan los medios digitales disponibles y reciban capacitación para usarlos.

La **Constitución de la República del Ecuador** en su **artículo 347**, numeral 1, establece que será responsabilidad del Estado: “Fortalecer la educación pública y la educación; asegurar el mejoramiento permanente de la calidad, la ampliación de la cobertura, la infraestructura física y el equipamiento necesario de las instituciones educativas públicas”. En el numeral 6 señala que es responsabilidad del Estado: “Erradicar todas las formas de violencia en el sistema educativo y velar por la integridad física, psicológica y sexual de las estudiantes y los estudiantes (...)”. En el numeral 8 señala: “Incorporar las tecnologías de la información y comunicación en el proceso educativo y propiciar el enlace de la enseñanza con las actividades productivas o sociales”. En el numeral 11 expresa: “Garantizar la participación de estudiantes, familias y docentes en los procesos educativos” (Ecuador A. N., 2008).

El **Código de la Niñez y Adolescencia** en su **artículo 11** señala que:

El interés superior del niño es un principio que está orientado a satisfacer el ejercicio efectivo del conjunto de los derechos de los niños, niñas y adolescentes; e impone a todas las autoridades administrativas y judiciales y a las instituciones públicas y privadas, el deber de ajustar sus decisiones y acciones para su cumplimiento. Para apreciar el interés superior se considerará la necesidad de mantener un justo equilibrio entre los derechos y deberes de niños, niñas y adolescentes, en la forma que mejor convenga a la realización de sus derechos y garantías. Este principio prevalece sobre el principio de diversidad étnica y cultural. El interés superior del niño es un principio de interpretación de la presente Ley. Nadie podrá invocarlo contra norma expresa y sin escuchar previamente la opinión del niño, niña o adolescente involucrado, que esté en condiciones de expresarla (Del Ecuador, C.N., 2003).

El Código de la Niñez y Adolescencia en su **artículo 52** señala las prohibiciones relacionadas con el derecho a la dignidad e imagen; específicamente, en el numeral 1 indica que se prohíbe:

1. La participación de niñas, niños y adolescentes en programas, mensajes publicitarios, en producciones de contenido pornográfico y en espectáculos cuyos contenidos sean inadecuados para su edad. 2. La utilización de niñas, niños y adolescentes en programas o espectáculos de proselitismo político o religioso (...).

En el **artículo 53** señala que:

(...) Sin perjuicio de la natural vigilancia de los padres y maestros, niñas, niños y adolescentes tienen derecho a que se respete la intimidad de su vida privada y familiar y la privacidad e inviolabilidad de su domicilio, correspondencia y comunicaciones telefónicas y electrónicas, de conformidad con la ley. Se prohíbe las injerencias arbitrarias o ilegales en su vida privada (Del Ecuador, C.N., 2003).

La **Ley Orgánica de Educación Intercultural** dispone en su **artículo 6**, que la principal obligación del Estado es el cumplimiento pleno, permanente y progresivo de los derechos y garantías constitucionales en materia educativa. Los principios y fines establecidos en esta ley señalan:

(...) h. Erradicar todas las formas de violencia en el sistema educativo y velar por la integridad física, psicológica y sexual de la comunidad educativa, con particular énfasis en las y los estudiantes (...) j. Garantizar la alfabetización digital y el uso de las tecnologías de la información y comunicación en el proceso educativo, y propiciar el enlace de la enseñanza con las actividades productivas o sociales; n. Garantizar la participación activa de estudiantes, familias y docentes en los procesos educativos; r. Asegurar que todas las entidades educativas desarrollen una educación acorde con participación ciudadana, exigibilidad de derechos, inclusión y equidad, igualdad de género, sexualidad y ambiente, con una visión transversal y enfoque de derechos (...) (Ecuador A. N., Ley Orgánica de Educación Intercultural, 2011).

De igual manera, el **Reglamento a la Ley Orgánica de Educación Intercultural**, en el **artículo 2**, último inciso señala que:

(...) El Sistema Nacional de Educación promoverá, entre los miembros de la comunidad educativa, el desarrollo de competencias digitales y de capacidades para gestionar el uso seguro del Internet y demás tecnologías, respetando cabal y permanentemente los derechos y responsabilidades que garanticen la convivencia armónica.

El **Código Orgánico Integral Penal** en su **artículo 103** establece:

La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años.

El **artículo 104** señala que:

La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio, para uso personal o para intercambiar pornografía de niñas, niños y adolescentes, será sancionada con pena privativa de libertad de diez a trece años (Ecuador A. N., Código Orgánico Integral Penal, 2014).

El **artículo 173** establece que:

La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años. Cuando el acercamiento se obtenga mediante la coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años. La persona que suplantando la identidad de un tercero o mediante el uso de una identificación falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena de tres a cinco años.

También, en el **artículo 174** se indica que son delitos la oferta de servicios sexuales con menores de dieciocho años por medios electrónicos (Ecuador A. N., Código Orgánico Integral Penal, 2014).

El **artículo 178** tipifica el delito de violación a la intimidad:

La persona que, sin contar con consentimiento o autorización legal acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años (Ecuador A. N., Código Orgánico Integral Penal, 2014).

La **Ley Orgánica de Protección de Datos Personales**, en su **artículo 1**, señala que su objeto y finalidad es el garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.

Además, en su **artículo 8.-** Consentimiento, señala que:

Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. El consentimiento será válido, cuando la manifestación de la voluntad sea:

- 1) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento;
- 2) Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento;
- 3) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia,
- 4) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular.

El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento. El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos.



Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste que dicho consentimiento se otorga para todas ellas (Ecuador A. N., Ley Orgánica de Protección de Datos Personales, 2021).

Se señala, además, en el **artículo 21**, sobre el:

Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas. Además, de los presupuestos establecidos en el derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas, no se podrán tratar datos sensibles o datos de niñas, niños y adolescentes a menos que se cuente con la autorización expresa del titular o de su representante legal; o, cuando, dicho tratamiento esté destinado a salvaguardar un interés público esencial, el cual se evalúe en atención a los estándares internacionales de derechos humanos, y como mínimo satisfaga los criterios de legalidad, proporcionalidad y necesidad, y además incluya salvaguardas específicas para proteger los derechos fundamentales de los interesados.

Las y los adolescentes, en ejercicio progresivo de sus derechos, a partir de los 15 años, podrán otorgar, en calidad de titulares, su consentimiento explícito para el tratamiento de sus datos personales, siempre que se les especifique con claridad sus fines (Ecuador A. N., Ley Orgánica de Protección de Datos Personales, 2021).

La **Política pública por una Internet Segura para niñas, niños y adolescentes** se construyó bajo la coordinación del Consejo Nacional para la Igualdad Intergeneracional (CNII), junto con 22 instituciones públicas, privadas y organismos internacionales, en la que también participó el Ministerio de Educación. El objetivo es proteger la dignidad e integridad física, psicológica, emocional y sexual de la niñez y adolescencia. También se apunta a potenciar las oportunidades y habilidades que ofrecen las tecnologías digitales en su vida y desarrollo integral.

En el eje II. Medidas técnicas y procedimentales, en el punto 2.2.1, de las acciones se señala: “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”. En el eje IV. Construcción y fortalecimiento de capacidades, en el punto 5.1.: “Fortalecer y consolidar las capacidades del Sistema Nacional de Educación para garantizar entornos seguros para que niñas, niños y adolescentes ejerzan su derecho a la educación” y en las acciones del punto 5.1.15.: “Promover la formación permanente de docentes en los contenidos y manejo de las TIC para la transformación e innovación de las tecnologías del aprendizaje y el conocimiento como un proceso de innovación pedagógica” (CNII, 2020).

Capítulo 2. Marco Conceptual

Alfabetización digital

Es la capacidad de una persona para realizar tareas en los medios digitales. Esta definición engloba la habilidad para localizar, organizar, entender, evaluar, investigar y analizar información usando la tecnología, así como ser capaz de elaborar contenidos y diseñar propuestas a través de medios digitales (Mineduc, 2021).

En el ámbito educativo, la alfabetización digital plantea una nueva forma de enseñar y aprender, con la participación de niñas, niños y adolescentes, desarrollando la creatividad, la innovación, la responsabilidad y el trabajo autónomo. El personal docente y las familias desempeñan un papel fundamental al fomentar esta habilidad entre las y los estudiantes, ya que son ellos quienes guían su proceso de aprendizaje.

Ciudadanía digital

Se refiere al conjunto de derechos y responsabilidades que las personas tienen en el entorno digital, entendiendo a la Internet como un espacio público, con oportunidades para el ejercicio pleno de derechos. La ciudadanía digital se construye a través del uso apropiado, responsable y empoderado de la tecnología, promoviendo experiencias digitales positivas, reconociendo las consecuencias de nuestras acciones y participando en la construcción de un bien común (Mineduc, 2021).

Las niñas, niños y adolescentes tienen derecho a estar protegidos de cualquier riesgo asociado a los entornos virtuales. Para que ellas y ellos ejerzan plenamente sus derechos en los entornos virtuales es necesario fortalecer las habilidades digitales que les permitan comprender sus usos, informarse y participar, así como reconocer riesgos y formas de pedir ayuda.

Competencias digitales

Son las capacidades para realizar tareas en dispositivos digitales y aplicaciones de la comunicación y las redes. Estas habilidades permitirán producir, reproducir, evaluar e intercambiar información usando la tecnología y participar en las redes de manera segura (Unesco, 2018).

Con el desarrollo de conocimientos que permitan hacer un uso crítico, consciente y responsable de las tecnologías de la información y la comunicación (TIC) se apuesta a un proceso educativo orientado a una buena convivencia en espacios virtuales y digitales. En este contexto, es necesario reflexionar sobre el rol de las personas adultas que acompañan a niñas, niños y adolescentes para generar acciones conjuntas que promuevan el uso adecuado de las tecnologías y la prevención de riesgos.

Uso seguro de la Internet

Cuando las personas conocen los riesgos y las ventajas de la Internet, gestionan adecuadamente sus cuentas, son cuidadosos con su privacidad y respetan la de los demás. Esto incluye cerrar sesión, navegar en páginas seguras, no compartir contraseñas ni datos personales de otra persona, no aceptar solicitudes de extraños, usar internet para buscar información educativa, respetar la identidad de las personas y configurar la privacidad de las redes sociales (Riamusi R. I., 2019).

Huella digital

Es la marca que deja cada persona usuaria en cada actividad que desarrolla en línea, las páginas y sitios que visita, videos o fotos que ve, crea y comparte, comentarios que hace, amistades que contacta, búsquedas que realiza, publicaciones que lee, música que escucha, películas o series que mira (Mineduc, 2021).

Las actividades que una persona desarrolla en la Internet dejan un rastro y forma parte de la identidad digital. Esta huella es pública y, por tanto, todas las personas pueden verla. Además, es difícil borrar esta huella; de hecho, la viralización de contenidos se extiende por las redes y llega a una gran cantidad de usuarios.



Prácticas online y offline

El mundo digital (online) y el mundo físico (offline) están interrelacionados; no es posible considerarlos por separado. Todo lo que sucede online tiene efectos offline. La relación e interacción de las personas (adultas, niños, niñas y adolescentes) del mundo online-off line implica nuevas posibilidades y riesgos que debemos considerar en la tarea de promover y proteger derechos (Mineduc, 2021).

Lo íntimo, lo privado y lo público

Se requiere estar atentas y atentos a la información que constantemente se comparte en las plataformas digitales; considerar que los datos entregados en la red son públicos, que una persona deja de tener control sobre esa información y que inclusive esos datos pueden ser usados con fines maliciosos. Esto obliga a reconsiderar los límites entre las esferas de la vida: lo íntimo, lo público y lo privado.

Lo íntimo: son acciones que corresponden al ámbito personal. Esta información NO debe compartirse porque puede afectar la integridad. Por ejemplo: se debe evitar compartir fotos íntimas, entregar contraseñas, datos bancarios o cualquier información que exponga la integridad de una persona.

Lo privado: pertenece a información y experiencias personales que SOLO se comparten con la familia y amistades del círculo de confianza. Por ejemplo: se debe restringir la publicación de fotos y videos personales, la transmisión de actividades familiares, de itinerarios de viajes y actividades del día a día.

Lo público: es la información que se PUEDE compartir abiertamente, como las vivencias o logros que se comparten abiertamente, pensamientos, sentimientos o denuncias que no perjudiquen a terceros ni a uno mismo; por ejemplo: campañas de salud o educación, denuncias de carácter social, transmisión en vivo de eventos educativos, situaciones injustas, actividades sociales que no perjudiquen a terceros, artículos y noticias de interés de fuentes confiables (Mineduc, 2021).

Brecha digital

La brecha digital es la diferencia entre las personas que tienen acceso a la Internet y las que no; incluye factores como el acceso, la asequibilidad, la calidad del servicio y la relevancia. A menudo, estas brechas coinciden con otras disparidades, como la desigualdad de ingresos y de género (Mineduc, 2021).

Tecnologías para el Aprendizaje y Conocimiento (TAC)

Las Tecnologías para el Aprendizaje y Conocimiento (TAC) usan las Tecnologías de la Información y la Comunicación (TIC) incorporadas a la enseñanza, es decir, aquellas que fomentan el trabajo colaborativo entre estudiantes y docentes, que permiten compartir materiales en la red y que identifican y difunden las buenas prácticas educativas (CNII, 2020).

Tecnologías para el Empoderamiento y la Participación (TEP)

Las tecnologías para el Empoderamiento y la Participación (TEP) son aquellas cuyo uso se propone para el ejercicio democrático y la autorrealización personal. Las niñas, niños y adolescentes se convierten en “prosumidores” utilizando las TIC tanto para consumir información y contenidos como para participar y expresarse ante temas que los afectan (Riamusi I. , 2018).

Tecnologías de la Información y Comunicación (TIC)

Las Tecnologías de la Información y Comunicación (TIC) son herramientas tecnológicas que nos conectan con el mundo digital. Con ellas podemos comunicarnos, aprender, explorar y expresarnos (Riamusi I. , 2018). Son parte de la vida cotidiana y brindan oportunidades para crecer y descubrir el potencial de las personas.

Nivel de riesgo

En el ámbito educativo, se puede clasificar las situaciones de riesgo en tres niveles: riesgo leve o de contenido, riesgo medio o de conducta y riesgo alto o de contacto³. Estos niveles abarcan desde situaciones en las cuales niñas, niños y adolescentes pueden hablar con extraños en las redes sociales hasta casos más graves como el grooming y la sextorsión.

³ La metodología utilizada para realizar la clasificación de riesgos de Internet tiene su base en la integración de información proveniente de CO:RE y RIAMUSI, adaptándola a la realidad y contexto ecuatorianos. Se establecieron parámetros aplicables al caso de Ecuador y se realizó una clasificación de acuerdo con los cuatro tipos de riesgos: contenido, contacto, conducta y contrato (4C) (“Children Online: Research and Evidence (CO:RE)” clasifica el riesgo en línea de acuerdo con las 4C. La clasificación reconoce que los riesgos surgen cuando una niña, niño o adolescente: interactúa y/o está expuesto a CONTENIDO potencialmente dañino; experimenta y/o es objetivo de CONTACTO potencialmente dañino; es testigo, participa y/o es víctima de una CONDUCTA potencialmente dañina; es parte de y/o explotado por un CONTRATO potencialmente dañino).

Es importante tener en cuenta que situaciones de riesgo aparentemente leves, como entablar conversaciones con desconocidos en redes sociales, pueden empeorar y volverse más peligrosas. Por ejemplo, compartir información privada o fotos, exponer públicamente el perfil, enviar contenido ofensivo, suplantar identidades y otros riesgos similares puede generar situaciones que evolucionen y lleguen a niveles más altos de riesgo, donde las niñas, niños y adolescentes se enfrentan a situaciones de violencia, como el acoso cibernético, grooming, sextorsión y otros delitos graves.

Grafico 1.

Niveles de riesgo en entornos digitales

Riesgo leve: cuando una niña, niño o adolescente tiene exposición a contenidos potencialmente dañinos.

Riesgo medio: cuando una niña, niño o adolescentes presencia o participa en comportamientos perjudiciales entre compañeras y/o compañeros.

Riesgo alto: conlleva peligro físico, psicológico, sexual para una niña, niño o adolescente. Abarca los riesgos de contacto con personas adultas.



Tabla 1.

Descripción de situaciones de riesgo en entornos digitales

Situaciones de riesgo leve		
Descripción	Prácticas	Ejemplos
<p>Son riesgos de contenido y se refieren a las situaciones en las cuales una niña, niño o adolescente se involucra o está expuesto a contenido potencialmente dañino.</p> <p>Esto puede ocurrir cuando una niña, niño o adolescente es receptor de contenidos masivos que pueden tener un impacto negativo en su bienestar y desarrollo.</p>	<p>Prácticas de sexting consensuadas.</p> <p>Exposición a contenidos nocivos.</p> <p>Portalitis (molestias musculares por uso de dispositivos tecnológicos).</p> <p>Fake news (noticias falsas).</p> <p>Discursos de odio, entre otros.</p>	<p>Estos riesgos incluyen hablar con desconocidos en las redes sociales, compartir su ubicación en la Internet, no cerrar sesión, tener cuentas públicas, aceptar solicitudes de personas que no conocen en el mundo real, descargar aplicaciones sin verificar su autenticidad e ingresar datos personales en aplicaciones que no son seguras, visitar páginas con contenido violento o sexual, etiquetar a un amigo con comentarios ofensivos, entre otros.</p>
Situaciones de riesgo medio		
Descripción	Prácticas	Ejemplos
<p>Se refieren a riesgos de conducta cuando una niña, niño o adolescente es testigo, participa o es víctima de una conducta potencialmente dañina entre compañeras y compañeros.</p> <p>Esto puede incluir: ser el agresor o la víctima de un intercambio negativo entre pares.</p>	<p>Ciberadicción y/o abuso de la internet/TIC.</p> <p>Ciberacoso o cyberbullying entre pares.</p> <p>Difusión no consentida de imágenes entre pares.</p> <p>Harassment (amenazas, insultos, rumores en línea).</p> <p>Hipersexualización infantil.</p> <p>Paliza feliz/Happy slapping (grabar una pelea y compartirla en la red).</p> <p>Phishing o suplantación de identidad.</p> <p>Pornovenganza entre pares, entre otros.</p>	<p>Aceptar solicitudes de extraños e intercambiar mensajes, chatear con extraños, compartir contraseñas, colocar anuncios con sus números de teléfono, prestar su computadora sin bloquear la contraseña, compartir información o fotos privadas, exponer su perfil al público, enviar videos o fotos ofensivos, compartir fotos desnudas o con contenido sexual, enviar mensajes violentos a otras personas, suplantar la identidad de otra persona, entre otras.</p>

Situaciones de riesgo alto

Descripción	Prácticas	Ejemplos
<p>Se tratan de riesgos de contacto y se refieren a situaciones en las cuales una niña, niño o adolescente experimenta o es objeto de un contacto potencialmente dañino con una persona adulta.</p> <p>Implican peligro y/o daño físico, psicológico o sexual para la niña, niño o adolescente.</p> <p>Cuando estas situaciones involucran a una persona adulta, son delitos. En situaciones de violencia entre pares, se debe analizar cada contexto y caso con una mirada amplia en la intervención.</p> <p>También hace referencia al riesgo de contrato; se refiere a la situación en la que una niña, niño o adolescente es parte o es explotado por un contrato potencialmente dañino. Esto puede incluir casos de robo de identidad, fraude, phishing, estafas, piratería, chantaje y otros riesgos de seguridad.</p>	<p>Abuso sexual de una niña, niño o adolescente en línea.</p> <p>Situaciones de violencia cometida por una persona adulta.</p> <p>Difusión de imágenes íntimas o de contenido sexual que involucre a una persona adulta.</p> <p>Pornografía y/o explotación sexual en línea.</p> <p>Exposición a contenidos nocivos de una persona adulta a una niña, niño o adolescente.</p> <p>Grooming (persona adulta que se hace pasar por un niño o adolescente con intención de obtener material sexualmente explícito).</p> <p>Hipersexualización infantil de una persona adulta a una niña, niño o adolescente.</p> <p>Lolicon/Shotacon (relación sentimental y/o sexual en la red entre preadolescente y una persona adulta)</p> <p>Phishing o suplantación de identidad por una persona adulta.</p> <p>Sexting con una persona adulta.</p> <p>Sextorsión.</p>	<p>Acoso cibernético, grooming, sextorsión, difusión no autorizada de imágenes o videos sexuales, ciberacoso sexual, violación de la privacidad y manejo de contenido inapropiado.</p>

Fuente: elaborado sobre la base de determinaciones del Protocolo para el uso seguro de la Internet de Panamá de 2019 y otras fuentes internacionales (CO:RE - Children Online: Research and Evidence, 2021).

Es importante distinguir entre situaciones de riesgo o violencia entre pares y violaciones de derechos cometidas por una persona adulta, ya que cada una debe ser abordada dentro del marco normativo correspondiente.

Las situaciones entre pares se refieren a problemas entre compañeras y/o compañeros de la institución, en las que participan niños, niñas y adolescentes. Aquí se puede incluir situaciones de riesgo de nivel leve o medio, que pueden abordarse a través de prácticas restaurativas como parte de acciones educativas disciplinarias. No obstante, cuando se trate de un caso de violen-

cia, no aplican estas prácticas, conforme con lo establecido en el Reglamento de la Ley Orgánica de Educación Intercultural.

Por otra parte, las situaciones perpetradas por una persona adulta contra niños, niñas y adolescentes pueden involucrar formas sofisticadas de violencia en línea que constituyen en su mayoría delitos y deben ser denunciadas.

A continuación, se enlistan situaciones agravantes a considerar cuando un riesgo se convierte en una vulneración de derechos contra niñas, niños y adolescentes:

- **Amenazas, coacciones**, presiones, intimidaciones o cualquier hecho que genere un ambiente de temor y vulnerabilidad.
- **Humillación y desprestigio** a través de comentarios, acciones humillantes, difamatorias o degradantes en plataformas digitales y que afecten a la autoestima, dignidad, reputación, bienestar emocional y social.
- **Atentados contra la dignidad** y que puedan tener consecuencias duraderas en su vida personal y social.
- **Violación a los derechos humanos** como el derecho a la privacidad, la integridad personal, protección contra la violencia y el acceso a un entorno seguro, requieren de una intervención inmediata y contundente.
- **Explotación y abuso**, ya que representan situaciones de extremo peligro y violencia que pueden ocasionar un daño grave y duradero a una niña, niño o adolescente.

Otros elementos agravantes para considerar son:

- **Edad y grado de madurez** de la niña, niño o adolescente. A menor edad puede ser más vulnerable y contar con menos preparación para identificar y protegerse de riesgos en línea.
- **Género**: pueden ser objeto de discriminación o acoso en línea. Los estudios sobre la dimensión de género de la violencia en línea, por ejemplo, indican que el 90% de las víctimas de la distribución digital no consentida de imágenes íntimas son mujeres (ONU Mujeres, 2020).
- **Discapacidad**: puede ser un factor de vulnerabilidad para ciertos riesgos en línea.
- Contexto familiar: puede influir en su exposición a riesgos en línea, así como en su capacidad para informar sobre ellos.
- **Orientación e identidad sexual**: se puede sufrir discriminación y acoso en línea debido a una orientación sexual o identidad de género.

Capítulo 3. Protocolo de actuación frente a situaciones de violencia digital

La atención a la población en el Sistema Nacional de Educación está enmarcada en un proceso integral de abordaje con especial énfasis en niñas, niños y adolescentes, para garantizar atención especializada, prioritaria y oportuna.

Prevención Integral

Desde una perspectiva de prevención integral, todo mecanismo preventivo que se implemente en la institución educativa debe estar dirigido a facilitar el que niñas, niños y adolescentes se empoderen y sean capaces de tomar decisiones con respecto a sus proyectos de vida de manera consciente, libre y autónoma (Ministerio de Educación de Ecuador, 2022).

Una estrategia para generar un uso seguro y prevenir riesgos en la Internet es el desarrollo de competencias digitales en las y los estudiantes, de manera proporcional a su edad y nivel de desarrollo con el fin de que puedan gestionar acciones de protección para sí mismos y para sus pares.

Para que niñas, niños y adolescentes desarrollen habilidades que les permitan producir, reproducir e intercambiar información en entornos digitales, se requiere de un proceso gradual que parte del acompañamiento, protección y regulación de las personas adultas en entornos familiares y educativos hasta que alcancen su propia autorregulación sobre la exposición y uso de estos recursos tecnológicos, como lo destaca el documento de Prevención del ciberacoso y delitos en medios digitales (Ministerio de Educación de Colombia, 2021).

Las instituciones educativas deben contar con insumos que les permitan ejercer su corresponsabilidad en la construcción de estas competencias digitales en las y los estudiantes. En este contexto, las instituciones educativas se convierten en espacios de encuentro, intercambio y reflexión a través de diversas actividades que permitan un diálogo intergeneracional. Es precisamente en este eje de prevención integral donde se busca modificar el entorno escolar, mejorando las relaciones entre estudiantes (pares) y fortaleciendo las capacidades del personal docente y las familias con acciones planificadas y permanentes.

Actuaciones preventivas que puede realizar la comunidad educativa

Los factores protectores son aquellas actuaciones que reducen la probabilidad de la aparición de conductas de riesgo y de consecuencias negativas, así como reducir la vulneración de derechos asociados al uso de la Internet y de los dispositivos tecnológicos.

La comunidad educativa tiene la responsabilidad de proteger a niñas, niños y adolescentes de riesgos y vulneraciones que ocurren en la red y en la convivencia con los demás. Sobre la base del documento de “Promoción de Derechos en el Uso Seguro de Internet desde las Familias” (Mineduc, 2021) se describe las 5C para la prevención:



Comunicación

El diálogo, con una escucha activa y empática, permite comprender, acercarse, escuchar sin juzgar, entender las dificultades, buscar soluciones y generar espacios de encuentro para conocerse más entre familias y entre docentes y estudiantes. También es importante dialogar sobre la convivencia digital como un espacio en donde las interacciones con otras y otros pueden tener el mismo o mayor impacto que en el mundo físico.

Confianza

Se trata de establecer relaciones seguras con niñas, niños y adolescentes para que puedan comunicar, libremente, las diferentes situaciones que atraviesan. El comportamiento de las familias con respecto a sus propios dispositivos electrónicos se transforma en un modelo para niñas, niños y adolescentes. No solamente hay que concentrarse en el tiempo que pasan en línea; se requiere acompañamiento en las actividades que realizan, en los contenidos que buscan, con las personas con las que interactúan y en los juegos en los que participan.

Compromiso

Las personas adultas deben establecer un firme compromiso en la promoción y protección de los derechos de la niñez y adolescencia. Este acompañar requiere de la revisión de prácticas de cuidado y crianza encaminadas a la garantía de entornos seguros y saludables, tanto en lo físico como en lo virtual; requiere tanto de la disposición a aprender e informarse sobre el uso de medios tecnológicos para acompañar a niñas, niños y adolescentes, como de participar en las actividades escolares y prácticas de convivencia relacionadas con el uso del tiempo en los dispositivos tecnológicos.

Conocimiento

No es posible operar sobre lo que no se conoce, solamente se puede intervenir desde el conocimiento. Esto involucra conocer a los niños, niñas y adolescentes; saber cómo interactúan en el entorno digital, conocer acerca del uso seguro y de posibles riesgos; informarse para orientarlos y dialogar sobre las diferencias entre los espacios públicos, privados e íntimos.

Cuidado y autocuidado

Las familias e instituciones educativas deben brindar información que permita a niñas, niños y adolescentes detectar alertas y contar con mejor preparación ante situaciones de riesgo que puedan suceder en la Internet. Anticiparse requiere de un esfuerzo para garantizar espacios seguros e información y orientación permanente. Implica también el tener una relación cercana de respeto y confianza para posibilitar el diálogo intergeneracional.

Acciones concretas desde la institución educativa:

A continuación, se describe algunas acciones que la comunidad educativa puede llevar a cabo, sobre la base de los documentos acerca de uso seguro desarrollados por el Ministerio de Educación. También se incluye los aportes de niñas, niños y adolescentes de los consejos consultivos como respuestas a la pregunta sobre las prácticas seguras que identifican y aplican al navegar en la Internet:

- Construir el Plan Educativo Institucional y el Código de Convivencia, considerando las necesidades de la comunidad educativa en los ambientes virtuales; fomentar prácticas de autocuidado y cuidado en los entornos virtuales.
- Fortalecer las estrategias pedagógicas con contenidos que desarrollen destrezas y competencias digitales.
- Identificar cursos de formación para docentes encaminados al manejo, desarrollo de competencias y destrezas en el uso de las TIC.
- Promover campañas para hacer frente a los riesgos en la Internet.
- Atender situaciones de riesgo y conflictos desde un enfoque educativo y positivo.
- Socializar el protocolo de actuación frente a situaciones de violencia en la Internet a todos los miembros de la comunidad educativa.
- Fomentar la igualdad de género en el aula, el respeto en línea y la empatía hacia aquellos que puedan estar experimentando violencia en línea para apoyarlos y denunciar estos actos.
- Ofrecer un espacio seguro y confidencial para que las y los estudiantes que experimentan violencia en línea puedan hablar sobre su experiencia y buscar apoyo.
- Definir medidas restaurativas para hacer frente a conductas de riesgo en la Internet; viabilizar actividades desde las comisiones con las que cuenta la institución educativa para favorecer la participación e involucramiento de todos los actores en los temas propuestos por la comunidad educativa.

- Coordinar acciones con entidades del Estado, organismos no gubernamentales de cooperación, sociedad civil y actores comunitarios para fortalecer las capacidades de la institución educativa en el uso seguro de la Internet y para generar propuestas de intervención individual, colectiva e institucional frente a conductas de riesgo.
- Establecer campañas y programas que promuevan la toma de decisiones en las y los estudiantes ante situaciones de riesgo y para uso seguro de la Internet.
- Solicitar al Consejo Estudiantil trabajar en planes de promoción para el uso seguro de la Internet y para la prevención de riesgos y vulneraciones de derechos.

Acciones concretas desde las familia

Acompañar a sus hijas e hijos en el uso de las TIC y establecer reglas y acuerdos sobre su uso.

- Evitar dejar a las hijas e hijos sin supervisión por períodos largos, tanto en espacios virtuales como físicos.
- Poner seguridades en las redes e instalar programas de control parental. Se puede usar los sistemas de protección disponibles para evitar el acceso a páginas no apropiadas para niñas, niños y adolescentes.
- Reflexionar con las niñas, niños y adolescentes sobre el contenido que publican y sobre las personas que contactan en sus redes.
- Establecer horarios para el uso de los dispositivos que deben ser cumplidos por toda la familia. Empezar dando el ejemplo.
- Conversar abiertamente sobre peligros posibles y construir espacios de confianza para ayudar a sus hijas e hijos en caso de que lo requieran.
- Asegurarse de que los videojuegos y dispositivos tecnológicos a los que acceden las niñas, niños y adolescentes sean apropiados para su edad.
- Evitar intercambios de direcciones, números de teléfono o datos personales que puedan identificarlos.
- Poner los mismos límites que establecerían en cualquier otro ámbito de la vida (mundo físico y mundo virtual).
- Ofrecer un ambiente seguro y protegido en el hogar y fuera de él (mundo físico y mundo virtual).
- Capacitarse en ciudadanía digital, así como en el uso seguro y prevención de riesgos y vulneraciones en entornos digitales.

Acciones concretas para niñas, niños y adolescentes:

- Identificar que contactarse con personas desconocidas en la Internet y redes sociales es un riesgo.
- Evitar publicar contenido íntimo o muy personal.
- Evitar las páginas con contenido inapropiado, desconfiar de los mensajes de personas desconocidas.
- Desconfiar cuando les ofrezcan algún premio o promoción.
- Considerar el tiempo que dedican a las pantallas y al resto de actividades de su interés.
- No permitir a nadie en la Internet cosas que no se permitiría a amigas o amigos en el mundo real.
- Considerar el contenido antes de publicarlo en las páginas web o redes sociales y recordar que cualquier persona puede ver esa información.
- No compartir imágenes, videos o textos ofensivos, discriminatorios o violentos.
- Usar los filtros de privacidad que estén a disposición para proteger información (público, amigos, ocultar, etc.).
- Evitar responder mensajes agresivos o amenazas. Si se presenta un problema, pedir ayuda a un familiar o docente, no es suficiente contarlo a una amiga o amigo.
- Concientizar acerca de que el uso frecuente de las redes sociales no sustituye a las relaciones sociales en el convivir diario.
- Lograr que niñas, niños y adolescentes comuniquen con frecuencia a una persona adulta de confianza (padre, madre, tutor u otros) que conozca del tema, con quién mantienen contacto mediante redes sociales y qué peligros han detectado.

Por otra parte, en el Modelo de Gestión del Departamento de Consejería Estudiantil, en el eje de promoción y prevención se describen acciones como las siguientes:

- Desarrollar espacios de sensibilización, diálogo, capacitación y asesoramiento para la comunidad educativa, enfocados en la prevención de riesgos psicosociales, incluidas las violencias en entornos digitales, prácticas discriminatorias y excluyentes a lo largo del proceso educativo.
- Los espacios de sensibilización deben responder a las temáticas que se hayan priorizado en la planificación del Departamento de Consejería Estudiantil considerando las necesidades de la población estudiantil.

DetECCIÓN

Al analizar los riesgos en entornos digitales en los que estén involucrados niños, niñas y adolescentes, es importante considerar la probabilidad de ocurrencia y gravedad de posibles daños con consecuencias para su bienestar emocional y físico (CO:RE - Children Online: Research and Evidence, 2021). La presencia de daño depende de factores relacionados con la niña, niño o adolescente, de las acciones de otros, de la tecnología y de las circunstancias.

1. El personal educativo y administrativo deberá detectar e identificar presuntos casos de violencia digital por medio de señales de alerta y/o de reportes de estudiantes, docentes, familiares o terceros:

a. Es importante tener en cuenta que los riesgos y las vulneraciones de derechos presentes en el mundo físico también se trasladan al entorno virtual, por ejemplo: el acoso escolar puede comenzar en el aula y continuar en las redes sociales, mientras que el grooming puede comenzar en línea y llevar a encuentros peligrosos en el mundo real. A continuación, se detalla las vulneraciones que se puede enfrentar en estas dos dimensiones y que es imperativo detectar:

Tabla 2.

Situaciones de violencia en el mundo físico y virtual

Vulneraciones de derechos en el mundo offline	Vulneraciones de derechos en el mundo online
Acoso escolar	Ciberacoso o ciberbullying
Violencia entre niñas, niños y adolescentes	Paliza feliz/happy slapping
Abuso sexual infantil/ violencia sexual	Grooming y sextorsión
Violencia intrafamiliar	Ciber control y acoso psicológico a través de la Internet
Explotación sexual de niñas, niños y adolescentes	Explotación sexual de niñas, niños y adolescentes a través de plataformas digitales
Exposición a contenidos inapropiados en medios tradicionales	Exposición a contenidos inapropiados en la Internet y redes sociales
Desaparición de niñas, niños y adolescentes	Exposición a personas peligrosas en la Internet y redes sociales (captación)
Robo o pérdida de identidad	Suplantación de identidad en la Internet
Exposición a violencia y delitos en el entorno urbano	Ciberdelitos y cibercrimen

Fuente: elaboración propia a partir del Protocolo de la RIAMUSI.

b. Frente a estas situaciones, es necesario estar atentas y atentos a las señales físicas, de comportamiento y de conducta de niñas, niños y adolescentes. A continuación, se detalla indicadores generales para tener en cuenta:

Tabla 3.

Signos o indicadores por niveles de riesgo en entornos digitales

Situaciones de riesgo leve	
Signos o indicadores	Preguntas para la detección del riesgo
<p>Disponer de una computadora o celular en la habitación, sin supervisión de una persona adulta referente.</p> <p>Dificultad de concentración en el salón de clases.</p> <p>Pasar muchas horas conectadas/os, sobre todo por la noche.</p> <p>Mostrar o subir constantemente cosas de la vida cotidiana a las redes, junto con datos, ubicación, etc.</p> <p>Estar pendiente todo el tiempo de las publicaciones en las redes sociales.</p> <p>Visitar páginas web con contenido violento o sexual.</p> <p>Tener la necesidad de estar siempre disponible en el celular.</p> <p>Etiquetar a un amigo o desconocido con comentarios ofensivos.</p>	<p>¿Habla con desconocidos en las redes sociales?</p> <p>¿No cierra sesión en sus cuentas?</p> <p>¿Tiene perfiles públicos en redes sociales?</p> <p>¿Acepta solicitudes de personas desconocidas en el mundo real?</p> <p>¿Descarga aplicaciones sin verificar su autenticidad?</p> <p>¿Ingresa datos personales en aplicaciones no seguras?</p> <p>¿Visita páginas con contenido violento o sexual?</p> <p>¿Etiqueta a amigos con comentarios ofensivos?</p> <p>¿Falta de autocuidado y conciencia de su huella digital?</p> <p>¿Usa el mismo nombre de usuario y contraseña en diferentes servicios?</p> <p>¿Comparte contraseñas con extraños?</p>

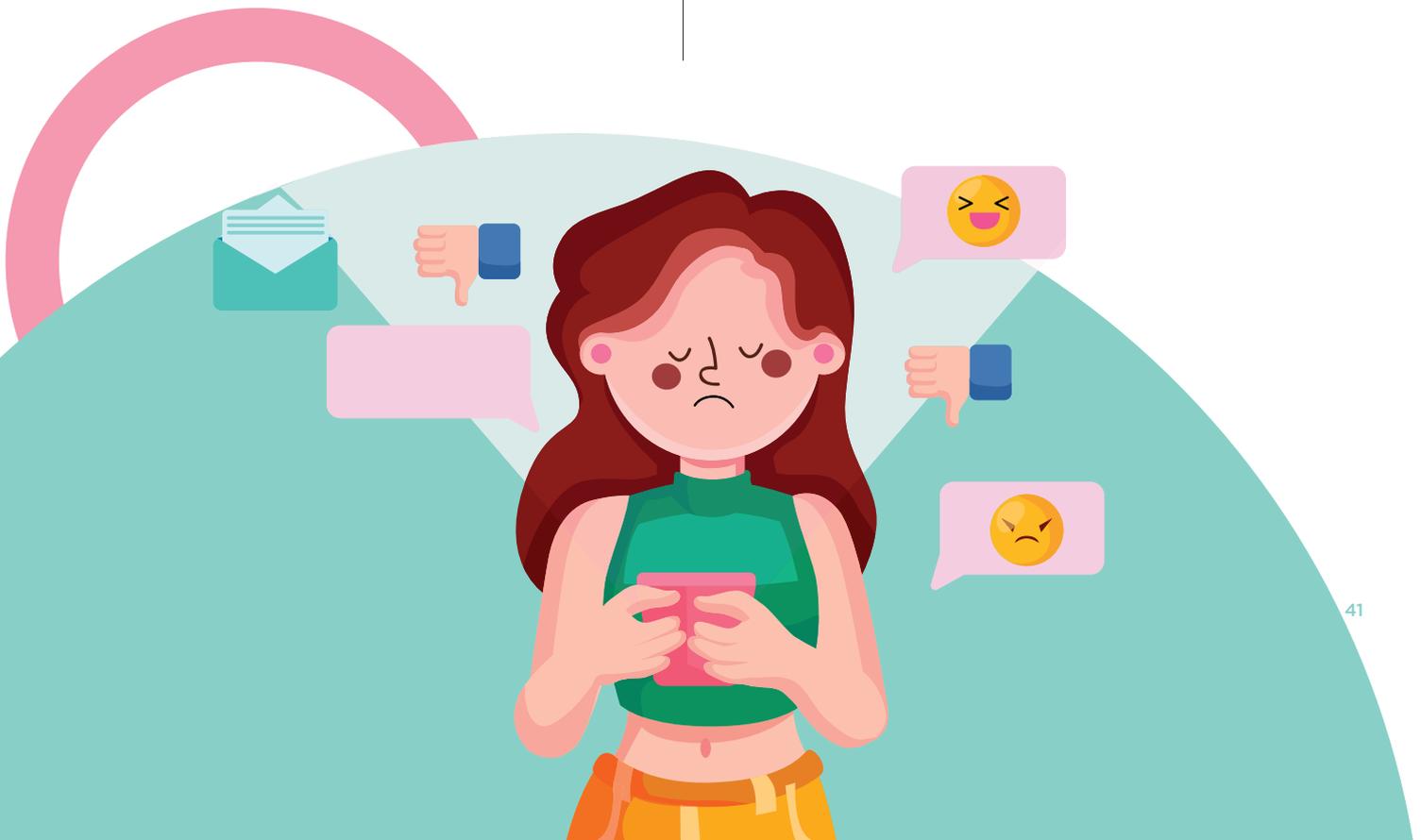
Situaciones de riesgo medios

Signos o indicadores

Dificultad de concentración en el salón de clase y afectación en el rendimiento académico.
Baja autoestima.
Soledad, aislamiento.
Callar y no denunciar situaciones de violencia.
Dificultad para conciliar el sueño (insomnio).
Cambios de comportamiento (agresivo, pasivo, triste, etc.).
Visitar páginas web con contenido sexual.
Ocultar las pantallas en las que está conectada o conectado.
Recibir llamadas o mensajes de desconocidos.
No comentar con su círculo cercano lo que hace o le sucede en Internet.
Tener la necesidad de estar siempre disponible en el celular, inclusive, en las horas de sueño.
Enviar mensajes ofensivos en redes sociales.
Aislarse de la vida familiar y participar cada vez menos de las actividades con sus pares en el mundo físico.
Suplantar la identidad de otra persona (crear perfiles falsos).
Conflictos en el hogar.

Preguntas para la detección del riesgo

¿Comparte su ubicación en Internet?
¿Tiene perfiles de redes sociales públicos?
¿Acepta solicitudes de amistad o contacto de extraños?
¿Chatea o intercambia mensajes con desconocidos?
¿Comparte contraseñas con amigos o desconocidos?
¿Coloca anuncios en línea con su número de teléfono?
¿Presta su computadora sin bloquear la contraseña?
¿Comparte información privada o fotos personales?
¿Expone públicamente su perfil en redes sociales?
¿Visita páginas con contenido violento o sexual?
¿Envía mensajes, videos o fotos ofensivos o violentos?
¿Comparte fotos con desnudos o con contenido sexual?
¿Suplanta la identidad de otra persona en línea?



Situaciones de riesgo alto	
Signos o indicadores	Preguntas para la detección del riesgo
<p>Soledad, aislamiento, nerviosismo, temor, depresión, ansiedad. Baja autoestima. Ha sido víctima de situaciones de violencia. Marcas en el cuerpo. Lesiones, fracturas o esguinces sin explicación coherente o que no concuerden con la causa alegada. Tener la necesidad de estar siempre disponible en el celular, sin discriminación de tiempo y espacio. Enviar mensajes despectivos o ser gravemente atacado en redes. Aislarse de la vida familiar y participar cada vez menos de las actividades en el mundo físico. Trastornos del sueño (pesadillas, temor nocturno o insomnio). Rehuir o negarse a hablar sobre sí mismo/a. No comentar lo que hace o le sucede en Internet. Cambios bruscos de comportamiento (agresión, depresión, ansiedad, etc.). Sentimientos de culpa. Recibir llamadas, mensajes, regalos de desconocidos frecuentemente. Mantener una relación sentimental y/o sexual en entornos digitales con personas que no conoce en el mundo real. Suplantar la identidad de otra persona y obtener información personal con fines lucrativos (crear perfiles falsos). Violencia en el hogar.</p>	<p>¿Ha experimentado acoso cibernético?</p> <p>¿Ha sido víctima de grooming?</p> <p>¿Ha sido víctima de sextorsión?</p> <p>¿Han difundido imágenes o vídeos sexuales sin su autorización?</p> <p>¿Ha sufrido ciberacoso sexual o acoso escolar en línea?</p> <p>¿Han violado su privacidad en línea?</p> <p>¿Ha estado expuesto a contenido inapropiado en Internet (violento, denigrante, etc.)?</p>

Fuente: elaboración propia a partir de determinaciones del Protocolo para el uso seguro de la Internet de Panamá (2019) y otras fuentes internacionales (CO:RE - Children Online: Research and Evidence, 2021).

2. Se deberá valorar el **nivel de riesgo** (leve, medio, alto) o emergencia para identificar el tipo de atención que se requerirá en cada uno de los casos.

3. Se considera un riesgo leve cuando una niña, niño o adolescente se involucra o está expuesto a contenidos potencialmente dañinos. Esto puede ocurrir cuando son receptores de contenidos masivos que pueden tener un impacto negativo en su bienestar y desarrollo. En esta situación se deberá realizar una atención preventiva para detener o disminuir el nivel de vulnerabilidad y determinar la intervención de manera individual y/o grupal.

4. Se considera un riesgo medio cuando una niña, niño o adolescente es testigo, participa o es víctima de una conducta potencialmente dañina entre compañeras y compañeros. Esto puede incluir ser el agresor o la víctima de un **intercambio negativo entre pares**. Estas situaciones deben ser atendidas de manera inmediata para evitar que se conviertan en un riesgo alto. Además, es necesario trabajar en el fortalecimiento de las habilidades socioemocionales, promover el manejo de emociones y resolución de conflictos de manera individual (agresor y víctima) y grupal (observadores). También hay que priorizar acciones específicas para promover el uso seguro y prevención de riesgos en línea.

5. Se considera un **riesgo alto** cuando la o el estudiante está expuesto a situaciones que implican **peligro y/o daño físico, psicológico o sexual**; además, aquellos relacionados con robo de identidad, fraude, phishing, estafas, piratería, chantaje y otros riesgos de seguridad. **Cuando estas situaciones involucran a una persona adulta son delitos**. En situaciones de violencia entre pares, se debe analizar cada contexto y caso considerando los agravantes desde una mirada integral para la intervención.

6. En situaciones de emergencia o si se presencia un hecho de violencia, se debe llamar de inmediato al ECU911.

7. Se debe comunicar al padre, madre o representante legal la situación ocurrida⁴.

a. Para casos de violencia entre pares se debe informar a los representantes legales tanto de la víctima o víctimas como del agresor o agresores sobre lo sucedido.

8. Cualquier miembro del personal educativo y administrativo que ha detectado o ha identificado la alerta, deberá elaborar la **ficha de reporte de hecho de violencia** por presunto caso de violencia digital. Cuando la familia o estudiantes comunican verbalmente o por otro medio una alerta, la ficha deberá ser llenada por la/el profesional del Departamento de Consejería Estudiantil (DECE).

9. La persona que elaboró la ficha de reporte de hecho de violencia deberá remitirla al Departamento de Consejería Estudiantil⁵ de manera inmediata.

10. El Departamento de Consejería Estudiantil deberá informar a la máxima autoridad institucional de la notificación de la alerta entregada.

4 Si el padre, madre o representante legal está implicado en la alerta, se debe tomar contacto con una persona adulta de confianza.

5 De no contar con profesional DECE, será la tutora/tutor el responsable de accionar el proceso.

11. Cualquier miembro del personal educativo y administrativo que tenga conocimiento de un presunto caso de violencia digital, tanto dentro como fuera de la institución educativa, debe presentar la denuncia inmediata ante las instancias correspondientes.

12. La máxima autoridad institucional deberá notificar el caso mediante oficio al Distrito Educativo, el cual, a su vez, reportará a la Coordinación Zonal o Subsecretaría de Educación (Quito o Guayaquil), según corresponda.

13. La/el profesional del Departamento de Consejería Estudiantil (DECE) deberá realizar el levantamiento de la ficha de datos informativos generales⁶ con el objetivo de recoger información que permita tener una visión amplia de la situación y de los caminos que se deba tomar para la atención psicosocial.



6 Esta ficha se encuentra en el Anexo 2: Orientaciones para el Eje de Atención Psicosocial del Modelo de Gestión del Departamento de Consejería Estudiantil (2023), páginas 81 a 85. Disponible en: <https://educacion.gob.ec/wp-content/uploads/downloads/2023/06/modelo-DECE.pdf>



Importante

- En ocasiones, es difícil identificar a la persona agresora en línea debido al anonimato de las redes sociales, la suplantación de identidad y la creación de perfiles falsos. Es importante guardar la evidencia digital y reunir la mayor cantidad de pruebas posibles, incluyendo capturas de pantalla, números de teléfono, usuarios de redes sociales y correos electrónicos. Evite borrar los intercambios y mensajes recibidos. Estos insumos deberán ser entregados a Fiscalía para la debida investigación.
- Antes de que inicie la investigación no es conveniente bloquear ni denunciar al perfil de la persona que acosa y tampoco amenazarla ni enfrentarla, ya que se corre el riesgo de perder pruebas. Una vez presentada la denuncia e iniciada la investigación se sugiere denunciar el perfil de la persona que acosa. Esto podría ayudar a establecer un precedente y evitar que se repitan los abusos con otras personas.
- Es importante no hacerse pasar por la víctima para sumar pruebas, ya que luego se puede entorpecer la investigación.
- Se debe garantizar la reserva y la confidencialidad de la información a lo largo del proceso.
- Se deberá analizar el tipo del presunto delito cometido, considerando si hubo un encuentro personal o si se mantuvo en el ámbito digital. Estos datos son importantes al momento de presentar la denuncia en Fiscalía.
- En los casos en los que las situaciones de violencia virtual también conllevan actuaciones que ocurren en entornos físicos es importante aplicar el “Protocolo y ruta de actuación frente a situaciones de violencia detectadas o cometidas en el sistema educativo”⁷.

¿Dónde denunciar un presunto caso de violencia digital?

Fiscalía General del Estado

1. Canal de denuncia on-line, por medio del cual se reciben denuncias de posibles hechos de violencia sobre la base de género e intrafamiliar, pornografía infantil, grooming, incluido el contacto con finalidad sexual y oferta de servicios sexuales con menores de dieciocho años usando medios electrónicos, a través del siguiente enlace: <https://www.fiscalia.gob.ec/denuncia-en-linea-violencia-contrala-mujer/>

2. Servicio de Atención Integral para la recepción de denuncias de forma presencial a escala nacional⁸

- Si en una situación de violencia digital relacionadas con el ciberbullying o acoso escolar entre estudiantes, la persona que detecte el hecho, al considerarse una contravención, debe denunciarlo de inmediato a las Unidades Judiciales Especializadas en Familia, Mujer, Niñez y Adolescencia. También puede acudir a la Junta Cantonal de Protección de Derechos o a la Defensoría Pública de su localidad.

- En situaciones de violencia entre estudiantes se debe analizar cada contexto y considerar los agravantes (niveles de riesgo alto) desde una mirada integral para la intervención, específicamente en casos que implican un presunto delito como violencia sexual, pornografía infantil, violación a la intimidad, extorsión, amenazas, entre otros, debe ser denunciado en Fiscalía.



Intervención – actuación

1. La persona que solicita y entrega la ficha de reporte de hecho de violencia debe indicar el motivo, cuáles fueron los primeros elementos de alarma y cuándo se produjeron, así como las medidas que ya se adoptaron.

2. Es importante considerar una adecuada **contención emocional** o **intervención en crisis** (observar-escuchar-conectar) antes de proceder con el abordaje o diagnóstico situacional.

Se deberá comunicar a la o el estudiante que el siguiente paso será el desarrollo de la valoración (**diagnóstico situacional**)⁹. El diagnóstico situacional se considerará desde la esfera individual, familiar -proceso psicoeducativo de corresponsabilidad- y grupal.

3. Se generará, además, un espacio para informar y proceder con las firmas de los representantes legales y del propio estudiante del consentimiento informado para la atención psicosocial¹⁰ que incluirá el plan de trabajo y los compromisos de ambas partes.

8 Puede encontrar el directorio de fiscalías a nivel nacional en el siguiente enlace: <https://www.fiscalia.gob.ec/directorio-fiscalias/>

9 Consta en el Modelo de gestión de los Departamentos de Consejería Estudiantil (2023).

10 Este documento se encuentra en el Anexo 2: orientaciones para el eje de atención psicosocial del modelo de gestión del departamento de consejería estudiantil (2023), pag 84 a 92.

4. En un **caso emergente** en el cual se debe actuar de manera oportuna, corresponde a la autoridad de la institución educativa comunicarse inmediatamente con los representantes del/la estudiante.

5. La/el profesional del Departamento de Consejería Estudiantil deberá elaborar la **ficha de plan de atención psicosocial**¹¹ por presunto caso de violencia digital.

Importante



- **En casos de violencia digital entre pares, la intervención-actuación se deberá realizar tanto con la víctima o víctimas como con el/la agresor/a o agresores/as (considerando el enfoque restaurativo).**
- Una vez que el director o directora Distrital o la Junta Distrital de Resolución de Conflictos tome conocimiento de una denuncia, debe dictar de inmediato medidas de protección a favor de la víctima/s.
- De acuerdo con Ley Orgánica de Educación Intercultural, la Junta Distrital de Resolución de Conflictos tiene la obligación de aplicar las acciones educativas disciplinarias en casos de violencia o acoso escolar, incluido el ciberacoso.
- El proceso disciplinario se aplicará respetando las garantías constitucionales y siguiendo los lineamientos establecidos en la normativa vigente, con el objetivo de proteger integralmente los derechos a la educación de las y los estudiantes involucrados.
- La Junta Distrital de Resolución de Conflictos, dentro de sus competencias, debe asegurar la implementación de medidas de protección a la víctima, tal como lo establece la ley. Estas medidas se aplicarán según la gravedad de lo sucedido. Es importante tener en cuenta que en ningún proceso disciplinario relacionado con violencia en línea se debe realizar confrontaciones, mediaciones o resoluciones alternativas de conflictos entre los implicados (víctima y agresor), ya que esto podría causar revictimización.

11 Son las acciones para la detección, intervención, derivación, seguimiento y reparación, dirigidas a estudiantes que se encuentren atravesando por situaciones como: inestabilidad emocional, conflictos (individual, escolar, familiar, social, adaptativo), desastre natural, vulneración de derechos, o de riesgo psicosocial que pueda afectar su desarrollo integral. La ficha se encuentra en el Anexo 2: orientaciones para el eje de atención psicosocial del modelo de gestión del departamento de consejería estudiantil (2023), pág. 87.

Estrategias

Para realizar el diagnóstico situacional

- Considerar en la valoración aspectos personales, familiares, sociales e institucionales de la o el estudiante.
- La valoración debe realizarse sin juicios de valor previos y con un alto nivel de asertividad, empatía y respeto, de manera que se pueda conocer de forma integral la situación que está viviendo la o el estudiante.
- Identificar fortalezas y potencialidades, riesgos y factores protectores, los vínculos afectivos y las diversas problemáticas específicas, entre otras.
- Las entrevistas¹² son una herramienta útil y necesaria al momento de realizar la valoración (diagnóstico situacional).
- Revisar el expediente de **bienestar estudiantil** podría resultar útil para visibilizar la historia de vida de la o el estudiante.
- Tomar en cuenta la información recolectada en la **ficha de datos informativos generales**.

Para elaborar el Plan de Atención Psicosocial

- Tomar en consideración las acciones para la intervención que se detallan en el Modelo de Gestión del Departamento de Consejería Estudiantil (2023).
- Trabajar en el fortalecimiento de las habilidades socioemocionales, pues es importante promover el manejo de emociones y resolución de conflictos. De igual manera, es relevante instaurar procesos resilientes y reparadores.
- Es relevante priorizar acciones específicas para fortalecer las habilidades de resolución alternativa de conflictos y promover el uso seguro y prevención de riesgos en línea.
- Se debe prestar especial atención al apoyo pedagógico y relacional de la persona que agredió a sus pares¹³.
- Incluir estrategias y metodologías de trabajo grupal (docentes/representantes/estudiantes) que permitan a cada miembro de la comunidad educativa reflexionar sobre las problemáticas detectadas, sin abordar directa y específicamente el caso de violencia, evitando exponer a las personas involucradas.



Lineamientos de acompañamiento

- Explicar en qué consiste el proceso de atención psicosocial y sensibilizar sobre su importancia.
- Enfatizar en el compromiso y participación que debe adoptar la madre, el padre o el representante legal y la o el estudiante frente al proceso de atención psicosocial.
- Sensibilizar sobre la relevancia de derivación a servicios especializados (psicoterapia) y la activa participación y responsabilidad que se debe tener con dicho proceso.
- La autoridad educativa institucional o el personal del Departamento de Consejería Estudiantil debe informar a los representantes legales tanto de la víctima como del agresor o agresores sobre lo sucedido. Durante esta reunión se compartirá información sobre los hechos ocurridos, las acusaciones existentes y las pruebas disponibles. Además, se informará sobre las acciones legales correspondientes que competen al centro educativo, los pasos a seguir y las medidas que se tomará desde la institución educativa.

12 En el apartado 6 del Anexo 2: Orientaciones para el Eje de Atención Psicosocial del Modelo de Gestión del Departamento de Consejería Estudiantil (2023), páginas 96 a 103, encontrará orientaciones para la entrevista.

13 En caso de no contar con DECE, esta intervención debería ser realizada por la/el docente tutor.

Derivación

La derivación es la activación de las redes de apoyo internas o externas a la institución educativa o al Ministerio de Educación para la atención especializada a estudiantes. Para esto, es importante que se haya identificado a los organismos internos de la institución educativa, dependencias del Sistema Nacional de Educación y a las entidades, instituciones, organizaciones y servicios que se encuentran en la localidad que pudiesen apoyar en la atención integral.

- 1.** Para efectos de derivación la/el profesional del Departamento de Consejería Estudiantil deberá elaborar la **ficha de derivación**¹⁴ hacia instancias externas a la institución educativa o al Ministerio de Educación.
- 2.** El/la profesional del Departamento de Consejería Estudiantil deberá remitir oportunamente la ficha de derivación a la máxima autoridad institucional para proceder con la derivación.
- 3.** La máxima autoridad institucional deberá remitir a las instancias externas correspondientes, mediante oficio, la ficha de derivación para la atención especializada de la o el estudiante y su familia, en caso de ser necesario.
- 4.** Si dentro del plan para la atención psicosocial se ha determinado que la o el estudiante requiere atención de **derivación interna** a la institución educativa (ejemplo: estrategias psicopedagógicas, actividades de tutoría y refuerzo académico) porque se encuentra hospitalizado/institucionalizado¹⁵ o se encuentra recibiendo tratamiento psicológico y/o psiquiátrico que le impide ejecutar sus actividades académicas con normalidad y/o similares; la derivación se realizará directamente desde el Departamento de Consejería Estudiantil y se pondrá en conocimiento de la máxima autoridad institucional. Esta acción se realizará con el fin de facilitar la permanencia en el sistema educativo de la o el estudiante y prevenir la deserción escolar, además, como un mecanismo que aporte en su recuperación.

¹⁴ Esta ficha se encuentra en el Anexo 2: orientaciones para el eje de atención psicosocial del Modelo de Gestión del Departamento de Consejería Estudiantil (2023), páginas 92 a 94.

¹⁵ Ingreso de una persona en una institución (hospital, residencia, etc.), donde residirá un tiempo determinado bajo observación estrecha por el riesgo de lastimarse a sí mismo y/o a los demás.

Instancias externas competentes en la atención de situaciones de violencia digital son:

Instancias		Competencias	
Defensa y exigibilidad de derechos			
Fiscalía General del Estado			<ul style="list-style-type: none"> -Es el órgano encargado de la investigación y persecución penal en Ecuador. -Entre sus competencias se encuentran la investigación previa, la acusación fiscal, la representación del Estado en juicio, puede proponer medidas de protección y reparación, protección a las víctimas y testigos, entre otras. Receptar denuncias sin la necesidad de un abogado o informe.
Consejo de la Judicatura			<ul style="list-style-type: none"> -Tiene competencias relacionadas con garantizar que los procesos judiciales y administrativos se lleven a cabo adecuadamente para lograr una reparación integral a las víctimas. -Son los jueces quienes determinan medidas de reparación judiciales.
Defensoría del Pueblo			<ul style="list-style-type: none"> -Brinda asesoría legal a las víctimas y realiza la vigilancia del debido proceso, incluyendo las medidas de reparación.
Juntas Cantonales de Protección de Derechos			<ul style="list-style-type: none"> -Atención de denuncias y restitución y protección de derechos de niñas, niños y adolescentes. -Disposición de medidas administrativas para la protección de las niñas, niños y adolescentes.
Atención integral			
Instancias		Competencias	
Ministerio de Inclusión Económica y Social			<ul style="list-style-type: none"> -Tiene competencias relacionadas con brindar servicios sociales y protección a niñas, niños y adolescentes víctimas de violencia (como casas de acogida), también el colaborar con la reparación integral a través del seguimiento y verificación del cumplimiento de las acciones dictadas en el marco de sus competencias.
Ministerio de Salud			<ul style="list-style-type: none"> -Tiene como competencias principales la regulación, planificación, coordinación, ejecución y control de políticas públicas en materia de salud. Estas competencias se encuentran detalladas en la Ley Orgánica de Salud de Ecuador. - Atención inmediata a niñas, niños y adolescente que han sido víctimas de violencia. -Las víctimas pueden recibir atención médica y apoyo psicológico. -Realizar la calificación de discapacidad.

Importante



- Una vez identificada la necesidad de que la/el estudiante requiera de un servicio externo, el representante legal, madre o padre de familia tiene la obligación de acompañar y garantizar la asistencia y el acceso al servicio. De lo contrario, el profesional del Departamento de Consejería Estudiantil (DECE) deberá reportarlo a la autoridad institucional para la activación inmediata de la ruta de “Actuación frente a casos de Violencia Intrafamiliar” por **NEGLIGENCIA**¹⁶, con el fin de garantizar y salvaguardar la integridad de niñas, niños, adolescentes.
- Se pondrá en conocimiento de la Junta Distrital de Resolución de Conflictos cualquier omisión o negligencia por parte de la autoridad institucional o cualquier miembro de la comunidad educativa, en referencia a la actuación y/o abordaje de situaciones que impliquen riesgos psicosociales.

Lineamientos de acompañamiento



Las causales para derivar a estudiantes que están en el proceso de atención psicosocial son:

- Cuando se identifica que las y los estudiantes requieren de un proceso psicoterapéutico.
- Cuando las y los estudiantes requieren de evaluación psicopedagógica y/o apoyo psicopedagógico.
- Cuando la situación de las y los estudiantes está relacionada con temas disciplinarios.
- Cuando las y los estudiantes requieren valoración en otras áreas distintas a la de atención psicosocial.

Seguimiento

El seguimiento es la observación oportuna que permite evidenciar el desarrollo de las estrategias contenidas en el plan de atención psicosocial que se ha trazado por profesionales del Departamento de Consejería Estudiantil y/o por profesionales, instancias u organismos a los cuales se ha derivado el caso, para brindar atención oportuna a estudiantes que se encuentren en una situación de vulnerabilidad o riesgo psicosocial.

Las instituciones educativas tienen la responsabilidad, a través de la autoridad institucional, docentes, profesional del Departamento de Consejería Estudiantil (DECE) y la familia, de realizar seguimiento a la condición de niños, niñas y adolescentes de forma continua, respetuosa y ágil, de manera interna y externa.

- 1.** La/el profesional del Departamento de Consejería Estudiantil (DECE) deberá evidenciar el avance de las estrategias planteadas en el plan de atención psicosocial a través de reuniones periódicas con la o el estudiante y su representante legal, madre o padre de familia. La periodicidad de las reuniones dependerá del nivel de riesgo existente, pero se establece en al menos una **reunión mensual** para evaluar el estado de caso.
- 2.** La/el profesional del Departamento de Consejería Estudiantil (DECE) deberá registrar en el apartado de **seguimiento de la atención psicosocial**¹⁷ las intervenciones y acciones realizadas de acuerdo con lo planificado, incluyendo el seguimiento a las derivaciones externas e internas, considerando la protección integral de niñas, niños, adolescentes en condición de vulnerabilidad.
- 3.** El seguimiento finaliza cuando las acciones planificadas para la atención psicosocial que brinda el personal del Departamento de Consejería Estudiantil (DECE), con el apoyo de instancias externas, se han cumplido conforme con los objetivos propuestos o cuando el estudiante ha concluido sus estudios.

Lineamientos de abordaje

Frente a casos de violencia cometidos por personas adultas:	Frente a situaciones de violencia o acoso escolar entre pares:
<p>El personal del Departamento de Consejería Estudiantil debe derivar a la víctima y a su familia a servicios de atención externa que brinden apoyo emocional y tratamiento psicológico sostenido, utilizando el formato de informe de derivación.</p>	<p>El equipo del Departamento de Consejería Estudiantil debe ofrecer apoyo psicosocial tanto a las víctimas como a los agresores y sus familias y generar espacios de reflexión dirigidos a la comunidad educativa a través de círculos restaurativos.</p>
<p>La Red de Consejería Estudiantil (RCE) debe estar activa permanentemente para generar estrategias y programas de prevención, derivación e intervención en coordinación con otras instancias, con el objetivo de proteger integralmente a la víctima y promover la corresponsabilidad y participación de la comunidad.</p>	<p>El personal del Departamento de Consejería Estudiantil o, en su ausencia, la autoridad educativa institucional debe derivar a la víctima y al presunto agresor a servicios de atención externa que brinden apoyo emocional y tratamiento psicológico sostenido, utilizando el formato de informe de derivación.</p>

17 El Seguimiento de la Atención Psicosocial se encuentra en el segundo apartado de la Ficha de Atención Psicosocial y Seguimiento, ubicada en el Anexo 2: Orientaciones para el Eje de Atención Psicosocial del Modelo de Gestión del Departamento de Consejería Estudiantil (2023), página 87.

Importante

- La autoridad institucional deberá garantizar la permanencia del estudiante en el sistema educativo con el apoyo del profesional del Departamento de Consejería Estudiantil (DECE) y las/los docentes.
- El seguimiento que realizan las/los profesionales del Departamento de Consejería Estudiantil (DECE), está enmarcado en la atención psicosocial.
- Se considerará de obligatoriedad la participación de la familia en el proceso.
- La familia deberá comunicar oportunamente a la institución educativa, a la figura de la autoridad educativa y/o profesional del Departamento de Consejería (DECE), el proceso de evolución o eventualidades de su representando/a que pueda influir en su proceso educativo y que, a su vez, amerite otras acciones.
- En el caso de derivación externa, se realizará seguimiento periódicamente para abordar, de manera integral, los avances de el o la estudiante.



Reparación

Es el conjunto de acciones que se realiza con el fin de reestablecer y garantizar el estado de bienestar de estudiantes que han sido afectados por algún o algunos tipos de riesgos psicosociales detectados o cometidos dentro del sistema educativo.

La reparación no es una responsabilidad exclusiva del Departamento de Consejería Estudiantil (DECE), sin embargo, este departamento debe velar por que las medidas de reparación que se hayan dictado se cumplan en la institución educativa.

- 1.** La máxima autoridad institucional deberá asegurar el cumplimiento del plan de atención psicosocial y seguimiento, confirmando que las acciones adoptadas hayan aportado con el restablecimiento y garantía del estado de bienestar de estudiantes en situación de violencia digital.
- 2.** La máxima autoridad institucional pondrá en conocimiento de la intervención al Distrito Educativo mediante oficio.

3. En caso de que la máxima autoridad institucional o el Distrito Educativo no aprobasen el plan de atención psicosocial y seguimiento, porque se ha determinado que las acciones adoptadas no han aportado con el restablecimiento y garantía del estado de bienestar de estudiantes en situación de violencia digital, el plan de atención psicosocial deberá ser reevaluado y reestructurado por el profesional del Departamento de Consejería Estudiantil, hasta cumplir con los objetivos propuestos; además, deberá considerar apoyarse en el perfil del DECE Distrital.

Importante



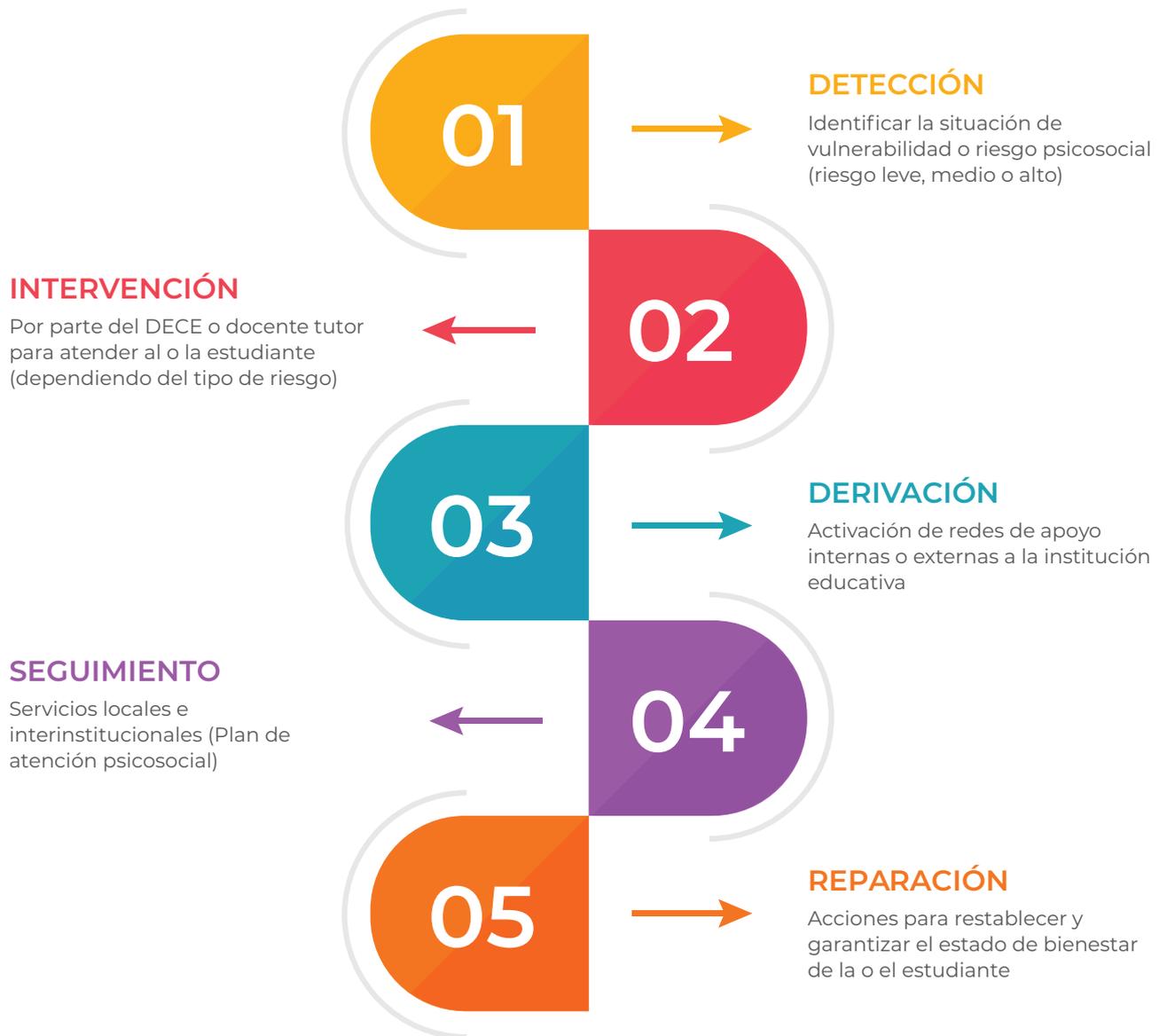
- Cuando las instancias competentes determinan la existencia de un delito, la/el profesional del Departamento de Consejería Estudiantil de la institución educativa estará a cargo de realizar el **seguimiento de los procesos de reparación y restitución de derechos de la víctima en el aspecto psicosocial.**
 - La Junta Distrital de Resolución de Conflictos y la autoridad educativa institucional garantizarán la permanencia y seguridad o protección del estudiante agredido y del agresor en el sistema educativo, cumpliendo con las responsabilidades establecidas en la Ley Orgánica de Educación Intercultural y su Reglamento General.
- La institución educativa deberá garantizar la prevención de situaciones de riesgo, protección y bienestar de niñas, niños y adolescentes y la reparación del tejido social con la comunidad educativa a través de sensibilizaciones, campañas preventivas, círculos restaurativos, entre otros.

Lineamientos de acompañamiento

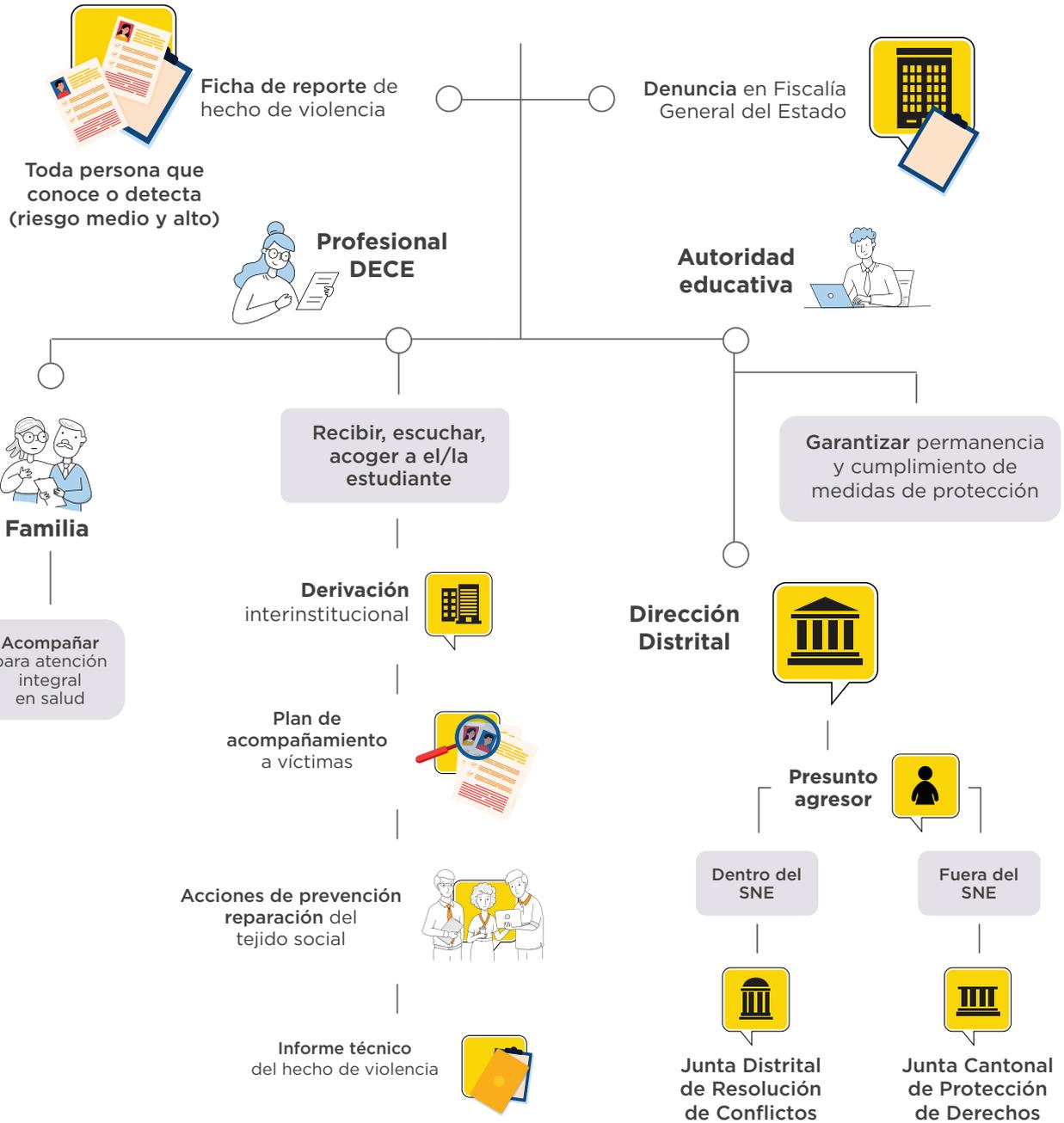
- De otra parte, el o la profesional del Departamento de Consejería Estudiantil deberá completar el expediente de bienestar estudiantil con las acciones que se realicen en los diferentes momentos de atención psicosocial, así como con las realizadas en los ejes de consejería, promoción - prevención e inclusión¹⁸.



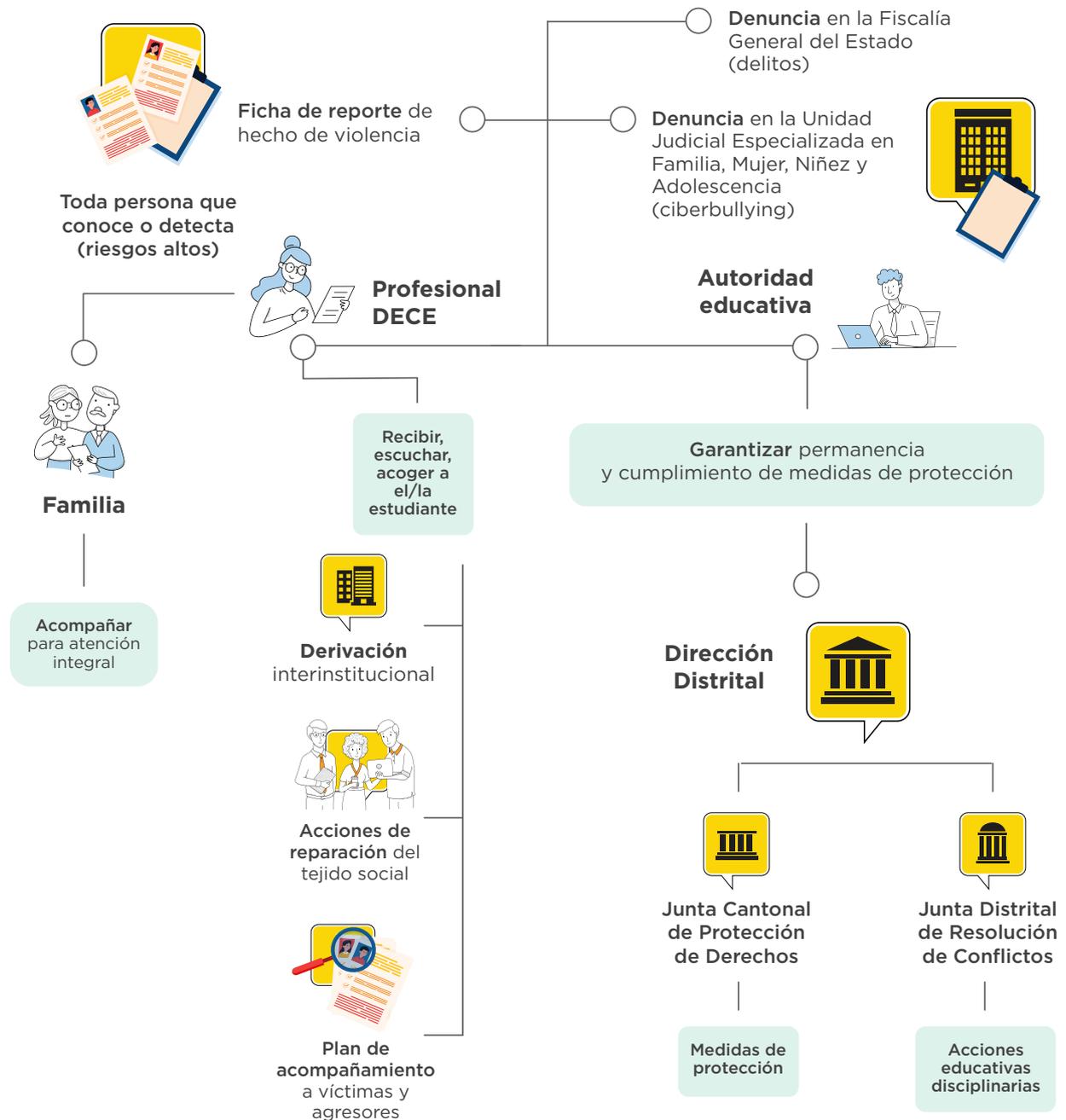
Ruta frente a casos de violencia digital



Ruta frente a casos de violencia digital que involucra a personas adultas



Ruta frente a casos de violencia digital entre pares



Anexo

Formato: ficha de reporte de hecho de violencia

FICHA DE REPORTE DEL HECHO DE VIOLENCIA							
Institución educativa:							
Informe N°:	Fecha:						
Nombre de profesional DECE:							
1. DATOS GENERALES DE IDENTIFICACIÓN DE EL O LA ESTUDIANTE							
Apellidos y nombres:							
Fecha de nacimiento:	Día:	Mes:	Año:				
Edad:							
Grado o curso:							
2. DATOS GENERALES DE LA MADRE, PADRE Y/O REPRESENTANTE LEGAL							
Nombres y apellidos:							
Vínculo entre la persona y el/la estudiante:							
Dirección del domicilio:							
Teléfono de contacto:							
3. DATOS SOBRE LA PRESUNTA SITUACIÓN DE VIOLENCIA							
Fecha y lugar en el que ocurrió la situación de violencia:							
Día:	Mes:	Año:					
Lugar:							
Nombres y apellidos de la presunta persona responsable de la agresión:							
Tipo de relación de quien realizó la agresión con la víctima:							
4. DATOS DE LA PERSONA QUE REFIERE EL CASO							
Nombres y apellidos:							
Cédula de identidad:							
Cargo:							
5. TIPO DE VIOLENCIA IDENTIFICADA							
Física	<input type="checkbox"/>	Psicológica	<input type="checkbox"/>	Sexual	<input type="checkbox"/>	Negligencia	<input type="checkbox"/>
A través de medios digitales:				<input type="checkbox"/>			
A través de contacto físicos:				<input type="checkbox"/>			
Observaciones: (identificar si el hecho ocurrió en el entorno digital y se trasladó al entorno físico o viceversa)							

6. MODALIDAD DE VIOLENCIA IDENTIFICADA

Intrafamiliar

Institucional

Acoso escolar

Violencia estudiante- persona adulta

Otras

7. RESUMEN DEL PRESUNTO HECHO DE VIOLENCIA COMETIDO O DETECTADO (Transcriba detalladamente lo expresado por el/la estudiante o la persona que refiere la presunta situación, de manera objetiva.

La persona refiere que...

(Si conoce o tiene información de que el presunto hecho de violencia se mantuvo en el ámbito digital o si hubo un encuentro o contacto personal se debe informar)

.....
Nombre y apellido persona que registra la ficha
del hecho de violencia

.....
Nombre y apellido de la autoridad educativa

Observaciones:

Recuerde el deber de denunciar según el artículo 422 del COIP.

Referencias

- ChildFund. (2023). Campaña “Naveguemos Seguros. Quito. Obtenido de <https://www.eloriente.com/articulo/childfund-presento-en-ecuador-la-campa-na-naveguemos-seguros/38860>
- CNII. (2020). Política pública por una internet segura para niños, niñas y adolescentes. Quito.
- CNII, C. N. (2020). Política pública por una internet segura para niños, niñas y adolescentes. Quito.
- CO:RE - Children Online: Research and Evidence, C. (2021). CO:RE. Obtenido de The 4Cs: Classifying Online Risk to Children: https://www.ssoar.info/ssoar/bitstream/handle/document/71817/ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf?sequence=4&isAllowed=y&lnkname=ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf
- Del Ecuador, C.N. (2003). Código de la Niñez y Adolescencia. Obtenido de https://www.igualdad.gob.ec/wp-content/uploads/downloads/2017/11/codigo_ninezyadolescencia.pdf
- ECPAT, E. C. (2016). Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexuales. Luxemburgo.
- Ecuador, A. N. (2008). Constitución de la República del Ecuador.
- Ecuador, A. N. (2011). Ley Orgánica de Educación Intercultural.
- Ecuador, A. N. (2014). Código Orgánico Integral Penal.
- Ecuador, A. N. (mayo de 2021). Ley Orgánica de Protección de Datos Personales. Ecuador: Registro oficial Nro. 459.

Federación Internacional de Periodistas. (2021). ¿QUÉ SON LAS FAKE NEWS? Guía para combatir la desinformación.

Fundación Paniamor, P. (2017). Uso de Internet.

INEC, I. N. (2021). Indicadores de tecnología de la información y educación. Ecuador: INEC.

MERCOSUR, M. (2022). Políticas públicas contra el acoso escolar y el ciberacoso en el MERCOSUR. Buenos Aires.

Methaodos, R. d. (2018). La representación del menor en la publicidad infantil. De la inocencia a la sexualización.

Mineduc. (2021). Promoción de Derechos en el uso seguro de la Internet, desde las familias. Guía para los docentes y tutores.

Mineduc. (2021). Promoción de Derechos en el uso seguro de la Internet, desde las familias. Guía para los docentes y tutores. Quito.

Ministerio de Educación Argentina, Argentina. (2021). Guía sobre Violencia Digital.

Ministerio de Educación de Colombia. (2021). Colombia aprende. Obtenido de Protocolo para la prevención del Ciberacoso y Delitos en medios digitales: https://www.colombiaprende.edu.co/sites/default/files/files_public/2021-04/PEQ_protocolo%20ciberacoso.pdf

Ministerio de Educación de Colombia. (2022). Guía Pedagógica para la Mediación Docente en el Uso de Internet.

Ministerio de Educación de Ecuador. (2020). Guía para la prevención de Riesgos durante el uso de internet y dispositivos tecnológicos.

Ministerio de Educación de Ecuador. (2022). Protocolos y rutas de actuación frente a SITUACIONES DE VIOLENCIA detectadas o cometidas en el sistema educativo. Quito: Mineduc.

ONU. (1989). Convención sobre los Derechos del Niño.

ONU. (2021). Observación general núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital. CRC.

- ONU Mujeres. (2020). Violencia contra las mujeres y niñas en el espacio digital. Obtenido de <https://mexico.unwomen.org/sites/default/files/Field%20Office%20Mexico/Documentos/Publicaciones/2020/Diciembre%202020/FactSheet%20Violencia%20digital.pdf>
- Ramos, I. L. (2017). Adaptation and validation of the yildirim & correia nomophobia scale in Spanish students.
- Real Academia de la Lengua. (2023). Diccionario panhispánico del español jurídico.
- Riamusi, I. (2018). Red Intergeneracional para la Promoción del Uso Seguro de Internet. República Dominicana: Riamusi.
- Riamusi, R. I. (2019). Protocolo para el Uso Seguro de Internet. Panamá: INN. Obtenido de Protocolo para el Uso Seguro de Internet.
- Unesco. (2018). UNESCO. Obtenido de Nota Conceptual. COMPETENCIAS PARA UN MUNDO CONECTADO: <https://es.unesco.org/sites/default/files/unesco-mlw2018-concept-note-es.pdf>
- Unesco. (2019). Seguridad de los niños en línea: minimizando el riesgo de la violencia, el abuso y la explotación en línea. Unesco.
- Unesco. (2020). Ciudadanía Digital. Curriculum para la Formación Docente. Montevideo.
- Unicef. (04 de Febrero de 2019). Unicef pide que se tomen medidas conjuntas para evitar el acoso y la intimidación que sufre el 70% de los jóvenes conectados mundialmente. Obtenido de <https://www.unicef.org/es/comunicados-Minpresna/d%C3%ADa-para-un-internet-m%C3%A1s-seguro-unicef-pide-que-se-tomen-medidas-conjuntas-para>
- Unicef. (2022). Internet Seguro, U-Report, Resultados encuesta. Obtenido de Unicef, Ministerio de Educación: <https://www.unicef.org/ecuador/sites/unicef.org.ecuador/files/2023-03/Resultados-Internet-Seguro.pdf>





Ministerio de Educación



República
del Ecuador