Protocolo para la prevención y atención de casos de violencia digital contra niñas, niños y adolescentes en escuelas de nivel básico en México

ChildFund®
México

ChildFund México

Misión

Construir capacidades en niños y niñas en condiciones de carencia, exclusión y vulnerabilidad para mejorar sus vidas y que se conviertan en líderes que generen cambios positivos y duraderos en sus comunidades; Promover sociedades cuyos individuos e instituciones valoren, protejan y fomenten los derechos de la infancia.

Enriquecer las vidas de nuestros seguidores a través del apoyo que brindan a nuestra causa.

Visión

Un mundo en el cual niñas y niños ejercen sus derechos y alcanzan su potencial. Más niñas y niños viven en condiciones que permiten su óptimo desarrollo en cada etapa de sus vidas, incluyendo la protección contra el maltrato, negligencia, explotación y violencia.

Avenida Patriotismo #889

01 55 5611 7733

www.childfundmexico.org.mx

/childfundmx

@ChildFundMexico

/company/childfundmx

Directorio

Directora Nacional:
Victoria Fuentes Castañeda

Gerente de Programas:
Morgane Bellion

Gerente de Patrocinio:
Silvia Herrera Balaguera

Especialista Sr., Protección a la niñez e Incidencia:
Yil Aida Felipe Wood

Especialista en Comunicación y Marketing:
Paola Barrera Vázquez

Créditos Protocolo

Coordinación de contenidos:
Yil Aida Felipe Wood

Elaboración de contenidos
Víctor Hugo Rodas Balderrama

Coordinación de diseño y edición:
Paola Barrera Vázquez y Yil Aida Felipe Wood

Diseño e Ilustración:
Víctor Hugo Rodas Balderrama

Créditos Historias para la Prevención de la Violencia Digital

Elaboración de contenidos
Carlos Díaz Espinoza y Yil Aida Felipe Wood

Diseño e Ilustración:
Rafael Barco de Vela

Agradecimientos

A las maestras y a los maestros de Coatepec (VER) y Atlacomulco (Edo. México) que participaron en los grupos focales de validación. A la Comisión para la Prevención y Atención de Conductas Antisociales (COPACA) de la Secretaria de Educación de Veracruz. A la organización Niños de Bobashi IAP, socio local de ChildFund México. A todos, muchas gracias.

Este material ha sido posible gracias a la colaboración de las madrinas y los padrinos de ChildFund México.

Primera edición, 2023.

Avenida Patriotismo #889
Col. Insurgentes Mixcoac
Del. Benito Juárez
Ciudad de México
CP 03920
www.childfundmexico.org.mx

Contenido

Contenidos

Presentación

El desarrollo de las tecnologías de la información y comunicación presenta grandes oportunidades para el ejercicio eficaz de los derechos de niñas, niños y adolescentes, pero también grandes riesgos para ellas y ellos cuando no se cuenta con los mecanismos suficientes para prevenir y atender la violencia en el entorno digital.

La protección y defensa de los derechos humanos de las personas menores de edad en el entorno digital es una obligación de quienes se encuentran a cargo de su cuidado, así como de todas las autoridades sin importar su rango o jerarquía en la administración pública.

Las instituciones del sistema educativo, como lugar de coincidencia entre niñas, niños y adolescentes, representan el espacio ideal para establecer mecanismos de capacitación sobre el uso adecuado y seguro del entorno digital, pero también para implementar procesos de prevención de la violencia digital, así como para la atención adecuada de los casos en los que esta forma de violencia se manifieste.

El presente Protocolo, busca aportar al establecimiento de un marco estandarizado de actuación para la prevención y atención de casos de violencia digital en contra de niñas, niños y adolescentes en escuelas de nivel básico de México, para su elaboración se recopilaron y sistematizaron diversos criterios establecidos por organismos internacionales y nacionales especializados en violencia digital y ciberseguridad, así como de la normatividad mexicana aplicable.

ChildFund México

PROTOCOLO PARA LA PREVENCIÓN Y ATENCIÓN DE CASOS DE VIOLENCIA DIGITAL EN CONTRA DE NIÑAS, NIÑOS Y ADOLESCENTES EN ESCUELAS DE NIVEL BÁSICO EN MÉXICO

I. OBJETO

El presente Protocolo ha sido diseñado para prevenir la violencia digital en contra de niñas, niños y adolescentes en las escuelas de nivel básico de México y establecer una ruta integral para la atención de los casos en los que esta forma de violencia se manifiesta.

Para lograrlo, el Protocolo establece:

- Los conceptos y definiciones de las diferentes formas de manifestación de la violencia digital en contra de niñas, niños y adolescentes.
- Los pasos a seguir para prevenir que niñas, niños y adolescentes sean víctimas de violencia digital.
- Los pasos a seguir para que madres, padres, tutores y cuidadores puedan identificar la violencia digital en contra de niñas, niños y adolescentes y hacerla del conocimiento de las autoridades responsables de su atención.
- El procedimiento que el personal docente, administrativo y directivo de las escuelas de nivel básico en México debe llevar a cabo para atender y documentar la violencia digital en contra de niñas, niños y adolescentes.
- Las herramientas metodológicas para evitar la revictimización de niñas, niños y adolescentes en el proceso de documentación de los casos de violencia digital.

II. ÁMBITO DE APLICACIÓN

El Protocolo está diseñado para su aplicación en el nivel básico del sistema educativo nacional mexicano el cual comprende los niveles de educación inicial, preescolar, primaria y secundaria.[1]

Está dirigido a niñas, niños y adolescentes de 0 a 18 años de edad que cursan el nivel básico de educación y/o bachillerato, a sus madres, padres, tutores o cuidadores, así como a las autoridades educativas que llevan a cabo funciones de docencia, administración o dirección en unidades educativas de nivel básico en México.

Para su adecuada implementación, el Protocolo contempla dos tipos de procedimientos distintos, uno especializado en la prevención de casos de violencia digital en contra de niñas, niños y adolescentes en escuelas de nivel básico y otro encaminado a la atención de los casos en los que este tipo de violencia se haya manifestado en contra de personas menores de edad.

El presente Protocolo contempla procedimientos para la prevención y atención de los siguientes tipos de violencia digital:

- Ciberacoso
- Ciberbullying
- Grooming
- Sexting
- Phishing, smishing, vishing
- Retos virales nocivos
- Violencia digital en la pareja o expareja
- Explotación sexual comercial infantil en el entorno digital
- Morphing
- Violencia digital en videojuegos.

El Protocolo está homologado a estándares de protección de niñas, niños y adolescentes establecidos por organismos nacionales e internacionales y constituye una herramienta metodológica que **no suple la obligatoriedad de cumplimiento de la normatividad aplicable en cada entidad federativa de la república mexicana.**

1 Cfr. Ley General de Educación, Publicada en el Diario Oficial de la Federación el 04 de diciembre de 2014, última reforma publicada en el Diario Oficial de la Federación el 26 de mayo de 2023, “Artículo 37. La educación básica está compuesta por el nivel inicial, preescolar, primaria y secundaria. [...]”

Si bien el Protocolo fue diseñado para escuelas de nivel básico, también puede ser aplicado a casos de personas menores de edad en bachillerato.

III. MARCO CONCEPTUAL

Para una adecuada implementación del presente **Protocolo**, se entenderá por:

- **Autoridad educativa**

Personal docente, administrativo y directivo responsable de la documentación de la violencia digital sufrida por las víctimas.

- **Ciberacoso**

Es una forma de violencia digital en la que un adulto acosa o intimida a una persona menor de edad a través del entorno digital. Puede ocurrir en redes sociales (Facebook, X "Twitter", Instagram, Tik Tok, etc.); plataformas de mensajería (WhatsApp, Telegram, Snapchat, etc.); plataformas de juegos y teléfonos móviles. Es un comportamiento que se repite y que busca atemorizar, enfadar o humillar a una niña, niño o adolescente.[2]

El acoso y el ciberacoso ocurren juntos a menudo, pero el ciberacoso deja una huella digital; es decir, un registro que puede servir de prueba para ayudar a detener el abuso. Al ser cometido por una persona adulta en contra de una niña, niño o adolescente puede tener consecuencias penales para quien la cometa.

Son ejemplos de esta forma de violencia digital los siguientes:

1. Difundir mentiras, publicar fotografías o videos vergonzosos de una niña o niño en las redes sociales.
2. Enviar mensajes, imágenes o videos hirientes, abusivos o amenazantes a través de plataformas de mensajería.
3. Hacerse pasar por otra persona y enviar mensajes agresivos en nombre de dicha persona o a través de cuentas falsas.
4. Robo de contraseñas.

2 Cfr. UNICEF, "Ciberseguridad, como protegerte en Internet" Artículo en línea, disponible en: https://www.unicef.org/mexico/ciberseguridad y; Gobierno de México, "Ciberguía 2.0", Secretaría de Seguridad y Protección Ciudadana, Dirección General de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico, disponible en: https://www.gob.mx/sesnsp/documentos/ciberguia-2-0

- **Ciberseguridad**

Acciones y medidas empleadas para proteger a niñas, niños y adolescentes de la violencia en el entorno digital.

- **Ciberbullying**

Es un término que se utiliza para describir cuando una niña, niño o adolescente es molestado, amenazado, acosado, humillado, avergonzado o abusado por otra persona menor de edad, a través del entorno digital. Se caracteriza porque el ciberacoso se da entre dos iguales, en este caso, personas menores de edad. Es importante distinguirlo, ya que existen otras prácticas en la que se involucran adultos y que se denominan simplemente ciberacoso o acoso cibernético, con las consecuencias legales que tienen los actos de un mayor de edad en contra de una niña, niño o adolescente. [3]

- **Entorno digital**

Todas aquellas plataformas, aplicaciones u otras tecnologías de información y comunicación que nos permiten interactuar con otras personas y organizaciones a través de medios virtuales, así como los dispositivos y entornos conectados, la realidad virtual y aumentada, la inteligencia artificial, la robótica, los sistemas automatizados, los algoritmos y el análisis de datos, la biometría y la tecnología de implantes. Forman parte de este entorno digital de manera enunciativa más no limitativa, plataformas como Facebook, WhatsApp, Snapchat, X “Twitter”, YouTube, Instagram, Tik Tok o videojuegos como Freefire, Minecraft o Animal Crossing los cuales son muy populares entre niñas, niños y adolescentes.[4]

- **Explotación sexual comercial infantil en el entorno digital**

Es una forma de violencia digital que constituye una violación grave a los derechos de niñas, niños y adolescentes. Consiste en la explotación realizada por un adulto de fotografías o videos con contenido sexual de niñas, niños o adolescentes con fines comerciales a través del entorno digital. Esta forma de violencia digital puede presentarse como consecuencia del grooming, morphing o sexting.[5]

---

3 Cfr. Pablo Corona, Asociación de Internet MX, artículo en línea, disponible en: https://www.gob.mx/ciberbullying/articulos/que-es-el-ciberbullying

4 Cfr. Comité de los derechos del Niño, Observación General 25. los derechos de los niños en relación con el entorno digital, CRC/C/GC/25, publicada el 02 de marzo de 2021.

5 La explotación sexual comercial y la pornografía infantil han sido reconocidas y definidas en diversos instrumentos internacionales, no obstante, dichas definiciones no abarcan al entorno digital. El Comité de los Derechos del Niño en su Observación General 25, “Los derechos de los niños en relación con el entorno digital”, párrafos 80 – 83, ha señalado que ambas pueden perpetrarse también en el entorno digital, por lo que los Estados deben adoptar medidas legislativas y administrativas para su atención. Cfr. OIT, Convenio 182, Sobre las Peores Formas de Trabajo Infantil, Art. 3, 1999 y ONU, Protocolo Facultativo de la Convención sobre los Derechos del Niño Relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de Niños en la Pornografía, 2002, Art. 2.

- **Grooming**

Es una forma de violencia sexual digital en la cual un adulto mediante engaños y mentiras se gana la confianza y establece algún tipo de amistad con una niña, niño o adolescente a través del entorno digital, ya sea vía redes sociales, aplicaciones de mensajería instantánea, correo electrónico, entre otros, con el fin de obtener imágenes o videos con connotación o actividad sexual. Estas imágenes o videos están destinados al consumo de pederastas o a redes de abuso sexual a menores con el objetivo de llevar a cabo abuso y/o explotación sexual comercial infantil.[6]

Ocurre cuando:

1. Se hace la búsqueda y el contacto con una niña, niño o adolescente.
2. Se indaga sobre su información personal y familiar, gustos y preferencias con el fin de crear una relación de confianza.
3. Con técnicas de persuasión obtienen imágenes o videos comprometedores.
4. Mediante el chantaje lo obligan a proporcionar más contenido sexual, amenazando con difundir la información obtenida a través de diferentes medios y/o enviarla a sus contactos personales, incluso pueden solicitar encuentros físicos para abusar sexualmente de la víctima.

- **Morphing**

Es una forma de violencia digital en la que a través de la edición de fotografías o videos reales de una niña, niño o adolescente se trasforma su contenido en uno nuevo potencialmente dañino para estos. Incluye la producción de material sexual a partir de imágenes editadas tomadas de internet o redes sociales, donde se simula actos y voces de personas menores de edad.[7]

- **Phishing, Smishing y Vishing**

Son formas de violencia digital por medio de las cuales los atacantes intentan engañar a sus víctimas para que revelen información confidencial o realicen ciertas acciones, como descargar y ejecutar archivos que parecen ser benignos, pero que en realidad son maliciosos. El Phishing es un método de ataque a través del cual el atacante envía

6 Cfr. Gobierno de México, Procuraduría Federal del Consumidor, “Grooming y Ciberacoso en niños”, artículo en línea, disponible en: https://www.gob.mx/profeco/es/articulos/grooming-y-ciberacoso-en-ninos?idiom=es

7 Cfr. Comité de los derechos del Niño, Observación General 13. El derecho del niño a no ser objeto de ninguna forma de violencia, CRC/C/GC/13, publicada el 18 de abril de 2011, párrafo 31 b.

un correo electrónico pretendiendo ser otra persona, compañía o sitio de confianza, para robar la contraseña o información sensible de la víctima. Este tipo de amenazas también pueden buscar tomar el control del dispositivo, computadora o celular. El Smishing ocurre cuando se recibe un mensaje de texto corto (SMS) en el teléfono celular, por medio del cual se solicita a la víctima llamar a un número de teléfono o ir a un sitio web a través del cual se robará su información sensible. El Vishing es la estafa que se produce mediante una llamada telefónica que busca engañar, suplantando la identidad de una persona o entidad para solicitar información privada o realizar alguna acción en contra de la víctima. [8]

- **Retos virales nocivos para niñas, niños y adolescentes**

Son una forma de violencia digital que consiste en llevar a cabo desafíos o pruebas populares riesgosas en el entorno digital utilizado por niñas, niños y adolescentes. Se presentan en forma de juegos en línea que se graban en video para compartirlos en redes sociales como un camino rápido para integrarse y adquirir popularidad dentro del mundo digital, que en muchas ocasiones no deja ver los peligros reales que asumen al ejecutarlos.[9]

- **Sexting**

Es una forma de violencia digital cometida entre personas menores de edad que consiste en el envío o recepción de imágenes o videos de carácter íntimo y/o de contenido sexual de una niña, niño y adolescente a través del entorno digital sin su consentimiento. Si bien no constituye una forma de violencia cuando, de forma consciente, la persona menor de edad envía imágenes o videos de sí misma, si se considera una actividad riesgosa.[10]

- **Violencia**

Toda acción o conducta que genere perjuicio, cause la muerte, daño, sufrimiento físico, sexual o psicológico; así como el descuido o trato negligente, malos tratos o explotación, en contra de niñas, niños y adolescentes que cursan el nivel básico de educación en México.[11]

---

8 Gobierno de México, Secretaría de Comunicaciones y Transportes, “Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo” disponible en: https://www.gob.mx/cms/uploads/attachment/file/555226/Gui_a_de_Ciberseguridad_SCT_VF.pdf

9 Gobierno de México, Sistema Nacional de Protección de Niñas, Niños y Adolescentes, “Retos virales en redes sociales: evitar que este mal se propague entre niñas, niños y adolescentes”, artículo en línea, disponible en: https://www.gob.mx/sipinna/articulos/retos-virales-en-redes-sociales-evitar-que-este-mal-se-propague-entre-ninas-ninos-y-adolescentes

10 Cfr. UNICEF, Guía de Sensibilización sobre Convivencia Digital, Buenos Aires, 2017, pp. 28 – 30. Disponible en: https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia_ConvivenciaDigital_ABRIL2017.pdf y; UNICEF, “Ciberseguridad, como protegerte en Internet” Artículo en línea, disponible en: https://www.unicef.org/mexico/ciberseguridad

11 Cfr. Comité de los derechos del Niño, Observación General 13. El derecho del niño a no ser objeto de ninguna forma de violencia, CRC/C/GC/13, publicada el 18 de abril de 2011, párrafo 4 y; Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia Contra la Mujer “Convención de Belem do Para”, Artículo 1.

- **Violencia digital**

Toda forma de violencia perpetrada a través del entorno digital en contra de niñas, niños y adolescentes que cursan el nivel básico de educación en México. Incluye actos de violencia cometidos, instigados o agravados, en parte o totalmente, por el uso de las tecnologías de la información y comunicación, plataformas de redes sociales y correo electrónico que pueden conducir a formas de violencia sexual y otras formas de violencia física.[12]

- **Violencia digital en la pareja o expareja**

Es una forma de violencia digital en la que se llevan a cabo un conjunto de comportamientos repetidos que pretenden controlar, menoscabar o causar un daño a la pareja o expareja a través del entorno digital. Se lleva a cabo mediante el intercambio de mensajes, control de las redes sociales o aplicaciones, apropiación de las contraseñas, difusión de secretos o información comprometida, amenazas e insultos. Se puede vigilar a la pareja controlando su ubicación, conversaciones, comentarios en línea, enviando correos, mensajes o comentarios humillantes, groseros o degradantes, o publicando fotos con la misma intención.[13]

- **Violencia digital a través de videojuegos**

Es una forma de violencia digital cometida en videojuegos utilizados por niñas, niños y adolescentes. Ocurre cuando en un videojuego, niñas, niños y adolescentes son violentados por otro jugador al margen de las reglas de programación del videojuego o cuando son contactados por personas adultas a través de los videojuegos con fines ilícitos. [14]

- **Víctima**

Niña, niño o adolescente que sufre violencia digital en el sistema educativo mexicano de nivel básico.

---

12 Cfr. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, Cyber Violence Against Women and Girls: A World-wide Wake-up Call, UNESCO, 2015 y; Consejo de Derechos Humanos de las Naciones Unidas, Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos, A/HRC/38/47, 18 de junio de 2018.

13 Save The Children, Violencia Viral: Análisis de la violencia contra la infancia y la adolescencia en el entorno digital, España, 2019.

14 La definición de violencia digital a traves de videojuegos se formuló a partir del estudio de diversos casos publicados en notas de prensa. Cfr. https://bit.ly/3NoVVEi

IV. PRINCIPIOS TRANSVERSALES

Para la correcta implementación del **Protocolo** las autoridades responsables de su aplicación deberán tomar en cuenta los siguientes principios y derechos:

A. Interés superior de la niñez.

De acuerdo a este principio, en todas las medidas concernientes a niñas, niños o adolescentes que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial será el interés superior de la niñez.

Se trata de un concepto triple, toda vez que se configura como: 1) un derecho sustantivo, 2) un principio jurídico interpretativo fundamental, y 3) una norma de procedimiento.

En ese sentido, niñas, niños y adolescentes tienen derecho a que se valore su interés superior; que en caso de que una norma admita más de una interpretación se elija la que mejor satisfaga sus derechos, y que, invariablemente, su interés sea considerado en todos los procesos de toma de decisiones, sea que estas se dirijan a una persona menor de edad en concreto o a un grupo de ellas. [15]

Los Estados y sus autoridades tienen tres tipos de obligaciones respecto al interés superior de la niñez:

1. La obligación de garantizar que el interés superior de la niñez se integre de manera adecuada y se aplique sistemáticamente en todas las medidas de las instituciones públicas.
2. La obligación de velar porque todas las decisiones judiciales y administrativas, las políticas y la legislación, relacionadas con niñas, niños y adolescentes, dejen patente que el interés superior de estos ha sido una consideración primordial.

15 Cfr. Convención sobre los Derechos del Niño, adoptada y abierta a la firma y ratificación por la Asamblea General en su Resolución 44/25, 20 de noviembre de 1989, artículo 3.1 y; Constitución Política de los Estados Unidos Mexicanos, art. 4.

3. La obligación de garantizar que el interés superior de la niñez se ha evaluado y ha constituido una consideración primordial en las decisiones y medidas adoptadas por el sector privado, incluidos los proveedores de servicios, o cualquier otra entidad o institución privada. [16]

Para incorporar el interés superior de la niñez en los procedimientos establecidos en el presente Protocolo, las autoridades responsables de la documentación de casos de violencia digital en contra de niñas, niños y adolescentes deberán realizar en todo momento una evaluación del impacto de sus acciones en la salud socioemocional de las víctimas, evitando acciones que puedan revictimizarlas. Asimismo, en todos los casos de violencia digital en los que tanto las personas agresoras como las víctimas sean menores de edad, se deberá escuchar la opinión de ambas partes, así como de las personas responsables de su cuidado previo a tomar una determinación sobre la aplicación de sanciones administrativas por las conductas de violencia que se hubieren documentado.

Recuerda que al aplicar el **Protocolo** deberás escuchar y tomar en cuenta en todo momento la opinión de las niñas, niños y adolescentes víctimas de violencia digital.

16 Comité de los Derechos del Niño, Observación General 14. Sobre el derecho del niño a que su interés superior sea una consideración primordial, CRC/C/GC/14, aprobada en su 62° periodo de sesiones, 2013.

B. Principio de Autonomía Progresiva.

Los tratados internacionales y la legislación nacional en materia de niñez y adolescencia, reconocen a niñas, niños y adolescentes como sujetos plenos de derechos, cuya autonomía se encuentra en evolución y desarrollo. Conforme crecen y adquieren mayor autonomía, el Estado, las familias y la sociedad deben apoyar y proteger su desarrollo, de forma que paulatinamente, adquieran la capacidad para ejercer y exigir por sí mismos sus derechos.[17]

En ese sentido, en el marco de la aplicación del presente **Protocolo**, las autoridades responsables de la documentación de casos de violencia digital en contra de niñas, niños y adolescentes deberán analizar y valorar dichos casos considerando su edad, grado de desarrollo y madurez, pues de este factor dependerá; por ejemplo, la viabilidad de practicar procedimientos de escucha, decidir el servicio o apoyo más adecuado para su atención, la necesidad de la presencia de una persona adulta que lo acompañe, la forma en que debe interpretarse sus declaraciones o testimonios, la expresión de su consentimiento ante determinadas diligencias o gestiones, entre otras decisiones.

El desarrollo de la autonomía de niñas y niños debe ir acompañada de su responsabilidad progresiva. Las personas adultas deben facilitar los mecanismos para que puedan tomar decisiones sobre su propia vida, en consonancia con la evaluación de sus facultades. Sin duda, es central en la construcción de ciudadanía aprender el ejercicio de los derechos propios, pero también es fundamental reconocer y respetar los derechos de las demás personas (sean menores o mayores de edad) como una responsabilidad colectiva.

17 Cfr. Convención sobre los Derechos del Niño, adoptada y abierta a la firma y ratificación por la Asamblea General en su Resolución 44/25, 20 de noviembre de 1989, artículo 5.

C. Principio de igualdad y no discriminación.

De acuerdo con este principio todas las autoridades del Estado deben respetar y proteger los derechos de niñas, niños y adolescentes, sin distinción alguna, independientemente de la raza, el color, el sexo, el idioma, la religión, la opinión política o de otra índole, el origen nacional, étnico o social, la posición económica, los impedimentos físicos, el nacimiento o cualquier otra condición del niño, de sus padres o de sus representantes legales. [18]

Asimismo, este principio contempla, tanto la discriminación directa como la indirecta, entendida la primera como el trato menos favorable a una persona o grupo de personas sobre la base de ciertas características como el sexo, la identidad de género la discapacidad, entre otras, y la segunda como las prácticas, reglas, requerimientos o cualquier otra condición que debería ser neutral, pero que en la práctica implica un impacto desproporcionado sobre un grupo en particular.

Los derechos se extienden igualitariamente a todos los niños y niñas, lo que implica que no se restringen a los que poseen una ciudadanía “legal” sino que también abarca a niñas y niños extranjeros, refugiados, solicitantes de asilo, los que no cuentan con la protección de su Estado y quienes carecen de documentos de identificación.

Es indispensable tener claro que la no discriminación no solo implica una prohibición de cometer algún tipo de distinción, implica también el deber de tomar las medidas positivas (afirmativas) necesarias para combatir todas las formas de desigualdad y lograr la igualdad en el ejercicio de los derechos en la vida cotidiana.

18 Cfr. Convención sobre los Derechos del Niño, adoptada y abierta a la firma y ratificación por la Asamblea General en su Resolución 44/25, 20 de noviembre de 1989, artículo. 2.

D. Derecho a vivir en condiciones de bienestar y a un sano desarrollo integral.

De conformidad con este derecho los Estados y sus autoridades están obligados a asegurar a las personas menores de edad, la protección y el cuidado necesarios para su bienestar, teniendo en cuenta los derechos y deberes de sus padres, tutores u otras personas responsables de ellos y ellas ante la ley Incluye el derecho a un nivel de vida adecuado para su desarrollo físico, mental, espiritual, moral y social. El bienestar debe interpretarse en un sentido amplio, pues comprende la supervivencia, salud, integridad física y seguridad emocional, nivel de vida y atención, oportunidades de juego y aprendizaje y libertad de expresión.[19]

En consecuencia, las autoridades responsables de la aplicación del presente Protocolo deberán llevar a cabo acciones integrales de protección de las niñas, niños y adolescentes afectados por la violencia digital, buscando en todo momento un entorno que favorezca su resiliencia.

E. Derecho de Prioridad.

De conformidad con este derecho todas las autoridades del Estado tienen la obligación de privilegiar la atención de las personas menores de edad en la protección y defensa de sus derechos. Otorgar prioridad a los derechos de niñas, niños y adolescentes, no significa que el Estado deba negar la importancia del cumplimiento y ejercicio de los derechos del resto de la población, sino que, al ponderar el orden de atención a proporcionar, debe privilegiar el de las personas menores de edad.[20]

En ese sentido las autoridades responsables de la aplicación del presente Protocolo deberán otorgar un tratamiento prioritario a la documentación de casos de niñas, niños y adolescentes afectados por la violencia digital por sobre otras actividades.

---

19 Cfr. Convención sobre los Derechos del Niño, adoptada y abierta a la firma y ratificación por la Asamblea General en su Resolución 44/25, 20 de noviembre de 1989, artículo 3.2 y 27.

20 Cfr. Ley General de los Derechos de Niñas, Niños y Adolescentes, artículo 17 y; Principio 11 de la Conferencia Internacional sobre Población y el Desarrollo adoptada del 5 al 13 de septiembre de 1994 en El Cairo, Egipto (1994).

F. Derecho a una vida libre de violencia.

De conformidad con este derecho, las autoridades y la sociedad en general están llamadas a prevenir, atender y sancionar toda forma de violencia en contra de niñas, niños y adolescentes y promover su recuperación física y psicológica, así como la restitución de sus derechos.[21]

En consecuencia, las autoridades responsables de la aplicación del presente **Protocolo** deberán adoptar acciones integrales para prevenir y sancionar toda forma de violencia digital y proteger y asistir a niñas y niños víctimas; asegurar su acceso a la justicia facilitando mecanismos de denuncia confidenciales y amigables de acuerdo a su edad, grado de madurez y desarrollo.

G. Derecho a la seguridad jurídica y debido proceso.

De conformidad con este derecho todas las autoridades que deban tomar decisiones sobre la situación jurídica de una persona menor de edad tienen que realizar y privilegiar su interés superior, el cual, como se mencionó, debe ser debidamente explicitado y considerar el impacto que la decisión generará para las niñas, niños y adolescentes en concreto.[22]

Para el cumplimiento de este derecho las autoridades responsables de la aplicación del presente **Protocolo** deberán implementar las siguientes medidas:

1. Proporcionar información clara, sencilla y comprensible para las niñas, niños y adolescentes sobre el procedimiento de documentación de casos de violencia digital y la importancia de su participación en el mismo, incluyendo, en su caso, formatos accesibles de fácil comprensión para niñas, niños víctimas.
2. Implementar mecanismos de apoyo para las niñas, niños y adolescentes víctimas que deseen denunciar hechos de violencia digital en su contra.
3. Garantizar el derecho de niñas, niños y adolescentes a ser asistidos por sus madres, padres tutores o cuidadores.
4. Proporcionar asistencia de profesionales especializados cuando la naturaleza del procedimiento lo requiera.
5. Proteger a niñas, niños o adolescentes de sufrimientos durante su participación y garantizar el resguardo de su intimidad y datos personales.

21 Cfr. Ley General de los Derechos de Niñas, Niños y Adolescentes, artículo 46 y 47.

22 Cfr. Ley General de los Derechos de Niñas, Niños y Adolescentes, artículo 82.

H. Derecho a la participación.

Es el derecho de niñas, niños y adolescentes a formarse un juicio propio y expresar su opinión libremente en todos los asuntos que les afecten, debiendo las autoridades tomar en cuenta sus opiniones en función de su edad y madurez; incluye la libertad de buscar, recibir y difundir información e ideas de todo tipo, ya sea oralmente, por escrito o impresas, en forma artística o por cualquier otro medio elegido por el niño o niña.

El derecho a la libertad de expresión y de acceso a la información son condiciones imprescindibles para el ejercicio del derecho a ser escuchado, y en términos más amplios, de participar. Por lo que, las autoridades responsables de la aplicación del presente Protocolo deberán explicar de forma clara y sencilla los procedimientos y los derechos que asisten a las niñas, niños y adolescentes víctimas de violencia digital, así como a aquellas personas menores de edad señaladas como agresoras.[23]

V. PREVENCIÓN DE CASOS DE VIOLENCIA

23 Cfr. Ley General de los Derechos de Niñas, Niños y Adolescentes, artículos 71 al 74.

De acuerdo con la Encuesta Nacional de Consumo de Contenidos Audiovisuales realizada en 2022 por el Instituto Federal de Telecomunicaciones (IFT):

80% de las niñas y niños se conectan al internet por celular.

69% de las niñas y niños que usan internet utilizan alguna red social.

66% usa WhatsApp

55% usa Youtube

49% usa TikTok

34% usa Facebook

El **96%** de las niñas y niños encuestados señaló que consume contenidos de internet desde su casa.

DIGITAL EN CONTRA DE NIÑAS, NIÑOS Y ADOLESCENTES

A. Los derechos de niñas, niños y adolescentes en el entorno digital.

El entorno digital está en permanente expansión y evolución como resultado de los avances de las tecnologías de la información y comunicación. Forman parte de este entorno los dispositivos celulares, tabletas, computadoras y cualquier dispositivo que pueda conectarse a internet, así como también las redes sociales, las aplicaciones digitales e incluso los algoritmos empleados por estas tecnologías para distribuir contenido a sus usuarios.

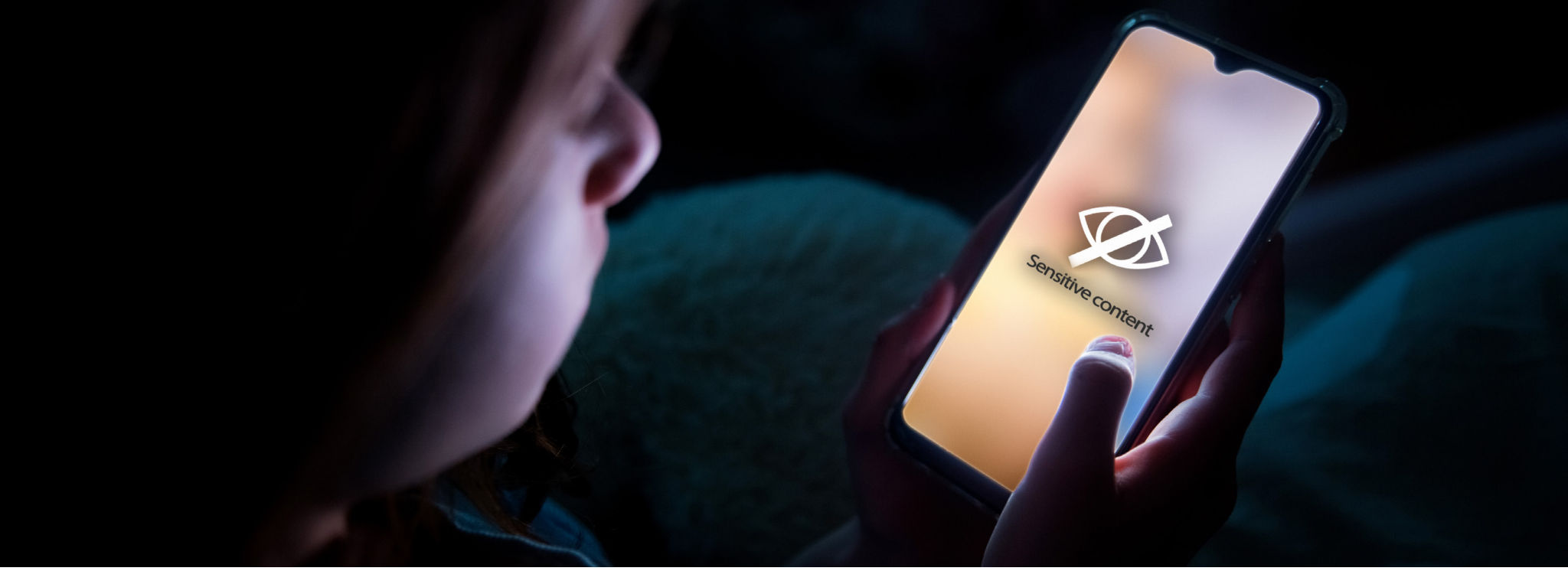
El entorno digital posee una gran importancia para niñas, niños y adolescentes, ya que es a través de él que pueden comunicarse con otras personas, así como acceder a múltiples servicios educativos o de recreación, entre otros.

Las niñas, niños y adolescentes tienen diversos derechos relacionados con el entorno digital siendo los de mayor importancia: 1) el derecho de acceso a tecnologías digitales seguras, libres de toda forma de violencia y discriminación; 2) el derecho de acceso a la información; 3) el derecho a la libertad de expresión; 4) la libertad de asociación y de reunión pacífica y; 5) el derecho a la privacidad y a la protección de sus datos personales e información sensible.[24]

Atender puntualmente a estos derechos es una condición esencial para la prevención de casos de violencia digital en contra de niñas, niños y adolescentes.

B. Factores de riesgo para niñas, niños y adolescentes en el entorno digital.

24 El contenido de estos derechos, así como su importancia se encuentra en el apartado de “Principios y derechos transversales” del presente Protocolo.



El entorno digital tiene múltiples beneficios para niñas, niños y adolescentes, pero su uso inadecuado puede implicar diversos factores de riesgo para sus usuarias y usuarios.

De manera general es posible clasificar los factores de riesgo en el entorno digital para niñas, niños y adolescentes en riesgos de contacto, contenido, conducta y privacidad.[25]

1) Riesgos de contacto. Son riesgos asociados al contacto con personas extrañas y que por lo tanto pueden implicar comunicaciones peligrosas debido a la información que personas adultas pueden enviar u obtener de niñas, niños y adolescentes. Estos se presentan cuando, por ejemplo, una niña, niño o adolescente entra en contacto con una persona adulta ignorando su edad, identidad o sus intenciones, las cuales pueden tener fines sexuales, o cuando niñas, niños y adolescentes son persuadidos para que participen en conductas poco saludables o peligrosas.

2) Riesgos de contenido. Es el riesgo asociado al acceso a la información del entorno digital de tipo inapropiado para personas menores de edad. Por ejemplo, imágenes sexuales, pornográficas o violentas; algunas formas de publicidad; material racista, discriminatorio o de odio; y sitios web que defienden conductas poco saludables o peligrosas, como autolesiones, suicidio y anorexia. Tener contacto con este tipo de contenidos puede abrir camino hacia materiales mucho más explícitos y que pueden herir o vulnerar a otros, en especial a niñas, niños y adolescentes.

3) Riesgos de conducta. Es el riesgo asociado a la posibilidad de anonimato que ofrece el entorno digital y a la facilidad para crear cuentas o publicar contenidos sin ningún límite. Puede incluir que niños y niñas escriban o elaboren materiales que inciten al racismo o al odio contra otras personas menores de edad o publiquen o distribuyan imágenes sexuales, incluido el material que ellos mismos produjeron.

4) Riesgos de privacidad: Es el riesgo asociado a la forma en cómo niñas, niños y adolescentes exponen sus datos personales sensibles e incluso sus contraseñas de acceso a redes sociales. Por ejemplo, cuando personas menores de edad publican en redes sociales su número celular o su domicilio o cuando comparten sus contraseñas con personas de su confianza.

25 Cfr. UNICEF, Niños, Niñas y Adolescentes en Línea, Riesgos de las Redes y Herramientas para Protegrese, 2019.

Es importante resaltar que todos los factores de riesgo mencionados devienen de la posibilidad de compartir información a través del entorno digital. Algunas prácticas comunes en las y los adolescentes que no constituyen en sí una forma de violencia digital sí son de alto riesgo para ellos y ellas, tal es el caso de sexting el cual no constituye una forma de violencia digital cuando se practica con el consentimiento de las y los adolescentes involucrados, pero que constituye una actividad de alto riesgo debido al manejo de información sensible de contenido sexual que puede filtrarse a través del entorno digital.

A continuación, se presentan algunas situaciones de riesgo vinculadas al sexting:

Situación	Riesgo
✓ Una pareja se filma o saca fotos teniendo relaciones sexuales. Uno de ellos, captura las imágenes y se las manda al otro, guardándolas al mismo tiempo en su dispositivo.	X Una vez que la pareja se separa o pelea, puede ocurrir que quien guardó las imágenes las haga circular entre sus contactos de mensajería instantánea y redes sociales (lo que suele llamarse "pornovengaza"). Si bien la obtención de la imagen fue deseada, no así la circulación por medios públicos.
✓ Enviar fotografías en poses o prácticas sexuales por parte de un chico o chica a otro para seducirlo es una práctica presente entre algunos de los adolescentes.	X Si bien la fotografía se enmarca en una comunicación privada entre dos personas, quien la recibe puede, en ese momento o en el futuro, hacerla circular por la web, volviéndola pública.
✓ El uso de cámara web durante conversaciones de mensajería instantánea puede derivar en una situación de sexting. Una chica o chico puede hacer poses sexuales delante de la cámara para mostrarlas a quien está del otro lado en una charla privada.	X Esa imagen puede ser capturada o grabada por el receptor, para luego ser publicada en la web, en este caso sin su consentimiento.

Fuente: UNICEF, Guía de sensibilización digital p. 17

C. Recomendaciones de ciberseguridad para garantizar un entorno digital seguro.

Una de las principales amenazas para los dispositivos tecnológicos utilizados por niñas, niños y adolescentes es el malware, también conocido como código malicioso. Este se define como cualquier programa informático que se coloca de forma oculta en un dispositivo, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema operativo. [26]

Las amenazas de malware pueden infectar cualquier dispositivo por medio del correo electrónico, los sitios web, las descargas y el uso compartido de archivos y la mensajería instantánea.

Prevenir la violencia digital en contra de niñas, niños y adolescentes depende en gran medida de un uso adecuado y responsable de las tecnologías de la información y comunicación. Algunas de las recomendaciones de ciberseguridad para acceder al entorno digital de manera segura, son las siguientes:

1) Usar antivirus y firewall.

Los antivirus y firewall (cortafuegos) son programas que al instalarlos en nuestros dispositivos (computadoras, tabletas, celulares, etc.) nos permiten acceder al entorno digital de forma segura. Un cortafuegos es la primera línea de defensa ante un ataque a tu red desde Internet y permite proteger el equipo de programas maliciosos o de atacantes que intenten conectarse al equipo de forma remota. Además, permite establecer reglas para indicar qué conexiones de red se deben aceptar y cuáles no. Por su parte los antivirus son programas que ayudan a proteger los dispositivos contra la mayoría de los virus, gusanos, troyanos y otros tipos de malware (programas maliciosos) que pueden infectar a los dispositivos. Existen diversas aplicaciones gratuitas contra programas maliciosos los cuales es recomendable instalar y mantener actualizados, prefiriendo aquellos que incorporan ambas funcionalidades (antivirus y cortafuegos) también conocidos como “suites de seguridad”.[27]

---

26 Gobierno de México, Secretaría de Comunicaciones y Transportes, “Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo” disponible en: https://www.gob.mx/cms/uploads/attachment/file/555226/Gui_a_de_Ciberseguridad_SCT_VF.pdf

27 Idem.

2) Actualizar el sistema operativo de los dispositivos a través de los cuales se accede al entorno digital.

Todos los dispositivos capaces de conectarse a internet cuentan con un sistema operativo, el cual es el medio para que las personas usuarias administren la información contenida en ellos. Son sistemas operativos comunes en computadoras los sistemas de Microsoft Windows, Mac OS o Linux, así como en celulares los sistemas Android, Mac OS y Harmony OS, entre otros. Para funcionar correctamente estos sistemas operativos se actualizan permanentemente, motivo por el cual para evitar ciber ataques es muy importante activar las funciones de actualización automática o hacerlo manualmente. Cada versión actualizada aumentará la seguridad del dispositivo y por lo tanto hará más difícil la instalación de programas maliciosos.

3) Usar contraseñas seguras.

Las contraseñas son parte del sistema de seguridad que las aplicaciones, programas y sistemas operativos exigen a las y los usuarios para utilizarlas. Para que dicho sistema de seguridad sea eficaz, es importante establecer contraseñas que incluyan al menos ocho caracteres y que cuenten con distintos símbolos (números, letras, mayúsculas y/o caracteres especiales). También es importante que establezcamos contraseñas que podamos recordar o que en su defecto usemos un programa que las administre el cual guardará de forma automática las contraseñas que sean creadas para la utilización de cada aplicación. Finalmente es importante no compartir las contraseñas con otras personas, ya que esto aumenta el riesgo de que nuestros equipos o nuestras redes sociales sean intervenidas.

4) Encriptar información sensible.

Es importante que la información sensible que tengamos en medios de almacenamiento digital como memorias USB, discos o la memoria interna de nuestras computadoras o celulares se encuentre encriptada, es decir que para acceder a ella se necesite ingresar alguna contraseña o información biométrica (huellas digitales o reconocimiento facial).

Si la información sensible se encuentra encriptada no será posible acceder a ella, lo que garantiza que en caso de extravío del medio digital en el que la información se encuentra almacenada terceras personas no podrán acceder a ella.

5) Configurar adecuadamente los permisos otorgados a las aplicaciones en teléfonos móviles, tabletas o computadoras.

Muchas de las aplicaciones que emplean niñas, niños y adolescentes como Facebook, TikTok o Instagram solicitan permisos para acceder a la cámara, al sistema de audio o a las imágenes y videos almacenados. Por ello es muy importante que con estas aplicaciones o con cualquier otra que solicite dichos accesos se lleve a cabo la configuración adecuada. En este sentido es importante no conceder permisos permanentes, sino únicamente permisos para acciones concretas también llamados permisos de única vez.

De acuerdo al reporte OPINNA sobre “Navegación Segura” elaborado por la Sistema Integral de Protección de Niñas, Niños y Adolescentes (SIPINNA) en 2022 en el que participaron 79,000 personas de entre 10 y 17 años:

53% de las niñas, niños y adolescentes señalarón que personas que ellas y ellos no conocen los siguen en redes sociales.

16% de las niñas, niños y adolescentes señalarón que otras personas los han hecho sentir mal en redes sociales.

12% de las niñas, niños y adolescentes señalaron que les han solicitado fotografías privadas en redes sociales.

10% de las niñas, niños y adolescentes señalaron que les han pedido encontrarse personalmente con personas que no conocen.

VI. ACCIONES PARA LA PREVENCIÓN DE VIOLENCIA DIGITAL EN CONTRA DE NIÑAS, NIÑOS Y ADOLESCENTES

Prevenir la violencia digital en contra de niñas, niños y adolescentes en el sistema educativo es una tarea que demanda la participación conjunta entre las personas responsables de su cuidado y las autoridades educativas. En ese mismo sentido, capacitar a las personas menores de edad para el uso adecuado de las tecnologías de la información y comunicación también es imprescindible como mecanismo de prevención de este tipo de violencia.

A. Acciones de prevención dirigidas a madres, padres tutores y cuidadores.

El entorno digital ofrece un universo de posibilidades para niñas, niños y adolescentes, desde obtener información con fines educativos hasta facilitar la convivencia y recreación con otras personas menores de edad. A pesar de ello existen diversos riesgos que pueden poner en peligro la vida y la integridad de niñas y niños, motivo por el cual es importante que madres, padres, tutores o cuidadores lleven a cabo las siguientes acciones.

1) Valorar la posibilidad de riesgo en función de la edad de niñas y niños usuarios del entorno digital.

El acceso seguro al entorno digital debe ser valorado para cada caso en concreto y atendiendo a la autonomía progresiva de niñas, niños y adolescentes, esto significa que las personas responsables de su cuidado en la familia deben establecer reglas para el acceso al entorno digital de acuerdo a su grado de madurez y desarrollo.

Es importante señalar que las niñas y niños son más vulnerables en sus primeros años de vida, por lo que el acceso al entorno digital en niños menores de 3 años no es recomendable. De los 3 a los 6 años de edad se recomienda que el acceso al entorno digital sea limitado únicamente a plataformas de video con contenidos educativos y durante espacios reducidos de tiempo, el acceso a videojuegos, inclusive si estos son educativos, no es recomendable para menores de 6 años.[28]

El acceso a internet es recomendable para personas de entre 6 y 12 años y siempre de manera supervisada, en ese mismo sentido redes sociales como Facebook, Twitter o TikTok establecen dentro de sus términos y condiciones que las y los usuarios deben ser mayores de 13 años de edad. Ahora bien, para el caso de personas mayores de 13 años de edad que acceden a dichas redes sociales existen opciones de configuración que permiten a madres y padres regular los contenidos a los que pueden acceder sus hijas e hijos.[29]

28 Cfr. Asociación Francesa de Pediatría Ambulatoria, “Reglas 3, 6, 9, 12”, 2008.

29 Cfr. Pantallas Amigas, “Guía de TikTok, para Padres y Madres” artículo en línea, disponible en: https://www.pantallasamigas.net/wp-content/uploads/2021/06/Guia-TikTok-Padres-Madres-PantallasAmigas.pdf

2) Establecer mecanismos de control parental.

Desde el momento en que se les permite a las personas menores de edad el acceso a internet y redes sociales es importante que padres, madres, tutores y cuidadores establezcan mecanismos de control parental. Estos mecanismos permiten controlar y supervisar los contenidos e interacciones que niñas, niños y adolescentes tendrán en el entorno digital. Así por ejemplo es posible configurar los navegadores de internet (Google Chrome, Fire Fox, Safari, Explorer, etc.) para restringir el acceso a páginas web específicas. También es posible restringir dicho acceso a través de antivirus o Firewall. Si estas opciones resultan complicadas es recomendable revisar el historial de navegación y verificar los sitios de internet a los cuales acceden niñas, niños y adolescentes.

Ahora bien, muchos sistemas operativos, redes sociales e incluso consolas de videojuegos cuentan con opciones de control parental las cuales una vez configuradas permiten a las personas responsables del cuidado de niñas, niños y adolescentes limitar el acceso a ciertos contenidos o incluso controlar el tiempo de exposición o de utilización a dichas tecnologías.

Es importante destacar que toda acción en el entorno digital siempre deja un registro (huella digital) que puede ser rastreado para prevenir la violencia digital en contra de personas menores de edad, por lo que usar los mecanismos de control parental reduce la probabilidad de ser víctima de esta forma de violencia**.** [30]

3) Familiarizarse con el entorno digital de niñas, niños y adolescentes.

El entorno digital ofrece un universo de posibilidades de acceso a plataformas, redes sociales y aplicaciones las cuales se adaptan a los gustos y necesidades de las personas usuarias. En ese sentido es importante la comunicación asertiva con niñas, niños y adolescentes a fin de conocer sus gustos en cuanto al acceso al entorno digital. Conocer las redes sociales que usan nuestros hijos e hijas, así como las aplicaciones que utilizan nos permitirá indagar sobre los posibles riesgos en cada una de ellas y adoptar las medidas de seguridad que sean necesarias.

Es recomendable crear un vínculo de confianza con niñas, niños y adolescentes para que, sin invadir su privacidad, podamos apoyarlos a lograr un acceso seguro al entorno digital.

4) Observar la conducta de niñas, niños y adolescentes al interactuar con el entorno digital.

Diversas formas de violencia digital como el ciberacoso o el ciberbullying ocasionan cambios en la conducta de niñas, niños y adolescentes, los cuales al ser víctimas de estas formas de violencia pueden manifestar cuadros de depresión, ansiedad o estrés, entre otras. Por ello es importante observar la conducta de las personas menores de edad antes, durante y después de sus interacciones con el entorno digital.

Identificar el cambio de conducta en niñas y niños usuarios del entorno digital nos permitirá acercarnos a ellos y ellas para corroborar si son víctimas de alguna forma de violencia.

5) Verificar la edad permitida para el uso de tecnologías de la información y comunicación en el entorno digital.

Las tecnologías de la información y comunicación en el entorno digital, como las redes sociales, los videojuegos e incluso la música en línea, poseen recomendaciones o restricciones de edad. Verificar la edad mínima requerida para el uso de una red social, plataforma, aplicación o videojuego es importante para prevenir la violencia digital y los riesgos que conlleva. En lo que respecta a redes sociales, la edad mínima exigida por la mayoría de las plataformas es de 13 años. De igual manera, en los videojuegos existe un sistema de clasificación internacional el cual determina la edad mínima necesaria para el acceso a videojuegos. Dicho sistema se basa en las siguientes categorías y clasificaciones:

30 Cfr. Unión Internacional de Telecomunicaciones, Protección de la Infancia en Línea: Guía para Padres, Tutores y Educadores", 2009, artículo en línea, disponible en: Protecciónde la Infanciaen Línea: Guía para padres, tutores y educadores (itu.int)

Clasificación Videojuegos

El contenido por lo general es apto para todas la edades. Puede que contenga una cantidad mínina de violencia.

Apto para todo publico

El contenido por lo general es apto para personas de 10 años o más. Puede que contenga más violencia.

Apto para mayores de 10 años

El contenido por lo general es apto para mayores de 13 años o más. Puede que contega violencia, temas insinuantes, humor grosero y una mínima cantidad de sangre.

Adolescentes

El contenido por lo general es apto para mayores de 17 años o más. Puede que contega violencia intensa, derramamiento de sangre, contenido sexual o lenguaje fuerte.

Apto para mayores de 17 años

El contenido es apto solo para adultos de 18 años o más. Puede que incluya escenas prologadas de violencia intensa, contenido sexual gráfico o apuestas con moneda real.

Adultos únicamente +18

No se ha asignado una calificación final de ESBR. Solo aparece en la publicidad, marketing y materiales promocionales relacionados con un juego físico.

Aún sin clasificar

Fuente: Elaboración propia con información de Entertainment Software Rating Board

B. Acciones de prevención dirigidas a personal del sistema educativo.

Prevenir la violencia digital en contra de personas menores de edad también es responsabilidad del personal educativo, el cual debe velar en todo momento por su seguridad sin invadir su privacidad e informar a las personas a cargo de su cuidado cuando una situación de riesgo sea detectada. Por ello es importante que se tomen en cuenta las siguientes acciones:

1) Educar a niñas, niños y adolescentes en el uso adecuado del entorno digital.

Con independencia de si la unidad educativa permite el uso de dispositivos para conectarse al entorno digital como celulares, computadoras portátiles o tabletas, es importante que el personal docente capacite a niñas, niños y adolescentes sobre el uso adecuado de estos dispositivos, así como de los sistemas para conectarse al entorno digital.

De manera general es importante capacitar a niñas, niñas y adolescentes sobre los riesgos del uso de ciertas plataformas, las violencias digitales a las que pueden exponerse a través del el entorno digital y las medidas de ciberseguridad básicas que deben adoptarse.

2) Implementar medidas de ciberseguridad en los dispositivos y puntos de conexión escolares.

Muchas unidades educativas cuentan con redes inalámbricas y dispositivos capaces de conectarse a internet, así como salas de cómputo para uso de alumnas y alumnos. Es importante que estas tecnologías de la información y comunicación cuenten con las medidas de ciberseguridad adecuadas para evitar que niñas, niños y adolescentes tengan acceso a contenidos inapropiados.

En ese mismo sentido, es importante que las unidades educativas cuenten con políticas de uso de estas tecnologías las cuales deben establecer como mínimo parámetros respecto al uso de equipos de cómputo, tiempo de utilización y acceso permitido a portales de internet. En caso de que dichas tecnologías recaben información personal y datos sensibles de niñas, niños y adolescentes deberán contar indefectiblemente con el consentimiento informado de las personas usuarias, así como de sus madres, padres, tutores o cuidadores.

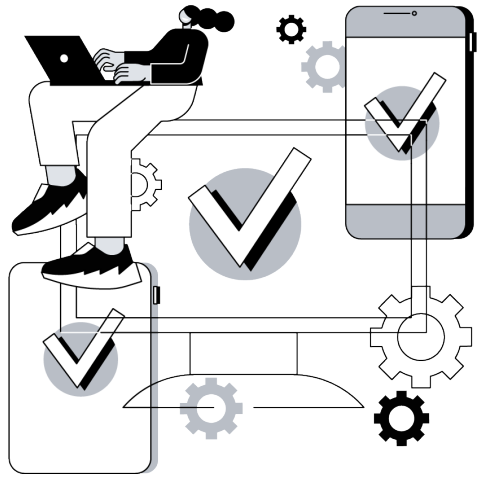
Aquellas unidades educativas que cuenten con conexiones a internet a través de redes inalámbricas de acceso a niñas y niños deben revisar periódicamente el historial de sitios visitados por las y los usuarios y en caso de detectar que se ha intentado acceder a contenidos inapropiados deben reportarlo inmediatamente a las autoridades escolares como a las personas responsables de su cuidado.

3) Generar un vínculo de confianza con las personas menores de edad usuarias del entorno digital.

En su trabajo cotidiano, las y los educadores tienen contacto permanente con sus alumnas y alumnos. Es importante que a través de una comunicación asertiva se genere un vínculo de confianza con niñas, niños y adolescentes con la finalidad de que estos puedan acercarse voluntariamente a reportar hechos de violencia digital en su contra o que sean de su conocimiento. Para lograrlo debe tomarse en cuenta no criminalizar a niñas y niños, sino por el contrario brindarles un entorno seguro a través del cual se les apoye a no reproducir formas de violencia digital y en caso de que sean víctimas a iniciar el proceso para la documentación y atención de dichos casos de acuerdo al procedimiento establecido en el presente Protocolo.

4) Utilizar adecuadamente el entorno digital para fines educativos.

En muchas ocasiones maestras y maestros utilizan el entorno digital como herramienta educativa, esto ocurre por ejemplo cuando se solicita a alumnas y alumnos que observen algún contenido multimedia como videos, audios, podcast, etc. Es importante que antes de solicitar a alumnos una tarea o trabajo sobre contenido multimedia en internet las y los maestros revisen cuidadosamente los materiales y las ligas web para su acceso. Esto debido a que hay mucho contenido en internet el cual ha sido alterado para parecer inofensivo, pero que sin embargo oculta contenido inapropiado. Ejemplo de lo anterior son algunos retos virales nocivos para niñas y niños ocultos en fragmentos de videos educativos.



C. Recomendaciones de prevención dirigidas a niñas, niños y adolescentes.

Niñas, niños y adolescentes pueden contribuir a la generación de un entorno digital seguro y libre de violencia para todos y todas, para ello es muy importante que tomen en cuenta las siguientes recomendaciones.

1) Respetar la privacidad de otros niños, niñas y adolescentes.

Al interactuar con el entorno digital es común que, como mecanismo de juego, recreación o esparcimiento, niñas, niños y adolescentes tomen fotografías, graben videos y capturen audios, sin embargo, es muy importante que cuando se lleven a cabo estas acciones respecto de otras personas menores de edad se hagan con su consentimiento.

Es importante que se distinga el consentimiento de una persona para salir en un video o fotografía del consentimiento para que dicha información sea compartida a través del entorno digital, ya que algunas formas de violencia digital como el sexting dependen de si se tiene, o no, el consentimiento de las personas involucradas.

2) Respetar la dignidad de otros niños, niñas y adolescentes y ser empáticos con ellos y ellas.

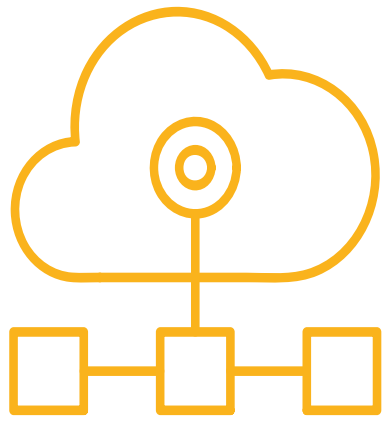
Al compartir mensajes, fotografías o videos de otras personas menores de edad a través de redes sociales como Facebook, Twitter, TikTok, Instagram u otras plataformas como WhatsApp o Telegram, es muy importante ser empáticos (ponernos en el lugar de la otra persona) y respetar la dignidad de quienes pueden verse afectados por estas acciones. Formas de violencia como el ciberbullying (acoso digital entre personas menores de edad) o el morphing (edición de videos o fotografías de otras personas menores de edad) pueden ocurrir como una forma de juego, pero en la práctica dañar o herir a las personas involucradas. Por ello es recomendable que las personas que editan o comparten información de otras niñas, niños y adolescentes sean empáticos con ellas y ellos y eviten estas prácticas cuando no cuentan con el consentimiento de las personas involucradas.

3) Adoptar medidas de ciberseguridad con nuestros dispositivos de conexión al entorno digital.

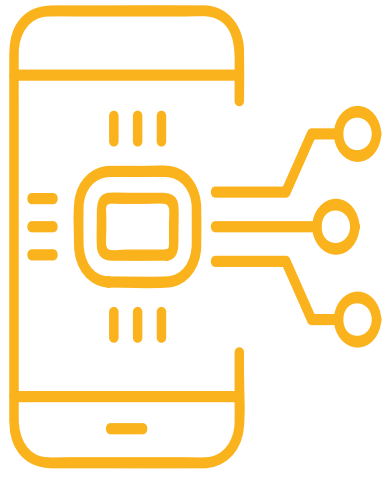
Para prevenir la violencia digital en contra de niñas, niños y adolescentes es muy importante que ellas y ellos adopten ciertas medidas de seguridad con sus dispositivos de conexión al entorno digital como teléfonos celulares, tabletas y equipos de cómputo. Entre las medidas de ciberseguridad más importantes destacan las siguientes:

- **Apagar el GPS (Sistema de Posicionamiento Global)** a través del cual terceras personas pueden conocer nuestra ubicación en tiempo real o en su defecto activarlo solo cuando sea necesario, como por ejemplo cuando nuestras madres, padres, tutores o cuidadores necesitan saber nuestra localización.

- **Apagar el Wifi y el bluetooth** de nuestros dispositivos cuando no los estemos utilizando, ya que a través de estas herramientas es posible que terceras personas, utilizando programas maliciosos (Malware), accedan a la información de nuestros equipos como nuestras fotografías o videos.

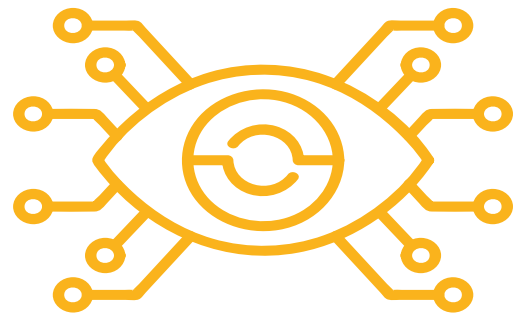


- **Revisar los permisos** otorgados al instalar una aplicación. Muchas aplicaciones utilizadas por niñas, niños o adolescentes como Tik Tok, Facebook o Instagram, solicitan permiso para acceder a la ubicación de las y los usuarios, así como a su cámara o galería fotográfica. En estos casos es recomendable conceder los permisos cada vez que se utilice la aplicación y no de forma permanente.



- **Configurar nuestras redes sociales como privadas.** Al configurar nuestras redes sociales como Facebook o Instagram o cualquier otra en la que subamos contenido como fotografías o videos personales, es muy importante configurarlas como privadas y no como públicas. Al tener una red privada nuestra información solo será visible para las personas que sean nuestros contactos, ya que si se configuran como públicas pueden ser visualizadas por cualquier persona. Muchas formas de violencia como el ciberacoso (acoso digital de una persona adulta hacia una persona menor de edad) o el grooming (persuasión de un adulto hacía un niño para obtener imágenes o contenidos sexuales) se llevan a cabo cuando las cuentas o perfiles de niñas, niños o adolescentes son públicas.

- **Aceptar como contacto solo a personas conocidas y verificar que se trata de ellas.** Es muy importante que en plataformas de mensajería como WhatsApp o Telegram o; en redes sociales como Facebook, Instagram o TikTok, entre otras, solo tengamos contacto con personas que conozcamos e incluso podamos verificar que se trata de ellas, ya que algunas formas de violencia digital como la explotación sexual infantil comercial a través de medios digitales se comete cuando terceras personas adultas se acercan a nosotros y nosotras como si fueran nuestros amigos para posteriormente obtener información nuestra.



- **Configurar adecuadamente nuestras contraseñas y sistemas de seguridad de verificación a dos pasos. La mayoría de plataformas de mensajería c**omo WhatsApp o Telegram o; redes sociales como Facebook, Instagram o TikTok, entre otras, permiten establecer contraseñas para el ingreso a nuestros perfiles de usuario. Por ello es muy importante que establezcamos contraseñas seguras y que no las compartamos con terceras personas. En ese mismo sentido, dichas plataformas permiten activar opciones de seguridad conocidas como “verificación a dos pasos” las cuales son un doble sistema de autenticación para corroborar que se trata de nosotros y no terceras personas las que acceden a nuestros perfiles, estos sistemas envían mensajes de texto con claves de acceso a nuestros teléfonos celulares para ingresar de forma segura a nuestras redes sociales o verificar nuestra identidad.

De acuerdo con una encuesta realizada a nivel nacional, por ChildFund México y Comunicación Política Aplicada (2023):

67% de las personas encuestadas considera que la principal causa de la violencia digital es el descuido o neglicencia de las personas a cargo del cuidado de niñas, niños y adolescentes.

58% de las personas encuestadas considera que la segunda causa más importante de la violencia digital es la falta de regulación de internet.

75% de las personas encuestadas identifica el ciberbullying como una forma de violencia común en niñas, niños y adolescentes.

66% de las personas encuestadas desconoce el grooming como una forma de violencia digital contra niñas, niños y adolescentes.

VII. ATENCIÓN DE CASOS DE VIOLENCIA DIGITAL EN CONTRA DE NIÑAS, NIÑOS Y ADOLESCENTES.

La violencia digital en contra de niñas, niños y adolescentes es quizá una de las formas de violencia más invisibilizada debido a la falta de formación y capacitación sobre los medios a través del cual es perpetrada y los mecanismos idóneos para su documentación y atención.

Muchas de las formas de manifestación de la violencia digital son extremadamente dañinas para la salud física y socioemocional de personas menores de edad, por lo que atender los casos que se presenten en las escuelas de nivel básico de educación de manera oportuna es muy importante.

Por lo anterior, el presente **Protocolo** establecerá lineamientos generales que deben ser tomados en cuenta por las autoridades educativas (personal docente, administrativo y directivo) en todos los casos de violencia digital en contra de personas menores de edad que sean detectados en las escuelas de nivel básico mexicanas, así como los procedimientos específicos para su atención y documentación.

A. Lineamientos generales para la atención y documentación de casos de violencia digital en contra de niñas, niños y adolescentes en escuelas de nivel básico de México.

Para la adecuada atención y documentación de los casos de violencia digital en contra de niñas, niños y adolescentes que sean detectados en las escuelas de nivel básico mexicanas deberán seguirse los siguientes lineamientos generales:

PRIMERO. Análisis de contexto.

Todas las autoridades educativas que tengan conocimiento de algún caso de violencia digital en contra de niñas, niños y adolescentes deberán analizar el contexto de la persona menor de edad afectada. Dicho análisis debe contemplar como mínimo los siguientes factores:

1) Edad. La edad y los ciclos de vida de las personas menores afectadas son un elemento importante a la hora de determinar las acciones y medidas de protección especial que deben llevarse a cabo. Los primeros años de vida de una niña o niño son los de mayor vulnerabilidad debido a las dificultades que pueden presentar para transmitir lo que les sucede o afecta. En ese sentido, se debe tener en cuenta el ciclo de vida en el cual se encuentra la persona afectada, es decir, si se trata de una persona: en primera infancia (niñas y niños de 0 a 5 años de edad); edad escolar (niñas y niños de 6 a 11 años de edad) o; adolescencia (personas menores de edad de entre 12 y 17 años de edad). La edad y ciclo de vida de las personas afectadas deberá, en todos los casos, motivar la urgencia de las acciones y medidas implementadas.

2) Sexo. Al igual que la edad, el sexo de las personas afectadas es un factor determinante a la hora determinar la vulnerabilidad a la que puede estar expuesta una niña, niño o adolescente, ya que, si bien todas y todos pueden ser víctimas de violencia, dicho factor aumenta la probabilidad de sufrir tipos específicos de violencia sexual digital como el grooming, sexting o el comercio sexual infantil a través de medios digitales.

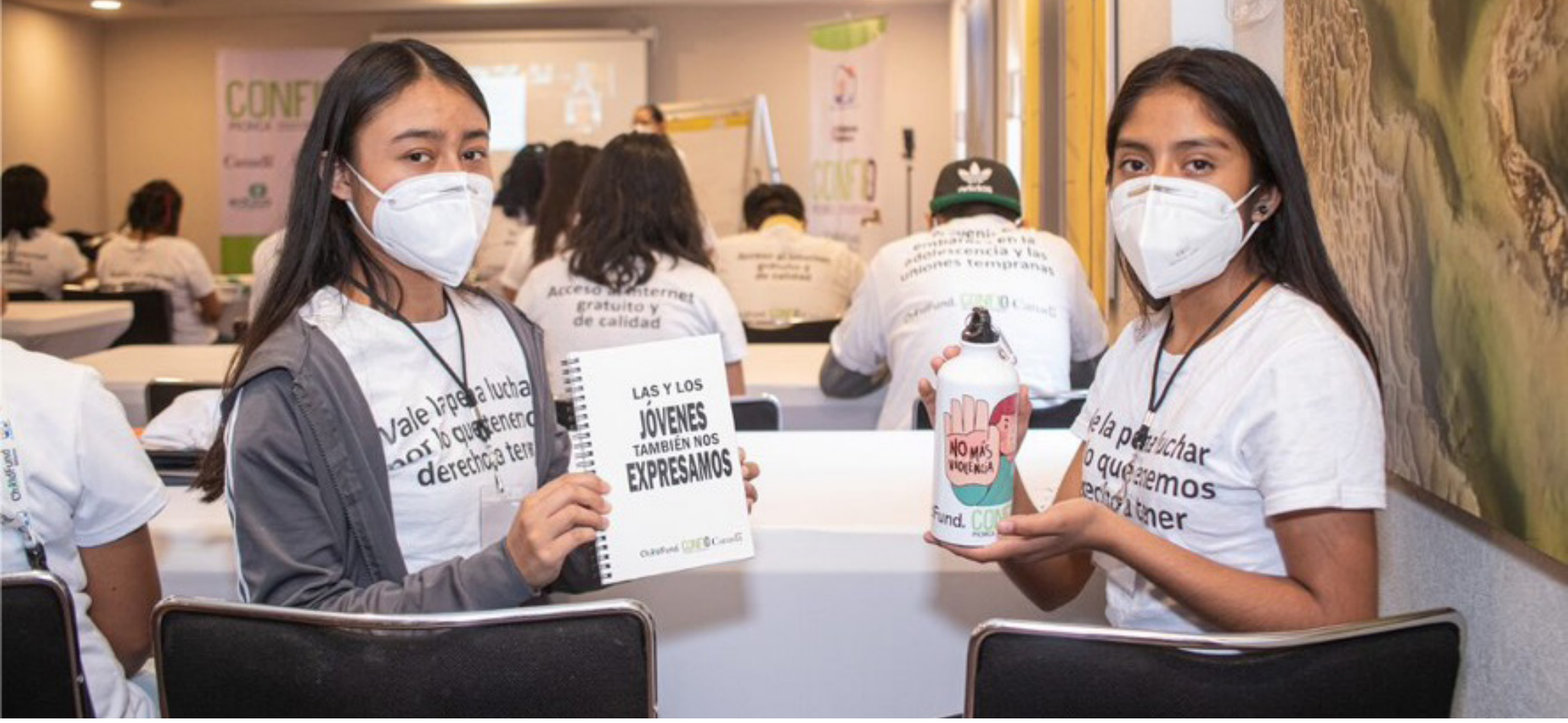
3) Condición de discapacidad. Niñas, niños y adolescentes, pueden verse afectados por alguna condición o situación de discapacidad. Dicho factor puede aumentar la vulnerabilidad a sufrir determinadas formas de violencia digital, así por ejemplo las personas menores de edad con alguna forma de discapacidad intelectual o psicosocial, pueden ser más propensos a sufrir violencia digital.

4) Tipo de violencia. Existen diferentes formas de violencia digital de las cuales pueden ser víctimas niñas, niños y adolescentes. Comprender cada una de ellas, así como sus principales riesgos nos ayudarán a establecer el mecanismo adecuado de atención, así como la urgencia en cuanto a la implementación de acciones de protección.

SEGUNDO. Prioridad en la atención a niñas, niños y adolescentes.

Los casos de violencia digital en contra de niñas, niños y adolescentes que sean de conocimiento de las autoridades educativas deben tener la máxima prioridad de atención. En aquellos casos en los que las formas de violencia digital denunciadas constituyan delitos de acuerdo a la legislación penal aplicable de las entidades federativas donde se aplique el presente Protocolo, se deberá informar de inmediato a las autoridades o instancias facultadas para su investigación (Sistema de Atención a Llamadas de Emergencia 911, Guardia Nacional 088 o Policía Cibernética), así como a las autoridades responsables de la procuración y restitución de sus derechos (Procuradurías de Protección de Niñas, Niños y Adolescentes).

En ese mismo sentido, deberá informarse de inmediato a las madres, padres, tutores o personas responsables de su cuidado, cuando estas no sean señaladas como perpetradoras.



TERCERO. Identificar si las niñas, niños y adolescentes cuentan con representación de una persona adulta.

Por regla general toda diligencia y actuación relacionada con una persona menor de edad debe realizarse con autorización de las personas adultas que ejercen la patria potestad, guarda, custodia o tutela. En los casos en los que una persona menor de edad sea señalada por la probable comisión de una forma de violencia digital que constituya un delito y sea necesario escucharla, deberá informarse indefectiblemente a las personas responsables de su cuidado y contar con su participación o autorización.

CUARTO. Identificar las interseccionalidades que atraviesan a niñas, niños y adolescentes.

La interseccionalidad es una categoría de análisis que permite identificar los elementos que, al confluir en un mismo caso o persona, multiplican las desventajas y discriminaciones. Con este enfoque es posible analizar los problemas que afectan a las personas menores de edad desde una perspectiva integral, evitando simplificar las conclusiones y, por lo tanto, el abordaje de dicha realidad. Las autoridades escolares que tengan conocimiento de un caso de violencia digital en contra de niñas, niños y adolescentes, deberán identificar las características particulares de las personas menores de edad afectadas que dificultan el acceso a sus derechos, por ejemplo, el sexo, la identidad de género, la condición de vivir con discapacidad, pertenecer a una comunidad indígena, residir en un centro de asistencia social, encontrarse en contexto de movilidad, vivir con VIH o SIDA, no contar con redes de apoyo familiar, ser víctima de violencia, pertenecer a una familia de escasos recursos, ser madre adolescente, pertenecer o identificarse con la comunidad LGBTTTIQ+, o cualquier otra.

Lo anterior posibilitará la toma de decisiones individualizadas que respondan de mejor manera al interés superior de las personas menores de edad, y que resulten más eficientes al momento de decidir las acciones para la protección y defensa de sus derechos, incluyendo, la adopción de medidas afirmativas.

QUINTO. Brindar información accesible a niñas, niños y adolescentes.

Durante la documentación de casos de violencia digital en contra de niñas, niños y adolescentes, al momento de llevar a cabo el primer contacto, las personas responsables de su atención deberán brindarles información sobre el procedimiento de documentación que se llevará a cabo utilizando un lenguaje sencillo y claro, adaptado a su edad y grado de madurez y desarrollo. En particular deberán informar sobre:

1. El papel o rol de niñas, niños y adolescentes en el proceso de documentación de casos de violencia digital, la importancia de su participación, el momento y la manera de prestar testimonio y la forma en que participará durante la documentación de los hechos.
2. Los mecanismos de apoyo disponibles (atención y acompañamiento psicológico, seminarios o talleres de sensibilización, etc.) cuando presenten una denuncia por hechos cometidos en su contra o de terceras personas menores de edad;
3. Sus derechos de conformidad con la legislación nacional, e internacional, en particular los contemplados en la Convención sobre los Derechos del Niño y la Ley General sobre Derechos de Niñas, Niños y Adolescentes.

SEXTO. Asistencia y acompañamiento.

Durante el tiempo que dure el proceso de documentación de casos de violencia digital contra niñas, niños y adolescentes, es recomendable que reciban acompañamiento y asistencia en las diligencias que, por sus características, impliquen someterlos a episodios estresantes o aquellos en los que su salud mental pueda verse afectada. En ese sentido es recomendable que las unidades educativas cuenten con el apoyo de personas especializadas en la atención de niñas, niños y adolescentes y capacitadas para brindar primeros auxilios psicológicos y atención en crisis.

En todos los casos en los que se advierta la necesidad de acompañamiento psicológico, deberá solicitarse el apoyo de personal especializado. Así mismo, en aquellos casos en los que se trate de niñas, niños y adolescentes con padecimientos de salud, deberá contarse con el apoyo de personal capacitado en medicina.

SÉPTIMO. Escucha y recolección de testimonios.

Cuando sea necesario escuchar a niñas, niños y/o adolescentes para documentar sus denuncias por violencia digital en su contra, deberá observarse los siguientes criterios:

1) Inicio de la escucha y primer acercamiento.

Al inicio del procedimiento de escucha, la persona responsable de efectuarla se presentará, señalando su nombre completo, así como su cargo y puesto en la unidad educativa.

Previo al inicio de las preguntas sobre lo sucedido, deberá trabajarse en generar un ambiente seguro y confiable para las personas víctimas. Para propiciar un clima adecuado es fundamental establecer el rapport, esto es, generar un contacto efectivo entre la persona a cargo de documentar lo sucedido y la víctima.

Es importante que la persona responsable de llevar a cabo la escucha haga sentir a la víctima relajada; ello contribuirá a que muestre una postura abierta y participativa. Es recomendable que durante el procedimiento de escucha se emplee lenguaje no verbal al saludar a las víctimas, así como iniciar la conversación con preguntas informales, que no tengan relación directa con el asunto que se tratará. Ambas acciones contribuirán a que la persona se sienta relajada y segura.[31]

2) Encuadre

Una vez se haya logrado el rapport se explicará, el objetivo de la escucha y las pautas que serán observadas por quienes participen en ella. Se informará a las personas participantes el tiempo de duración estimada del procedimiento, las partes que lo comprenden, la confidencialidad y protección que se brindará a la información proporcionada.

En todos los casos la persona responsable del procedimiento deberá advertir a las víctimas que si se sienten agotadas y desean parar el procedimiento pueden hacerlo. A manera de ejemplo se sugiere adoptar el siguiente formato al inicio del encuadre:

31 Cfr. Comisión de Derechos Humanos de la Ciudad de México, Técnicas para la realización de entrevistas, 2012, p.28.

“El procedimiento de escucha que vamos a tener es acerca de los hechos de violencia digital en tu contra de los cuales hemos recibido reportes. Algunas cosas de las que vamos a platicar pueden ser recuerdos dolorosos para ti. Si en algún momento no quieres responder a una pregunta o sientes la necesidad de parar el procedimiento, lo podemos hacer sin ningún problema. Tu bienestar es lo más importante para nosotros.”

Como parte del encuadre, las personas responsables del proceso de escucha podrán explicar brevemente a las y los participantes que tienen derechos y que uno de ellos es el del respeto a sus opiniones y decisiones. Asimismo, podrán explicar cuál es la función de la unidad educativa en la documentación del caso en concreto.

3) Desarrollo

Para el desarrollo de la escucha, la persona a cargo de su aplicación deberá preparar previamente un cuestionario, en el cual, se aborde como mínimo las condiciones de modo (Qué pasó), tiempo (Cuándo pasó) y lugar (Dónde pasó) sobre el hecho denunciado, así como los elementos indispensables necesarios para llevar a cabo el análisis de contexto al que hicimos referencia en páginas anteriores.

Durante la escucha se registrará por escrito en una bitacora la información proporcionada, así como el lenguaje verbal y no verbal de la víctima.

Durante el desarrollo del procedimiento la persona responsable deberá escuchar activa y afectivamente a la víctima y observar su lenguaje no verbal. Al aplicar el cuestionario de preguntas deberá procurarse el empleo de metodologías que permitan la libre expresión de la víctima (no cortar la narración de la víctima, emplear parafraseo para aclarar aspectos señalados de carácter ambiguo, resumir lo narrado por la víctima y solicitar su confirmación, permitirle corregir aspectos erróneamente interpretados).

La persona responsable del procedimiento deberá evitar la repetición innecesaria de preguntas sobre las cuales observe que el lenguaje no verbal de la víctima cambia generando dolor o angustia.

4) Cierre

Al concluir las últimas preguntas de la escucha deberá anunciarse que el proceso está por concluir, esto ayudará a disminuir el estrés y desgaste emocional que pudiera haberse generado en la víctima.

Una vez obtenida la última respuesta es recomendable hacer un resumen general de la información obtenida en el procedimiento permitiendo que la víctima haga las correcciones que estime pertinentes o señale información adicional que consideré oportuna.

Por último, se reiterará la confidencialidad y el tratamiento que se dará a la información brindada y se le proporcionará información de contacto en caso de necesitar ayuda o tener dudas con relación a los hechos narrados.

En todos los procedimientos de escucha y recopilación de testimonios, deberán seguirse las siguientes recomendaciones:

- Mostrarse accesibles y dispuestos a escuchar a las niñas, niños y adolescentes. Destinar un tiempo propicio para ello, en un espacio seguro y con privacidad.
- De acuerdo a la edad de la niña, niño o adolescente, es recomendable colocarse físicamente a su altura para una mejor escucha. Se evitará postergar la escucha o derivarla con alguna otra persona.
- Escuchar el relato con detenimiento, paciencia, respeto y sin interrupciones o cuestionamientos. Quien escucha deberá mantener la calma y abstenerse de demostrar sentimientos de ira, asombro, tristeza, preocupación o inquietud por la situación, que pudiera desincentivar el relato de la persona menor de edad.
- Manifestar solidaridad hacia niñas, niños y adolescentes, hacerlos sentirse seguros y enfatizar que no son culpables de lo que sucede, reconocer su valor al solicitar apoyo. Hacerles saber que su relato tiene credibilidad y es tomado en cuenta. Abstenerse de utilizar frases como: “¿estás seguro(a)?”, “¿estás diciendo la verdad?”, “¿no será que te confundiste o lo imaginaste”, “¿por qué no dijiste nada?”, “¿por qué lo hiciste?”, “¿por qué no corriste o te defendiste?” o bien “si me mientes vas a tener problemas”,

"¿por qué no le dijiste a tus papás?", "No debes hacer eso, pórtate bien y hazle caso a tu mamá/papá", entre otras.

- Abstenerse de realizar preguntas para ahondar en los detalles de la narración del/los hechos de violencia, inducir u ofrecer alternativas de respuesta ante el silencio o falta de información; por ejemplo: "¿fue en el sillón, la cama o el patio?", "¿entonces fue tu papá verdad?", "¿y qué hiciste, te dieron ganas de llorar o gritar?" únicamente con la intención de ampliar el relato podrán formulársele preguntas abiertas: "¿quién?", "¿dónde?", "¿cuándo?", "¿cómo?". Respetar si es su deseo no decir nada y no forzarlo a hablar.

- Abstenerse de obligar a la niña, niño o adolescente a que muestre sus lesiones, marcas o huellas de violencia en el cuerpo, si las tuviere, es recomendable que se expresen a través del relato o dibujos.

- Abstenerse de emitir comentarios negativos o juicios de valor sobre el comportamiento de las niñas, niños y adolescentes afectadas, sus familiares o demás personas involucradas.

- Hablar con honestidad con la niña, niño o adolescente, explicarle que se le va a brindar la atención adecuada, pero que no es posible mantener el secreto hacia las autoridades o su familia. El personal deberá explicarle los pasos que se van a seguir para la atención de sus peticiones.

OCTAVO. Recolección de pruebas.

Durante el proceso de documentación, las únicas pruebas que serán recolectadas por las autoridades educativas son los testimonios de las personas involucradas y la información de los equipos de cómputo pertenecientes a la unidad educativa que hubieren sido utilizados. Para la recolección de estos elementos las autoridades educativas deberán tener presente el interés superior de la infancia, la obligación de protección especial de las autoridades públicas, las características de los distintos ciclos de vida de niñas, niños y adolescentes, entre otros.

En ningún caso se solicitará a niñas, niños y adolescentes entreguen sus dispositivos de acceso al entorno digital como celulares, tabletas o computadoras portátiles, ya que esta es una competencia exclusiva de las autoridades correspondientes a las Fiscalías Generales de Justicia.

NOVENO. Diligencias, actuaciones y gestiones.

Toda decisión de las autoridades educativas sobre las gestiones o acciones que se realizarán para atender los casos de violencia digital en contra de niñas, niños y adolescentes, deberán basarse en el interés superior de la niñez. Para ello, se considerarán los siguientes criterios:

- Adoptar, en el ámbito de sus respectivas atribuciones, las decisiones que brinden la protección más amplia de todos los derechos de niñas, niños y adolescentes.
- Privilegiar la protección de los derechos de niñas, niños y adolescentes por encima de los derechos, intereses o pretensiones de las personas adultas responsables de su cuidado, o de quienes se encuentren involucrados en los hechos; por ejemplo, personal educativo, de seguridad, personas cuidadoras, autoridades o cualquier otra.
- Cuando existan casos de conflicto de derechos, para tomar la decisión más adecuada, se deberá realizar un ejercicio de ponderación en el que se examine, la necesidad de ejecutar o implementar la gestión o medida, su idoneidad, es decir, si es la única alternativa posible, y si es proporcional al caso concreto.
- Valorar las posibles consecuencias a corto, mediano y largo plazo que la decisión tendrá en la vida de niñas, niños y adolescentes.
- Evitar la revictimización de niñas, niños y adolescentes o sus familiares, a través de diligencias, acciones o gestiones ociosas, repetitivas o innecesarias.

DÉCIMO. Gestiones ante autoridades e instancias públicas.

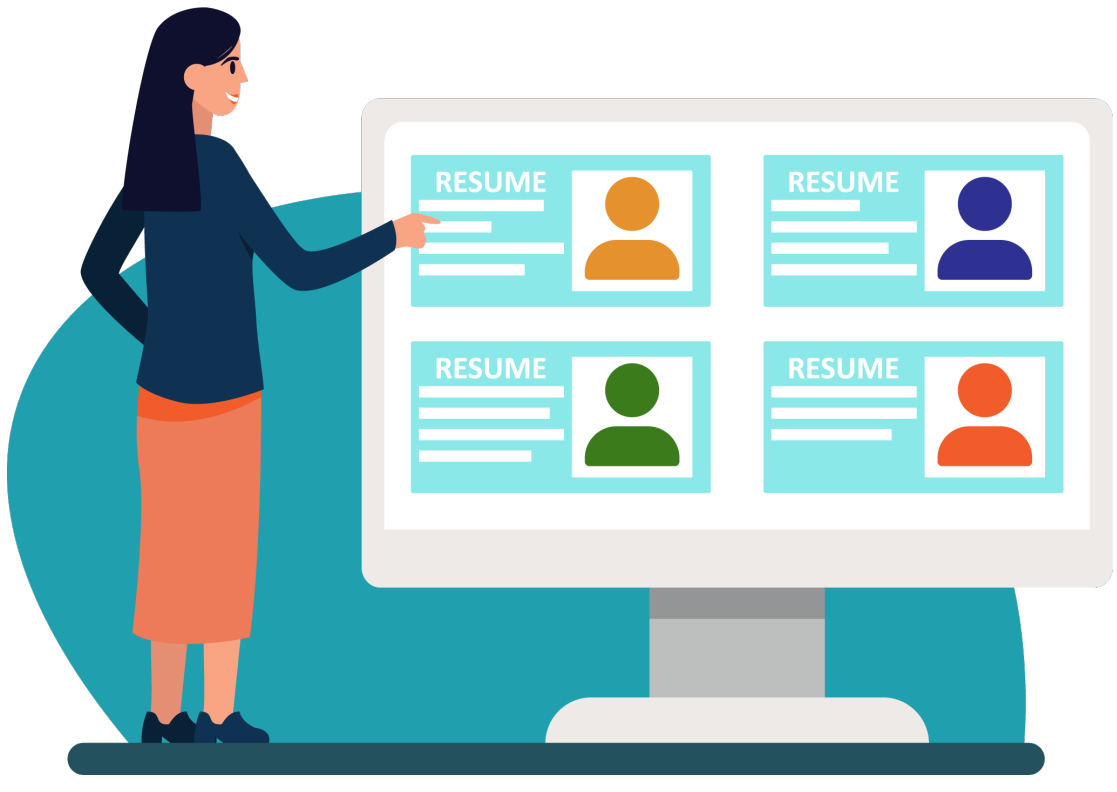
Cuando los hechos de violencia digital en contra de niñas, niños y adolescentes sean considerados hechos delictivos, las autoridades educativas deberán llevar a cabo las gestiones que sean necesarias para informar a las autoridades competentes. Las gestiones podrán consistir, de forma enunciativa más no limitativa en las siguientes: realizar llamadas, enviar oficios, correos electrónicos, o cualquier otra donde se haga de conocimiento de la autoridad pública lo ocurrido. En ese mismo sentido es recomendable llevar una bitácora de las gestiones realizadas en las que se especifique el caso o hecho de violencia documentado, el nombre de las personas afectadas y las autoridades públicas a las cuales se dio intervención.

En todos los casos de violencia digital en contra de niñas, niños y adolescentes en los que se considere que existe la probabilidad de la comisión de un hecho delictivo se deberá dar parte a las Procuradurías de Protección de Derechos de Niñas, Niños y Adolescentes y supletoriamente a las Procuradurías y Fiscalías Generales de Justicia, Guardia Nacional, Policía Cibernética a través del Servicio de Atención a Llamadas de Emergencia 911.[32]

DÉCIMO PRIMERO. Tratamiento de datos personales de personas menores de edad.

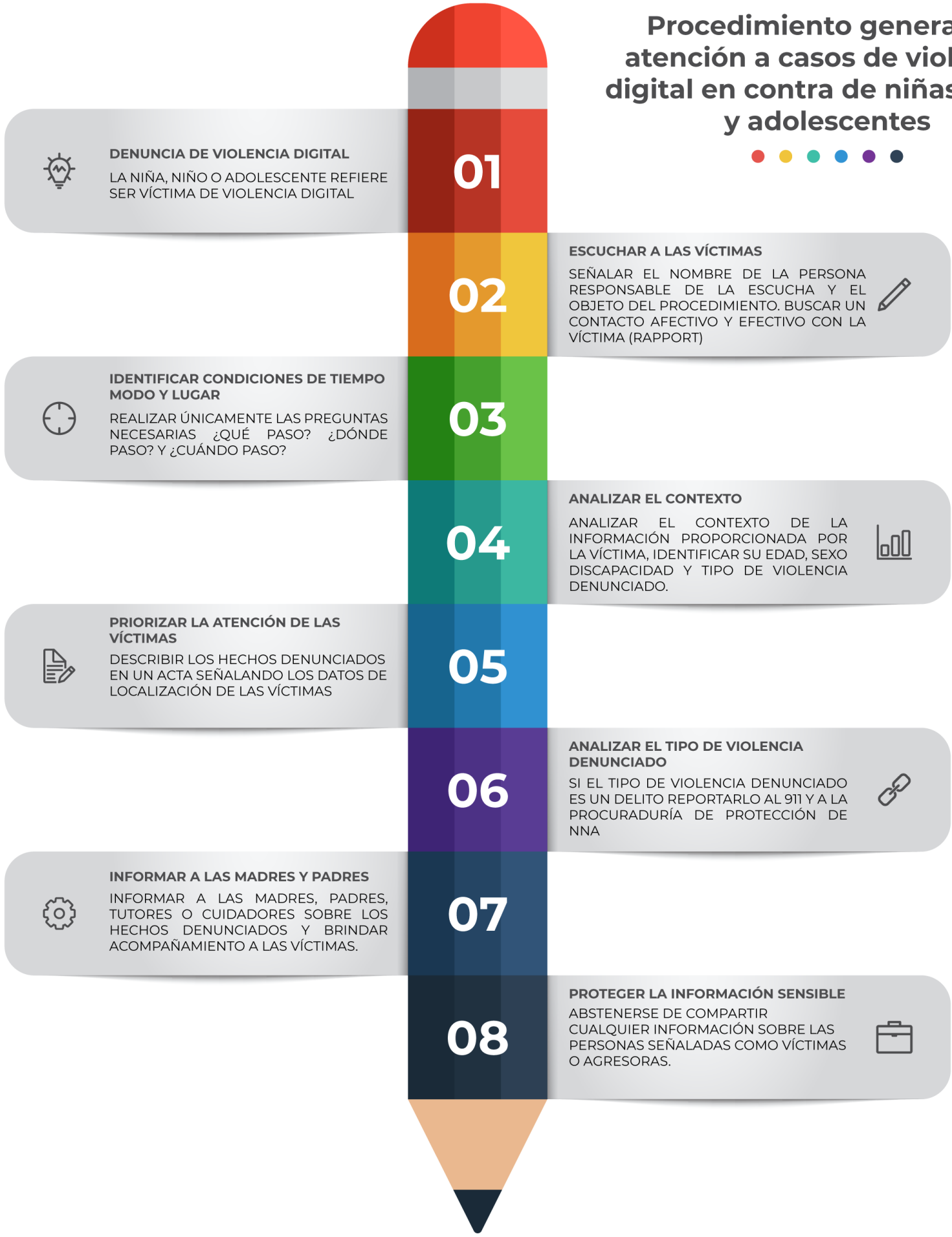
En todas y cada una de las acciones de documentación de violencia digital realizadas, se protegerán los datos personales de las personas menores de edad conforme a lo dispuesto por la Ley General de Transparencia y Acceso a la Información Pública y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Las autoridades educativas deberán abstenerse de compartir datos personales o cualquier otra información sobre niñas, niños y adolescentes, víctimas o agresores con personas diversas a quienes acrediten ejercer la patria potestad o las autoridades a que corresponda conforme a los supuestos de las disposiciones normativas citadas. De igual forma, deberán ser protegidos los datos personales de quienes reporten o informen sobre casos de violencia digital en contra de niñas, niños y adolescentes.



32 Cfr. Sistema Nacional de Protección de Niñas, Niños y Adolescentes, Protocolo Nacional de Coordinación Interinstitucional para la Protección de Niñas, Niños y Adolescentes Víctimas de Violencia, 2021, pp. 47-55.

Procedimiento general de atención a casos de violencia digital en contra de niñas, niños y adolescentes



Fuente: ChildFund México.

B. Lineamientos específicos para la atención y documentación de casos de violencia digital en contra de niñas, niños y adolescentes en escuelas de nivel básico de México.

La atención y documentación de los casos de violencia digital en contra de niñas, niños y adolescentes realizada en el marco del presente **Protocolo**, requiere de la participación de al menos tres autoridades educativas, a saber, una que realice el procedimiento de escucha de las personas víctimas y describa los hechos en la bitácora; una que realice el proceso de canalización o puesta en conocimiento de las autoridades responsables y; una que lleve a cabo el registro y archivo de los casos documentados. En todos los casos las autoridades educativas deberán observar además de los lineamientos generales, los siguientes lineamientos específicos:

1) Atención y documentación de casos de ciberacoso.

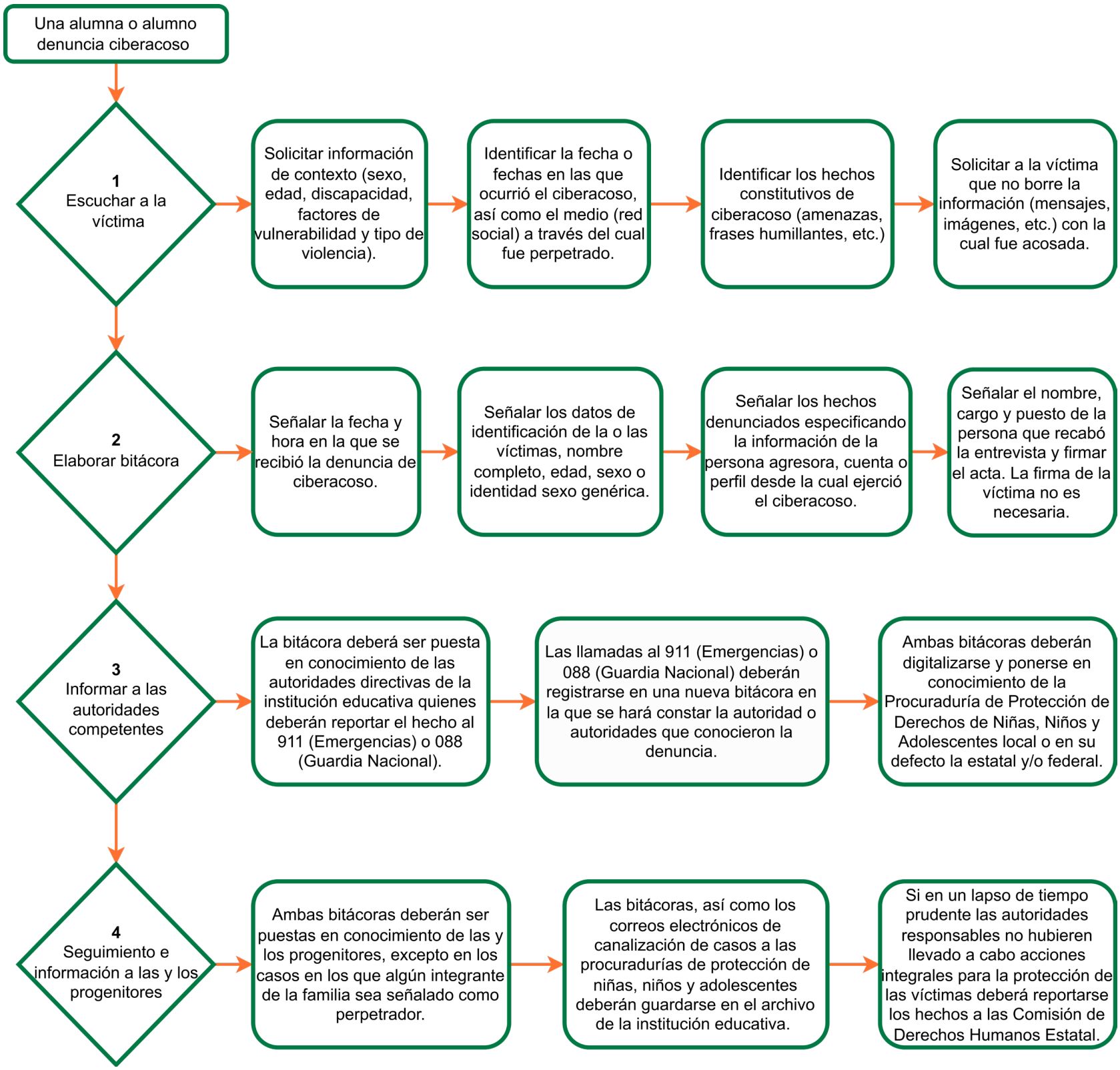
Identificación. El **ciberacoso** ocurre cuando una persona adulta acosa o intimida a una persona menor de edad a través del entorno digital. Puede ocurrir en redes sociales (Facebook, Twitter, Instagram, Tik Tok, etc.); plataformas de mensajería (WhatsApp, Telegram, Snapchat, etc.); plataformas de juegos y teléfonos móviles. Es un comportamiento que se repite y que busca atemorizar, enfadar o humillar a una niña, niño o adolescente.

Acciones integrales para su atención. Ante un caso de **ciberacoso** el personal docente o primer respondiente, deberá escuchar a la niña, niño o adolescente afectado con la finalidad de recabar la información mínima necesaria (revisar análisis de contexto), para documentar los hechos. Durante la escucha deberá solicitarse información sobre las tecnologías (redes sociales, plataformas de mensajería, etc.) utilizadas para perpetrar la violencia denunciada, así como información de los perfiles o cuentas desde las cuales se perpetraron los hechos, solicitando a las personas afectadas no borrar o eliminar los mensajes recibidos, ya que constituyen el medio principal de prueba. Deberán observarse los lineamientos generales establecidos por el presente Protocolo señalados en el apartado referente a “Escucha y recolección de testimonios”.

Con la información proporcionada durante la escucha, se elaborará una bitácora que deberá contener indefectiblemente la fecha, lugar y nombre de la persona responsable de su elaboración, el nombre domicilio e información de contacto de las personas menores de edad afectadas, así como los hechos narrados, precisando condiciones de tiempo, modo y lugar. Dicho documento deberá ser puesto en conocimiento de las autoridades directivas de la institución educativa quienes deberán reportarlo de manera inmediata al Servicio de Atención a Llamadas de Emergencia 911, la policía cibernética local o la Guardia Nacional al número 088, dichas diligencias deberán hacerse constar en otra bitácora. Ambas bitácoras serán enviadas por correo institucional a la Procuraduría de Protección de Derechos de Niñas, Niños y Adolescentes local o en su defecto a la estatal o federal.

Deberá citarse a las personas responsables del cuidado de niñas, niños y adolescentes víctimas de ciberacoso a objeto de que se les informe personalmente sobre el procedimiento llevado por la unidad educativa. Se les entregará una copia de las bitácoras elaboradas para su conocimiento, salvo en los casos en los que sean señalados como perpetradores. En caso de requerir mayor información de las y los afectados podrá llevarse a cabo una segunda escucha en presencia de su madre, padre tutor o cuidador. No es recomendable recabar capturas de pantalla de celulares o dispositivos como evidencia o prueba ya que esta labor será llevada a cabo a través de software especializado empleado por las autoridades de investigación. Si en un lapso prudente de tiempo no se tuviere noticias de las acciones de protección iniciadas por las autoridades de investigación deberá reportarse los hechos a la Comisión de Derechos Humanos estatal. Toda la documentación generada deberá permanecer en el archivo de la institución educativa.

Flujograma 1
Proceso para la atención de casos de ciberacoso



Fuente: ChildFund México

2) Atención y documentación de casos de ciberbullying.

Identificación. El **ciberbullying** se da cuando un cuando una niña, niño o adolescente es molestado, amenazado, acosado, humillado, avergonzado o abusado por otra persona menor de edad, a través del entorno digital. Es posible identificar este tipo de violencia a través de mensajes de texto en aplicaciones de mensajería como WhatsApp o redes sociales como Facebook, entre otras.

Acciones integrales para su atención. Ante un caso de **ciberbullying** el personal docente o primer respondiente, deberá escuchar a la niña, niño o adolescente afectado con la finalidad de recabar la información mínima necesaria (revisar análisis de contexto) para documentar los hechos. Durante la escucha deberá solicitarse información sobre las tecnologías (redes sociales, plataformas de mensajería, etc.) utilizadas para perpetrar la violencia denunciada, solicitando a las personas afectadas no borrar o eliminar los mensajes recibidos ya que constituyen el medio principal de prueba.

Deberán observarse los lineamientos generales establecidos por el presente **Protocolo** señalados en el apartado referente a “Escucha y recolección de testimonios”.

Con la información proporcionada durante la escucha, deberá elaborarse una bitácroa que deberá contener indefectiblemente la fecha, lugar y nombre de la persona responsable de su elaboración, el nombre domicilio e información de contacto de las personas menores de edad afectadas, así como los hechos narrados, precisando condiciones de tiempo, modo y lugar. Dicho documento deberá ser puesto en conocimiento de las autoridades directivas de la institución educativa quienes deberán reportarlo de manera inmediata a la madre, padre, tutor o cuidador de la persona menor de edad afectada, así como de los responsables del cuidado de la niña, niño o adolescente señalado como persona agresora.

Deberá citarse a las personas responsables del cuidado de las partes involucradas (personas agresoras y personas víctimas) para que a través de pláticas de sensibilización se les informe sobre las formas en las que se perpetra este tipo de violencia y los riesgos para las personas afectadas. Se deberá emplear mecanismos de conciliación entre las partes a objeto de establecer mecanismos que garanticen la no repetición de los hechos denunciados. Es muy importante precisar que no deben emplearse

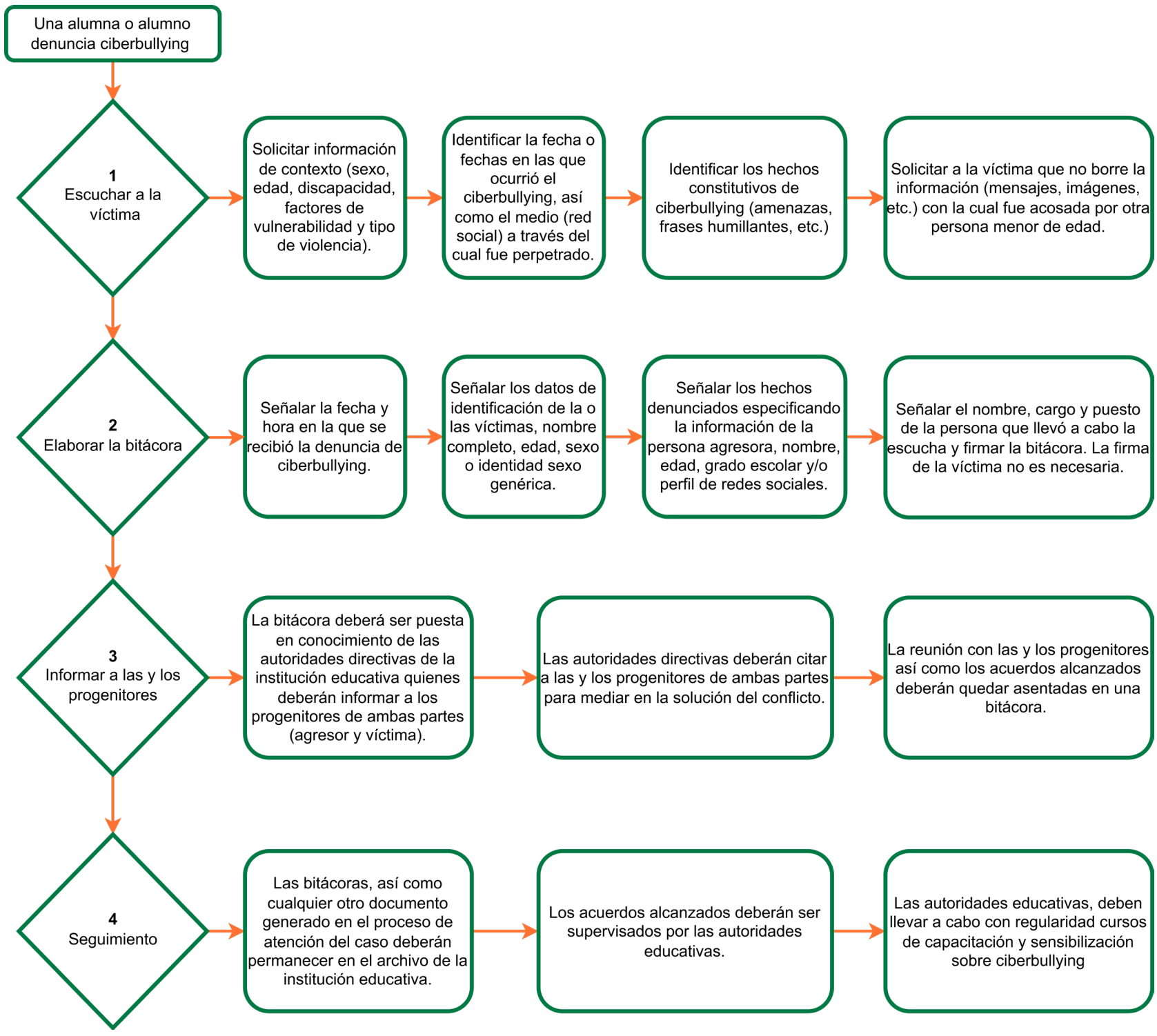
mecanismos de sanción basados en castigos corporales o humillantes, ya que estos están prohibidos por la ley y constituyen formas de violencia que se deben erradicar, en su lugar es preferible emplear mecanismos de justicia restaurativa los cuales están encaminados a que las personas generadoras de violencia, con apoyo de un facilitador o facilitadora, reconozcan sus faltas, se responsabilicen de las consecuencias de sus actos y reparen los daños causados.

Las reuniones o pláticas que las autoridades directivas realicen con las personas responsables del cuidado de ambas partes (víctima y agresor) deberán hacerse constar en bitácoras, señalando los acuerdos alcanzados.

Las bitácoras, así como cualquier otro documento generado durante el proceso de atención del caso deberá permanecer en el archivo de la institución educativa. Las autoridades educativas deberán dar seguimiento a los acuerdos alcanzados y a la no repetición de los hechos.

Las instituciones educativas que apliquen el presente **Protocolo** deberán llevar a cabo procesos de capacitación y sensibilización con las alumnas y alumnos sobre este tipo de violencia como mecanismo de prevención.

Flujograma 2
Proceso para la atención de casos de ciberbullying



Fuente: ChildFund México

3) Atención y documentación de casos de grooming.

Identificación. El **grooming** se da cuando una persona adulta, mediante engaños y mentiras, se gana la confianza y establece algún tipo de amistad con una niña, niño o adolescente a través del entorno digital, ya sea a través de redes sociales, aplicaciones de mensajería instantánea, correo electrónico u otros, con el fin de obtener imágenes o videos con connotación o actividad sexual. Es posible identificar este tipo de violencia a través de mensajes de texto en aplicaciones de mensajería como WhatsApp o redes sociales como Facebook, entre otras.

Acciones integrales para su atención. Ante un caso de **grooming** el personal docente o primer respondiente, deberá escuchar a la niña, niño o adolescente afectado con la finalidad de recabar la información mínima necesaria (revisar análisis de contexto) para documentar los hechos. Durante la escucha deberá solicitarse información sobre las tecnologías (redes sociales, plataformas de mensajería, etc.) utilizadas para perpetrar la violencia denunciada, así como información de los perfiles o cuentas desde las cuales se perpetraron los hechos, solicitando a las personas afectadas no borrar o eliminar los mensajes recibidos, ya que constituyen el medio principal de prueba.

Deberán observarse los lineamientos generales establecidos por el presente **Protocolo** señalados en el apartado referente a “Escucha y recolección de testimonios”.

Con la información proporcionada durante la escucha, se elaborará una bitácora que deberá contener indefectiblemente la fecha, lugar y nombre de la persona responsable de su elaboración, el nombre domicilio e información de contacto de las personas menores de edad afectadas, los datos con los que se cuente de las personas señaladas como agresoras, así como los hechos narrados, precisando condiciones de tiempo, modo y lugar. Dicho documento deberá ser puesto en conocimiento de las autoridades directivas de la institución educativa quienes deberán reportarlo de manera inmediata al Servicio de Atención a Llamadas de Emergencia 911, la policía cibernética local o la Guardia Nacional al número 088, dichas diligencias deberán hacerse constar en otra bitácora. Ambas bitácoras serán enviadas por correo institucional a la Procuraduría de Protección de Derechos de Niñas, Niños y Adolescentes local o en su defecto a la estatal o federal.

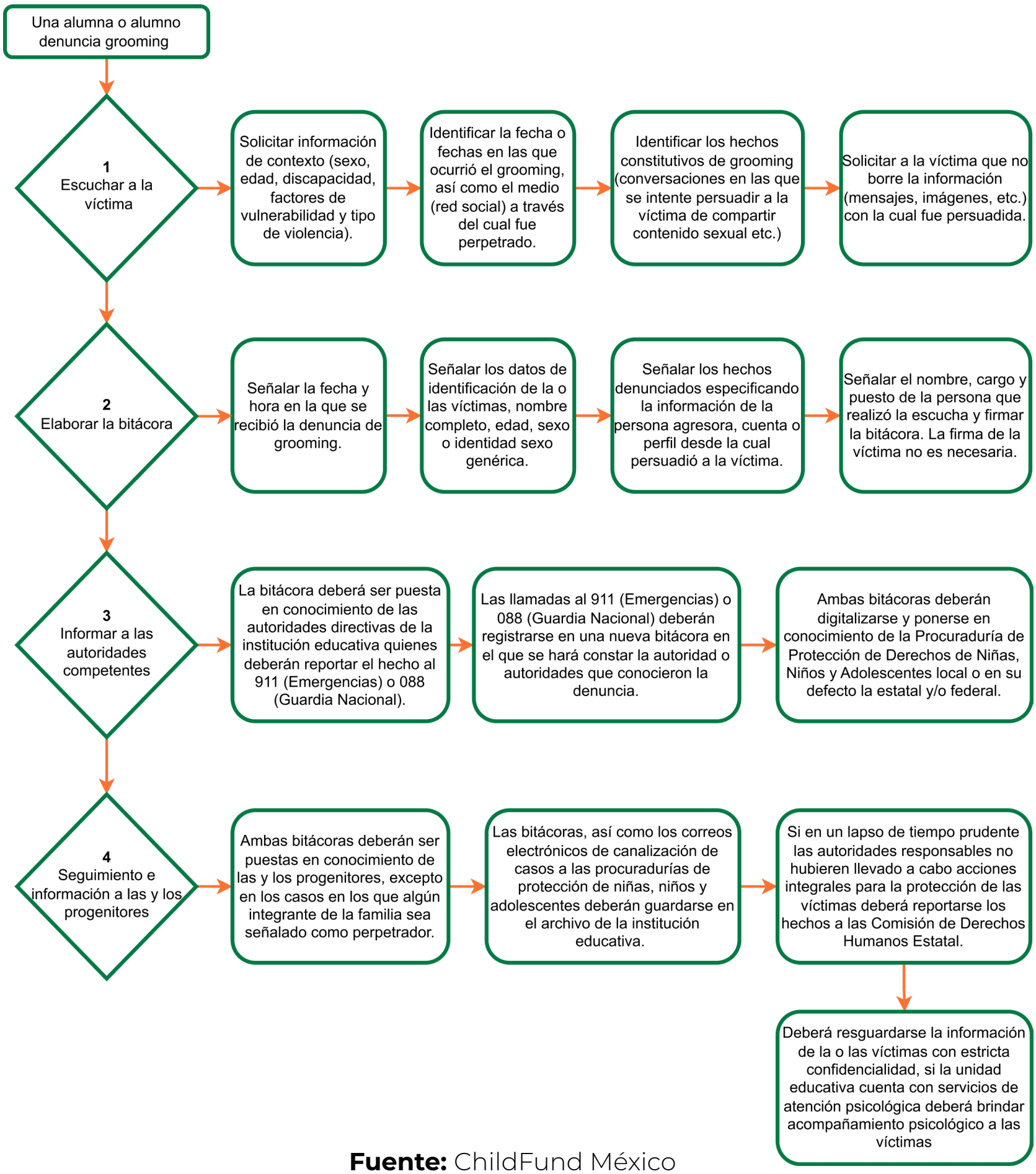
Deberá citarse a las personas responsables del cuidado de niñas, niños y adolescentes víctimas de grooming a objeto de que se les informe personalmente sobre el procedimiento llevado por la unidad educativa. Se les entregará una copia de las bitácoras elaboradas para su conocimiento, salvo en los casos en los que sean señalados como perpetradores. En caso de requerir mayor información de las y los afectados podrá llevarse a cabo una segunda escucha en presencia de su madre,

padre tutor o cuidador. No es recomendable recabar capturas de pantalla de celulares o dispositivos como evidencia o prueba ya que esta labor será llevada a cabo a través de software especializado empleado por las autoridades de investigación. Si en un lapso prudente de tiempo no se tuviere noticias de las acciones de protección iniciadas por las autoridades de investigación deberá reportarse los hechos a la Comisión de Derechos Humanos estatal. Toda la documentación generada deberá permanecer en el archivo de la institución educativa.

Al ser una forma de violencia sexual digital deberá cuidarse en todo momento la confidencialidad de la información de las víctimas, así como los contenidos que se hubieran producido en el ejercicio de esta violencia. Es muy importante no compartir las imágenes y/o videos de contenido sexual a través de aplicaciones de mensajería como WhatsApp ya que dicha información podría filtrarse. En ese sentido, únicamente la autoridad pública responsable de la investigación estará facultada para capturar y obtener dicha información a través de los medios y métodos idóneos.

Es muy importante brindar acompañamiento psicológico a las personas víctimas, en caso de que la unidad educativa cuente con dicho servicio, deberá solicitarse la autorización de las personas a cargo del cuidado de las niñas, niños y adolescentes afectados para implementarlo.

Flujograma 3
Proceso para la atención de casos de grooming



Fuente: ChildFund México

4) Atención y documentación de casos de sexting.

Identificación. El **sexting** es una forma de violencia digital cometida entre personas menores de edad que consiste en el envío o recepción de imágenes o videos de carácter íntimo y/o de contenido sexual de una niña, niño y adolescente a través del entorno digital sin su consentimiento.

Acciones integrales para su atención. Ante un caso de **sexting** el personal docente o primer respondiente, deberá escuchar a la niña, niño o adolescente afectado con la finalidad de recabar la información mínima necesaria (revisar análisis de contexto) para documentar los hechos. Durante la escucha deberá solicitarse información sobre las tecnologías (redes sociales, plataformas de mensajería, etc.) utilizadas para perpetrar la violencia denunciada, solicitando a las personas afectadas no borrar o eliminar los mensajes recibidos ya que constituyen el medio principal de prueba.

Deberán observarse los lineamientos generales establecidos por el presente **Protocolo** señalados en el apartado referente a “Escucha y recolección de testimonios”.

Con la información proporcionada durante la escucha, se elaborará una bitácora que deberá contener indefectiblemente la fecha, lugar y nombre de la persona responsable de su elaboración, el nombre domicilio e información de contacto de las personas menores de edad afectadas, la o las personas agresoras, así como los hechos narrados, precisando condiciones de tiempo, modo y lugar. Dicho documento deberá ser puesto en conocimiento de las autoridades directivas de la institución educativa quienes deberán reportarlo de manera inmediata al Servicio de Atención a Llamadas de Emergencia 911, la policía cibernética local o la Guardia Nacional al número 088, dichas diligencias deberán hacerse constar en otra bitácora. Ambas bitácoras serán enviadas por correo institucional a la Procuraduría de Protección de Derechos de Niñas, Niños y Adolescentes local o en su defecto a la estatal o federal. Si en un lapso prudente de tiempo no se tuviere noticias de las acciones de protección iniciadas por las autoridades de investigación deberá reportarse los hechos a la Comisión de Derechos Humanos estatal. Toda la documentación generada deberá permanecer en el archivo de la institución educativa.

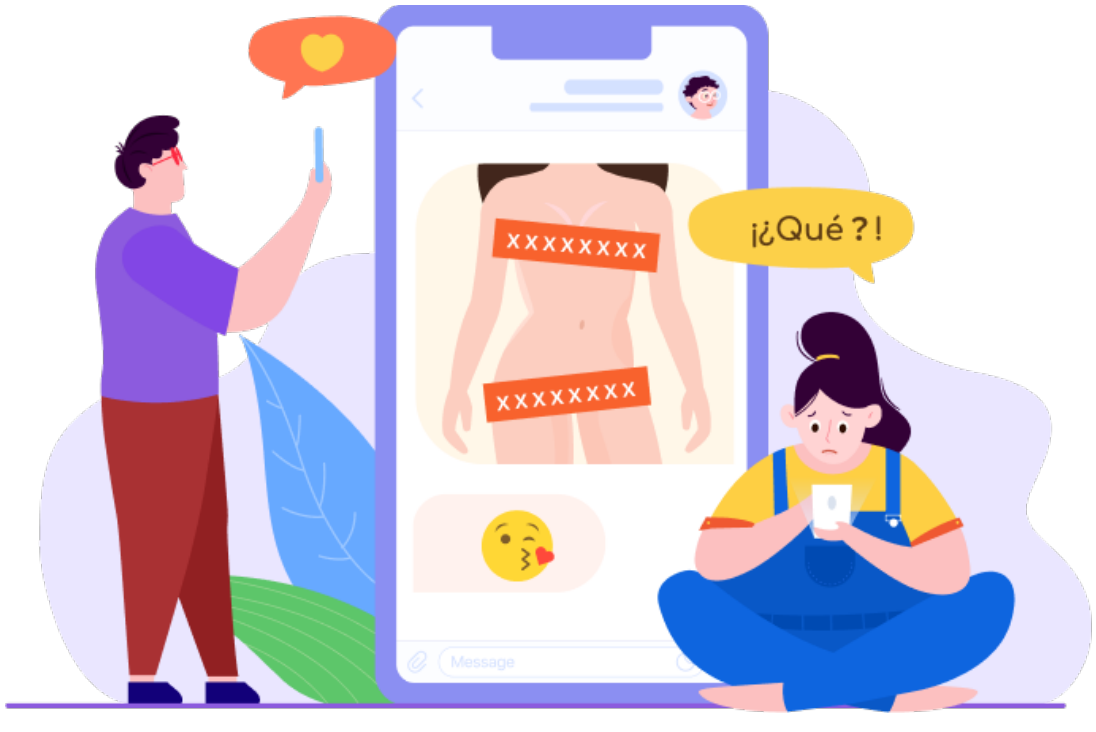
Ambas bitácoras deberán ser puestas en conocimiento de la madre, padre, tutor o cuidador de la persona menor de edad afectada, excepto en aquellos casos en los que la persona señalada como agresora sea un integrante de su familia.

En los casos en que la persona señalada como agresora no sea un familiar de la víctima, deberá informarse también a los responsables del cuidado de la niña, niño o adolescente señalado como persona agresora, a quienes deberá solicitarse supervisen que la información de contenido sexual no sea compartida, advirtiéndoseles de la posible comisión de un hecho delictivo.

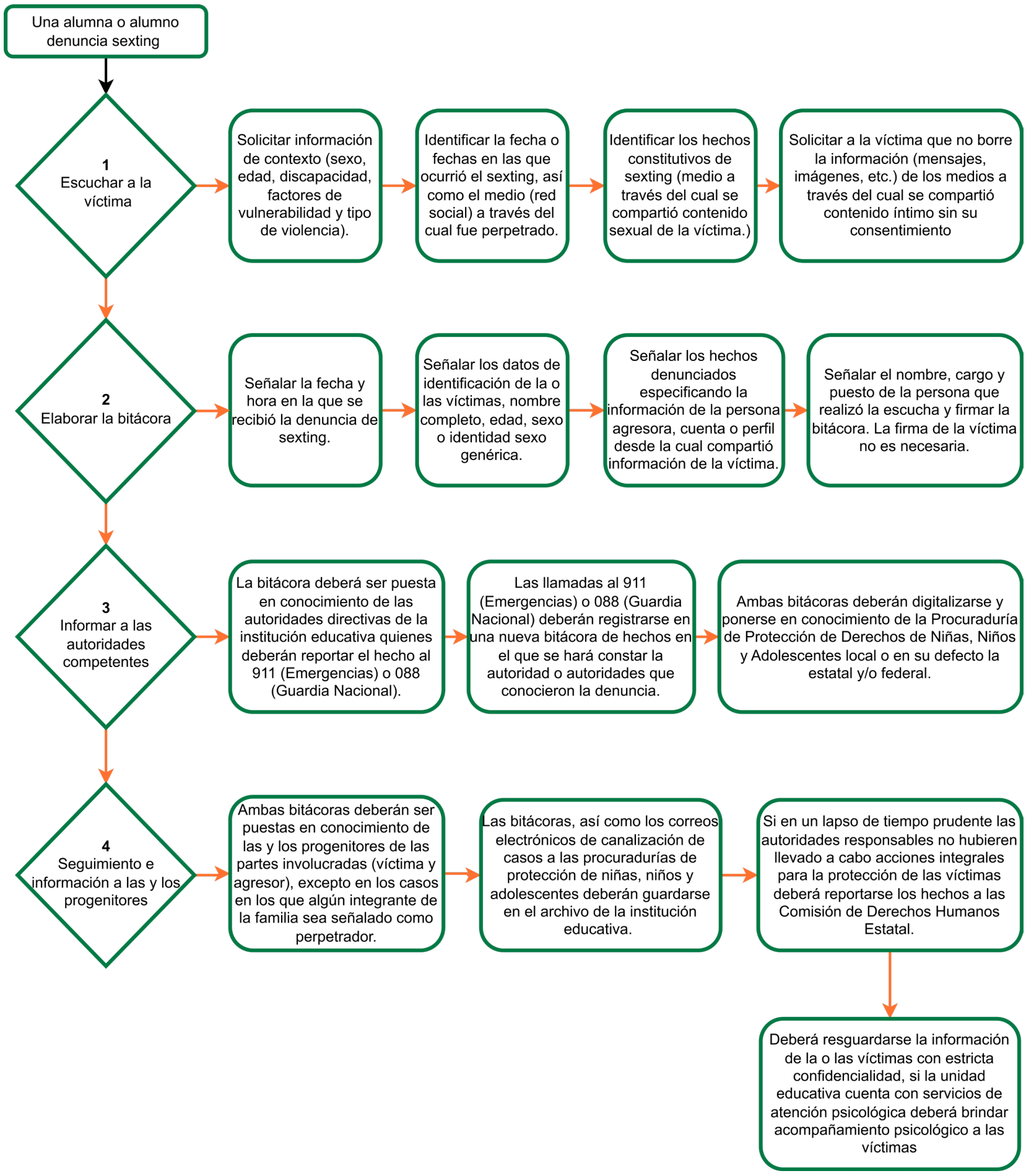
En caso de que el material con contenido sexual se haya viralizado a través de redes sociales, deberá brindarse apoyo a la o las víctimas para reportar las ligas de acceso a dicho material a través de plataformas especializadas o a la policía cibernética y/o la guardia nacional para su depuración.

Al ser una forma de violencia sexual digital deberá cuidarse en todo momento la confidencialidad de la información de las víctimas, así como los contenidos que se hubieran producido en el ejercicio de esta violencia. Es muy importante no compartir las imágenes y/o videos de contenido sexual a través de aplicaciones de mensajería como WhatsApp ya que dicha información podría filtrarse. En ese sentido, únicamente la autoridad pública responsable de la investigación estará facultada para capturar y obtener dicha información a través de los medios y métodos idóneos.

Es muy importante brindar acompañamiento psicológico a las personas víctimas, en caso de que la unidad educativa cuente con dicho servicio, deberá solicitarse la autorización de las personas a cargo del cuidado de las niñas, niños y adolescentes afectados para implementarlo.



Flujograma 4
Proceso para la atención de casos de sexting



Fuente: Child Fund México

5) Atención y documentación de casos de phishing, smishing o vishing.

Identificación. Se presentan cuando personas adultas intentan engañar a personas menores de edad a través de mensajes de correo electrónico falsos (phishing), mensajes de texto falsos (smishing) o llamadas telefónicas falsas (vishing) para que revelen información confidencial o realicen ciertas acciones, como descargar y ejecutar archivos que parecen ser benignos, pero que en realidad son maliciosos, con la intención de robar su información o datos sensibles como contraseñas de redes sociales o aplicaciones de mensajería.

Acciones integrales para su atención. Ante un caso de **phishing, smishing o vishing**, el personal docente o primer respondiente, deberá escuchar a la niña, niño o adolescente afectado con la finalidad de recabar la información mínima necesaria (revisar análisis de contexto) para documentar los hechos. Durante la escucha deberá solicitarse información sobre las tecnologías (llamadas telefónicas, mensajes de texto o correos electrónicos) utilizadas para perpetrar la violencia denunciada, solicitando a las personas afectadas no borrar o eliminar los mensajes recibidos ya que constituyen el medio principal de prueba.

Deberán observarse los lineamientos generales establecidos por el presente **Protocolo**

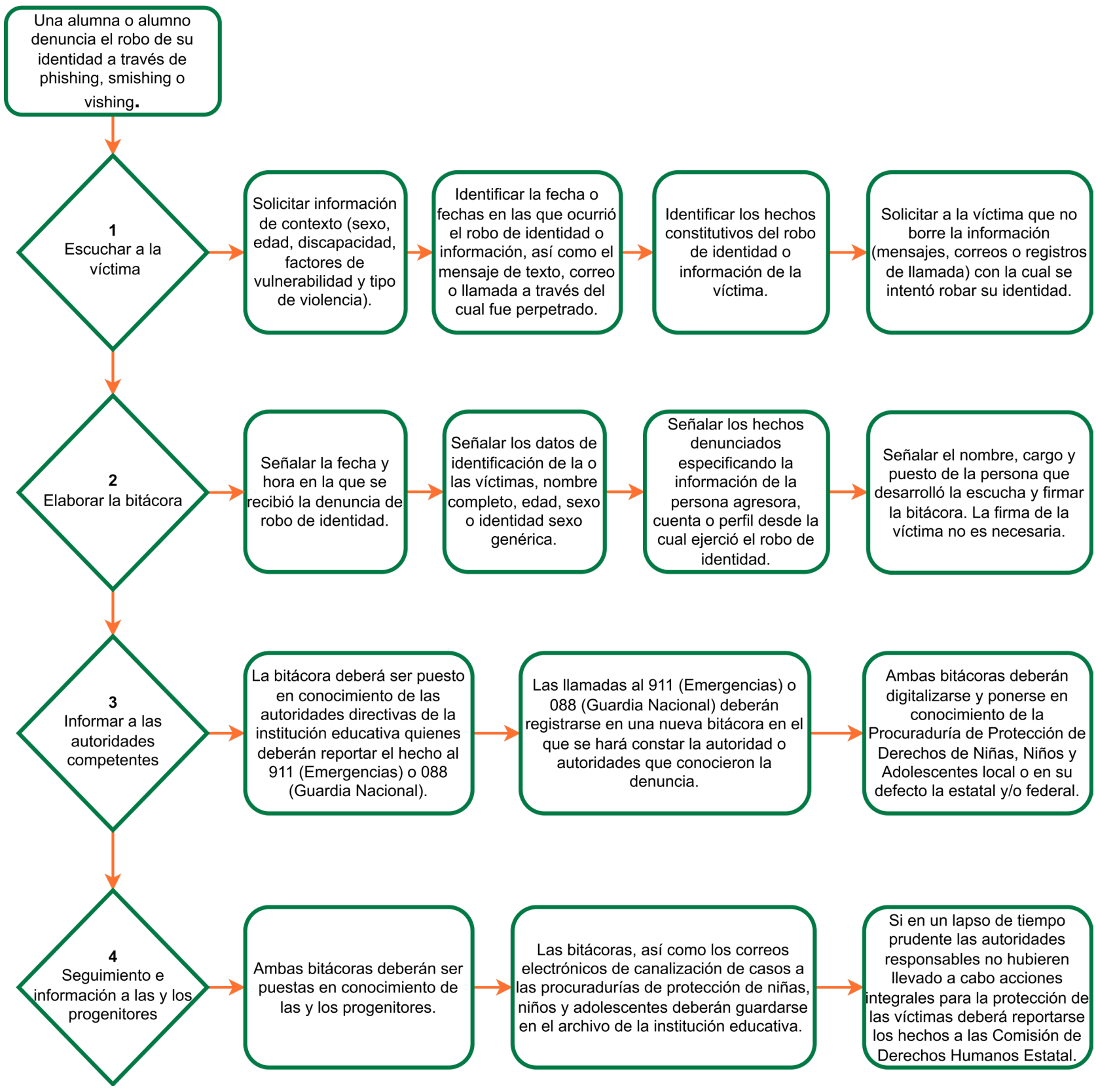
señalados en el apartado referente a “Escucha y recolección de testimonios”.

Con la información proporcionada durante la escucha, se elaborará una bitácora que deberá contener indefectiblemente la fecha, lugar y nombre de la persona responsable de su elaboración, el nombre domicilio e información de contacto de las personas menores de edad afectadas, los datos con los que se cuente de las personas señaladas como agresoras y los medios empleados para el robo de identidad o información, así como los hechos narrados, precisando condiciones de tiempo, modo y lugar. Dicho documento deberá ser puesto en conocimiento de las autoridades directivas de la institución educativa quienes deberán reportarlo de manera inmediata al Servicio de Atención a Llamadas de Emergencia 911, la policía cibernética local o la Guardia Nacional al número 088, dichas diligencias deberán hacerse constar en otra bitácora. Ambas bitácoras serán enviadas por correo institucional a la Procuraduría de Protección de Derechos de Niñas, Niños y Adolescentes local o en su defecto a la estatal o federal.

Deberá citarse a las personas responsables del cuidado de niñas, niños y adolescentes víctimas a objeto de que se les informe personalmente sobre el procedimiento llevado por la unidad educativa para la denuncia de los hechos ante las autoridades públicas competentes, así como entregarles una copia de las bitácoras generadas. En caso de requerir mayor información de las y los afectados podrá llevarse a cabo una segunda escucha en presencia de su madre, padre tutor o cuidador.

Si en un lapso prudente de tiempo no se tuviere noticias de las acciones de protección iniciadas por las autoridades de investigación deberá reportarse los hechos a la Comisión de Derechos Humanos estatal. Toda la documentación generada deberá permanecer en el archivo de la institución educativa.

Flujograma 5
Proceso para la atención de casos de Phishing, Smishing o Vishing.



Fuente: ChildFund México

6) Atención y documentación de casos sobre retos virales nocivos de niñas, niños y adolescentes.

Identificación. Se presentan cuando personas menores de edad llevan a cabo desafíos o pruebas populares riesgosas en el entorno digital. Estos retos pueden llevarse a cabo como un juego en el que, a través de un video, se establece un desafío riesgoso y se comparte en redes sociales para incentivar a otras personas menores de edad a llevarlos a cabo.

Acciones integrales para su atención. Ante un caso de **retos virales nocivos,** el personal docente o primer respondiente, deberá escuchar a la niña, niño o adolescente afectado con la finalidad de recabar la información mínima necesaria (revisar análisis de contexto) para documentar los hechos. Durante la escucha deberá solicitarse información sobre las tecnologías utilizadas para perpetrar la violencia denunciada, solicitando a las personas afectadas no borrar o eliminar los videos o mensajes ya que constituyen el medio principal de prueba. En ese mismo sentido deberá precisarse las plataformas o redes sociales utilizadas en la que se detectó el reto viral nocivo explicando en que consiste.

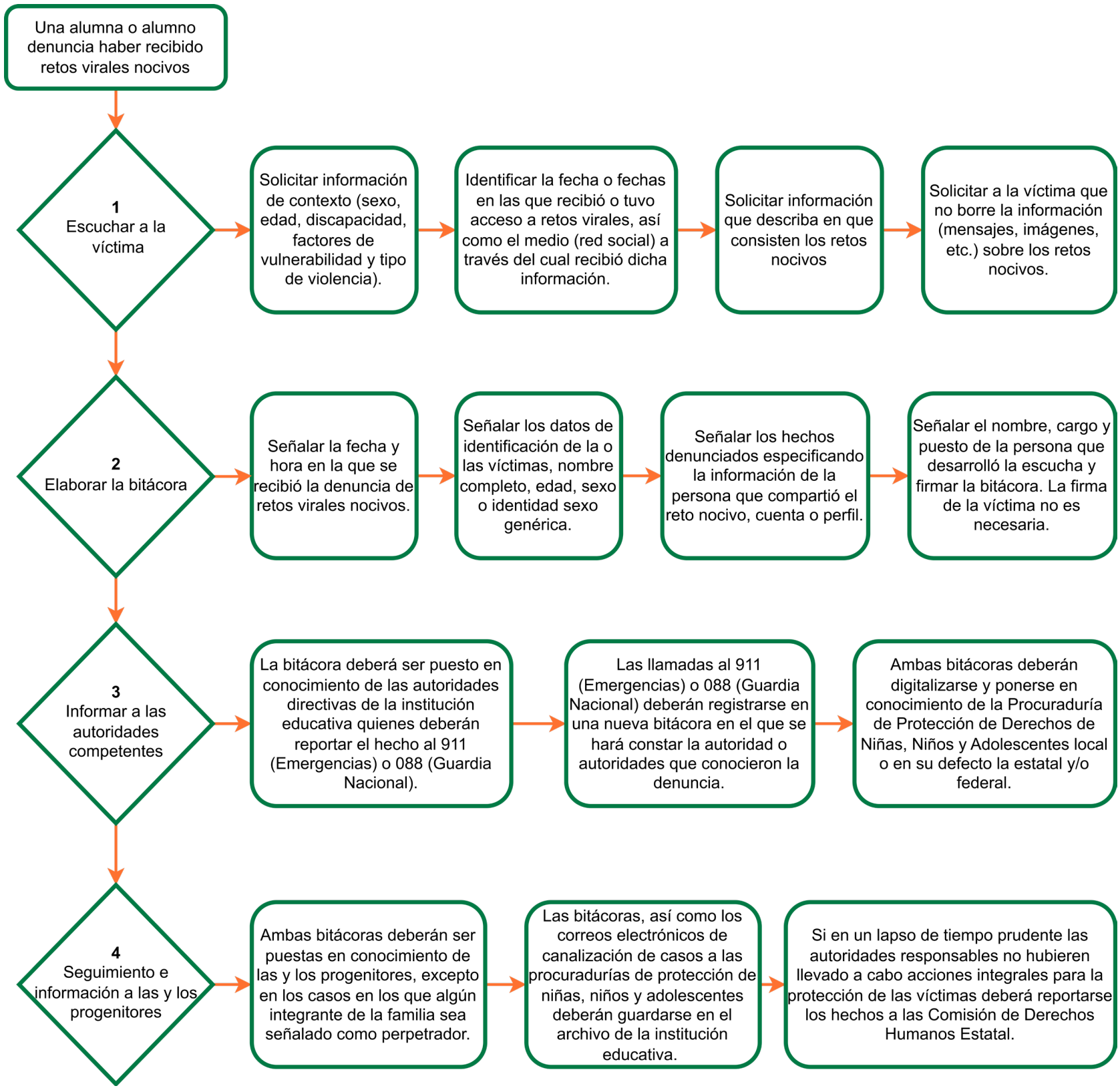
Deberán observarse los lineamientos generales establecidos por el presente **Protocolo** señalados en el apartado referente a “Escucha y recolección de testimonios”.

Con la información proporcionada durante la escucha, se elaborará una bitácora que deberá contener indefectiblemente la fecha, lugar y nombre de la persona responsable de su elaboración, el nombre domicilio e información de contacto de las personas menores de edad afectadas, así como los hechos narrados, precisando condiciones de tiempo, modo y lugar. Deberá incluirse también la liga o portal a través del cual puede accederse al video o audio en el que se encuentra el reto nocivo. Dicho documento deberá ser puesto en conocimiento de las autoridades directivas de la institución educativa quienes deberán reportarlo de manera inmediata al Servicio de Atención a Llamadas de Emergencia 911, la policía cibernética local o la Guardia Nacional al número 088, dichas diligencias deberán hacerse constar en otra bitácora. Ambas bitácoras serán enviadas por correo institucional a la Procuraduría de Protección de Derechos de Niñas, Niños y Adolescentes local o en su defecto a la estatal o federal.

Deberá citarse a las personas responsables del cuidado de niñas, niños y adolescentes víctimas a objeto de que se les informe personalmente sobre el procedimiento llevado por la unidad educativa para la denuncia de los hechos ante las autoridades públicas competentes, así como entregarles una copia de las bitácoras generadas. En caso de requerir mayor información de las y los afectados podrá llevarse a cabo una segunda escucha en presencia de su madre, padre tutor o cuidador.

Si en un lapso prudente de tiempo no se tuviere noticias de las acciones de protección iniciadas por las autoridades de investigación deberá reportarse los hechos a la Comisión de Derechos Humanos estatal. Toda la documentación generada deberá permanecer en el archivo de la institución educativa.

Flujograma 6
Proceso para la atención de casos de retos virales noscivos



Fuente: ChildFund México

7) Atención y documentación de casos de violencia digital en la pareja o expareja.

Identificación. Se presenta cuando la pareja o expareja lleva a cabo un conjunto de comportamientos repetidos que pretenden controlar, menoscabar o causar daño a través del entorno digital. Se lleva a cabo mediante el intercambio de mensajes, control de las redes sociales o aplicaciones, apropiación de las contraseñas, difusión de secretos o información comprometida, amenazas e insultos. Se puede vigilar a la pareja controlando su ubicación, conversaciones, comentarios en línea, enviando correos, mensajes o comentarios humillantes, groseros o degradantes, o publicando fotos con la misma intención.

Acciones integrales para su atención. Ante un caso de **violencia en la pareja o expareja** el personal docente o primer respondiente, deberá escuchar a la niña, niño o adolescente afectado con la finalidad de recabar la información mínima necesaria (revisar análisis de contexto) para documentar los hechos. Durante la escucha deberá solicitarse información sobre las tecnologías utilizadas para perpetrar la violencia denunciada (mensajes de texto, correos electrónicos, etc.) solicitando a las personas afectadas no borrar o eliminar los videos o mensajes ya que constituyen el medio principal de prueba. Deberán observarse los lineamientos generales establecidos por el presente Protocolo señalados en el apartado referente a “Escucha y recolección de testimonios”.

Con la información proporcionada durante la escucha, deberá elaborarse una bitácora que deberá contener indefectiblemente la fecha, lugar y nombre de la persona responsable de su elaboración, el nombre domicilio e información de contacto de las personas menores de edad afectadas, así como los hechos narrados, precisando condiciones de tiempo, modo y lugar. Dicho documento deberá ser puesto en conocimiento de las autoridades directivas de la institución educativa quienes deberán reportarlo de manera inmediata a la madre, padre, tutor o cuidador de la persona menor de edad afectada, así como de los responsables del cuidado de la niña, niño o

adolescente señalado como persona agresora a quienes deberá solicitarse supervisen el cese de toda forma de violencia en contra de la persona afectada.

Cuando los hechos denunciados no constituyan delitos deberá citarse a las personas responsables del cuidado de las partes involucradas (personas agresoras y personas víctimas) para que a través de pláticas de sensibilización se les informe sobre las formas en las que se perpetra este tipo de violencia y los riesgos para las personas afectadas. Se deberá emplear mecanismos de conciliación entre las partes a objeto de establecer mecanismos que garanticen la no repetición de los hechos denunciados.

Es muy importante precisar que no deben emplearse mecanismos de sanción basados en castigos corporales o humillantes, ya que estos están prohibidos por la ley y constituyen formas de violencia que se deben erradicar, en su lugar es preferible emplear mecanismos de justicia restaurativa los cuales están encaminados a que las personas generadoras de violencia, con apoyo de un facilitador o facilitadora, reconozcan sus faltas, se responsabilicen de las consecuencias de sus actos y reparen los daños causados.

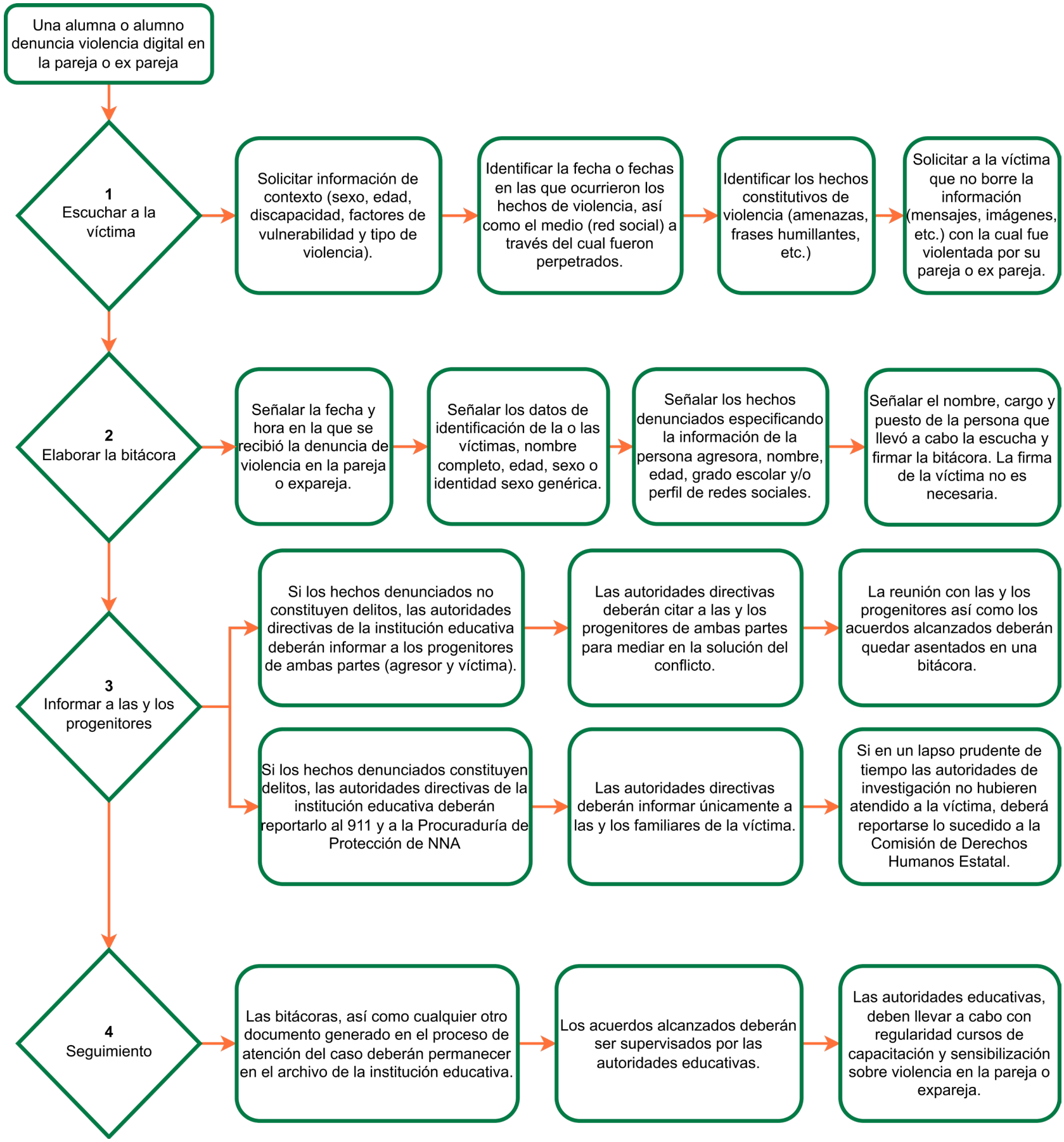
Las reuniones o pláticas que las autoridades directivas realicen con las personas responsables del cuidado de ambas partes (víctima y agresor) deberán hacerse constar en bitácoras, señalando los acuerdos alcanzados.

Las bitácoras, así como cualquier otro documento generado durante el proceso de atención del caso deberá permanecer en el archivo de la institución educativa. Las autoridades educativas deberán dar seguimiento a los acuerdos alcanzados y a la no repetición de los hechos.

Las instituciones educativas que apliquen el presente **Protocolo** deberán llevar a cabo procesos de capacitación y sensibilización con las alumnas y alumnos sobre este tipo de violencia como mecanismo de prevención.

En el caso de que alguno de los hechos denunciados constituya un delito, las autoridades directivas de la institución educativa deberán reportarlo de manera inmediata al Servicio de Atención a Llamadas de Emergencia 911, la policía cibernética local o la Guardia Nacional al número 088, dichas diligencias deberán hacerse constar en otra bitácora. Ambas bitácoras serán enviadas por correo institucional a la Procuraduría de Protección de Derechos de Niñas, Niños y Adolescentes local o en su defecto a la estatal o federal.

Flujograma 7
Proceso para la atención de casos de violencia en la pareja o ex pareja



Fuente: ChildFund México

8) Atención y documentación de casos de explotación sexual comercial infantil en el entorno digital

Identificación. Consiste en la explotación realizada por un adulto de fotografías o videos con contenido sexual de niñas, niños o adolescentes con fines comerciales a través del entorno digital. Esta forma de violencia digital puede presentarse como consecuencia del grooming, morphing o sexting.

Acciones integrales para su atención. Ante un caso de explotación sexual comercial infantil en el entorno digital el personal docente o primer respondiente, deberá proceder con extremo cuidado a escuchar a la niña, niño o adolescente afectado con la finalidad de recabar la información mínima necesaria (revisar análisis de contexto) para documentar los hechos. Durante la escucha deberá observarse en todo momento el lenguaje no verbal de la persona afectada y en su caso brindar los primeros auxilios psicológicos necesarios. Esta se limitará a documentar los medios digitales en los que se encuentren las imágenes o videos de contenido sexual y a recabar información de las posibles personas perpetradoras.

Deberán observarse los lineamientos generales establecidos por el presente **Protocolo** señalados en el apartado referente a “Escucha y recolección de testimonios”.

Con la información proporcionada durante la escucha, se elaborará una bitácora que deberá contener indefectiblemente la fecha, lugar y nombre de la persona responsable de su elaboración, el nombre domicilio e información de contacto de las personas menores de edad afectadas, los datos con los que se cuente de las personas señaladas como agresoras, así como los hechos narrados, precisando condiciones de tiempo, modo y lugar. Dicho documento deberá ser puesto en conocimiento de las autoridades directivas de la institución educativa quienes deberán reportarlo de manera inmediata al Servicio de Atención a Llamadas de Emergencia 911, la policía cibernética local o la

Guardia Nacional al número 088, dichas diligencias deberán hacerse constar en otra bitácora. Ambas bitácoras serán enviadas por correo institucional a la Procuraduría de Protección de Derechos de Niñas, Niños y Adolescentes local o en su defecto a la estatal o federal.

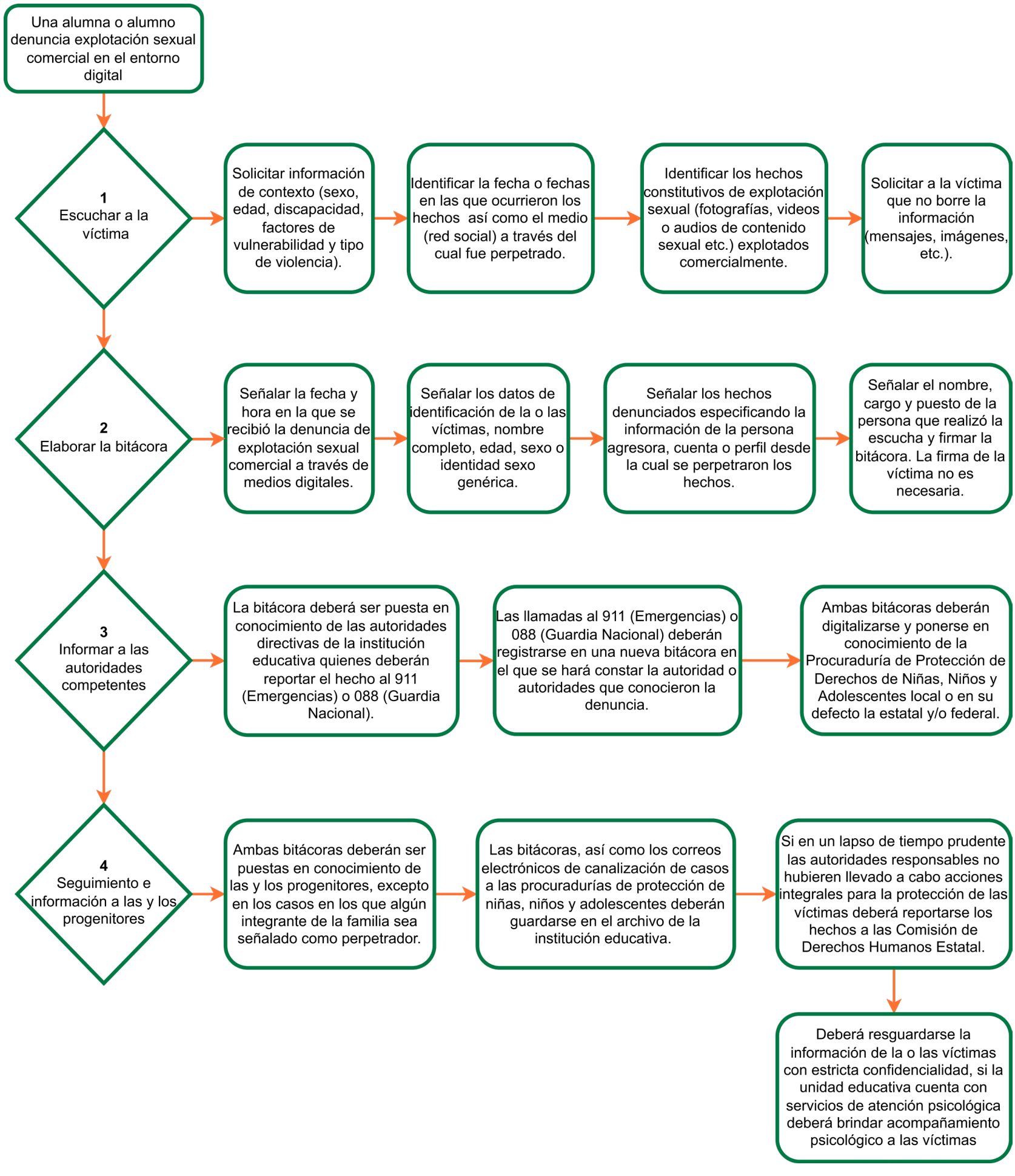
Deberá citarse a las personas responsables del cuidado de niñas, niños y adolescentes víctimas a objeto de que se les informe personalmente sobre el procedimiento llevado por la unidad educativa. Se les entregará una copia de las bitácoras elaboradas para su conocimiento, salvo en los casos en los que sean señalados como perpetradores. En caso de requerir mayor información de las y los afectados podrá llevarse a cabo una segunda escucha en presencia de su madre, padre tutor o cuidador. No es recomendable recabar capturas de pantalla de celulares o dispositivos como evidencia o prueba ya que esta labor será llevada a cabo a través de software especializado empleado por las autoridades de investigación. Si en un lapso prudente de tiempo no se tuviere noticias de las acciones de protección iniciadas por las autoridades de investigación deberá reportarse los hechos a la Comisión de Derechos Humanos estatal. Toda la documentación generada deberá permanecer en el archivo de la institución educativa.

Al ser una forma de violencia sexual digital deberá cuidarse en todo momento la confidencialidad de la información de las víctimas, así como los contenidos que se hubieran producido en el ejercicio de esta violencia. Es muy importante no compartir las imágenes y/o videos de contenido sexual a través de aplicaciones de mensajería como WhatsApp ya que dicha información podría filtrarse. En ese sentido, únicamente la autoridad pública responsable de la investigación estará facultada para capturar y obtener dicha información a través de los medios y métodos idóneos.

Es muy importante brindar acompañamiento psicológico a las personas víctimas, en caso de que la unidad educativa cuente con dicho servicio, deberá solicitarse la autorización de las personas a cargo del cuidado de las niñas, niños y adolescentes afectados para implementarlo.

En caso de que exista información de contenido sexual en páginas de internet deberá informarse inmediatamente a la Guardia Nacional y la Policía Cibernética para que procedan a eliminar dicho contenido lo antes posible.

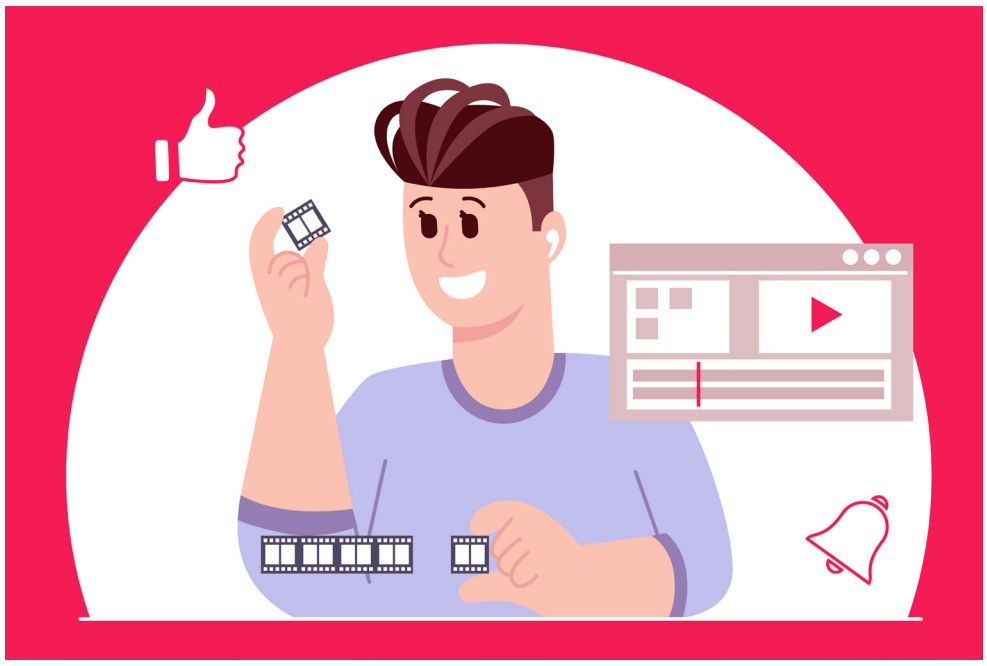
Flujograma 8
Proceso para la atención de casos de explotación sexual comercial en el entorno digital



Fuente: ChildFund México

9) Atención y documentación de casos de morphing.

Identificación. El **morphing** se da cuando a través de la edición de fotografías o videos reales de una niña, niño o adolescente se trasforma su contenido en uno nuevo potencialmente dañino para éstos. Incluye la producción de material sexual a partir de imágenes editadas tomadas de internet o redes sociales, donde se simula actos y voces de personas menores de edad.



Acciones integrales para su atención. Ante un caso de **morphing** el personal docente o primer respondiente, deberá escuchar a la niña, niño o adolescente afectado con la finalidad de recabar la información mínima necesaria (revisar análisis de contexto) para documentar los hechos. Durante la escucha deberá solicitarse información sobre las tecnologías (redes sociales, plataformas de mensajería, etc.) utilizadas para perpetrar la violencia denunciada, solicitando a las personas afectadas no borrar o eliminar los mensajes recibidos ya que constituyen el medio principal de prueba.

Deberán observarse los lineamientos generales establecidos por el presente **Protocolo** señalados en el apartado referente a “Escucha y recolección de testimonios”.

Con la información proporcionada durante la escucha, se elaborará una bitácora que deberá contener indefectiblemente la fecha, lugar y nombre de la persona responsable de su elaboración, el nombre domicilio e información de contacto de las personas menores de edad afectadas, así como los hechos narrados, precisando condiciones de tiempo, modo y lugar. Dicho documento deberá ser puesto en conocimiento de las autoridades directivas de la institución educativa quienes deberán reportarlo de

manera inmediata a la madre, padre, tutor o cuidador de la persona menor de edad afectada, así como de los responsables del cuidado de la niña, niño o adolescente señalado como persona agresora.

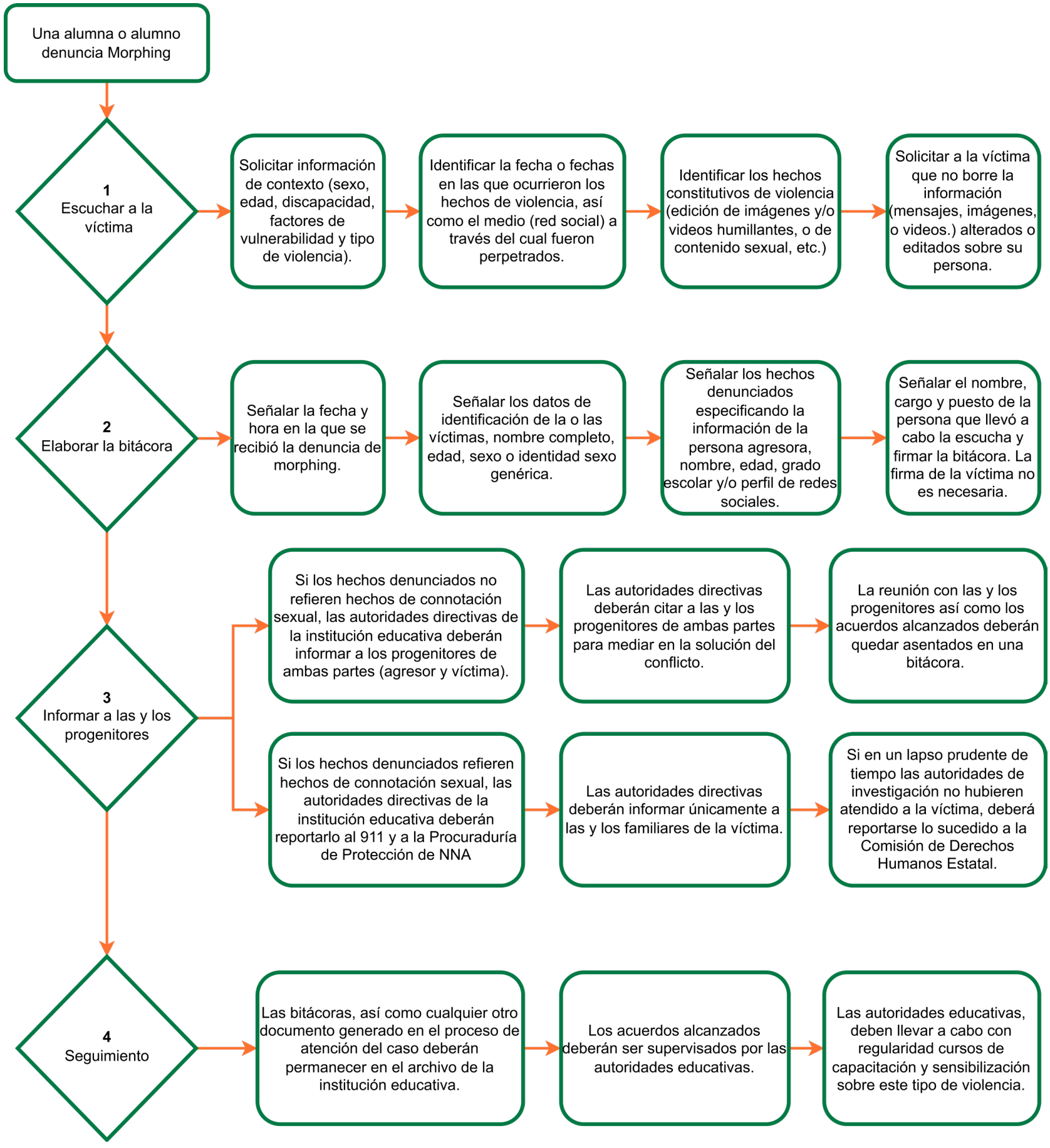
Deberá citarse a las personas responsables del cuidado de las partes involucradas (personas agresoras y personas víctimas) para que a través de pláticas de sensibilización se les informe sobre las formas en las que se perpetra este tipo de violencia y los riesgos para las personas afectadas. Se deberá emplear mecanismos de conciliación entre las partes a objeto de establecer mecanismos que garanticen la no repetición de los hechos denunciados. Es muy importante precisar que no deben emplearse mecanismos de sanción basados en castigos corporales o humillantes, ya que estos están prohibidos por la ley y constituyen formas de violencia que se deben erradicar, en su lugar es preferible emplear mecanismos de justicia restaurativa los cuales están encaminados a que las personas generadoras de violencia, con apoyo de un facilitador o facilitadora, reconozcan sus faltas, se responsabilicen de las consecuencias de sus actos y reparen los daños causados. Las reuniones o pláticas que las autoridades directivas realicen con las personas responsables del cuidado de ambas partes (víctima y agresor) deberán hacerse constar en bitácoras, señalando los acuerdos alcanzados.

Las bitácoras, así como cualquier otro documento generado durante el proceso de atención del caso deberá permanecer en el archivo de la institución educativa. Las autoridades educativas deberán dar seguimiento a los acuerdos alcanzados y a la no repetición de los hechos.

Las instituciones educativas que apliquen el presente Protocolo deberán llevar a cabo procesos de capacitación y sensibilización con las alumnas y alumnos sobre este tipo de violencia como mecanismo de prevención.

En el caso de que las fotografías o videos editados tengan connotación sexual, las autoridades directivas de la institución educativa deberán reportarlo de manera inmediata al Servicio de Atención a Llamadas de Emergencia 911, la policía cibernética local o la Guardia Nacional al número 088, dichas diligencias deberán hacerse constar en otra bitácora. Ambas bitácoras serán enviadas por correo institucional a la Procuraduría de Protección de Derechos de Niñas, Niños y Adolescentes local o en su defecto a la estatal o federal.

Flujograma 9
Proceso para la atención de casos de morphing



Fuente: ChildFund México

10) Atención y documentación de casos sobre violencia digital en videojuegos.

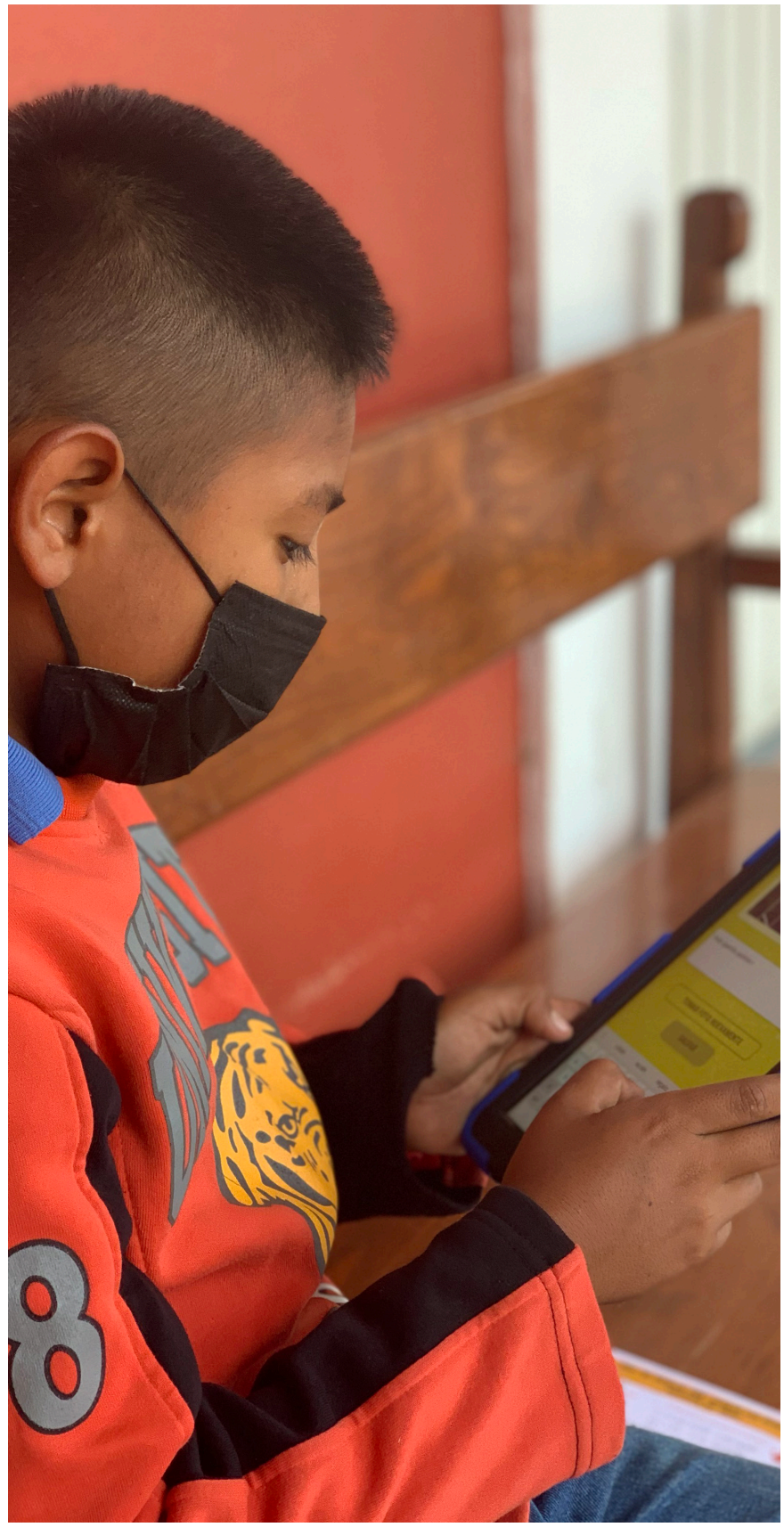
Identificación. Es una forma de violencia digital cometida en videojuegos utilizados por niñas, niños y adolescentes. Ocurre cuando en un videojuego, niñas, niños y adolescentes son violentados por otro jugador al margen de las reglas de programación del videojuego o cuando son contactados por personas adultas a través de los videojuegos con fines ilícitos.

Acciones integrales para su atención. Ante un caso de **violencia digital en videojuegos**, el personal docente o primer respondiente, deberá escuchar a la niña, niño o adolescente afectado con la finalidad de recabar la información mínima necesaria (revisar análisis de contexto) para documentar los hechos. Durante la escucha deberá solicitarse información sobre las tecnologías utilizadas para perpetrar la violencia denunciada (nombre del videojuego y perfil o nikname de las personas agresoras).

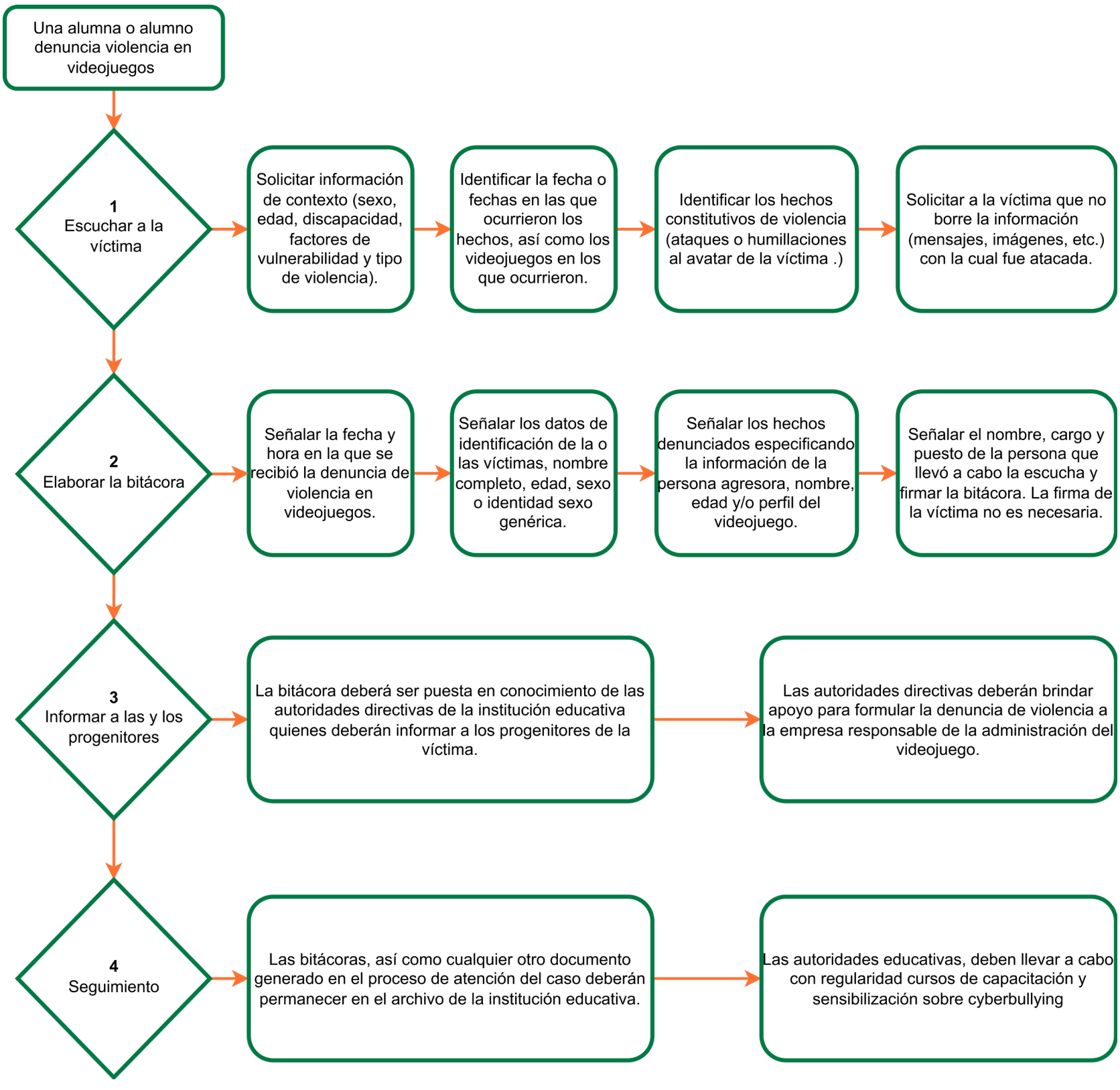
Deberán observarse los lineamientos generales establecidos por el presente **Protocolo**

señalados en el apartado referente a “Escucha y recolección de testimonios”.
Con la información proporcionada durante la escucha, deberá elaborarse una bitácora que deberá contener indefectiblemente la fecha, lugar y nombre de la persona responsable de su elaboración, el nombre, domicilio e información de contacto de las personas menores de edad afectadas, así como los hechos narrados, precisando condiciones de tiempo, modo y lugar. Deberá incluirse también el nombre del videojuego y sus características. Dicho documento deberá ser puesto en conocimiento de las autoridades directivas de la institución educativa quienes deberán reportarlo de manera inmediata a la madre, padre, tutor o cuidador de la persona menor de edad afectada.

Deberá citarse a las personas responsables del cuidado de niñas, niños y adolescentes víctimas a objeto de que se les informe personalmente sobre este tipo de violencia digital y los riesgos que presentan para niñas, niños y adolescentes. Así mismo deberá hacerse de su conocimiento que pueden levantar denuncias por correos electrónicos en el portal oficial del videojuego o compañía responsable de su programación.



Flujograma 10
Proceso para la atención de casos de violencia digital en videojuegos



Fuente: ChildFund México

VIII. CAJA DE HERRAMIENTAS

El presente **Protocolo** contiene diversos procedimientos para la prevención y atención de casos de violencia digital en contra de niñas, niños y adolescentes en escuelas de educación básica mexicanas, los cuales pueden llevarse a cabo con auxilio de las siguientes herramientas.

Cuadro 1
Configuración de control parental en navegadores de internet

Navegador	Liga de acceso
Google Chrome	https://support.google.com/families/answer/7087030?hl=es-419
Microsoft Edge	https://support.microsoft.com/es-es/microsoft-edge/m%C3%A1s-informaci%C3%B3n-sobre-el-modo-ni%C3%B1os-en-microsoft-edge-4bf0273c-1cbd-47a9-a8f3-895bc1f95bdd
Mozilla Fire Fox	https://support.mozilla.org/es/kb/bloquea-o-desbloquea-las-paginas-web-con-el-contro
Safari	https://www.avast.com/es-es/c-how-to-set-parental-controls-on-mac

Fuente: Elaboración propia

Cuadro 2
Configuración de control parental en consolas de videojuego

Consola	Liga de acceso
Nintendo Switch	https://www.nintendo.com/es-mx/switch/parental-controls/
Play Station 4	https://www.playstation.com/es-mx/support/account/ps4-parental-controls-and-spending-limits/
Xbox One	https://eloutput.com/videojuegos/guias/xbox-control-parental/
Steam	https://shorturl.at/ajpvF

Fuente: Elaboración propia

Cuadro 3
Configuración de control parental para sistemas operativos de teléfonos móviles

Sistema Operativo	Liga de acceso
Android	https://www.xataka.com/basics/control-parental-android-como-se-configura-que-otras-opciones-hay
IOS	https://support.apple.com/es-es/HT201304

Fuente: Elaboración propia

Cuadro 4
Manuales de Ciberseguridad en redes sociales y videojuegos

Red Social	Liga de acceso
Guía de TikTok para madres y padres	https://www.pantallasamigas.net/wp-content/uploads/2021/06/Guia-TikTok-Padres-Madres-PantallasAmigas.pdf
Guía de Roblox para madres y padres	https://www.videojuegosenfamilia.com/pdf/ROBLOX-guia-madres-y-padres.pdf
Guía de mediación parental para el disfrute saludable de videojuegos	https://www.videojuegosenfamilia.com/guia/Guia-Mediacion-Parental-Adiccion-Videojuegos-cs.pdf

Fuente: Elaboración propia

Cuadro 5
Plataforma de reporte de violencia sexual en línea “Te Protejo”

Reportes	Liga de acceso
Material de abuso sexual	https://www.teprotejomexico.org/report/mas
Explotación sexual	https://www.teprotejomexico.org/report/esc
Material de contenido sexual enviada por mensaje	https://www.teprotejomexico.org/report/os

Fuente: Elaboración propia

Cuadro 6
Directorio de Unidades de Policía Cibernética

Estado	Aguascalientes
Teléfono	4499102055
Extensión	6605, 1710, 1711
Correo electrónico	policia.cibernetica@aguascalientes.gob.mx
Estado	Baja California
Teléfono	6868373900
Extensión	13862
Correo electrónico	policiacibernetica@seguridadbc.gob.mx
Estado	Baja California Sur
Teléfono	6121750400
Extensión	1053
Correo electrónico	cibernetica@pgjebcs.gob.mx
Estado	Campeche
Teléfono	9818119106
Extensión	10052, 10053, 10054
Correo electrónico	cibernetica@pgjebcs.gob.mx
Estado	Chiapas
Teléfono	9616113958
Extensión	31200
Correo electrónico	cibernetica@sspc.chiapas.gob.mx

Estado	Chihuahua	
Teléfono	6144293300	
Extensión	10955; 23010	
Correo electrónico	ciberpolicia.sspe@chihuahua.gob.mx; delitos.electronicos@chihuahua.gob.mx	
Estado	Ciudad de México	
Teléfono	5552425100	5552426489
Extensión	5086	6489
Correo electrónico	policia.cibernetica@ssc.cdmx.gob.mx; ciberneticapdi@fgjcdmx.gob.mx	
Estado	Coahuila	
Teléfono	8444389800	8444380700
Extensión	7946	7579
Correo electrónico	policiaciberneticacoahuila@gmail.com; policiacibernetica.fge@coahuila.gob.mx	
Estado	Colima	
Teléfono	3123120301	
Extensión	227	
Correo electrónico	policiacibernetica@gobiernocolima.gob.mx	
Estado	Durango	
Teléfono	6182040400	6181373730
Extensión	49003	73618
Correo electrónico	udai@durango.gob.mx; unidad.cibernetica@durango.gob.mx	

Estado	Estado de México
Teléfono	7222758300
Extensión	10163
Correo electrónico	cibernetica.edomex@ssedomex.gob.mx
Estado	Guanajuato
Teléfono	4727485200
Extensión	19013
Correo electrónico	policiaciberneticafspe@guanajuato.gob.mx
Estado	Guerrero
Teléfono	7474719201
Extensión	10218
Correo electrónico	policiacibernetica@guerrero.gob.mx
Estado	Hidalgo
Teléfono	7717174796
Extensión	10461
Correo electrónico	ssph.cibernetica@hidalgo.gob.mx; policiaciberneticapgj@hidalgo.gob.mx
Estado	Michoacán
Teléfono	4433228100
Extensión	10211
Correo electrónico	policia.ciberneticassp@michoacan.gob.mx; delito.cibernetico@aic.fiscaliamichoacan.gob.mx

Estado	Morelos
Teléfono	7776047074
Extensión	N/A
Correo electrónico	unidadcibernetica@morelos.gob.mx
Estado	Nayarit
Teléfono	3113426703; 3111296000
Extensión	N/A
Correo electrónico	pcibernetica@nayarit.gob.mx; policiacibernetica@fiscaliageneral.nayarit.gob.mx
Estado	Nuevo León
Teléfono	8120332870
Extensión	3632
Correo electrónico	ciberpol.fc.ssp@nuevoleon.gob.mx
Estado	Oaxaca
Teléfono	9515015045
Extensión	32061, 32062, 32063
Correo electrónico	denunciacibernetica@sspo.gob.mx
Estado	Puebla
Teléfono	2222138150
Extensión	8136
Correo electrónico	ga.delitosciberneticos@puebla.gob.mx

Estado	Quintana Roo
Teléfono	9988817150
Extensión	2245
Correo electrónico	policiaciberneticaqroo@policiaquintanaroo.com.mx; coord.inteligencia.dgpdi@fgeqroo.gob.mx
Estado	San Luis Potosí
Teléfono	4442550103
Extensión	N/A
Correo electrónico	ciberprevencion@sspslp.gob.mx
Estado	Sinaloa
Teléfono	6677142833
Extensión	N/A
Correo electrónico	inteligenciapie@gmail.com
Estado	Sonora
Teléfono	6622594500
Extensión	13303
Correo electrónico	ciberssp@sonora.gob.mx
Estado	Tabasco
Teléfono	9933136550
Extensión	4264
Correo electrónico	denunciadi@fiscaliatabasco.gob.mx

Estado	Tamaulipas
Teléfono	8343186200
Extensión	16099
Correo electrónico	policiacibernetica.ssp@tamaulipas.gob.mx
Estado	Tlaxcala
Teléfono	2464652057
Extensión	N/A
Correo electrónico	policia.cibernetica@tlaxcala.gob.mx
Estado	Veracruz
Teléfono	2288418000
Extensión	10035
Correo electrónico	policiacientificapre@veracruz.gob.mx
Estado	Yucatán
Teléfono	9999303200
Extensión	49211
Correo electrónico	cibernetica.pei.ssp@yucatan.gob.mx; policia.cibernetica@yucatan.gob.mx
Estado	Zacatecas
Teléfono	4924914075
Extensión	N/A
Correo electrónico	cibernetica.ssp@zacatecas.gob.mx

Fuente: Secretaría de Seguridad y Protección Ciudadana, Ciberguía 2.0

Historias para la prevención de la violencia digital

Prevenir la violencia digital es tarea de todas y de todos por eso, te invitamos a conocer las siguientes historias sobre casos de violencia digital en contra de niñas, niños y adolescentes.

ChildFund México

Nudes en el foro

Diego tiene 15 años y es conocido en el mundo digital como MaquinaD_Fuego.

Hace *streams* por Twitch y le encanta jugar Fornite.

En una ocasión Diego conoció a XStarFire mientras jugaba y, al tener una buena partida, decidieron seguir jugando por más tiempo.

Diego y XStarFire pasaban mucho tiempo jugando, al punto de quedarse despiertos hasta las 3 de la mañana platicando en Discord.

XStarfire era muy dulce, pero algo penosa y por alguna razón que Diego no entendía, ella no le pasaba sus redes sociales.

Diego le dijo a XStarfire que si le pasaba sus redes sociales le regalaría algunas *skins*, por lo que ella accedió.

Dejaron de ser MaquinaD_Fuego y XStarFire y se presentaron como Diego y Sofi.

Las redes sociales de Sofi parecían muy extrañas, pues tenían muy pocos amigos y nada de fotos de ella.

Diego empezó a pedirle *nudes* a Sofi con la condición de seguirle regalando más *skins*.

Sofi lo hacía sin problemas, pero de repente ella también comenzó a pedirle *nudes*.

Pasaron algunas semanas y Diego se encontró con sus ***nudes*** dentro de un foro de Telegram, donde las ofrecían a la venta.

Diego le reclamó a Sofía, pues era la única persona a la que se las había enviado.

Ella le respondió que si no quería que se difundieran, él no debió enviarlas primero.

Diego sospechó que Sofi no era quien decía ser, pues ella le envió audios que sonaban con voz de persona adulta.

En los audios, ella lo culpaba por haberle enviado sus ***nudes***, y le dijo que solo las borraría, si él le depositaba dinero en una cuenta.

Diego no sabía qué hacer, y ante la vergüenza y los nervios, eliminó todas sus redes sociales, pero aún así sus ***nudes*** llegaron hasta sus amigos

Diego se sentía desesperado, al nivel de romper en llanto en plena escuela, pues se sentía utilizado, engañado y con mucha pena.

Su amiga Gaby lo vio sufriendo, así que lo abrazó y le recomendó no confrontar a Sofía nuevamente, le dijo que lo mejor era denunciarla.

Le recordó que hay personas adultas que por medio del engaño se ponen en contacto con niñas, niños o adolescentes...

...a través de alguna red social y así ganar su confianza para pedir fotos, videos o cualquier forma de exhibicionismo por gusto personal o con el interés de vender el material. Esta situación o fenómeno social lo denominan violencia sexual digital contra la niñez y adolescencia o ***grooming***.

Diego dudó en decirle a sus papás, por lo que prefirió contarle a su maestro. Él le aconsejó cambiar las contraseñas de sus redes sociales.

También que no borrara las conversaciones con Sofi porque estas iban a servir como evidencia. Su maestro lo orientó sobre cómo presentar una denuncia ante la policía cibernética.

La policía les comentó que si tenían dudas de qué hacer revisaran en Twitter y Facebook la campaña #InternetSeguroParaTodasYTodos y les recordó que su función es proteger a las niñas y los niños de la violencia sexual digital contra la niñez y adolescencia o ***grooming***.

TIPS ¿Qué hacer en casos de violencia sexual digital?

Si sospechas que eres víctima de grooming o violencia sexual digital te recomendamos lo siguiente:

1. Acércate a una persona adulta de confianza, puede ser tu mamá, papá, abuelitos, algún maestro o a quien tú prefieras.
2. Evita borrar conversaciones o cualquier material que más adelante pueda servir como pruebas (conversaciones, capturas de pantalla, vídeos, posibles fotos o capturas de pantallas del perfil de la persona acosadora, etc.)
3. Cambia las contraseñas y claves de seguridad de tus redes sociales.
4. Mantener un antivirus actualizado, con el fin de evitar que exista algún malware que pueda dañar la información recopilada.
5. Evita denunciar las redes sociales dentro de la misma plataforma, puesto que podría eliminar la cuenta y borrar información importante.
6. Puedes pedir orientación a la Procuraduría de Protección de Niñas, Niños y Adolescentes o al DIF más cercano a tu comunidad.

Recuerda que en el 088, te pueden apoyar.

ChildFund México

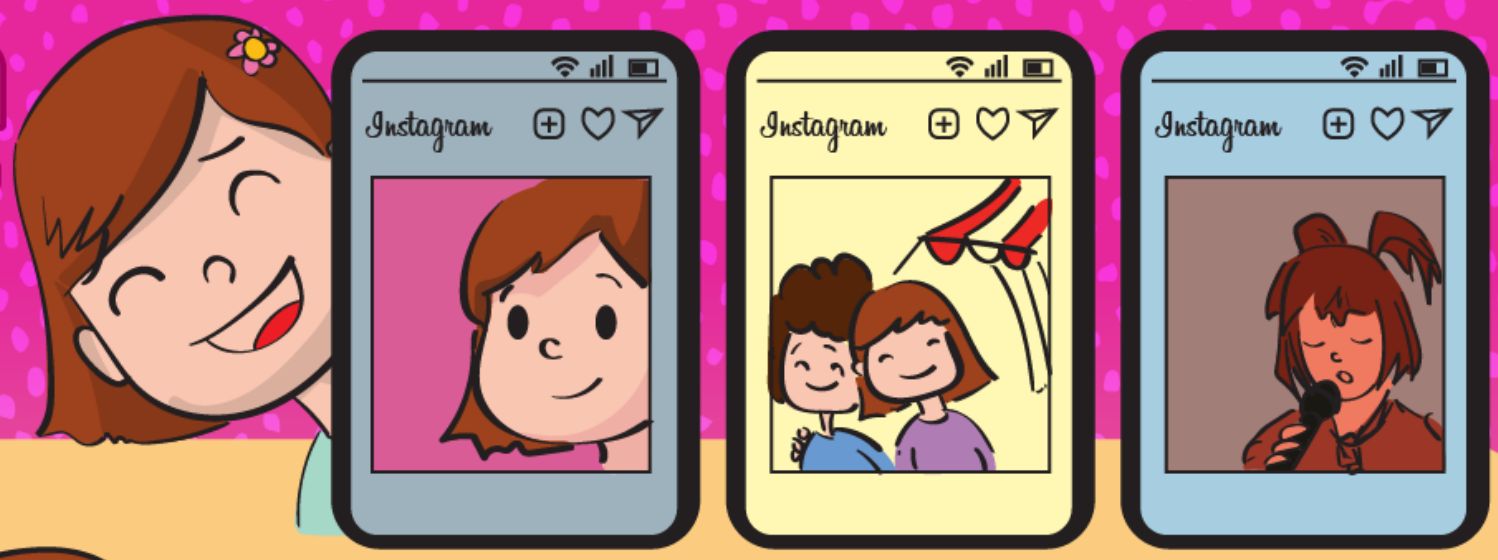
ChildFund México

En busca del amor

Ana es una chica de 14 años que cursa su primer año de secundaria.

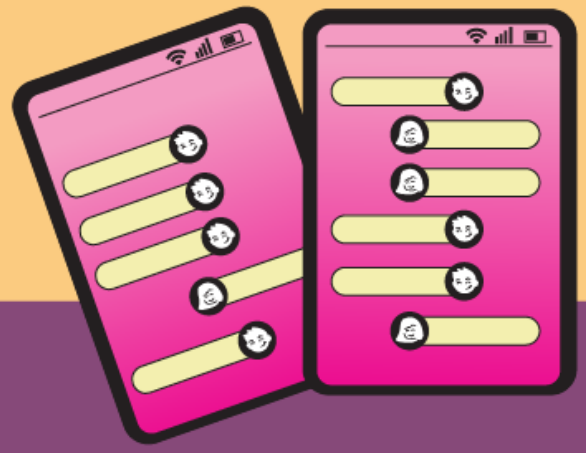
Es amante de la cultura Pop y las redes sociales.

Tiene una cuenta pública de Instagram donde sube fotos suyas, de sus amigas y también de sus ídolos.



Un día Ana recibió un mensaje de un desconocido. Este último resultó ser súper fan de la cultura pop, al igual que Ana.

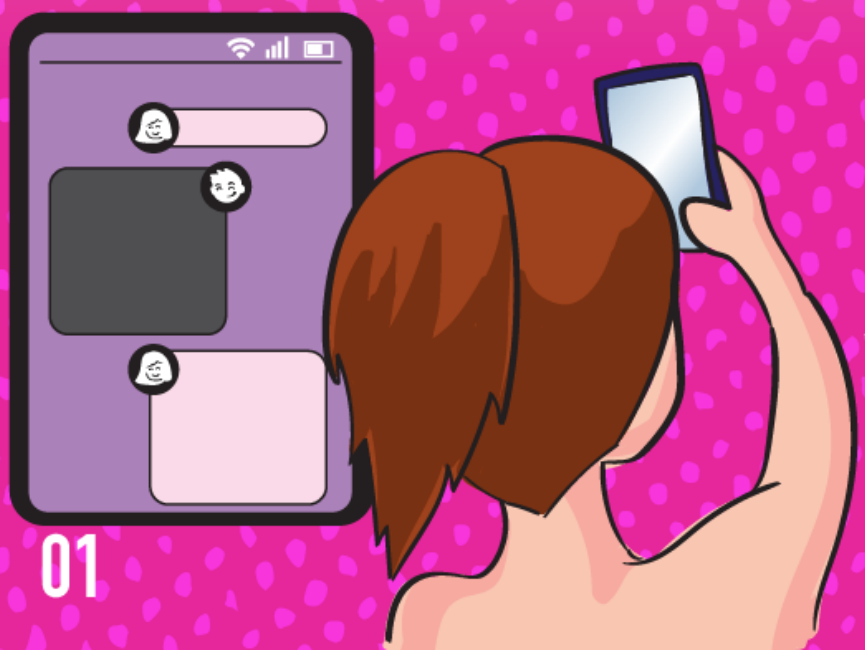
Con el paso de los días, Ana y #desconocido se hicieron muy buenos amigos.



A las semanas, Ana comenzó a sentir mariposas en la panza cada vez que le llegaba una notificación de #desconocido, pero él insistía en que aún no podían verse porque él vivía en otra ciudad.

02

Aún así, ambos quisieron tener una relación de noviazgo a distancia por lo que comenzaron a compartirse fotos, noticias y datos personales.
Poco a poco, #desconocido insistía en que ella le mandara nudes para demostrarle su amor.



01

Después de mucha insistencia, Ana accedió a demostrarle su "verdadero amor", enviándole fotografías de ella desnuda.

Ella no sabía si lo que hizo había estado bien, sin embargo, confió en #desconocido y en su amor.

Días más tarde #desconocido convenció a Ana de tener un encuentro para pasar el rato juntos, ya que él se encontraba en la ciudad. Ana estaba feliz porque al fin iba a conocer a su amor virtual en persona.

Llegó el día del encuentro y muy emocionada Ana acudió al lugar indicado, pero estando allí se percató que #desconocido era diferente a sus fotos, no parecía tener 15 años como le había dicho, sino que se trataba de una persona adulta.

DÍA

1

Ana se sorprendió mucho y de inmediato se dió cuenta de que #desconocido no era quien decía ser. En ese momento se asustó y decidió volver a su casa. En el camino, llamó a su mamá y le dijo que iba de regreso y le pidió que pasaran por ella.

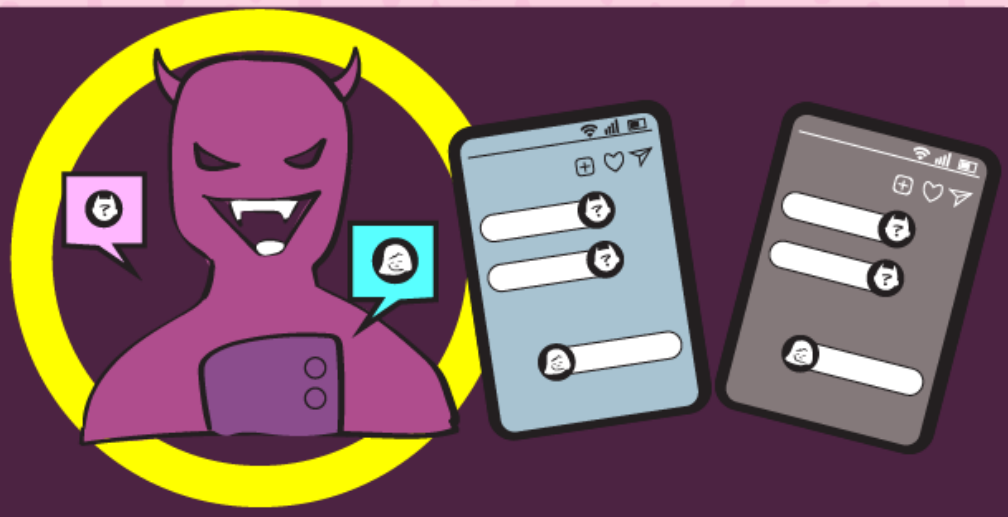
A Ana le dio pena hablar con su madre de lo que había pasado, así que solo le dijo que se había cancelado la cita con su amigo.

Sin embargo, al día siguiente recibió un mensaje de un nuevo usuario, era #desconocido diciéndole que si no cooperaba para verse de nuevo, publicaría sus fotos etiquetándola.

Ella sabía que eso era extorsión, pero no sabía qué hacer, ni a quién acudir, pensó que nadie le iba a creer y tenía miedo de decirle a sus padres.

Decidió acudir con la psicóloga de su escuela, quien le explicó que hay ocasiones en que existen personas adultas que por medio del engaño se ponen en contacto con una niña o niño, a través de redes sociales...

...y así ganar su confianza para pedir fotos, videos o cualquier forma de exhibicionismo por gusto personal o con ánimos de vender el material. Este tipo de situación es una forma de violencia sexual digital contra la niñez y adolescencia, en inglés es conocido como grooming.



La psicóloga se acercó a Ana, le dió un abrazo respetuoso y le dijo que no se preocupara, que no estaba sola y que podía contar con su ayuda...

También le comentó que la Guardia Nacional es la encargada de perseguir estos delitos, y si tenía dudas sobre qué hacer, podía revisar en Facebook la campaña #InternetSeguroParaTodasYTodos

De regreso a casa lo primero que hizo Ana, fue hablar del tema con sus padres, quienes le brindaron su apoyo y juntos decidieron denunciar a #desconocido.

Llamaron al 088 comunicándose con la Guardia Nacional. De igual manera se contactaron con ellos por redes sociales y correo electrónico para tener una respuesta más rápida.

La Guardia Nacional les recomendó:

- Evitar publicar datos personales en redes sociales abiertas
- Evitar aceptar solicitudes de amistad de desconocidos, de preferencia, mantener sus cuentas privadas.
- Si en algún momento se siente incómoda en la conversación lo mejor es no continuar.

ChildFund México

ChildFund® México

La trampa de los regalos a Mateo

En una comunidad de Guerrero, vivía junto a sus padres Mateo, quien era el menor de 8 hermanos.

Mateo es un adolescente que cursa segundo año de bachillerato y tiene 17 años. Debido a que sus papás trabajaban todo el día y sus hermanos habían migrado a otras ciudades por la situación económica, Mateo casi siempre se encontraba solo en casa.

Cuando Mateo concluyó su primer año de bachillerato, sus hermanos le enviaron un celular.

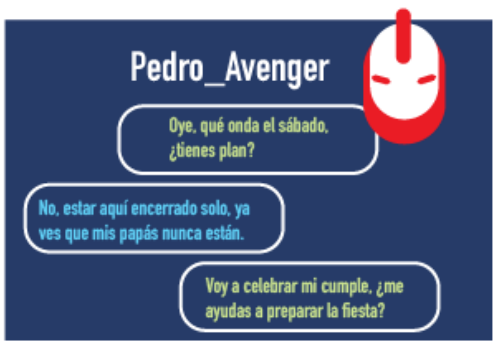
Era su dispositivo favorito y en Facebook ya tenía más de 1000 seguidores.

Como casi siempre estaba solo, sus papás no conocían el contenido que él visitaba o con quien se comunicaba a través de las redes sociales o los juegos en línea.

Un día recibió una solicitud de amistad de un #desconocido y aunque al inicio dudó en aceptarla, vio que tenían 3 amigos en común.

Cada vez más seguido se enviaban mensajes a través de la red social.

Mateo se sentía muy a gusto con las conversaciones, platicaban de todo y él sentía que era ya muy amigo de #desconocido, quien se hacía llamar Pedro_avenger.



El día que #Pedro_avenger iba a organizar su fiesta de cumpleaños, invitó a Mateo a que lo ayudara. Estaba felliz de que se iban a conocer.

Al llegar a casa de Pedro se sorprendió de que no era un adolescente como él, ya era mayor de edad, bastante más grande que Mateo.

Pedro lo trató muy bien, lo hizo sentir tranquilo y en casa; Mateo se sintió tan a gusto que decidió seguir viéndolo de manera frecuente.

Los papás de Mateo notaron que él tenía ropa nueva y algunos objetos como una tablet y un reloj, entre otras cosas.

Tímidamente lo cuestionaron sobre el origen de estos regalos, pero Mateo se limitaba a decir que Pedro se los había dado.

Cada vez, Mateo pasaba más tiempo en casa de Pedro y un día no volvió a casa.

Sus padres muy preocupados lo fueron a buscar e incluso dieron aviso en el Palacio Municipal.

Mateo regresó al siguiente día, pero solo dijo que había estado con Pedro, su amigo.

La promotora social de la comunidad aconsejó a los padres de Mateo sobre la importancia de denunciar, pero ellos tenían pena sobre lo que iban a decir las demás personas.

Ella les recodó que hay personas adultas que por medio del engaño se ponen en contacto con niñas, niños o adolescentes utilizando las redes sociales y creando falsos perfiles.

Dicho fenómeno social se conoce como violencia sexual digital contra la niñez o ***grooming*** que inicia con el contacto de una persona adulta a través de medios digitales para engañar y manipular a una niña, niño o adolescente y utilizarlo con fines sexuales.

Los papás de Mateo decidieron hablar con él y le comentaron lo que la promotora social les dijo sobre el ***grooming*** o violencia sexual digital contra la niñez.

Mateo no estaba seguro de lo que decían sus papás, pero saber que la promotora social de la comunidad había hablado con ellos lo hizo dudar de las verdaderas intenciones de Pedro.

Por tal razón, Mateo decidió dejar de contestarle a Pedro, pero este se enojó y comenzó a mandarle mensajes de forma muy insistente a través de las redes sociales.

Pedro amenazó a Mateo con compartir fotos donde estaban juntos si él no le respondía pronto los mensajes que le había enviado.

Mateo se sintió agobiado con los mensajes y la insistencia de Pedro, y después de pensarlo un poco, decidió contarle a sus papás, sabía que lo apoyarían, por la plática que habían tenido previamente.

Los papás de Mateo le hicieron sentir comprendido y amado y además lo acompañaron a realizar la denuncia con la policía municipal. Esta vez las cosas serían diferentes.

La policía les comentó que si tenían dudas de qué hacer deben revisar en Twitter y Facebook la campaña #InternetSeguroParaTodasYTodos y les recordó que su función es proteger a las niñas y los niños de la violencia sexual digital contra la niñez y adolescencia o ***grooming***.

TIPS ¿Qué hacer en casos de violencia sexual digital?

Si sospechas que eres víctima de grooming o violencia sexual digital te recomendamos lo siguiente:

1. Acércate a una persona adulta de confianza, puede ser tu mamá, papá, abuelitos, algún maestro o a quien tú prefieras.
2. Evita borrar conversaciones o cualquier material que más adelante pueda servir como pruebas (conversaciones, capturas de pantalla, vídeos, posibles fotos o capturas de pantallas del perfil de la persona acosadora, etc.)
3. Cambia las contraseñas y claves de seguridad de tus redes sociales.
4. Mantener un antivirus actualizado, con el fin de evitar que exista algún malware que pueda dañar la información recopilada.
5. Evita denunciar las redes sociales dentro de la misma plataforma, puesto que podría eliminar la cuenta y borrar información importante.
6. Puedes pedir orientación a la Procuraduría de Protección de Niñas, Niños y Adolescentes o al DIF más cercano a tu comunidad.

Recuerda que en el 088, te pueden apoyar.

ChildFund México

ChildFund México

Redes tóxicas

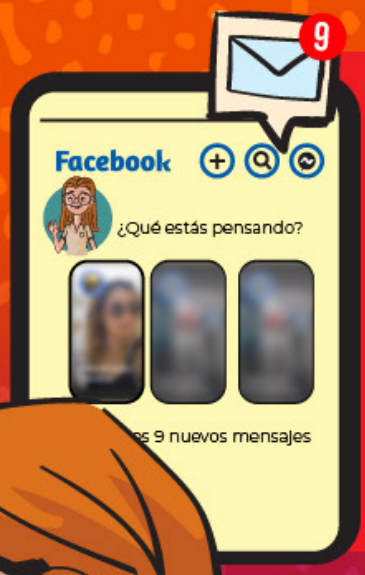
Tere tiene 15 años y está en su último año de secundaria.

Vive con su mamá, su abuela y sus hermanas. A su papá casi no lo ve, pues trabaja en otra ciudad.

Las amigas de Tere le contaron de las redes sociales, por lo que tuvo curiosidad y decidió abrir una cuenta de Facebook.

Empezó a subir fotos de sus actividades diarias. Tere se sentía emocionada de tener cada vez más amigos en su cuenta de Facebook.

Un día recibió una solicitud de amistad de un perfil sin foto y con un nombre extraño, pero decidió aceptarla al ver que tenían amigos en común.



Comenzaron a escribirse y Tere sentía confianza porque parecía que esta persona la conocía, ya que sabía el nombre de algunas de sus compañeras y compañeros de clase e incluso de algunos vecinos.

Pasaron algunas semanas de mensajes constantes hasta que las pláticas tomaron otro rumbo.

#Desconocido comenzaba a enviarle mensajes halagando su forma de vestir, sobre todo de una blusa rosa y un pantalón que Tere usaba.

Tere se sintió halagada, pero también sintió un poco de inseguridad. No imaginaba que #desconocido fuera tan cercano, pero todo parecía indicar que sí.

Un día Tere recibió un mensaje de #desconocido en donde le reclamaba que la había visto con Rogelio, un compañero de la escuela.

Tere sintió mucho miedo y ansiedad, sobre todo cuando #desconocido le dijo que ya no podía seguir hablando con Rogelio.

Ante el miedo que le provocó dicha situación, Tere decidió alejarse de #desconocido y lo bloqueó de su Facebook. Sin embargo, poco tiempo después empezó a recibir mensajes de otras cuentas con amenazas sobre hacerle daño a ella y a sus hermanas.

Tere no sabía qué hacer, por lo que decidió preguntarle a una maestra sobre qué era lo mejor. Su maestra tampoco contaba con la información necesaria y únicamente le sugirió que dejara de usar Facebook.

Después de pensarlo, Tere cerró su cuenta de Facebook, pero días después empezó a recibir amenazas por WhatsApp.

Su madre se dio cuenta de que Tere había cambiado, bajó sus calificaciones y ya no quería salir a la calle con sus amigos ni tampoco de su cuarto, por lo que decidió hablar con ella. Tere tuvo miedo de contarle a su mamá, pues se sentía culpable de lo que estaba pasando, por lo que se limitó a decirle que había estado muy cansada.

En una ocasión, mientras Tere se bañaba, su celular comenzó a sonar.

La madre de Tere lo revisó y vio los mensajes violentos y amenazantes que recibía.

Tere por fin habló con su mamá y confesó cómo se sentía y que no sabía qué hacer. Su mamá llamó al DIF municipal y ahí les brindaron orientación.

Les recomendaron una plática sobre riesgos en las redes sociales y las ayudaron a comunicarse con la Guardia Nacional; Tere y su mamá se sintieron escuchadas y acompañadas.

La policía les comentó que si tenían dudas de qué hacer revisaran en Twitter y Facebook la campaña #InternetSeguroParaTodasYTodos y les recordó que su función es proteger a a las niñas y los niños de la violencia sexual digital contra la niñez y adolescencia o ***grooming.***

TIPS ¿Qué hacer en casos de violencia sexual digital?

Si sospechas que eres víctima de grooming o violencia sexual digital te recomendamos lo siguiente:

1. Acércate a una persona adulta de confianza, puede ser tu mamá, papá, abuelitos, algún maestro o a quien tú prefieras.
2. Evita borrar conversaciones o cualquier material que más adelante pueda servir como pruebas (conversaciones, capturas de pantalla, vídeos, posibles fotos o capturas de pantallas del perfil de la persona acosadora, etc.)
3. Cambia las contraseñas y claves de seguridad de tus redes sociales.
4. Mantener un antivirus actualizado, con el fin de evitar que exista algún malware que pueda dañar la información recopilada.
5. Evita denunciar las redes sociales dentro de la misma plataforma, puesto que podría eliminar la cuenta y borrar información importante.
6. Puedes pedir orientación a la Procuraduría de Protección de Niñas, Niños y Adolescentes o al DIF más cercano a tu comunidad.

Recuerda que en el 088, te pueden apoyar.

ChildFund México

BIBLIOGRAFÍA CONSULTADA

A. Normas y resoluciones internacionales

CONDICIÓN JURÍDICA Y DERECHOS HUMANOS DEL NIÑO, Corte Interamericana de Derechos Humanos, Opinión Consultiva OC-17/2002 del 28 de agosto de 2002, Serie A núm. 17.

CONVENCIÓN INTERAMERICANA PARA PREVENIR, SANCIONAR, ERRADICAR LA VIOLENCIA CONTRA LA MUJER "CONVENCIÓN DE BELEM DO PARÁ", firmada por la Organización de Estados Americanos, 09 de junio de 1994.

CONVENCIÓN SOBRE LA ELIMINACIÓN DE TODAS LAS FORMAS DE DISCRIMINACIÓN CONTRA LA MUJER, adoptada y abierta a la firma y ratificación, o adhesión, por la Asamblea General de la Organización de Naciones Unidas en su Resolución 34/180, 18 de diciembre de 1979.

CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO, adoptada y abierta a la firma y ratificación por la Asamblea General de la Organización de Naciones Unidas en su Resolución 44/25, 20 de noviembre de 1989.

DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS, adoptada y proclamada por la Asamblea General de la Organización de Naciones Unidas en su Resolución 217 A (III), París, 10 de diciembre 1948.

EL DERECHO DEL NIÑO A NO SER OBJETO DE NINGUNA FORMA DE VIOLENCIA, Observación General 13, Comité de los derechos del Niño, CRC/C/GC/13, publicada el 18 de abril de 2011.

INFORME DE LA RELATORA ESPECIAL SOBRE LA VIOLENCIA CONTRA LA MUJER, SUS CAUSAS Y CONSECUENCIAS ACERCA DE LA VIOLENCIA EN LÍNEA CONTRA LAS MUJERES Y LAS NIÑAS DESDE LA PERSPECTIVA DE LOS DERECHOS HUMANOS, Consejo de Derechos Humanos de la Organización de Naciones Unidas, A/HRC/38/47, 18 de junio de 2018.

LOS DERECHOS DE LOS NIÑOS EN RELACIÓN CON EL ENTORNO DIGITAL, Observación General 25, Comité de los derechos del Niño, CRC/C/GC/25, publicada el 02 de marzo de 2021.

PROTOCOLO FACULTATIVO DE LA CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO RELATIVO A LA VENTA DE NIÑOS, LA PROSTITUCIÓN INFANTIL Y LA UTILIZACIÓN DE NIÑOS EN LA PORNOGRAFÍA, adoptado y abierto a la firma y ratificación por la Asamblea General de la Organización de Naciones Unidas en su Resolución 54/263, 14 de noviembre de 2000.

SOBRE EL DERECHO DEL NIÑO A QUE SU INTERÉS SUPERIOR SEA UNA CONSIDERACIÓN PRIMORDIAL, Observación General 14, Comité de los Derechos del Niño, CRC/C/GC/14, aprobada en su 62° periodo de sesiones, 2013.

SOBRE LAS PEORES FORMAS DE TRABAJO INFANTIL, Organización Internacional del Trabajo, Convenio 182, 1999.

B. Normas nacionales

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, publicada en el Diario Oficial de la Federación el 05 de febrero de 1917, última reforma publicada en el Diario Oficial de la Federación el 06 de junio de 2023.

LEY GENERAL DE LOS DERECHOS DE NIÑAS, NIÑOS Y ADOLESCENTES publicada en el Diario Oficial de la Federación el 04 de diciembre de 2014, última reforma publicada en el Diario Oficial de la Federación el 26 de mayo de 2023.

LEY GENERAL DE EDUCACIÓN, publicada en el Diario Oficial de la Federación el 04 de diciembre de 2014, última reforma publicada en el Diario Oficial de la Federación el 26 de mayo de 2023.

LEY GENERAL DE ACCESO DE LAS MUJERES A UNA VIDA LIBRE DE VIOLENCIA publicada en el Diario Oficial de la Federación el 01 de febrero de 2007, última reforma publicada en el Diario Oficial de la Federación el 08 de mayo de 2023.

C. Libros y artículos académicos

Comisión de Derechos Humanos de la Ciudad de México, Técnicas para la Realización de Entrevistas, 2012, disponible en: https://piensadh.cdhdf.org.mx/images/publicaciones/material_de_capacitacion/fase_de_formacion_especializada/2012_Tecnicas_para_la_realizacion_de_entrevistas.pdf

Gobierno de México, “Ciberguía 2.0”, Secretaría de Seguridad y Protección Ciudadana, Dirección General de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico, disponible en: https://www.gob.mx/sesnsp/documentos/ciberguia-2-0

Gobierno de México, Procuraduría Federal del Consumidor, “Grooming y Ciberacoso en niños”, artículo en línea, disponible en: https://www.gob.mx/profeco/es/articulos/grooming-y-ciberacoso-en-ninos?idiom=es

Gobierno de México, Secretaría de Comunicaciones y Transportes, “Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo” disponible en: https://www.gob.mx/cms/uploads/attachment/file/555226/Gui_a_de_Ciberseguridad_SCT_VF.pdf

Gobierno de México, Sistema Nacional de Protección de Niñas, Niños y Adolescentes, “Retos virales en redes sociales: evitar que este mal se propague entre niñas, niños y adolescentes”, artículo en línea, disponible en: https://www.gob.mx/sipinna/articulos/retos-virales-en-redes-sociales-evitar-que-este-mal-se-propague-entre-ninas-ninos-y-adolescentes

Pablo Corona, Asociación de Internet MX, ¿Qué es el ciberbullying?, artículo en línea, disponible en: https://www.gob.mx/ciberbullying/articulos/que-es-el-ciberbullying

Save The Children, “Violencia Viral: Análisis de la violencia contra la infancia y la adolescencia en el entorno digital”, España, 2019, disponible en: https://www.savethechildren.es/publicaciones/informe-violencia-viral-y-online-contra-la-infancia-y-la-adolescencia

UNESCO, “Cyber Violence Against Women and Girls: A World-wide Wake-up Call”, 2015, artículo en línea, disponible en: https://www.gob.mx/cms/uploads/attachment/file/144565/cyber_violence_gender_report.pdf

UNICEF, “Ciberseguridad, como protegerte en Internet”, artículo en línea, disponible en: https://www.unicef.org/mexico/ciberseguridad.

UNICEF, “Guía de Sensibilización sobre Convivencia Digital”, artículo en línea, Buenos Aires, 2017, disponible en: https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia_ConvivenciaDigital_ABRIL2017.pdf

UNICEF, “Niños, Niñas y Adolescentes en Línea: Riesgos de las Redes y Herramientas para protegerse” 2019, disponible en: https://ciberconscientes.com/wp-content/uploads/2019/12/TICs_en_ninos_y_ninas.pdf

ChildFund®
México