UN VIAJE SEGURO POR LA RED

Metodologías para prevenir los riesgos digitales y fortalecer el acceso a información segura

InfoPa'lante
ECUADOR

2024

UN VIAJE SEGURO POR LA RED

Metodologías para prevenir los riesgos digitales y fortalecer el acceso a información segura

Esta publicación fue posible gracias al trabajo conjunto entre *International Rescue Committee* (IRC, por sus siglas en ingles) y Fundación Alas de Colibrí (ACF) en el marco de implementación de la estrategia de protección InfoPa´lante Ecuador.

Fundación Alas de Colibrí, es una organización de la sociedad civil sin fines de lucro, creada mediante Acuerdo Ministerial 1142 cuyo fin es la promoción y defensa de los derechos humanos y la naturaleza, así como la restitución de los mismos, mediante la intervención de un equipo especializado e interdisciplinario, con enfoque de género, movilidad humana, intergeneracional, de discapacidades y étnico-cultural constituyéndose en un aporte para la construcción de una sociedad justa, equitativa, libre y solidaria.

InfoPa´lante Ecuador que se ejecuta con el apoyo de Fundación Alas de Colibrí, es parte de la iniciativa global denominada *SignPost* que facilitar el acceso a información segura y confiable de las personas migrantes, refugiadas y poblaciones locales para que conozcan sus derechos, accedan a información de servicio adecuados y encuentren alternativas de integración comunitaria. En Latinoamérica esta estrategia está presente en el Norte de Centro América, México, Colombia, Ecuador y Perú.

Fundación Alas de Colibrí (ACF)

Daniel Rueda, Presidente.

Revisión y edición:
Verónica Supliguicha Cárdenas, Coordinadora General de Proyectos.

Equipo técnico:
Jorge Ruíz, María Guamán, Nathaly Tapia.

Editado por: ACF

Metodología Un Cuento Para No Caer En Cuentos: Catherine Alayón

Primera edición: Año 2024

Quito, Ecuador

Financiado por la Unión Europea Ayuda Humanitaria

Presentación

"Un viaje seguro por la red", es un compendio de tres metodologías cuyo objetivo primordial es educar sobre los riesgos digitales, proveer recursos y herramientas para mitigar dichos riesgos y promover hábitos de navegación seguros. En la era digital actual, la seguridad en la navegación por Internet es clave para proteger la información personal de todos y todas; sin embargo, es importante comprender que niñas, niños y adolescentes son aquellos que se encuentran en situación de mayor vulnerabilidad.

"Un viaje seguro por la red", está dirigido a todos y todas quienes trabajen directamente con niños, niñas, adolescentes, personas en situación de vulnerabilidad, espacios comunitarios, organizaciones de base, grupos de jóvenes, mujeres y todos aquellos que tengan interés en mejorar el espacio digital que hoy, por hoy es un espacio de encuentro común.

La Fundación Alas de Colibrí (ACF), con el apoyo del *International Rescue Committee* (IRC), implementan desde el año 2022 la Estrategia de protección InfoPa'lante Ecuador, que proporciona un servicio de orientación e información segura y que busca promover y defender el acceso a servicios para mitigar los riesgos de vulneración de derechos de las personas. Esperamos que el presente documento sea una guía y un apoyo para el trabajo cotidiano de las organizaciones, instituciones, colectivos y personas que quieren hacer del espacio digital un lugar de intercambio, crecimiento, aprendizaje y resiliencia.

Equipo Fundación Alas de Colibrí

Contenido

Introducción

Las tecnologías de la información y comunicación (TIC) nos ofrecen una diversidad de posibilidades para observar el mundo. Los entornos virtuales facilitan la conexión con diversos lugares y la creación de relaciones interpersonales extensas, en la que podemos interactuar con personas de todo el mundo, nos brinda acceso a una amplia variedad de información desde el ámbito laboral y educativo hasta aspectos cotidianos como contratar y solicitar servicios, realizar compras y entretenernos, todo ello a través de dispositivos electrónicos. La interacción digital ha traído consigo numerosas ventajas en términos de comunicación y acceso a información, relaciones familiares, productividad, automatización y servicios.

Sin embargo, junto con estas ventajas, la evolución de la tecnología e Internet ha traído también riesgos digitales que afectan a la seguridad e integridad de las personas exponiéndolas a delitos en línea y amenazando su derecho al acceso información segura. Todas las personas están expuestas a estos riesgos, especialmente para niños, niñas y adolescentes, o personas en situación de vulnerabilidad (personas que están sin trabajo, personas en contexto de movilidad humana, con dificultades para generar vínculos sociales, etc.), quienes pueden enfrentarse a fallas de seguridad informática, contacto con acosadores, delincuentes, redes de trata de personas, extorsiones, divulgación de datos personales, violencia sexual y otros delitos poniendo en riesgo su bienestar físico, psicológico, social y emocional. Conocer y comprender estos riesgos

nos permite adoptar medidas de prevención y protegernos en el entorno digital a través del acceso a información segura.

"Un viaje seguro por la red", incluye tres guías metodológicas denominadas: "Cultura Digital", "Rompiendo el Silencio" y "Un Cuento para no caer en cuentos", cada una de ellas cuenta con un objetivo, se delimita a quienes puede ir dirigido el taller, un marco conceptual amigable que contiene breves recomendaciones y una propuesta de agenda de taller. Cada una de estas actividades tienen una secuencia lógica y se presenta como una guía que puede ser adaptada al contexto, al conocimiento del o la facilitadora. Incluyen también recursos legales y elementos de apoyo como videos, y notas de prensa que permitirán que quien se forma para implementar los talleres, cuente con claridad en la información que va a compartir.

Recorrer la red, puede ser un viaje seguro si partimos desde el conocimiento y si conocemos herramientas que faciliten este espacio de encuentro cada vez más presente en la actual era digital. Es responsabilidad de todos y todas, promover espacios digitales libres de violencia y seguros para niñas, niños y adolescentes.

Acrónimos

ACF	Fundación Alas de Colibrí
COIP	Código Orgánico Integral Penal
CRE	Constitución de la República del Ecuador
CONA	Código de la Niñez y Adolescencia
IRC	International Rescue Committe
IA	Inteligencia Artificial
NNA	Niñas, niños y adolescentes
ONU	Organización de Naciones Unidas
OMS	Organización Mundial de la Salud
TdP	Trata de Personas
TIC	Tecnologías de la información y la comunicación
UNICEF	Fondo de las Naciones Unidas para la Infancia (por sus siglas en inglés)
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
VBG	Violencia Basada en Género

UN VIAJE SEGURO POR LA RED

Un viaje seguro por la red, incorpora un marco conceptual amigable y una serie de actividades diseñadas para facilitar espacios de reflexión sobre los riesgos digitales, la violencia basada en género en el ciberespacio y la relación de los NNA con el mundo digital. El enfoque metodológico es comunitario, participativo y dialógico, promoviendo la integración social desde una perspectiva que facilita el intercambio de experiencias, conocimientos e información. A través de la identificación y reflexión sobre los riesgos en los entornos digitales, fomenta el intercambio de conocimientos, experiencias y fortalece las competencias de las personas en los entornos digitales de manera segura.

Estas metodologías están diseñadas para ser aplicadas por equipos técnicos, así como por otros actores organizacionales, interinstitucionales y comunitarios, ya que también permiten generar incidencia en la importancia del acceso a información segura.

Contiene tres metodologías:

- Pueden ser aplicadas de forma individual
- Se pueden adaptar a los contextos
- Incluyen recursos audiovisuales y legales
- Cuenta con actividades lúdicas que permiten que sea más cercana a la comunidad

Para que tu taller sea un éxito

Elige el tema

Paso 01

Revisa el objetivo del taller, y el público objetivo al que está dirigido. Si es lo que te interesa, avanza al siguiente paso.

Paso 02

Estudia el contenido teórico, familiarízate con los temas, revisa el material de apoyo. Recuerda que te harán preguntas y el conocimiento es tu mejor herramienta.

Paso 03

Revisa la agenda de taller propuesta, tómalo solamente como una guía, imprime tu creatividad, tu conocimiento, tu experiencia y ajústala.

Paso 04

Estás lista o listo para compartir la jornada de taller. Serán aproximadamente una hora y media de aprendizaje mutuo.
¡Disfruta el momento!

Capítulo I


Cultura
digital

Cultura Digital

1. Objetivo General

Desarrollar en las y los participantes, un sentido crítico para el uso de las TIC e implementar mecanismos de prevención y mitigación de los riesgos digitales.

2. Público Objetivo

- Niñas, niños y adolescentes
- Adultos/as de las comunidades
- Padres, madres y adultos responsables de NNA
- Profesionales en cualquier área
- Público en general que use la red

3. Principales definiciones

3.1 Datos de interés

Según el informe de *Data Reportal*[1] publicado en enero de 2024, Ecuador cuenta con 12,66 millones de perfiles activos en redes sociales, 15,29 millones de usuarios de Internet y 17,56 millones de conexiones móviles celulares activas. El 52,3% de usuarios de redes sociales son mujeres, mientras que el 47,7% son hombres.

Las plataformas sociales más utilizadas son *Facebook*, *YouTube*, *Instagram*, *TikTok*, y los canales de mensajería más utilizados son *WhatsApp*, *Messenger* y *Telegram*. Aunque la mayoría de estas plataformas tienen restricciones para usuarios menores de 13 años, los filtros de seguridad pueden ser fácilmente evadidos, lo que plantea desafíos y riesgos significativos, especialmente para NNA.

Lo que ocurre en internet tiene efectos y consecuencias reales entre lo virtual y lo presencial, tanto para NNA como las personas adultas inmersas en esta experiencia. Además, debemos considerar que las personas en situaciones de vulnerabilidad, como aquellos en contextos de emergencia, violencia, discriminación o extorsión, enfrentan mayores riesgos y amenazas en los entornos digitales.

Aunque cualquier persona puede enfrentarse a amenazas en línea, independientemente de su edad, los NNA son particularmente susceptibles a los riesgos digitales asociados con un uso inadecuado de la tecnología, por el desconocimiento, y falta de control parental o de adultos. Por estos motivos, la protección de NNA en internet se ha convertido en un desafío crítico.

Además, en los contextos de vulnerabilidad, las NNA son particularmente propensos a los riesgos digitales debido a la falta de información y precaución al usar la tecnología. Esto los expone a amenazas de acoso en línea, exposición a contenido perjudicial y violencia sexual digital. Todo esto tiene un impacto negativo en su desarrollo emocional, psicológico y social porque causa

---

1 DATA REPORTAL. (enero 2024). Digital 2024: Ecuador. https://datareportal.com/

ansiedad, depresión, problemas de autoestima y dificultades en sus relaciones interpersonales[2].

Para dar una respuesta a la necesidad de fortalecer la prevención de los riesgos digitales, se ha desarrollado el taller **Cultura Digital**, con el propósito de proporcionar conceptos y recursos para prevenir y actuar ante los principales riesgos digitales actuales.

3.2 Conceptos generales

La cultura digital es la manera en que las personas acceden, utilizan e interpretan la información y las herramientas digitales, engloba prácticas, valores, actitudes y conocimientos relacionados con el uso e integración de tecnologías digitales en la sociedad. Esto abarca desde la forma en que nos relacionamos con la información, la comunicación, el entretenimiento y el trabajo, hasta otros aspectos de la vida cotidiana a través de dispositivos y plataformas digitales en línea. Es decir, son creencias, hábitos y conductas desde el uso básico de herramientas digitales hasta la participación activa en comunidades en línea, la creación de contenido digital, la privacidad en línea y la ética digital. La cultura digital es esencial en la actualidad.[3]

Nuestras acciones en línea, los sitios que visitamos, la información que compartimos y publicamos dejan una "huella digital"[4] y nos exponen a riesgos como el robo de información y la violencia digital. Por ello, fomentar una cultura digital responsable en el uso de dispositivos y en la gestión de la información que consumimos y compartimos es fundamental para protegernos en los entornos digitales, prevenir riesgos y posibles delitos digitales.

Tomar acción para promover una cultura digital positiva es indispensable y una responsabilidad compartida por todos los sectores de la sociedad que están comprometidos en la protección y seguridad de las personas en los entornos digitales, así como en el fortalecimiento de una comunicación y acceso a información segura, confiable, coherente y auténtica.

---

2 UNICEF. (2017). Niños en un mundo digital.

3 MDPI. (2020). Cultura y Sociedad en la Era Digital.

4 Faro Digital. (2022). La huella digital está compuesta por los rastros que se dejan en Internet, de las publicaciones, comentarios, fotos, etiquetas, videos, likes y también de las publicaciones, etiquetas, fotos o videos que pertenecen a otras personas y se asocian a nuestro nombre y/o rostro.

El uso responsable del Internet y las redes sociales implica utilizarlas de manera ética y consciente. Esto implica aprender a considerar el impacto de nuestras acciones en nosotros mismos y en los demás, evitar la difusión de información falsa, respetar los derechos y la dignidad de las personas y mantener un equilibrio saludable entre el tiempo en línea y fuera de línea.

3.3 Nuestros derechos digitales

El acceso a la información es un derecho fundamental que facilita la participación de todas las personas y permite el ejercicio de otros derechos. Por este motivo, es crucial que la conectividad a Internet y los entornos de redes sociales proporcionen recursos para proteger nuestra seguridad y dignidad, permitiéndonos ejercer plenamente nuestra "Ciudadanía digital".[5]

El numeral 2 del artículo 16 de la Constitución de la República del Ecuador (CRE) , garantiza el acceso universal a las TIC. Asimismo, **el artículo 18** de la citada ley establece que todas las personas, tanto individual como colectivamente, tienen derecho a buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa sobre hechos, acontecimientos y procesos de interés general, con responsabilidad ulterior.

En los entornos digitales, estos derechos implican que las personas los ejerzan con libertad y protección. Esto incluye el acceso a información verificada, el intercambio de información y la pluralidad informativa. También abarca aspectos fundamentales como la inclusión y educación digital, la privacidad, la protección física, emocional y sexual, el derecho al acceso a internet, la desconexión digital y la protección de datos personales.

Por otro lado, el derecho a la información en NNA se encuentra garantizado en el art. 45 del CONA[6], los cuales, pueden buscar y escoger información utilizando los diferentes medios y fuentes de comunicación con las limitaciones establecidas en la ley, el art. 46 de mismo cuerpo legal establece limitaciones relativas al derecho a la información, como la prohibición de circular y publicaciones videos y grabaciones que contengan

5 UNESCO. (2024) Ciudadanía digital es el ejercicio de la ciudadanía en entornos digitales. Incluye una serie de competencias que permiten a las personas acceder, recuperar, comprender, evaluar, utilizar, crear y compartir información y contenidos.

6 CONA, Código Orgánico de la Niñez y Adolescencia.

imágenes, textos, o mensajes inadecuados para su desarrollo.

En relación a la protección de NNA en los entornos digitales, el artículo 44 de la CRE establece que el Estado, la sociedad y la familia, deben promover el desarrollo integral de NNA, garantizando el ejercicio pleno de sus derechos. Por otro lado, el artículo 23 de la Ley Orgánica de Protección de Datos Personales, enfatiza el derecho a la educación digital, garantizando el acceso al conocimiento relacionado con el uso adecuado y seguro de las tecnologías de la información y comunicación, incluyendo a las personas con necesidades educativas especiales.

Dentro de este marco normativo, el derecho a la educación digital promueve el uso adecuado, sano, constructivo, seguro y responsable de las tecnologías de la información y comunicación, con apego a la dignidad e integridad humana; los derechos fundamentaleS y libertades individuales, enfatizando la intimidad, la vida privada, la autodeterminación informativa, la identidad y la reputación en línea, la ciudadanía digital y el derecho a la protección de datos personales.[7]

La normativa analizada resalta la importancia de promoción de la protección de la información personal, la confidencialidad, el consentimiento en la divulgación de información, el acceso a información personal, el derecho a la educación digital, el derecho a la rectificación y a la eliminación de información.

7 *Internet Segura. (2020). Ecuador.* https://internetsegura.gob.ec/

3.4 Principales riesgos digitales

a. Desinformación

La desinformación es una causa y un obstáculo en los entornos digitales, ya que impide la toma de decisiones informadas y aumen ta la exposición a riesgos digitales, como ataques a la integridad personal a través de acoso, extorsiones, violencia sexual digital, y promueve comportamientos inadecuados en el uso de las tecnologías de información y comunicación.

La desinformación es un riesgo digital global con efectos significativos en nuestra seguridad, economía y salud mental. Este fenómeno puede surgir de errores, rumores, o la falta de fuentes confiables de información. **La manipulación de la información contribuye a distorsionar la realidad y dificulta la toma de decisiones especialmente en situaciones de emergencia y crisis.**[8]

Sus consecuencias son diversas y graves, incluyendo la toma de malas elecciones, la pérdida de confianza, daños económicos, impactos en la salud pública, polarización social, entre otros. Además, la desinformación da lugar a discursos de odio[9] y permite la propagación de información falsa, lo cual se ve agravado por la falta de filtros de veracidad y prevención.

Desde una perspectiva más amplia, la desinformación puede alcanzar la dimensión de Infodemia[10]. El término "infodemia" describe la saturación de información y la rápida propagación en las redes sociales, tanto verdadera como falsa, que dificulta su procesamiento y análisis, generando problemas como la "infoxicación"[11], que afecta la salud mental de las personas, esta afectación es mucho más grave en NNA, dado que por su edad son más propensos a ser impactados negativamente.

Combatir la desinformación es un elemento indispensable para prevenir riesgos digitales y a contribuir a la integridad y la seguridad de las personas.

---

8 APA. (2021). Controlando la propagación de la desinformación.

9 ONU. Hace referencia a un discurso ofensivo dirigido a un grupo o individuo y que se basa en características inherentes (como son la raza, la religión o el género) y que puede poner en peligro la paz social.

10 OMS. Término definido para advertir sobre la práctica de difundir noticias falsas sobre la pandemia del COVID-19 que provocó un aumentó en el pánico social.

11 Alfons Cornellá. Institute of the Next.

MEDIDAS DE PREVENCIÓN	MEDIDAS DE ACTUACIÓN
1. Identifica las fuentes de información oficiales y canales confiables.	1. Busca fuentes oficiales cuando tengas dudas y compara el contenido con otros medios para asegurarte de su veracidad.
2. Verifica la fecha de publicación de la noticia para asegurar que la información está vigente.	2. Ten cuidado con las noticias falsas o "*Fake News*" que suelen tener enlaces con virus o "*Malware*".
3. Cuestiona la información y reflexiona sobre su intención y veracidad.	3. Comprueba que la información publicada esté respaldada por fuentes confiables, cifras y datos verificables.
4. Respeta el derecho a la privacidad de las personas y no compartas información sin consentimiento.	4. Protege tu privacidad evitando compartir información personal y evitando ingresar tus datos en sitios *web*.
5. Participa de manera responsable y respetuosa en conversaciones en redes sociales y grupos de mensajería instantánea.	5. Notifica y reporta noticias falsas en las redes sociales. Los medios de información suelen tener mecanismos de retroalimentación para este fin.

b. Riesgos de fraude cibernético

Los riesgos de seguridad informática y fraude cibernético son cada vez más comunes debido al crecimiento del uso de redes sociales, acceso a páginas *web*, videojuegos y aplicaciones de mensajería instantánea. Estos riesgos pueden llevar a la filtración de información personal y bancaria, la pérdida de datos, la suplantación de identidad y el contacto con ciberacosadores y delincuentes.

Es necesario tener consciencia que, la falta de cuidado al abrir enlaces desconocidos, sospechosos y no verificados puede comprometer nuestra privacidad, seguridad e información personal ante la piratería de información o "*hacking*". Los ciberdelincuentes utilizan diversas técnicas para cometer fraude o delitos cibernéticos, como virus[12] troyanos, *ransomware, spyware y phishing*[13], para atacar y obtener información confidencial de personas y organizaciones.

¿CÓMO SE LLAMA?	¿QUÉ ES?
Hacking	Se define como piratería informática y se refiere al acto de acceder de manera no autorizada a un sistema informático o a una red, ya sea para obtener información, alterarla o causar daños.
Virus Troyanos	Es un tipo de "*malware*"[14] capaz de alojarse en una computadora u otro dispositivo electrónico para captar información y transmitirla a usuarios ajenos.
Ransomware	Se distingue de otros ciberataques en que su objetivo es restringir el acceso al sistema del ordenador que infecta, es decir, secuestrar el dispositivo exigiendo un pago a su propietario por eliminar el bloqueo.
Spyware	Es un tipo de "*malware*" que intenta mantenerse oculto mientras registra información en secreto y sigue las actividades en línea del usuario.
Phishing	Los ataques de phishing son correos electrónicos fraudulentos, mensajes de texto, llamadas telefónicas o sitios web diseñados para engañar a las y los usuarios para descargar *malware*, compartir información confidencial, datos personales u otras acciones que expongan a sus organizaciones.[15]

12 NORTON. (2018). Un virus informático, al igual que un virus de la gripe, está diseñado para propagarse de un host a otro y tiene la habilidad de replicarse.
13 Taller de Comunicación Mujer (TCM). (2021). Moverse seguras y seguros.
14 Malwarebytes. Malware o "software malicioso" es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.
15 IBM. ¿Qué es el phishing?

El “*phishing*”, además, busca establecer contactos con personas desconocidas a través de canales de mensajería instantánea o de citas en línea. Esta intromisión y sus consecuencias posteriores pueden causar daños económicos, robo de identidad y acoso cibernético, tanto en entornos virtuales como en situaciones presenciales. Es crucial estar alerta y tomar medidas para protegerse contra estos riesgos a fraudes cibernéticos, como parte del proceso de educación digital a niñas, niños y adolescentes es entregarles información de acuerdo a su edad sobre estos riesgos y cómo prevenirlos.

Recursos Legales: COIP

Art. 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tratamiento de información, dispositivos electrónico o infraestructura tecnológica con el propósito de obstaculizar de forma grave, deliberada e ilegítimas el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

MEDIDAS DE PREVENCIÓN	MEDIDAS DE ACTUACIÓN
1. Cambia las claves constantemente en tus perfiles sociales, servicios y tus aplicaciones. Utiliza autenticación de dos factores (2FA)[16] siempre que sea posible para agregar una seguridad adicional..	1. Es IMPORTANTE no dejar tus redes sociales abiertas en equipos de uso público y evitar abrir perfiles en dispositivos que no sean personales.
2. Mantén actualizados tus sistemas operativos, aplicaciones y programas antivirus para proteger tus dispositivos.	2. No ingreses tus datos ni compartas información de perfiles sociales con sitios web desconocidos o sospechosos.
3. Sé cauteloso al descargar archivos adjuntos o hacer clic en enlaces en correos electrónicos, mensajes de texto o redes sociales.	3. Notifica y reporta mensajes inadecuados o sospechosos de spam[17]. Es importante cuidarse de enlaces que ofrecen beneficios, productos o servicios gratis. Verifica la información y la fuente antes de compartir o hacer clic en dichos enlaces.
4. Realiza copias de seguridad periódicas de tus datos importantes en una ubicación segura para evitar la pérdida de datos en caso de un ataque cibernético.	4. Protege tu privacidad configurando el acceso y publicaciones en redes sociales. Es recomendable no publicar todo lo que haces porque esta información puede ser utilizada por personas malintencionadas.
5. Prepárate para identificar señales de phishing, como correos electrónicos o mensajes que solicitan información personal o financiera, y evita proporcionar datos a menos que tengas seguridad del remitente.	5. Revisa periódicamente quién puede ver tu información, publicaciones y fotos, y ajusta la configuración según tus preferencias de privacidad. Ten cautela al aceptar solicitudes de amistad o seguir perfiles desconocidos.
6. Conversa con familiares y amigos sobre prácticas seguras en línea para que también puedan protegerse contra fraudes y riesgos cibernéticos.	

16 Microsoft. (2FA) significa autenticación en dos fases, método de seguridad de administración de identidad y acceso que requiere dos formas de identificación para acceder a los recursos y los datos.

17 ESET. Correo electrónico no solicitado.

c. *Ciberbullying/ Acoso escolar en línea*

El ciberacoso escolar, también conocido como "*Ciberbullying*", es una forma de violencia que se lleva a cabo de manera constante y repetitiva contra NNA con el objetivo principal de intimidarlos, humillarlos o someterlos. Este tipo de violencia suele prolongarse en el tiempo y ocurre tanto en el mundo físico como en el digital.

En muchos casos, el acosador es alguien del entorno cercano de la víctima, como compañeros de clase, jóvenes o adultos conocidos. Actualmente, las redes sociales y otras plataformas en línea son las principales herramientas utilizadas para el "*Ciberbullying*".

Esta forma de violencia, se manifiesta de diversas maneras, como la persecución y acercamiento constante a la víctima, intentos de contacto no deseados, uso indebido de sus datos personales, difusión de información privada sin consentimiento o ataques contra su integridad. Así también lo que comienza como ciberacoso o *ciberbullying* se traslada, con frecuencia, a un acoso en la vida real.[18]

Este problema afecta a NNA, quienes son objeto de insultos, burlas, hostigamiento, ofensas, publicaciones humillantes y mensajes discriminatorios, principalmente a través de aplicaciones en las que participan: videojuegos, *WhatsApp, Instagram, Facebook, TikTok, Messenger* y otras plataformas similares.

18 *Save The Children. Ciberacoso o Ciberbullying.* https://www.savethechildren.es

MEDIDAS DE PREVENCIÓN	MEDIDAS DE ACTUACIÓN
1. Ante todo, es importante sensibilizar a padres, madres y cuidadores sobre la importancia de brindar apoyo en situaciones de acoso.	1. Responder frente al acoso escolar y el *ciberbullying* requiere la participación activa y apoyo de adultos responsables.
2. Educa a las niñas, niños y adolescentes en valores como la tolerancia, el respeto y la igualdad. Esto les ayudará a comprender la importancia de abordar el acoso con respeto y empatía, y a reconocer situaciones de *Ciberbullying*.	2. Si se detecta un caso de acoso o *ciberbullying*, se debe actuar de inmediato trabajando en colaboración con la institución educativa y los entornos pertinentes para abordar el problema y realizar un seguimiento.
3. Fomenta una comunicación abierta y honesta. Es importante crear un ambiente en el que niñas, niños y adolescentes sientan seguridad para hablar sobre sus experiencias, incluyendo posibles situaciones de acoso escolar.	3. Promueve el diálogo abierto y positivo con los NNA. Es necesario no juzgar o "culpabilizar" por la situación de acoso. 4. Si un niño, niña o adolescente es víctima de *ciberbullying*, es importante recopilar evidencia como capturas de pantalla de mensajes insultantes para respaldar una denuncia y acciones de protección.
4. Reitera a niñas, niños y adolescentes, que ante una situación de *ciberbullying* y acoso escolar, es importante mantener la calma y buscar soluciones constructivas junto con personas de confianza.	5. Es fundamental, brindar apoyo emocional, hablar sobre la importancia de bloquear a los agresores en las redes sociales y abandonar grupos donde se produzcan los ataques.

Recursos Legales: COIP

Art. 154.3.- Contravenciones de acoso escolar y académico

1. Acoso académico: Se entiende por acoso académico a toda conducta negativa, intencional, metódica y sistemática de agresión, intimidación, ridiculización, difamación, coacción, aislamiento deliberado, amenaza, incitación a la violencia, hostigamiento o cualquier forma de maltrato psicológico, verbal, físico que, de forma directa o indirecta, dentro o fuera del establecimiento educativo, se dé por parte de un docente, autoridad o con quienes la víctima o víctimas mantiene una relación de poder asimétrica que, en forma individual o colectiva, atenten en contra de una o varias personas, por cualquier medio incluyendo a través de las tecnologías de la información y comunicación.

Esta contravención será sancionada con una o más de las medidas no privativas de libertad previstas en los números 1, 2, 3 y 6 del artículo 60 de este Código, y además el juzgador impondrá las medidas de reparación integral que correspondan según el caso.

2. Acoso escolar entre pares: Cuando las mismas conductas descritas en el párrafo anterior se produzcan entre estudiantes niñas, niños y adolescentes, se aplicarán las medidas socioeducativas no privativas de libertad correspondientes y el tratamiento especializado reconocido en la ley de la materia, garantizando los derechos y protección especial de niñas, niños y adolescentes.

Art. 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos. - La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años.

Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años.

La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años.

d. Grooming - Acoso sexual infantil en medios digitales

La palabra "*grooming*" viene del verbo inglés "*groom*", que se refiere a conductas de "acercamiento o preparación para un fin determinado"[19]. Es una acción deliberada e intencionada realizada por una persona adulta para acosar sexualmente a un niño, niña o adolescente a través de medios digitales.[20] Los ciberacosadores o "*groomers*", se acercan a sus víctimas para establecer lazos de amistad y complicidad, manteniendo un contacto que puede prolongarse en el tiempo. En estas interacciones, buscan obtener imágenes, videos o contenido de carácter erótico o sexual e incluso buscan llegar a mantener

19 INFOBAE. (2019). Qué es el grooming, cómo reconocerlo y qué pasos hay que tomar para denunciarlo.
20 Faro Digital. (2022). Guía de acompañamiento de adolescencias en entornos digitales.

encuentro personal.

Para prevenir el *grooming*, es fundamental conocer y saber identificar todos los riesgos y peligros que enfrentan niñas, niños y adolescentes al usar la tecnología, así como saber cómo actuar si alguna vez ocurre.

En este contexto, es necesario comprender que las NNA, debido a su edad, falta de información y contextos de vulnerabilidad, son sensibles a la falta de privacidad y seguridad en las nuevas tecnologías, lo que les pone en riesgo es esta forma de violencia y acoso sexual, que implica el engaño realizado por pedófilos,[21] pederastas[22] y redes de trata. Usualmente, el contacto con NNA por parte de adultos se da a través de identidades falsas, juegos en línea y mensajería instantánea.

De acuerdo al informe sobre 'Violencia viral' de *Save the Children* (2019), el 21,45% de NNA encuestados han sufrido grooming durante su infancia, y el 15% más de una vez. También se concluye que normalmente la persona que intenta el abuso es desconocida en un 49,18%, y que la edad media de los afectados es de 15 años. Según el informe *EU Kids online II* promovido por la Comisión Europea, el 42% de los menores de entre 12 y 16 años afirma haber recibido mensajes de carácter sexual por Internet.

Comúnmente, acosadores o "*groomers*", buscan sus víctimas en redes sociales, juegos en línea y otras plataformas digitales, utilizando perfiles falsos o usurpados[23]. Se aprovechan del anonimato y la información obtenida para establecer un vínculo de cercanía con las víctimas. Por este motivo, es importante estar alertas, ya que la persona que comete *grooming* suele tomarse el tiempo necesario para obtener información y la confianza de su potencial víctima.

También es común que los ciberacosadores o "*groomers*" sean personas del entorno cercano, como familiares o personas conocidas. Cuando el acosador es del entorno cercano, los medios digitales permiten generar una conversación sexual que en otros contextos no sería posible. Si se trata de una persona desconocida, es común que se contacte usualmente a través de perfiles falsos.

---

21 Real Academia Española. Pedofilia. Atracción erótica o sexual que una persona adulta tiene hacia niños.

22 Real Academia Española. Pedofilia. Abuso sexual cometido con niños.

23 GAPTAIN. PEDERASTAS online Y PEDÓFILOS. https://gaptain.com/

Una vez ganada la confianza de NNA, los "*groomers*" utilizan la seducción, chantaje o amenazas para efectuar una "sextorsión"[24] contra sus víctimas y buscar conseguir imágenes de contenido sexual o para cometer otros delitos como abuso sexual, tráfico de pornografía infantil, Trata de Personas (TdP), desapariciones y secuestro. Sin embargo, el acosador o "*groomer*" podría obtener fotos o videos sexuales de la víctima sin necesidad de contacto previo[25], mediante el robo de contraseñas, hackeo de dispositivos o alternado imágenes con Inteligencia Artificial (IA)[26].

En este escenario, el "*grooming*" constituye una experiencia que causa en NNA daños graves a nivel físico y psicológico. Ante esta realidad, es necesario estar alertas a su bienestar porque podrían estar desorientados sin poder contarle a nadie que está sufriendo esta forma de abuso. Además, los ciberacosadores suelen convencer a las víctimas de que su relación debe mantenerse en secreto, "culpabilizan" a la víctima y les hacen creer que las personas adultas de confianza no le creerán y se enojarán si cuentan lo que están sucediendo.

Hay señales a las que podemos prestar atención para identificar este tipo de acoso, como el descenso del rendimiento académico, tristeza, aislamiento, comportamientos agresivos, autolesiones, cambio de conducta, manifestaciones frecuentes de enfermedades y otras señales.

---

24 PrivacySavvy. La sextorsión es una actividad delictiva. Puedes pensar en ella como un tipo de extorsión en la cual el elemento de chantaje tiene que ver con material o actividades sexuales.

25 ChildFund. ¿Qué es el Grooming? Naveguemos Seguros - ChildFund

26 IBM. John McCarthy (2004) Se relaciona con la tarea similar de usar equipos para comprender la inteligencia humana, pero la IA no tiene que ajustarse a los métodos biológicos observables

MEDIDAS DE PREVENCIÓN	MEDIDAS DE ACTUACIÓN
1. Conversa con las niñas, niños y adolescentes sobre los riesgos digitales, la importancia de la privacidad en línea y los hábitos saludables en Internet.	1. Presta atención a personas desconocidas que buscan hacerse amigos de niñas, niños y adolescentes por videojuegos, redes sociales y otras aplicaciones; pueden fingir ser personas de la misma edad.
2. Explica el "*grooming*": ▪ Importancia de NO compartir o revelar datos personales a desconocidos y de NO enviar fotos ni vídeos. ▪ Importancia de NO ceder ante chantajes o extorsiones de acosadores y buscar ayuda.	2. En muchos casos, la víctima de *grooming* no informa sobre la situación que está viviendo por vergüenza o miedo. Presta atención a sus cambios y genera confianza para conocer lo que necesita. **NO cuestiones ni culpabilices ante esta situación.**
3. Dialoga con ellos sobre el respeto, los derechos y la sexualidad saludable. La confianza y comunicación es la clave para su bienestar.	3. Realiza la denuncia, busca información segura y encuentra apoyo con organizaciones e instituciones para la protección de NNA.
4. Aprende a manejar y utilizar las nuevas tecnologías para conocer las actividades en las que se incluyen las niñas, niños y adolescentes.	4. Es importante **NO** contactar con la o el acosador ni borrar información que luego será importante para las investigaciones correspondientes.[27]
5. Investiga alternativas disponibles de control parental para moderar su tiempo en Internet, los sitios web que visitan y los contactos con quienes interactúan. Una opción es Google "*FamilyLink*"[28].	5. Lo fundamental es mantener la confianza y la comunicación para prevenir y detectar posibles riesgos, así como brindarles apoyo incondicional para afrontar estas situaciones de acoso.
6. Es importante la empatía, respeto y amor para conocer sus preocupaciones y actuar oportunamente.	

27 GAPTAIN. PEDERASTAS online Y PEDÓFILOS. https://gaptain.com/evitar-pederastas-pedofilos-internet/

28 Google. https://familylink.google.com

Art. 172.- Utilización de personas para exhibición pública con fines de naturaleza sexual. - La persona que utilice a niñas, niños o adolescentes, a personas mayores de sesenta y cinco años o personas con discapacidad para obligarlas a exhibir su cuerpo total o parcialmente con fines de naturaleza sexual, será sancionada con pena privativa de libertad de siete a diez años.

Art. 91.- Trata de personas. - Toda persona que capte, transporte, traslade, retenga o reciba; en el país, desde o hacia otros países con fines de explotación; para lo cual un tercero recurre a la amenaza, uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder o de una situación de vulnerabilidad, a la concesión o aceptación de pagos o beneficios, constituye delito de trata de personas.

Constituye explotación, toda actividad de la que resulte un provecho material o económico, una ventaja inmaterial o cualquier otro beneficio, para sí o para un tercero, mediante el sometimiento de una persona o la imposición de condiciones de vida o de trabajo.

Art. 103.- Pornografía con utilización de niñas, niños o adolescentes. - La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años. Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a diecinueve años.

Cuando la persona infractora sea el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima, será sancionada con pena privativa de libertad de veintidós a veintiséis años.

Art. 166.- Sobre Acoso sexual. - La persona que solicite algún acto de naturaleza sexual, mantenga vínculo familiar o cualquier otra forma que implique subordinación de la víctima, con la amenaza de causar a la víctima o a un tercero un mal relacionado con las legítimas expectativas que pueda tener en el ámbito de dicha relación de subordinación, será sancionada con pena privativa de libertad de uno a cinco años.

Se considerará ciberacoso sexual cuando la conducta descrita en el inciso anterior se realice utilizando cualquiera de las tecnologías de la información y comunicación, medios tecnológicos, electrónicos o digitales, y será sancionado con una pena privativa de libertad de uno a cinco años.

Cuando la víctima sea menor de dieciocho años de edad, o persona con discapacidad o cuando la persona no pueda comprender el significado del hecho o por cualquier causa no pueda resistirlo, será sancionada con pena

privativa de libertad de tres a cinco años.

Cuando este ilícito sea cometido por miembros del núcleo familiar o personas con las que se determine que el procesado o la procesada mantenga o haya mantenido vínculos familiares, íntimos, afectivos, conyugales, de noviazgo, de cohabitación, o de convivencia o aun sin ella, se aplicará el máximo de pena establecida en este artículo, según el caso que corresponda.

- Mantén tus perfiles privados en redes sociales.
- NO aceptes solicitudes de amistad ni converses con perfiles desconocidos.
- Rechaza mensajes de tipo sexual o pornográfico.
- NO compartas fotos íntimas ni información que pueda afectar tu imagen digital o la de otras personas.
- Solicita ayuda a tus padres, madre o a una persona adulta de tu confianza para garantizar más seguridad en tu dispositivo.
- Si alguna conversación o contacto te incomoda, habla con las personas de confianza sobre ello.
- Si estás siendo atacada o atacado, NO cedas al chantaje o extorsión. ¡Solicita ayuda de inmediato!

Mensaje para niñas, niños y adolescentes

e. Sharenting – sobreexposición de NNA en redes sociales de padres, madres y familiares

El "*sharenting*", es un riesgo digital que se genera por la práctica padres, madres y otros familiares, que comparten información e imágenes de NNA a través de sus redes sociales. Esto representa un riesgo para su privacidad y seguridad. El termino proviene de la combinación de las palabras "*sharing*" (compartir) y "*parenting*" (crianza) en inglés[29].

En este punto, es esencial comprender que las imágenes, videos y otra información compartida desde el afecto y el orgullo de NNA, expone su integridad a otros riesgos digitales, puesto que los contenidos pueden ser sacados de contexto[30], pueden ser utilizados de forma indebida, desde ciberbullying hasta modalidades de explotación sexual infantil.

También es necesario tener en cuenta que imágenes, videos y contenidos que se comparten en medios digitales con "buenas intenciones" para tener una memoria de "buenos momentos", formarán parte de la huella digital[31] de NNA. Ese contenido puede ser utilizados en prácticas de ciberbullying, grooming, sextorsión y el cometimiento de diversos delitos. En este sentido, es fundamental tomar consciencia sobre este riesgo para tomar medidas de seguridad y prevenir riesgos de protección de las niñas, niños y adolescentes.

29 INFOBAE. (2023). Sharenting: cómo impacta en los niños el compartir fotos y videos de su crianza en las redes sociales
30 Faro Digital. (2022). Guía de acompañamiento de adolescencias en entornos digitales.
31 Kaspersky. Una huella digital (a veces llamada sombra digital o huella electrónica) se refiere al rastro de datos que dejas cuando usas Internet. Esto incluye los sitios web que visitas y los correos electrónicos y la información

MEDIDAS DE PREVENCIÓN	MEDIDAS DE ACTUACIÓN
1. Ten en cuenta que los acosadores y consumidores de pornografía suelen aprovechar la información disponible en línea sobre sus víctimas. Por lo tanto, es imprescindible proteger la privacidad en las redes sociales.	1. Antes de publicar una imagen, video o cualquier contenido en redes sociales, es importante configurar la privacidad de cada una de ellas. Puedes restringir los contactos que no deseas que accedan a la información.
2. Es importante crear conciencia sobre la información delicada que no debe ser compartida, como datos personales, ubicaciones y rutinas. Evalúa cuidadosamente si es adecuado compartir contenido relacionado con niñas, niños y adolescentes, ya que esto puede ser utilizado por acosadores o redes de pornografía.	2. Infórmate sobre las condiciones de privacidad de las plataformas donde vayas a ingresar contenidos que involucren a NNA.
	3. Evita compartir imágenes que puedan ser utilizadas de manera indebida con fines pornográficos u otras formas de explotación.
3. Al compartir información, fotografías y videos, es crucial asegurarnos de que solo personas de confianza puedan acceder a estas publicaciones. Siempre es recomendable pensar dos veces antes de compartir algo en línea.	4. NO compartas información sobre rutinas, centros de estudio o ubicaciones frecuentes. Se recomienda desactivar el GPS del celular al tomar fotos y grabar videos.
4. Es recomendable supervisar la cantidad y el tipo de información que las niñas, niños y adolescentes publican en las redes sociales para evitar una sobreexposición innecesaria.	5. NO etiquetes ni incluyas perfiles o nombres de menores en los contenidos que decidas publicar.
5. Promueve conversaciones en casa sobre el significado y la importancia del consentimiento antes de publicar imágenes de otras personas en línea.	6. Promueve la eliminación de contactos no reconocidos o sospechosos y supervisa la interacción en grupos en línea para detectar posibles situaciones de riesgo.

f. Adicción a internet

La adicción a Internet es un fenómeno común que implica el abuso de la tecnología buscando constante información. Esta práctica afecta negativamente las vidas de las personas, especialmente de NNA quienes son más propensos y pueden

llegar a tener efectos emocionales y físicos que comúnmente desencadenen en bajo rendimiento escolar, descuido de la alimentación, estados de ánimo irritables, trastornos del sueño y otras conductas que afectan la atención. Además, pueden generar aislamiento social, falta de sentido personal y pérdida de intimidad.[32]

Podemos vincular la adicción al Internet a un trastorno denominado "nomofobia", un término proveniente del anglicismo ("*no-mobile-phone-phobia*"). Consiste en el miedo irracional a estar sin teléfono móvil o no tener acceso a Internet. Asimismo, la "nomofobia" puede desencadenar otros problemas personales, sociales y económicos causado por la distracción contante en el Internet e incapacidad de mantener la concentración[33].

Algunos síntomas de la nomofobia pueden ser ansiedad y nerviosismo ante la pérdida de conexión, utilización del móvil en situaciones prohibidas y peligrosas, (como revisar redes sociales mientras se conduce), realizar constante revisión de las notificaciones en la pantalla y el uso cada vez más frecuente del Internet, restando tiempo a actividades presenciales.

Superar la adicción a Internet podría requerir intervención especializada y acompañamiento. Pero una decisión saludable, inicia por prestar más atención a actividades cotidianas fuera de línea, como practicar deportes, leer, juegos de mesa, compartir espacios con los demás y otras que contribuyen al bienestar de las personas y un equilibrio saludable con el uso de la tecnología.

32 GAPTAIN. Adicción a Internet, redes sociales y Móviles. https://gaptain.com/prevenir-adiccion-movil-internet/
33 Orbium. https://orbiumadicciones.com/nuevas-tecnologias/que-es-nomofobia/

<table>
<tr><th>MEDIDAS DE PREVENCIÓN</th><th>MEDIDAS DE ACTUACIÓN</th></tr>
<tr><td>1. Supervisa de cerca el uso de dispositivos tanto a nivel personal como familiar. Es esencial que las niñas, niños y adolescentes cuenten con una supervisión adecuada.</td><td>1. Reconocer el uso abusivo de Internet es el primer paso para abordar esta problemática, similar a otras adicciones. Es fundamental escuchar las preocupaciones y sentimientos de la persona afectada.</td></tr>
<tr><td>2. Considera la creación de perfiles infantiles[34] en aplicaciones diseñadas específicamente para NNA, ya que estas suelen restringir contenidos inapropiados y promover un uso más seguro.</td><td rowspan="2">2. Fomenta un ambiente familiar de apoyo donde la persona pueda expresar sus inquietudes y plantear compromisos y responsabilidades. Estos compromisos pueden incluir la adopción de nuevas rutinas, establecimiento de límites y utilización de herramientas para mantener el control y equilibrio en el uso de dispositivos e Internet.</td></tr>
<tr><td>3. Utiliza herramientas de control parental para monitorear la actividad en línea de los menores, lo que facilitará la prevención de riesgos y el manejo de situaciones potencialmente peligrosas.</td></tr>
<tr><td>4. Mantén conversaciones abiertas en casa acerca de los riesgos asociados con el uso de dispositivos e Internet. Lleguen a acuerdos sobre reglas y horarios para el uso de tecnología, así como para realizar otras actividades importantes.</td><td>3. Si es necesario, busca orientación en fuentes de información seguras y considera la posibilidad de recurrir a atención especializada para obtener el apoyo.</td></tr>
</table>

3.5 Recurso adicional: Hábitos de una cultura digital responsable

Para contribuir a una Cultura Digital responsable, es indispensable promover espacios comunitarios de reflexión y análisis sobre los diversos riesgos digitales y peligros asociados con el acceso a las tecnologías de la información y comunicación. La educación para el uso adecuado de Internet, constituye la base principal para garantizar la seguridad en línea.

34 GAPTAIN. Adicción a Internet, redes sociales y Móviles. https://gaptain.com/prevenir-adiccion-movil-internet/

Educar a NNA sobre las consecuencias de ciertos usos de Internet y cómo evitarlos promueve una cultura digital responsable. Además, fomentar diálogos en espacios educativos y hogares facilita la reflexión sobre los riesgos digitales y permite compartir experiencias y recursos para la protección en línea.

Se recomienda abordar los diálogos y reflexiones de manera abierta y participativa, relacionando los siguientes temas para reforzar la prevención de riesgos digitales presentados en esta metodología. Esto facilitará el intercambio de conocimientos y la definición de mejores herramientas de seguridad, así como el desarrollo de hábitos positivos en el uso de las tecnologías de la información y comunicación.

TEMAS PARA FACILITAR EL DIÁLOGO COMUNITARIO

1. ¿Cómo abordar los riesgos digitales en casa con niñas, niños y adolescentes?

Es esencial hablar en casa sobre los beneficios y riesgos de Internet, estableciendo normas de uso responsables para protegernos. Motiva conversaciones respetuosas para conocer sus inquietudes, explorar sus conocimientos de aplicaciones y compartir consejos útiles.

2. ¿Cómo acceder a métodos de protección de datos en línea?

Investiga alternativas para crear y proteger contraseñas seguras, utiliza programas antivirus y asegúrate de usar dispositivos personales de forma segura, especialmente si son compartidos. Cierra sesiones e información de manera segura y elimina datos de navegación. Identifica alertas de seguridad, activa “alertas de inicio de sesión” y “autenticación en dos pasos” para proteger el acceso a tus cuentas. Evita interacciones con spam y sitios sospechosos.

3. ¿Cómo tener un uso responsable y saludable en el Internet y dispositivos?

Investiga alternativas para crear y proteger contraseñas seguras, utiliza programas antivirus y asegúrate de usar dispositivos personales de forma segura, especialmente si son

compartidos. Cierra sesiones e información de manera segura y elimina datos de navegación. Identifica alertas de seguridad, activa “alertas de inicio de sesión” y “autenticación en dos pasos” para proteger el acceso a tus cuentas. Evita interacciones con spam y sitios sospechosos.

4. ¿Cómo podemos garantizar nuestra privacidad en línea?

Revisa las herramientas de configuración de privacidad disponibles en todas las aplicaciones de mensajería instantánea y redes sociales. Reflexiona sobre los límites en la información que compartimos, genera conciencia sobre la huella digital y evita interacciones con cuentas desconocidas. Estar alertas ante posibles estafas, explotación, ciberacoso, grooming y trata de personas. En caso de ser víctimas de estafas, chantajes o acoso, es importante buscar apoyo, denunciar, guardar pruebas, bloquear y reportar el contacto.

5. ¿Cómo mantener nuestra seguridad en espacios sociales?

Comparte tu ubicación con confianza, evita publicaciones en tiempo real y sé cauteloso al buscar empleo en línea. Evita compartir información personal por teléfono y navegar en sitios web desconocidos. Sé responsable y respetuoso, obteniendo el consentimiento de otras personas antes de publicar información sobre ellos en línea.

4. Agenda de taller

UNIDAD UNO: PRESENTACIÓN Y DINÁMICA		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Preséntate y expón el objetivo del taller. 2. Realiza una dinámica de acuerdo al público objetivo, procuae que esta permita al grupo distenderse. 3. Elabora acuerdos comunes y escríbelos en una pizarra o papelotes.	▪ Recuerda que el primer momento te permitirá contar con un grupo distendido y abierto al aprendizaje. ▪ Genera confianza y tranquilidad en el grupo. ▪ Usa tarjetas con los nombres, esto facilitará la relación durante el taller. ▪ Haz que los acuerdos sean participativos y úsalos a lo largo del taller.	▪ Etiquetas para los nombres ▪ Marcadores ▪ Papelotes ▪ Cinta adhesiva

UNIDAD DOS: CONTENIDO POR CADA RIESGO DIGITAL		
DESINFORMACIÓN: TELÉFONO DESCOMPUESTO		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Diseña previamente una frase de 10 a 12 palabras que contenga una noticia o información relevante. 2. Forma un círculo con las personas participantes, asegurándose de que estén sentadas y puedan comunicarse fácilmente. 3. Inicia transmitiendo la frase inicial a una persona y solicítale que la susurre al oído la misma información a la siguiente persona. 4. Continúa transmitiendo la frase hasta que llegue al final del círculo. 5. La última persona en recibir el mensaje deberá decir en voz alta la frase que escuchó para compararla con la frase original.	▪ Después de realizar el juego del teléfono descompuesto, facilita una reflexión grupal a través de las siguientes preguntas (incluye otras preguntas que consideres adecuadas): ¿Has tenido alguna vez acceso a información que después descubriste que era falsa? ¿Cómo te sentiste al descubrirlo? ¿Has visto en las redes sociales información que te pareció un engaño o fraude? ¿Qué medidas crees que podrían tomarse para identificar este tipo de información? ¿Conoces algún caso en el que el acceso a información falsa haya tenido consecuencias negativas? ¿Qué podríamos hacer para evitar que esto ocurra en el futuro?	▪ Hojas de papel, bolígrafos o lápices para anotar las frases transmitidas. ▪ Espacio adecuado para que las personas puedan sentarse en círculo y comunicarse con claridad

RIESGOS DE FRAUDE CIBERNÉTICO: TRIVIA CIBERNÉTICA		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Crea tarjetas con los nombres en inglés de las principales formas de ataque cibernético. 2. Forma dos o tres grupos de personas para participar en la trivia. Utiliza una dinámica para que las y los participantes se mezclen. 3. Informa las instrucciones para que cada grupo compita y sume puntos de acuerdo a sus respuestas. Puedes establecer una dinámica para que respondan, por ejemplo, decir una frase, realizar un movimiento específico, utilizar una corneta o sonido particular.	▪ Después de completar la actividad, es importante realizar una evaluación para medir el aprendizaje y la comprensión de los temas. ▪ Esta evaluación puede realizarse a través de un diálogo sobre situaciones relacionadas a los riesgos de seguridad informática y fraude cibernético.	Tarjetas con los nombres de las principales técnicas de ataques cibernéticos. ▪ *Hacking* ▪ *Virus troyano* ▪ *Ransomware* ▪ *Spyware* ▪ *Phishing* Distintivos para identificar a los equipos. Instrumento disponible para participar y responder cada pregunta.

CIBERBYLLYING ACOSO ESCOLAR EN LÍNEA: DIBUJA A TU COMPAÑERO O COMPAÑERA		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Invita a las y los participantes a dibujar a su compañero/a de lado y a describirlo/a incluyendo dos cualidades positivas de esa persona. **2.** Proporciona una hoja de papel y lápices de colores. **3.** Motiva a las y los participantes a presentar su dibujo. Reitera que el propósito de esta actividad es promover la empatía, el reconocimiento de las cualidades de los demás y la importancia del respeto.	▪ Al finalizar la actividad, promueve una reflexión sobre la importancia de reconocer y valorar las cualidades positivas de los demás, fomentando así la empatía y el respeto en las interacciones diarias.	▪ Hojas de papel y pinturas o lápices de colores. ▪ Puedes incluir un papelógrafo o pizarra para ubicar todos los dibujos.

GROOMING ACOSO SEXUAL INFANTIL EN MEDIOS DIGITALES: CAPERUCITA ROJA Y LAS MENTIRAS		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Invita a los participantes a formar pequeños grupos y asigna a cada grupo un escenario del cuento de Caperucita Roja donde se presente una situación engañosa o una mentira en la que fue víctima. **2.** Pídeles que desarrollen una breve dramatización de esa situación en los entornos digitales, enfocándose en cómo se desarrolla el engaño y sus consecuencias.	▪ Finaliza la actividad con una discusión abierta sobre la importancia de la empatía y la seguridad en línea. ▪ Utiliza preguntas cómo ¿Qué podría haber hecho diferente Caperucita para no caer en la trampa? ¿Qué recomendaciones le hubieses dado a Caperucita antes de caer en la trampa?	▪ Espacio adecuado para las dramatizaciones. ▪ Accesorios simples para representar los personajes (opcional).

SHARENTING/ SOBREEXPOSICIÓN DE NNA EN REDES SOCIALES POR PARTE DE PADRES, MADRES Y FAMILIARES: CADAVER EXQUISITO		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Presenta la técnica del "Cadáver Exquisito", que consiste en crear una historia o dibujo de manera colaborativa, donde cada participante contribuye una parte sin conocer la totalidad de lo que los demás han aportado. 2. Divide a los participantes en grupos pequeños de 4 a 6 personas, asegurándote de que haya diversidad de edades representados en cada grupo. 3. Empieza a relatar una historia que empiece sobre una situación de exposición de información "*sharenting*" en redes sociales y da el paso.	▪ Observa cómo interactúan las y los participantes en sus grupos durante la actividad, prestando atención a la colaboración, comunicación y respeto mutuo. ▪ Facilita un diálogo grupal y participativo relacionada con la prevención del "sharenting", haciendo hincapié en la importancia de la seguridad y el respeto por la privacidad.	▪ Para incentivar la creatividad, puedes incluir en esta actividad material lúdico, revistas para recortar, papel, cartulinas o pizarras en los que se realicen sus aportes visuales.

ADICCIÓN AL INTERNET: CARAS EXPRESIVAS		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Explica la adicción a internet y la nomofobia. 2. Invita a las personas participantes a reflexionar sobre sus propias experiencias y a identificar comportamientos relacionados con el uso excesivo de la tecnología. 3. Después, plantea un reto emocional donde las personas deben compartir su experiencia imitando un "emoticón" que represente una emoción específica. 4. Luego, facilita que todas o un grupo de participantes explique la situación que les haya generado esa emoción relacionada con el uso de la tecnología.	▪ Facilita un ejercicio abierto donde las y los participantes compartan sus opiniones, preocupaciones y desafíos relacionados con el uso de la tecnología en su vida diaria. ▪ Pide a cada participante que elabore un compromiso personal para utilizar la tecnología de manera responsable y evitar caer en la adicción o la nomofobia.	▪ Hojas de papel, cartulinas, bolígrafos, pinturas para que los participantes tomen notas y elaboren su compromiso personal. ▪ Ejemplos de casos reales o testimonios sobre la adicción a Internet y la nomofobia
UNIDAD TRES: HÁBITOS DE UNA CULTURA DIGITAL RESPONSABLE Y CIERRE		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Modera un diálogo abierto y participativo para intercambiar recursos y experiencias que contribuyan a la prevención de riesgos digitales.	▪ ¿Qué aprendí y cómo lo aplicaré en mi vida? ▪ ¿Cuál es mi compromiso con la prevención de riesgos digitales?	▪ Dinámica de cierre.

Capítulo II


ROMPIENDO
EL SILENCIO

ROMPIENDO EL SILENCIO

1. Objetivo General

Implementar acciones de sensibilización sobre la Violencia Basada en Género en espacios digitales y dar a conocer cómo la información puede ser mecanismo clave para prevenirla.

2. Público Objetivo

- Niñas, niños y adolescentes
- Adultos/as de las comunidades
- Padres, madres y adultos responsables de NNA
- Profesionales en cualquier área .

3. Principales Definiciones

3.1 Datos de interés

Aquí hemos clasificado algunas formas de violencia y comportamientos digitales que representan un riesgo para la identidad de las personas, ya que implican la distribución, difusión, exhibición, comercialización o compartición de imágenes, audios, videos o conversaciones personales.

Con el acceso al software de inteligencia artificial, también existe el riesgo de que el contenido pueda ser alterado o simulado para representar contenido íntimo sexual de una persona sin su consentimiento. Por este motivo, es fundamental proteger la privacidad al publicar información e interactuar en redes sociales.

Uno de los riesgos más significativos y amenazantes para la integridad personal en el entorno digital es la violencia digital, que incluye toda forma de discriminación, acoso, explotación, abuso, hostigamiento, amenaza, agresión, difamación o extorsión con la intención de discriminar o agredir a través de redes sociales, correo u otros canales. Un ejemplo es la difusión no autorizada de imágenes e información privada obtenidas de manera consentida o no, el acoso, el envío de contenido pornográfico y la explotación sexual. Esto incluye tipos de ataques como el acoso sexual digital, la pornografía no consentida, el acoso de naturaleza sexual, la extorsión sexual, la difamación de carácter sexual, la explotación sexual facilitada por la tecnología y la difusión de imágenes o videos de agresiones sexuales. [35]

La violencia de género (VBG) es una crisis mundial que afecta a un gran número de mujeres, socavando su dignidad, libertad y capacidad de decisión. Esta forma de violencia sigue siendo un problema generalizado y devastador, como lo demuestran los datos proporcionados por la Organización Mundial de la Salud. Según sus estadísticas, aproximadamente 736 millones de mujeres, lo que equivale a una de cada tres, son víctimas de violencia física o sexual perpetrada por sus parejas íntimas, así como de agresiones sexuales por parte de terceros.

---

35 Taller de Comunicación Mujer (TCM). (2022). MOVERSE SEGURAS Y SEGUROS, https://navegandolibres.org/wp-content/uploads/2023/09/Moverse_seguras_final_compressed.pdf

Estas cifras se han mantenido constantes a lo largo de la última década (OMS, 2021).

La implementación de esta metodología permitirá abordar la Violencia Basada en Género desde su dimensión comunitaria al ser una construcción socio-histórica cultural que se reproduce en diversos comportamientos situacionales y esto a su vez se desarrollará tanto talleres como contenido digital sobre cómo podemos prevenir la Violencia Basada en Género en entornos comunitarios y también desde ámbitos públicos y privados con la finalidad de brindar información segura para buscar alternativas de erradicación, sensibilización y prevención de posibles casos de violencia. De este modo mediante la participación podemos promover acciones, comportamientos y nuevas capacidades para frenar la Violencia Basada en Género, con la finalidad de que la información segura, confiable y de calidad permita la integración comunitaria, la participación, corresponsabilidad y la defensa de derechos humanos.

3.2 Conceptos generales

a. Violencia basada en género

La Organización Mundial de la Salud define a la violencia como “el uso deliberado de la fuerza física o el poder, ya sea en grado de amenaza o efectivo, contra uno mismo, otra persona o un grupo o comunidad, que cause o tenga muchas probabilidades de causar lesiones, muerte, daños psicológicos, trastornos del desarrollo o privaciones” (2021).

El género abarca un espectro más amplio y complejo que el sexo y proporciona un marco para examinar cómo se han construido a lo largo de la historia las ideas, creencias, representaciones, prácticas y atribuciones relacionadas con lo femenino y lo masculino, basándose en la diferencia biológica sexual. En otras palabras, el género ayuda a comprender que lo masculino y lo femenino no son simples reflejos de la realidad natural o biológica, sino el resultado de un proceso histórico y cultural de construcción (Organización Mundial de la Salud, 2018).

De este modo, la violencia basada en género se refiere a cualquier acción u omisión que cause daño físico, psicológico o sexual a una persona debido a las desigualdades de género,

es decir, al desequilibrio de poder existente entre hombres y mujeres. El concepto de violencia basada en género se utiliza principalmente para resaltar el hecho de que las disparidades de poder basadas en el género exponen especialmente a las niñas, adolescentes y adultas mujeres, miembros de la comunidad LGBTIQ+ a diversos tipos de violencia, y aunque las son las principales víctimas de la violencia basada en género, los hombres y los niños especialmente también pueden ser afectados.

La CRE dentro del artículo 66, reconoce el derecho a la integridad personal que incluye, una vida libre de violencia en el ámbito público y privado; además de establecer que el Estado adoptará las medidas necesarias para prevenir, eliminar y sancionar toda forma de violencia, en especial la ejercida contra las mujeres, niñas, niños y adolescentes, personas adultas mayores, personas con discapacidad y contra toda persona en situación de desventaja o vulnerabilidad; idénticas medidas se tomarán contra la violencia, la esclavitud y la explotación sexual.

b. Tipos de violencia basada en género

En el Ecuador desde el año 2018, a través de la Ley para Prevenir y Erradicar la Violencia Contra las Mujeres y su última reforma en el año 2021, en su artículo 10 se definieron 8 tipos de violencia, esto después de un largo proceso de lucha histórica de los movimientos de mujeres; no son las únicas formas de violencia, sin embargo, son aquellas que están dentro de esta ley.

¿CÓMO SE LLAMA?	¿QUÉ ES?
Violencia física	Acto intencionado que cause daño, sufrimiento, dolor físico; mediante maltrato, agresiones, castigos corporales, que afecte la integridad física de la víctima provocando: lesiones externas o internas, en el cuerpo de la persona violentada y en otros casos hasta la muerte, por el deliberado uso de la fuerza con o sin la utilización de algún objeto.
Violencia psicológica	Acción, omisión o comportamiento dirigido a causar daño a la identidad e integridad psicológica, emocional, a la autoestima, honra y dignidad de una persona mediante insultos, gestos, mensajes, mentiras, intimidación, amenazas, chantajes, menosprecio o manipulación, afectando así la estabilidad emocional, psicológica, prestigio o dignidad de una persona. Este tipo de violencia puede darse en cualquier contexto y lugar.

Violencia sexual	Toda acción que implique la vulneración o restricciones de los derechos sexuales e integridad sexual de una persona, haya o no un vínculo cercano o relación entre la víctima y el victimario. La violencia sexual es todo tipo de contacto sexual no autorizado, por medio de relaciones sexuales de tipo oral, anal o vaginal no consentidas, caricias o acercamientos de la persona y sus genitales sin aprobación previa, acoso, explotación o intimidación. (Ley Orgánica Integral para Prevenir y Erradicar la Violencia Contra las Mujeres en Ecuador,2018).
Violencia económica y patrimonial	Omisión o Acción a que ocasiona deterioro o daños a los bienes, recursos económicos y patrimoniales de una persona, sociedad conyugal o unión de hecho, a través de tenencia o posesión abusiva, sustracción, destrucción o retención de objetos, instrumentos de trabajo, documentos personales, bienes, valores y derechos patrimoniales; limitación de recursos económicos y control de ingresos; o percepción del salario injusto de acuerdo al trabajo y actividad desempeñada, de una persona a otra sea en el contexto de convivencia personal o laboral.
Violencia simbólica	Toda conducta que, a través de su producción, reproducción, publicación, imágenes, signos e iconos, perpetúan la disparidad de género y naturalizan la discriminación y cosificación de las mujeres en la sociedad.
Violencia política	Violencia que ejerce una persona o un grupo de personas directa o indirectamente que acorta, impide, restringe o evita la participación o accionar de una mujer en un cargo público, político o social.
Violencia gineco-obstétrica	Acción u omisión que limite el derecho de atención a una salud de calidad a las mujeres en periodo de embarazo o no. Se evidencia este tipo de violencia a través del maltrato, imposición de prácticas culturales o científicas sin autorización de la persona atendida, abuso del conocimiento profesional, falta de aplicación ética de rutas, protocolos y guías; impidiendo la decisión sobre su cuerpo y el libre ejercicio de sus derechos, a una mujer que requiera de la atención de este tipo personal médico.
Violencia Sexual Digital	Acción que implique principalmente la vulneración o restricción del derecho a la intimidad, realizada contra las mujeres en el entorno digital a través de cualquiera de las tecnologías de la información y comunicación haciendo uso de contenido de carácter personal o íntimo misma que contenga una representación visual de desnudos, semidesnudos o actitudes sexuales que la mujer haya confiado de su intimidad o haya sido obtenido de cualquier otro medio.

c. Violencia de género digital

La violencia de género en el entorno digital se refiere a todas las formas de discriminación, acoso, explotación, abuso y agresión que ocurren a través de redes sociales, correos electrónicos, dispositivos móviles y cualquier otro medio relacionado con las tecnologías de la información y la comunicación (TIC) (Diego, Córdova, Godoy & Paz, 2020). Esta violencia tiene repercusiones físicas, psicológicas, sexuales y económicas. La violencia en línea o digital no está separada de la que se produce en entornos reales (OMS, 2020).

Algunas expresiones o evidencias de violencia de género digital incluyen acosar o controlar a la pareja o expareja con la finalidad de discriminar, dominar e intromisión sin consentimiento a la privacidad de las personas. Se realiza a través de los dispositivos buscando interferir en relaciones con otras personas, espiar la información, censurar fotos en redes sociales, controlar sus actividades, exigir su geolocalización, obligarla a enviar imágenes íntimas, comprometerla para que revele sus claves personales, exigir ver sus conversaciones con otras personas.

"Esta violencia afecta principalmente a mujeres, niñas, niños, adolescentes y personas LGBTIQ+ debido a la reproducción de relaciones de poder que se dan en contextos de desigualdad social e histórica. Dichas relaciones de poder se manifiestan en brechas de acceso a servicios y recursos, incluidas las TICs; la reproducción de condiciones de vulneración en espacios fuera y dentro de línea y la limitación del ejercicio de los derechos humanos en el ejercicio de los derechos humanos, lo que se extiende a los derechos digitales".[36]

- **Tipos de violencia basada en género digital**

La violencia en línea dentro de diversidades de plataformas y formas de interacción pueden generar múltiples tipos de violencia en los entornos digitales. De acuerdo a la guía Navegando Libres por la Red[37], las formas de violencias de género en los entornos digitales son:

---

36 Taller de Comunicación Mujer, ACNUR (2022). GUÍA METODOLÓGICA SOBRE VIOLENCIA DE GÉNERO DIGITAL DIRIGIDA A EQUIPOS DE ATENCIÓN A PERSONAS EN MOVILIDAD HUMANA

37 Taller de Comunicación Mujer (TCM). https://navegandolibres.org/

¿CÓMO SE LLAMA?	¿QUÉ ES?
Acoso digital o en línea (ciberacoso)	Hostigamiento, amenaza, agresión, difamación o extorsión dirigidas a una persona con el propósito de discriminar, desalentar o intimidar debido a su género, expresiones que se suelen interrelacionar con otros tipos de violencia de manera.
Violencia sexual digital o en línea	Engloba el acoso, las amenazas, la agresión, la difamación o la extorsión de naturaleza sexual o con objetivos sexuales. Comprende acciones que afectan el ejercicio libre de la sexualidad de las víctimas, incluso aquellas que pudieron haberse dado mediante intimidación y manipulación.
Difusión de información privada (*doxxing*)	Este término se utiliza para describir el acto de divulgar información en línea acerca de la identidad, vida privada o vida sexual de una o más personas sin su consentimiento. El propósito de este tipo de agresiones es exponer a las víctimas de tal manera que su seguridad física y psicológica se vea amenazada.
Discursos de odio y expresiones discriminatorias	Este concepto se emplea para explicar los actos de violencia, intimidación y manifestaciones de discriminación basadas en el género, con el objetivo de perjudicar a individuos o colectivos que han sido históricamente vulnerables. Estas conductas tienen la intención de difundir mensajes de odio y/o respaldar estereotipos relacionados con el género y la diversidad sexual.
Ataques a la libertad de expresión	Se refiere a cualquier acción dirigida a intimidar o amedrentar a una persona o grupo debido a su género. Estos actos ocurren con frecuencia hacia personas que ejercen su derecho a la libertad de expresión en espacios públicos, como defensoras/es de derechos humanos, periodistas, candidatas políticas, y miembros de la comunidad LGBTIQ, entre otros.
Hackeo de dispositivos y cuentas	Consiste en ingresar sin consentimiento a dispositivos y perfiles de redes sociales con la intención de intimidar, extorsionar, manipular o robar información personal y/o corporativa. [38]

37 Taller de Comunicación Mujer (TCM). https://navegandolibres.org/
38 Taller de Comunicación Mujer (TCM). (2020). Diagnóstico violencia de género digital en Ecuador)


Ciberacoso
Violencia sexual digital
Hackeo
VBG DIGITAL
Doxxing
Ataques a la libertad de expresión
Discurso de odio

MEDIDAS DE PREVENCIÓN	MEDIDAS DE ACTUACIÓN
1. Identificar las expresiones y manifestaciones que nos alerten sobre la violencia de género	1. Ante una situación de violencia de género digital, es vital tomar medidas y buscar apoyo
2. Fortalecer la seguridad en nuestros dispositivos y perfiles sociales es fundamental. Esto implica utilizar contraseñas fuertes y actualizarlas periódicamente para prevenir accesos no autorizados.	2. Denuncia los incidentes a las autoridades y a las plataformas en línea donde ocurrió la violencia. Las redes sociales y otras plataformas tienen normativas y términos de uso que incluyen rutas de denuncia.
3. Además, es recomendable activar las opciones de autenticación en el ingreso a nuestros perfiles para añadir un elemento más de seguridad.	3. Bloquea a los agresores y reporta cualquier contenido dañino que hayan publicado sobre ti en aplicaciones de mensajería y redes sociales. Guarda evidencia de la violencia recibida para respaldar la denuncia judicial y activar medidas de protección.
4. Evita entablar conversaciones con personas desconocidas y no compartas información personal.	4. Busca orientación confiable para acceder a apoyo emocional y psicológico. Es importante contar con ayuda especializada.
5. Es especialmente importante tener precaución con las aplicaciones de citas, ya que pueden convertirse en fuentes de ciberacoso o grooming.	5. Refuerza la seguridad de tu información: instala un antivirus en tus dispositivos digitales, filtra y elimina contactos desconocidos, y mantén actualizados tus protocolos de seguridad para prevenir accesos no autorizados.
6. No expongas tu vida privada en redes sociales y configura adecuadamente la privacidad de la información que publicas.	6. Apoya a otras personas que enfrentan violencia de género digital. Evita cuestionar o culpar, y en su lugar, ofrece acompañamiento y apoyo para denunciar y reportar estos actos violentos. Juntos podemos crear entornos digitales más seguros y respetuosos.
7. Reflexiona sobre el impacto digital de tus acciones en línea y mantén conversaciones con las personas de tu confianza sobre los diferentes tipos de violencia digital.	
8. Fomenta el respeto y la empatía, incluyendo el respeto al consentimiento al compartir información, y promueve relaciones basadas en la igualdad e integridad en el entorno digital.	

Recursos Legales: COIP

Art. 157.- Violencia psicológica contra la mujer o miembros del núcleo familiar.- Comete delito de violencia psicológica la persona que realice contra la mujer o miembros del núcleo familiar **amenazas, manipulación, chantaje, humillación, aislamiento, hostigamiento, persecución, control de las creencias, decisiones o acciones, insultos o cualquier otra conducta que cause afectación psicológica** y será sancionada con pena privativa de libertad de seis meses a un año. Si con ocasión de la violencia psicológica se produce en la víctima, enfermedad o trastorno mental, la sanción será pena privativa de libertad de uno a tres años.

Art. 9.- Derechos de las mujeres.- Las mujeres: niñas, adolescentes, jóvenes, adultas y adultas mayores, en toda en su diversidad, tienen derecho al reconocimiento, goce, ejercicio y protección de todos los derechos humanos y libertades contemplados en la Constitución de la República, los instrumentos internacionales ratificados por el Estado y en la normativa vigente.[39]

d. Peligros del sexting

El "*Sexting*"[40] procede de usar las palabras inglesas "*sex*" (sexo) y "*texting*" (enviar mensajes). Es una práctica sexual de carácter íntimo mediada por tecnologías digitales. Pueden ser intercambio de contenido erótico ya sea fotos, textos, audios o videos, con otra persona a través de mensajería instantánea y videollamadas. Aunque es una práctica regular por medio del consentimiento de ambas partes, está práctica representa un gran riesgo de violencia de género y de integridad de las personas.

Un riesgo potencial asociado al *sexting* es la divulgación no autorizada de contenido íntimo o "*sexting*" sin consentimiento[41], lo cual permite que terceros accedan a estos materiales de carácter sexual o erótico sin el consentimiento de la persona involucrada. [42] O ser víctimas de prácticas conocidas como "pornovenganza", "*revengeporn*" o "venganza pornográfica". Tras una ruptura amorosa, se suele utilizar este tipo de violencia digital para humillar y "castigar" a la persona por abandonar la relación.[43]

---

39 LEY ORGANICA INTEGRAL PARA PREVENIR Y ERRADICAR LA VIOLENCIA CONTRA LAS MUJERES

40 ABS. (2020), Sexting. Es una práctica que consiste en enviar mensajes con contenido erótico a través de dispositivos tecnológicos de manera voluntaria

41 Save The Children. (2019) El sexting sin consentimiento es una forma de violencia, ya que la víctima no da su consentimiento para su difusión.

42 Faro Digital. (2022). Guía de acompañamiento a las adolescencias en los entornos digitales

43 Internet Segura. (2020). Ecuador

El *sexting* representa un riesgo, y aunque en la actualidad en las relaciones sexo afectivas, la manera de expresar la sexualidad y construir vínculos se desenvuelven en los entornos digitales como los juegos en línea, redes sociales, mensajería instantánea y otros. Está práctica puede tener resultados nocivos. Por este motivo, es importante no exponer nuestra vida íntima ni enviar contenido sexual a nadie. Porque nunca sabremos quien pueda verlo o difundirlo y al enviar una fotografía o video sexual perdemos el control sobre ello.

Si este contenido cae en manos malintencionadas y redes de comercialización y grupos de difusión de contenido pornográfico, nuestra identidad se verá vulnerada y podríamos ser víctimas de extorsión y chantaje "Sextorsión"[44] para solicitar dinero o el envío de más contenidos íntimos. A partir de material sexual, el agresor o agresora amenaza con hacer público contenido íntimo de la persona a la que extorsiona. dicha información podría incluir mensajes de texto sexuales fotos íntimas e, incluso, vídeos.

MEDIDAS DE PREVENCIÓN	MEDIDAS DE ACTUACIÓN
1. Es importante entender que el "*sexting*" NO representa amor y requiere un nivel más profundo de respeto y equidad. Además, nadie debe sentirse obligado a participar en el "*sexting*".	1. El "*sexting*" representa un riesgo de acceso no autorizado a nuestra información, lo cual puede conducir a la vulneración de nuestra privacidad, el ciberacoso, el grooming, la sextorsión y la publicación no autorizada de contenido en sitios de pornografía.
2. Para proteger la información en tus dispositivos, evita compartir contraseñas y emplea claves difíciles de descifrar. Limita el acceso de terceros a tu dispositivo.	2. Es crucial promover la educación digital entre niñas, niños y adolescentes para concienciar sobre las consecuencias de los riesgos digitales y la importancia de la privacidad en línea.
3. Elimina imágenes sensibles de tus dispositivos para prevenir posibles pérdidas o robos de información. Además, es recomendable utilizar software antivirus y abstenerse de descargar enlaces o aplicaciones de fuentes no confiables. Los delincuentes podrían aprovechar estas vulnerabilidades para acceder a nuestra información privada.	3. Además, es fundamental mantener medidas de seguridad en nuestras interacciones y conversaciones. Por ejemplo, evita encender tu cámara o tápala cuando no la estés usando, configura tus mensajes con la opción de "autoeliminación" y evita compartir contenidos que revelen rasgos específicos de tu identidad.

44 Kaspersky. (2016). Sextorsión: una amenaza para todos, en especial para los adolescentes

e. Manipulación con Inteligencia Artificial (IA)

La tecnología en todo el mundo está experimentando una evolución casi ilimitada a través de los sistemas y plataformas disponibles de Inteligencia Artificial (IA)[45]. En este contexto, el uso de la Inteligencia Artificial se ha vuelto preocupante desde el año 2023, ya que si bien está proporcionando muchas herramientas prácticas aplicables a la productividad, educación y creación de contenidos. Representa un riesgo y un foco de atención de VBG digital, ya que con estas herramientas se pueden manipular fotografías, que, en manos de acosadores, "*groomers*" y redes de pornografía utilizan imágenes especialmente de mujeres, niñas y adolescentes para convertirlas en material sexual, pornográfico explícito.

La creciente accesibilidad de esta tecnología ha facilitado la creación de material sexual llamativamente realista y engañoso.[46] Este proceso, de alteración de imágenes facilita que las y los agresoras puedan superponer rostros y voces en fotografías, videos o audios generando así contenido "*deepfake*"[47] pornográfico. En este ámbito, esta herramienta puede ser utilizada para extorsionar, publicar o comercializar contenido ilegal explícito o como una forma de humillación y desacreditación.

De acuerdo a un estudio realizado en el año 2019 por la compañía de ciberseguridad *Deeptrace*, arrojó que un 96% de esta clase de videos y fotografías alteradas eran de naturaleza íntima o sexual y que las principales víctimas eran fundamentalmente mujeres. (Hidalgo, 2023.)

La manipulación de imágenes con Inteligencia Artificial (IA), también supone otros riesgos asociados, ya que este contenido alterado puede ser utilizado para prácticas de suplantación de identidad y cometer otros delitos o accesos no autorizados a información. También existen situaciones donde acosadores pueden fotografiar personas sin su

45 Parlamento Europeo. (2020). La IA permite que los sistemas tecnológicos perciban su entorno, se relacionen con él, resuelvan problemas y actúen con un fin específico. La máquina recibe datos (ya preparados o recopilados a través de sus propios sensores, por ejemplo, una cámara), los procesa y responde a ellos.

46 Autonomía Digital. (2023) Pornografía Deepfake y Violencia de Género.

47 LISA Institute. Los Deepfakes o "falsedades profundas" son archivos de vídeo, imagen o voz manipulados mediante un software de inteligencia artificial de modo que parezcan originales, auténticos y reales.

consentimiento para luego manipular dichas imágenes con fines de generar contenido pornográfico en imagen o video o también relacionar esto a otras formas de violencia como *ciberbullying*, sextorsión, etc.

Otro riesgo relacionado es la facilidad con la que cualquier persona, especialmente NNA, pueden acceder y utilizar de manera nociva a estas herramientas sin necesidad de conocimientos avanzados. De esta manera, las imágenes manipuladas con Inteligencia Artificial se convierten actualmente en una de las principales formas de violencia digital lo que produce un daño a su imagen e integridad.

MEDIDAS DE PREVENCIÓN	MEDIDAS DE ACTUACIÓN
1. Es importante no compartir en redes sociales fotos que puedan ser fácilmente manipuladas y convertidas en contenido explícito. Se recomienda mantener los perfiles en modo privado para evitar que personas desconocidas *bots*[48] accedan y capturen nuestra información.	1. Si una persona tiene acceso a material manipulado, es importante cortar la cadena de difusión de inmediato y denunciarlo a las autoridades competentes.
2. Asimismo, es crucial acceder a fuentes seguras de información. Aunque la Inteligencia Artificial se utiliza para generar material pornográfico, también se emplea para difundir noticias falsas, desacreditar personas, manipular y cometer fraudes.	2. Al revisar imágenes e información recibida, busca fallos en la manipulación de imágenes, como ubicación de elementos extraños, expresiones sin sentido, bordes borrosos, movimientos entrecortados, entre otros.
	3. Cuando recibas información, verifica las fuentes y el origen de la grabación, así como el interés detrás de su publicación.

f. *Sextorsión*

La sextorsión o en el anglicismo "*sextortion*"[49], es una forma de ciberacoso que tienen que ver con la exigencia de material o información íntima con contactos que pueden realizarse por las redes sociales, llamadas o mensajes reiterativos. Esta extorsión

48 Kaspersky. Un "bot", término que proviene de acortar la palabra "robot", es un programa que realiza tareas repetitivas, predefinidas y automatizadas. Los bots están diseñados para imitar o sustituir el accionar humano.

49 Asociación REA. La Sextorsión es un tipo de extorsión sexual en la que la persona que sufre el chantaje es amenazada con la publicación y/o la posibilidad de compartir una o varias imágenes suyas, ya sean vídeos o fotografías), en las que está desnuda o realizando actos sexuales.

implica comúnmente la amenaza de difundir información íntima de manera indebida con tus contactos o exponerla en grupos o redes de pornografía. Las y los extorsionadores pueden utilizar varios mecanismos de manipulación haciendo creer a las víctimas que tienen control de todos sus datos y contactos. También puede implicar suplantación de identidad.

Asimismo, en esta forma de extorsión sexual puede implicar la amenaza de divulgar imágenes de índole eróticos y sexual sin autorización o también podrían utilizar imágenes alteradas a través de Inteligencia Artificial (IA) con el objetivo de ejercer control sobre la persona afectada, obtener algún beneficio económico o solicitarle más contenidos privados.

La persona que acosa pide de manera insistente el envío de contenido íntimo que en muchas ocasiones se realiza desde la manipulación con el pretexto de un vínculo romántico (como, por ejemplo: "Si me amas, envíame una foto"[50]. Asimismo, este delito puede ser cometido contra NNA con la amenaza de publicar contenido audiovisual o información personal de carácter sexual[51]. Por lo que este tipo de violencia se convierte en formas de vulneración adicionales como el "*grooming*" y comercialización de pornografía infantil.

MEDIDAS DE PREVENCIÓN	MEDIDAS DE ACTUACIÓN
1. Evita compartir imágenes íntimas a través de redes sociales, aplicaciones de mensajería instantánea o correo electrónico.	1. En casos de "Sextorsión", no cedas al chantaje. No accedas a las demandas, ya que, si lo haces, seguirán extorsionándote.
2. Investiga y utiliza herramientas para proteger tu privacidad, ya que la información puede ser filtrada o manipulada mediante Inteligencia Artificial (IA).	2. Si estás siendo extorsionada o extorsionado, asegúrate de tomar capturas de pantalla de los mensajes y la información relevante para poder realizar una denuncia efectiva.
3. Filtra regularmente tus contactos que acceden a tu información en redes sociales para prevenir riesgos.	3. Es crucial solicitar la eliminación del contenido de todos los sitios o plataformas donde haya sido publicado.

50 Faro Digital. (2022). Guía de acompañamiento a las adolescencias en los entornos digitales, 2022
51 Save The Children. (2019). Violencia Viral.

4. No mantengas conversaciones con personas o usuarios desconocidos, ya que esto aumenta el riesgo de contacto con acosadores o extorsionadores.	4. Busca orientación de fuentes confiables y encuentra alternativas de apoyo y atención especializada para proteger tu seguridad y tu salud física y emocional.
5. No te encuentres con personas que hayas conocido en entornos digitales, ya que siempre existe la posibilidad de que sea un perfil falso.	5. Si conoces a alguien que esté pasando por esto, actúa con empatía y acompaña a la persona que esté sufriendo la difusión no consensuada de su información personal.
6. Ten precaución con las cámaras digitales y cúbrelas para evitar ser grabado sin tu consentimiento.	6. Cuida tu huella digital y protege tu imagen. Es fundamental comprender que toda la información que compartimos en Internet puede volverse pública.
7. Recuerda que el amor no se basa en el control ni en la desconfianza. No compartas contraseñas ni des acceso a información privada como prueba de amor o confianza.	

Recursos Legales: COIP

Art. 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales.

2. La persona que ilegalmente diseñe, desarrolle, ejecute, produzca, programe o envío contenido digital, códigos de acceso o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que posea, venda, distribuya o, de cualquier forma, disemine o introduzca uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior.

g. La privacidad: Nuestra mejor amiga

La privacidad es un derecho fundamental de todas las personas que nos permite tener la capacidad de controlar la información personal en el entorno digital. Implica comprender cómo se recopila, utiliza y comparte nuestra información en línea, así como tomar medidas para proteger nuestra identidad y datos personales ante posibles violaciones de privacidad.

La falta de privacidad puede agravar la desigualdad de género, la discriminación[52] y la exposición a los diferentes riesgos digitales, afectando diversos aspectos de la vida de las personas. Por lo que su conocimiento y análisis es fundamental, especialmente para la protección de NNA.

En la actualidad digital, la privacidad debe ser tema central para promover la seguridad, autonomía y prevenir las consecuencias de los riesgos digitales y la violencia. Conocer, analizar y reflexionar sobre la privacidad es fundamental para la protección de datos personales y la prevención de exposición no deseada de nuestra información en internet.

Al proteger nuestra privacidad, también contribuimos a la seguridad de quienes nos rodean, ya que nuestras acciones en línea pueden afectar no solo nuestra información, sino también la de nuestra familia, amigos y contactos. La seguridad de nuestra información se convierte tanto en una responsabilidad personal como comunitaria. Al protegernos a nosotros mismos, contribuimos a la seguridad de quienes nos rodean.[53]

MEDIDAS DE PREVENCIÓN	MEDIDAS DE ACTUACIÓN
1. Toma conciencia de que La privacidad es un derecho de determinar cuándo, cómo y en qué medida compartimos nuestros datos personales con terceros.	1. La eliminación de comentarios, fotos, videos, información personal u otro contenido que circule a través de dispositivos electrónicos o en el espacio digital depende de la plataforma por la cual se compartió. La desaparición de dicho contenido será parcial o casi definitiva según el sitio donde se encuentre.

52 Naciones Unidas. Normas internacionales relativas a la privacidad digital. El ACNUDH y la privacidad en la era digital
53 Autonomía Digital. (2023). Privacidad en línea.

2. Busca información sobre tutoriales para configurar tu privacidad. La mayoría de las aplicaciones tienen opciones para poner tu perfil en privado, definir qué tipo de información es pública y controlar quién puede acceder o no a tus contenidos. Puedes encontrar estas herramientas explorando tus aplicaciones en las secciones relacionadas con seguridad, privacidad y protección.	2. Eres responsable de tus dispositivos. Nadie más que tú misma será responsable de un mal uso de tus móviles o redes sociales, por lo tanto, no debes dejarlos en manos de nadie, ni siquiera de tu pareja. Ten cuidado a quién le prestas tus dispositivos.
3. Si tienes dudas, contacta a los servicios de ayuda de las aplicaciones para fortalecer tu privacidad en línea.	

Recursos Legales: COIP

Art. 154.2 Hostigamiento.- La persona natural o jurídica que, por sí misma o por terceros o a través de cualquier medio tecnológico o digital, moleste, perturbe o angustie de forma insistente o reiterada a otra, **será sancionada con una pena privativa de la libertad de seis meses a un año**, siempre que el sujeto activo de la infracción busque cercanía con la víctima para poder causarle daño a su integridad física o sexual.

Cuando la víctima sea menor de dieciocho años de edad, o persona con discapacidad o cuando la persona no pueda comprender el significado del hecho o por cualquier causa no pueda resistirlo, será sancionada con pena privativa de libertad de uno a tres años. En los casos que no se configure el delito de instigación al suicidio tipificado en el artículo.

Cuando este ilícito sea cometido por miembros del núcleo familiar o personas con las que se determine que el procesado o la procesada mantenga o haya mantenido vínculos familiares, íntimos, afectivos, conyugales, de noviazgo, de cohabitación, o de convivencia o aún sin ella, se aplicará los presupuestos y la pena establecida en los artículos relativos a la violencia contra la mujer y miembros del núcleo familiar.

Art. 172.- Utilización de personas para exhibición pública con fines de naturaleza sexual.- En la reforma se agrega un artículo, **el Art. 172.1** que habla sobre **Extorsión sexual**, dice que la persona que, mediante el uso de la violencia, amenaza o chantaje induzca, incite y obligue a otra a exhibir su cuerpo desnudo, semidesnudo, o en actitudes sexuales, con el propósito de obtener un provecho

personal o para un tercer, ya sea de carácter sexual o de cualquier otor, será sancionada con pena privativa de libertad de tres a cinco años.

Art. 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

Será sancionada con pena privativa de libertad de uno a tres años quien revele o divulgue a terceros contenidos digitales, mensajes, correos, imágenes, audios o vídeos o cualquier otro contenido íntimo de carácter sexual de una persona en contra de su voluntad.

Art. 170 y artículo 171 sobre Abuso sexual y violación.- La persona que, en contra de la voluntad de otra, ejecute sobre ella o la obligue a ejecutar sobre sí misma u otra persona, un acto de naturaleza sexual, sin que exista penetración o acceso carnal, será sancionada con pena privativa de libertad de tres a cinco años. Cuando la víctima sea menor de catorce años de edad o con discapacidad; cuando la persona no tenga capacidad para comprender el significado del hecho o por cualquier causa no pueda resistirlo; o si la víctima, como consecuencia de la infracción, sufra una lesión física o daño psicológico permanente o contraiga una enfermedad grave o mortal, será sancionada con pena privativa de libertad de cinco a siete años.

En la Ley Orgánica Reformatoria del COIP para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha Contra los Delitos Informáticos, se incluye: "Se sancionará con el máximo de las penas establecidas en los incisos precedentes, cuando dicho abuso sexual fuese grabado o transmitido en video de manera intencional por la persona agresora, por cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación".

3.3 Recurso adicional: Protección y Justicia

Parte de la prevención de la violencia basada en género requiere que se indique a las personas cómo pueden actuar frente a dichas situaciones con información segura, transparente y confidencial nos permite avanzar en la protección y sensibilización comunitaria para mitigar los riesgos y nuevos casos de VBG.

En ese sentido, es necesario promover cuales son las rutas de los accesos a una atención en casos de Violencia Basada en Género, promover y garantizar la defensa de los derechos y

procesos de denuncia con la finalidad de apoyar los espacios de restauración y exigibilidad de las garantías de protección.

Es por ello que, es necesario facilitar y promover la ruta de Violencia Basada en Género como también de las MAPIS (Medidas Administrativas de Protección Inmediatas).[54] Este tipo de medidas tiene como objetivo proteger a la mujer y detener la violencia, no requiere entrega de pruebas, son temporales, son de cumplimiento inmediato y su incumplimiento genera responsabilidad administrativa, civil o penal. (UNFPA, 2022).

Todas las personas independientes de su género, origen, estatus migratorio, creencias religiosas, o cualquier otra característica tienen el derecho a solicita Medidas Administrativas de Protección Inmediata (MAPIS), así también cualquier persona que tenga conocimiento de un hecho de violencia de género.

3.3.1 Ruta de protección ante VBG

Pide Auxilio: El Estado Ecuatoriano ha puesto a disposición una serie de mecanismos de emergencia como lo es ECU 911, 1800 DELITO, Policía Nacional, Red Pública de Salud (hospitales, centros de salud, subcentros de salud, etc. Se pueden pedir certificados médicos dentro de la red.), Servicios de Protección Integral (SPI) del Ministerio de la Mujer y Derechos Humanos (Equipo de protección especial que activa el Sistema Local de Protección). Si alguien es víctima o tiene conocimiento de algún caso de Violencia Basada en Género puede hacer uso de los mecanismos descritos previamente de forma totalmente gratuita. (UNFPA, 2022)

Pide Protección: Todas las personas tienen derecho a Medidas de Protección, en ese orden, para recibirlas se debe realizar una denuncia en cualquiera de los siguientes establecimientos:

- Unidades judiciales.
- Fiscalía General del Estado.
- Junta Cantonal de Protección de Derechos.
- Tenencias Políticas.
- Comisarías de Policía.

54 Medidas de Protección Inmediata (MAPIS) (2022). medidas que se dan de forma inmediata y provisional para detener y evitar la amenaza o vulneración de la vida e integridad de las mujeres, niñas, adolescentes, jóvenes, adultas y adultas mayores. (UNFPA, 2022) https://www.derechoshumanos.gob.ec/7412-2/

- También se incluyen los Servicios de Protección Integral (SPI)[55]

En caso de poseer un certificado médico, se recomienda presentarlo al momento de realizar la denuncia. Una vez realizada la denuncia, se puede acceder a las siguientes medidas de protección:

- Boleta de Auxilio.
- Orden de salida del agresor del domicilio.
- Reintegro al domicilio a la víctima.
- Tratamientos médicos a víctima y familia.
- Botón de alerta (mismo que se gestiona en la Unidad de Policía Comunitaria más cercana y no requiere de una denuncia).

Pide Justicia: El proceso puede seguir más allá de las medidas de protección si la víctima desea seguir con el proceso para obtener justicia y que el daño sea reparado, hay dos formas de proceder:

- **Contravención:** Si el daño inhabilita a la víctima hasta 3 días el caso se procesa en la ***Unidad Judicial*** más cercana (UNFPA, 2022).

- **Delito:** Si el daño inhabilita a la víctima más de 3 días el caso se atiende en la ***Fiscalía General del Estado.***

Restitución de Derechos afectados: Una vez finalizado el proceso judicial, se puede obtener para la víctima una reparación psicológica, física y económica. Esta reparación restituye los derechos, el bienestar de la víctima y de su entorno familiar (UNFPA, 2022).

55 Sistema Nacional Integral para Prevenir y Erradicar la Violencia contra las Mujeres – SNIPEVCM

4. Agenda de Taller

UNIDAD UNO: PRESENTACIÓN Y DINÁMICA		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Preséntate y expón el objetivo del taller. 2. Realiza una dinámica de acuerdo al público objetivo, procura que esta permita al grupo distenderse. 3. Elabora acuerdos comunes y escríbelos en una pizarra o papelotes.	▪ Recuerda que el primer momento te permitirá contar con un grupo distendido y abierto al aprendizaje. ▪ Genera confianza y tranquilidad en el grupo. ▪ Usa tarjetas con los nombres, esto facilitará la relación durante el taller. ▪ Haz que los acuerdos sean participativos y úsalos a lo largo del taller.	▪ Etiquetas para los nombres ▪ Marcadores ▪ Papelotes ▪ Cinta adhesiva

UNIDAD DOS: CONTENIDO POR CADA RIESGO DIGITAL		
VIOLENTÓMETRO		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Explica qué es el "violentómetro"[56] y su función para comprender la dinámica de las relaciones de pareja, especialmente en el contexto de la violencia contra las mujeres. 2. Luego, realiza preguntas aleatorias basadas en un banco de preguntas que ayuden a reflexionar sobre expresiones cotidianas de violencia de género. 3. Finalmente, facilita la reflexión sobre las respuestas y experiencias compartidas en el espacio.	▪ Observa y facilita un diálogo constructivo fomentando la participación activa durante la actividad. Algunos ejemplos de preguntas podrían ser: ¿Tu pareja controla con quién te comunicas?[57] ¿Te ridiculiza u ofende, tanto en persona como de forma virtual? ¿Controla o monitorea tu teléfono o redes sociales? ¿Te exige que le envíes fotografías personales? ¿Te exige compartir constantemente tu ubicación?	▪ Un "violentómetro" y preguntas enfocadas en violencia de género digital. ▪ Material didáctico para facilitar la participación, papel, cartulinas, pinturas

56 El Violentómetro es un material gráfico y didáctico desarrollado originalmente por la Unidad Politécnica de Gestión con Perspectiva de Género del Instituto Politécnico Nacional (México).

57 ESE TIPO NO. Contra todo tipo de violencia hacia las mujeres https://ninguntipodeviolencia.ec/

FINALES ALTERNATIVOS		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Cuenta la siguiente historia ficticia: "María y Juan son dos jóvenes de 18 años que están saliendo desde hace unos meses. Durante una conversación por mensajes, Juan le pide a María que le envíe fotos íntimas. María accede, confiando en Juan. Sin embargo, luego de un tiempo, la relación termina mal y Juan comparte esas fotos de forma maliciosa en redes sociales." 2. Facilita un espacio para discutir las implicaciones emocionales y legales del sexting sin consentimiento y el "revengeporn". Anima a los participantes a expresar sus opiniones y reflexionar sobre cómo estas acciones pueden afectar a las personas involucradas. 3. Divide a los participantes en grupos pequeños y pídeles que propongan finales alternativos para la historia, centrándose en acciones concretas de seguridad en línea que podrían haber evitado o mitigado las consecuencias negativas.	■ Evalúa las acciones individuales y de protección que las y los participantes proponen para intervenir en la situación presentada. Fomenta la discusión sobre la importancia de la privacidad en línea, el consentimiento y las medidas de seguridad digital. ■ Refuerza con las y los participantes los siguientes mensajes: ■ No compartir imágenes íntimas o personales en línea. ■ Mantener actualizados los ajustes de privacidad en redes sociales y aplicaciones de mensajería. ■ NO confiar ciegamente en personas nuevas en línea y establecer límites claros sobre lo que se está dispuesto a compartir. ■ Buscar apoyo y orientación en caso de ser víctima de sexting sin consentimiento o "revengeporn".	■ Hojas, cartulinas, esferos y lápices para que los participantes anoten sus ideas y propuestas.

ENCUENTRA LOS PARES		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Invita a las y los participantes a dibujar a su compañero/a de lado y a describirlo/a incluyendo dos cualidades positivas de esa persona. 2. Proporciona una hoja de papel y lápices de colores. 3. Motiva a las y los participantes a presentar su dibujo. Reitera que el propósito de esta actividad es promover la empatía, el reconocimiento de las cualidades de los demás y la importancia del respeto.	▪ Al finalizar la actividad, promueve una reflexión sobre la importancia de reconocer y valorar las cualidades positivas de los demás, fomentando así la empatía y el respeto en las interacciones diarias.	▪ Hojas de papel y pinturas o lápices de colores. ▪ Puedes incluir un papelógrafo o pizarra para ubicar todos los dibujos.

GROOMING ACOSO SEXUAL INFANTIL EN MEDIOS DIGITALES: CAPERUCITA ROJA Y LAS MENTIRAS		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Prepara una selección de 10 imágenes, de las cuales 2 sean generadas por Inteligencia Artificial (IA) y las restantes sean imágenes reales. 2. Organiza a los participantes en parejas o grupos pequeños y distribuye las imágenes de manera aleatoria entre ellos. 3. Ubica las imágenes al revés sobre una mesa de forma ordenada y establece turnos para que los equipos abran las imágenes de par en par. 4. Al finalizar el tiempo, invita a las y los participantes a compartir sus conclusiones y a señalar cuáles 5. consideran que son las imágenes generadas por IA. 6. Comparte las respuestas correctas y brinda una breve explicación sobre cómo la IA puede generar imágenes muy realistas y cómo esto puede tener implicaciones en la seguridad digital.	■ Observa la participación activa de los participantes durante la actividad. ■ Evalúa la capacidad de los participantes para discernir entre imágenes generadas por IA e imágenes reales. ■ Promueve una discusión posterior sobre la importancia de la educación digital en la prevención de riesgos digitales y la necesidad de conocer las tecnologías de IA.	■ 10 imágenes (2 generadas por IA y 8 imágenes reales). ■ Espacio adecuado para la actividad. ■ Cartulinas o pizarras para que los participantes anoten sus conclusiones.

ÁRBOL DE CAUSAS		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Prepara un papelógrafo con la forma de un árbol, dibujando raíces, tronco, hojas y frutos tanto en buen estado como en mal estado. Coloca imágenes que representen la violencia de género y los riesgos de “sextorsión” en las partes del árbol en mal estado (raíces, tronco, hojas y frutos). 2. Distribuye tarjetas o notas adhesivas a las y los participantes. 3. Posteriormente, solicita que escriban en los post-it qué acciones se pueden realizar para prevenir y actuar ante situaciones de “Sextorsion”, así como las herramientas disponibles para prevenir e invita a pegar sus post-it en las partes correspondientes. 4. Realiza una retroalimentación grupal para discutir las reflexiones expresadas en las tarjetas y para identificar aprendizajes y posibles mejoras en futuras actividades similares.	■ Fomenta la participación activa de las y los participantes durante la actividad. ■ Extrae opiniones y reflexiones expresadas en las tarjetas. ■ Promueve un diálogo alrededor de empatía y comprensión. ■ Concluye aprendizajes y nuevas herramientas para contribuir a la seguridad en línea y la prevención de la “Sextorsión”.	■ Papelotes con la forma de un árbol y dibujos representativos. ■ Tarjetas o notas adhesivas. ■ Marcadores.

LA SABANA INVERSA		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Los participantes se colocan de pie sobre una tela o papel grande que representa una “sábana”. Esta “sabana” representa la seguridad y privacidad en línea. Deben ocupar la mitad de la superficie de la tela. 2. El objetivo es que las y los participantes trabajen juntos para darle la vuelta a la sábana sin salirse de ella. Para hacerlo deben comunicarse, coordinarse y tomar decisiones en grupo para lograr este objetivo. 3. Una vez que hayan completado la dinámica, se lleva a cabo una sesión de reflexión que comparte sus impresiones sobre los fallos y aciertos durante la actividad. En este paso, se debe facilitar analogías que contribuyan a una mayor sensibilización sobre la importancia de la privacidad.	■ Observa la capacidad de los participantes para trabajar en equipo y colaborar para lograr un objetivo común. ■ Analiza las reflexiones y opiniones expresadas para identificar aprendizajes sobre acciones prácticas y directas para cuidad la privacidad de las personas. ■ Se recomienda presentar y revisar configuraciones de privacidad en las principales redes sociales y canales de mensajería instantánea.	■ Tela o papel grande que represente una “sábana”. ■ Espacio amplio para realizar la actividad de forma segura.

UNIDAD TRES: RUTA DE PROTECCIÓN Y CIERRE		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Asigna a cada participante una tarjeta con un rol relacionado con la ruta de protección ante VBG (víctima, testigo, autoridad, médico, etc.). 2. Plantea una situación hipotética de VBG y pide a los participantes que actúen según su rol asignado, considerando los pasos que se deben seguir en la ruta de protección (pide auxilio, pide protección, pide justicia). 3. Fomenta la interacción y la discusión entre las y los participantes. 4. Muestra la presentación visual o cartel con la información clave sobre la ruta de protección ante VBG en Ecuador. 5. Invita a las y los participantes a compartir sus reflexiones, preguntas y experiencias relacionadas con la dinámica y la información presentada.	▪ Facilitar un espacio para que los participantes compartan sus percepciones, preguntas y reflexiones sobre la ruta de protección ante VBG en Ecuador. ▪ Facilita un espacio para que los participantes expresen sus opiniones sobre la dinámica y cómo esta les ayudó a comprender mejor la ruta de protección ante VBG en Ecuador.	▪ Hojas de papel y marcadores. ▪ Tarjetas con roles (víctima, testigo, autoridad, médico, etc.). ▪ Presentación visual o cartel con la información clave sobre la ruta de protección ante VBG en Ecuador.

Capítulo III

UN CUENTO

PARA NO CAER EN CUENTOS

UN CUENTO PARA NO CAER EN CUENTOS

1. Objetivo General

Sensibilizar a niños, niñas, adolescentes y cuidadores sobre los principales riesgos digitales y la importancia de acceder a información confiable, a través de actividades lúdicas y participativas.

2. Público Objetivo

- Niñas y niños de cualquier edad
- Personal que trabaja con niños y niñas

3. Principales definiciones

3.1 Datos de interés

En la etapa de vida que se encuentran las niñas, niños y adolescentes, exploran y experimentan con su propia identidad, sexualidad o relaciones sociales para mejorar su autoconocimiento y reforzar su autoestima. En este proceso, niñas, niños y adolescentes encuentran en los entornos digitales, un mundo de posibilidades y ventajas, pero también están expuestos a peligros que ponen en riesgo su seguridad física y mental.

En este contexto enfrentan mayores riesgos causados por la desinformación, la sobreexposición al internet y las redes sociales, el ciberbullying, así como otros riesgos dentro de su entorno presencial y virtual. Aunque existen herramientas, aplicaciones y sitios en línea creados específicamente para NNA, no todo el contenido que encuentran es adecuado para ellos.

Comúnmente, ante su falta de experiencia, de información y de controles parentales, NNA se sienten cómodos usando dispositivos e internet puesto que les suele parecer un entorno seguro. Sin embargo, en los fenómenos de violencia e identificación de los diferentes riesgos digitales de manera directa o indirecta, accidental o voluntariamente están expuestos a contenido inadecuado, peligroso o inapropiado.

Es necesario educar a NNA, así como a las y los adultos a su cuidado, sobre la importancia de proteger su privacidad en línea, configurar la privacidad en todas las plataformas digitales, evitar compartir información privada con desconocidos y establecer herramientas de control parental, protección de la privacidad y acceso a información adecuada que contribuyan a prevenir y actuar ante situaciones de violencia en los entornos digitales.

La metodología “Un cuento para no caer en cuentos” surge como una respuesta a esta necesidad urgente de educar a NNA sobre cómo identificar y evitar los principales riesgos digitales. Al utilizar títeres como herramienta pedagógica, esta metodología ofrece un enfoque lúdico y participativo que permite a los niños y niñas involucrarse activamente en el proceso de aprendizaje.

Esta metodología fue diseñada en colaboración con el proyecto "**Manos que cuidan**" del IRC con el propósito de contribuir al desarrollo integral de la primera infancia, de esta manera, esta herramienta ha proporcionado un marco propicio para abordar los riesgos digitales a través de presentaciones de títeres y cuentos adaptados a cada situación de riesgo.

La elección de los títeres como medio de enseñanza se basa en su capacidad para crear un ambiente seguro y atractivo donde los NNA pueden explorar conceptos complejos de manera accesible. Además, la interacción con títeres fomenta el desarrollo del pensamiento crítico al estimular la reflexión sobre diferentes puntos de vista y la toma de decisiones, habilidades fundamentales para discernir la información veraz de la desinformación (Livingstone, 2004).

La integración de InfoPa'lante como recurso central en la actividad complementa esta estrategia al proporcionar a los NNA acceso a información verificada y segura. Al familiarizarse con esta plataforma como una fuente confiable de información, las y los participantes están mejor equipados para discernir entre información verdadera y falsa, fortaleciendo así su capacidad para enfrentar los riesgos digitales.

a. Exposición de niñas, niños y adolescentes a riesgos digitales

Los NNA son especialmente vulnerables a los riesgos digitales debido a su creciente exposición a plataformas en línea y su relativa falta de habilidades para evaluar críticamente la información que encuentran (Livingstone, 2004). Además, la abundancia de contenido digital no verificado y la facilidad con la que se comparte en redes sociales pueden llevar a la internalización de creencias erróneas y la adopción de comportamientos riesgosos o perjudiciales (Ferrara et al., 2016).

De este modo, uno de los aspectos más relevantes cuando se aborda este tema, es la temprana exposición a la tecnología y la complejidad de generar herramientas que posibiliten un uso cuidado y protegido por parte de NNA.[58] Especialmente para comenzar a utilizar las redes sociales.

58 Faro Digital (2022). Guía de acompañamiento a niños y niñas en los entornos digitales.

Por otro lado, el mal uso de las redes sociales en una etapa de "especial vulnerabilidad" como la niñez y la adolescencia puede agravar las situaciones de acoso escolar a través del *ciberbullying* o ciberacoso facilitados por la falta de controles, desconocimiento de la privacidad en línea y ataques externos como el acceso a información inadecuada y la Inteligencia Artificial (IA) y la suplantación de la identidad.[59]

En este contexto, es fundamental desarrollar estrategias educativas que equipen a NNA con las habilidades necesarias para protegerse y promover conductas saludables para prevenir consecuencias relacionadas al excesivo uso de tecnología, ya que esta puede afectar su desarrollo físico, mental y social, provocando problemas como retraso en el desarrollo, desórdenes alimenticios, alteraciones del sueño, enfermedades y otros síntomas.

El entorno digital contemporáneo presenta una serie de riesgos para NNA que los expone a delitos de "*grooming*", pornografía infantil, Trata de Personas, desapariciones, entre otros.

b. Principales riesgos digitales para niñas, niños y adolescentes

59 *Amnistía Internacional. (2017).*

¿CÓMO SE LLAMA?	¿QUÉ ES?
Contactos y relaciones inadecuadas	A través de los diferentes juegos en línea, redes sociales y canales de mensajería instantánea, NNA pueden tomar contacto con acosadores, "groomers" o participar en conductas inadecuadas para su edad. De esta manera, se exponen a que sean manipulados y extorsionados para compartir información personal, fotos o videos de carácter sexual.
Videojuegos con enfoque violento	Los videojuegos violentos a los que tienen acceso, usualmente tienen contenido que no es apropiado para su edad y producen comportamientos violentos, sexuales y discriminatorios. Debido a la edad de los NNA lo que está en pantalla se puede confundir con la realidad.
Retos virales e incitación a conductas dañinas	Son un riesgo potencialmente peligroso que puede afectar su integridad y la de los demás. Consisten usualmente en diferentes niveles de retos que pueden poner en riesgo la integridad física y emocional e incluso llegar al suicidio[60] o comportimientos lesivos contra otras personas. En este tipo de riesgo, se pueden incluir sectas y grupos violentos o que infunden el "terrorismo" y que a través del convencimiento y creación de un "aparente" sentido de pertenencia reclutan niñas, niños y adolescentes y les convencen de que estar dentro de estos grupos es la única manera de vivir.
Exposición involuntaria a material sexual y/o violento	NNA podrían estar expuestos al acceso ilimitado a Internet, realizar búsquedas o descargar archivos en principio completamente inocentes, pero que pueden incluir enlaces maliciosos y material de escenas sexuales o violentas. También es posible que este contenido sea enviado o publicado por una persona desconocida, familiar, amigo o amiga, bien mediante un chat o que utilice algún dispositivo para obligarle a mirar.[61] Este contenido usualmente pueden incluir enlaces de "phishing", discursos de odio.

60 La verdadera historia del reto suicida de la "Ballena Azul" que se hizo viral en internet - BBC News Mundo

61 ChildFund. (2019). VIOLENCIA VIRAL

MEDIDAS DE PREVENCIÓN	MEDIDAS DE ACTUACIÓN
1. Lo más importante es retrasar al máximo el acceso a dispositivos de uso individual como el celular o la tableta electrónica.	1. Es fundamental acompañar en la exploración digital de niñas, niños y adolescentes a través de aplicaciones diseñadas para su edad y el análisis sobre el contenido encontrado.
2. Si los NNA han comenzado a utilizar dispositivos electrónicos e Internet, es importante supervisar su acceso a los dispositivos, el compartimiento de información, así como los juegos y aplicaciones que utilizan.	2. Para identificar si un menor de edad está siendo víctima de algún peligro en línea, presta atención a cualquier manifestación física o de conducta que pueda revelar que están teniendo experiencias negativas en internet. Algunos síntomas comunes que podrían ayudar a identificar esto son cambios en el comportamiento, conflictos de identidad, desconfianza, búsqueda de atención y reconocimiento, pérdida de habilidades sociales, problemas de rendimiento escolar, dificultades en la convivencia.[62]
3. Configura la privacidad de los perfiles en juegos y aplicaciones que utilicen, asegurándote de que estén diseñados y dirigidos específicamente a NNA de su edad.	
4. Educa en casa sobre los riesgos digitales, la importancia de la huella digital, y los riesgos asociados a la publicidad y enlaces maliciosos que a menudo se encuentran en los juegos y pueden exponerlos a contenidos inapropiados, violencia, robo de información, entre otros.	3. Es importante crear un espacio de diálogo respetuoso y sin distracciones donde se pueda hablar de los riesgos sin señalar ni juzgar.

62 Faro Digital (2022). Guía de acompañamiento a niños y niñas en los entornos digitales.

Recursos legales: Código de la Niñez y Adolescencia.

Art. 46.- Prohibiciones relativas al derecho a la información.- Se prohíbe 1. La circulación de publicaciones, videos y grabaciones dirigidos y destinados a la niñez y adolescencia, que contengan imágenes, textos o mensajes inadecuados para su desarrollo; y cualquier forma de acceso de NNA a estos medios;

Derechos de protección

Art. 50.- Derecho a la integridad personal.- Los NNA tienen derecho a que se respete su integridad personal, física, psicológica, cultural, afectiva y sexual. No podrán ser sometidos a torturas, tratos crueles y degradantes.

Art. 52.- Prohibiciones relacionadas con el derecho a la dignidad e imagen. Se prohíbe en el inciso 1. La participación de NNA en programas, mensajes publicitarios, en producciones de contenido pornográfico y en espectáculos cuyos contenidos sean inadecuados para su edad.

RECURSOS LEGALES: COIP

Art. 168.- Distribución de material pornográfico a niñas, niños y adolescentes.- La persona que difunda, venda o entregue a niñas, niños o adolescentes, material pornográfico, será sancionada con pena privativa de libertad de uno a tres años

Art. 169.- Corrupción de niñas, niños y adolescentes.- La persona que permita el acceso o exposición de niñas, niños y adolescentes de forma intencionada a contenido nocivo sexualizado, violento o que llame a cometer actos de odio será sancionada con pena privativa de uno a tres años. La persona que incite, conduzca o permita la entrada de niñas, niños o adolescentes a prostíbulos o lugares en los que se exhibe pornografía, será sancionada con pena privativa de libertad de tres a cinco años.

c. Falta de control parental en internet

Según la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador, el control parental es una herramienta que busca monitorear, restringir o bloquear el acceso de NNA a sitios *web* cuyo contenido sea inapropiado o ponga en riesgo su integridad. También permite establecer un tiempo límite para el uso de dispositivos como computadoras, TV, smartphones, tablets y cualquier otro dispositivo que tenga acceso a una red WiFi.

Se recomienda el uso de control parental para NNA de entre 4 y 18 años debido a que ellos y ellas comienzan su aprendizaje digital en la escuela y en sus hogares a temprana edad, lo que implica una mayor exposición a internet conforme crecen, aumentando así el uso de dispositivos y redes sociales.

El control parental es indispensable si NNA disponen de teléfono móvil u otro dispositivo con acceso a Internet. Es absolutamente necesario para limitar el acceso a contenidos, videos y sitios web que se consideren peligrosos o no adecuados para su edad, o simplemente para saber qué tipo de contenido están consumiendo.

Los controles parentales son aplicaciones que las personas adultas pueden configurar en los dispositivos electrónicos con

conexión a internet para que los buscadores y plataformas solo ofrezcan contenidos adecuados a las edades de los NNA.

El control parental a través de herramientas tecnológicas disponibles y la supervisión personal contribuye a evitar que los NNA sean contactados o se comuniquen con personas desconocidas previniendo así casos de *grooming*, ciberacoso, *sexting*, sextorsión, entre otros.

Entre las principales funciones de las herramientas de control parental están: limitar el tiempo de uso y los horarios en que los NNA utilizan aplicaciones en sus dispositivos móviles, así como establecer hábitos saludables para su uso. Además, funcionan para controlar la descarga de las aplicaciones que los NNA deseen instalar en sus dispositivos móviles, evitar compras en línea no deseadas, activar la geolocalización de los dispositivos para conocer en tiempo real su ubicación y permiten la supervisión de los dispositivos para conocer qué están haciendo y ofrecer asistencia remota en la solución de situaciones de riesgos.

Toma en cuenta algunas recomendaciones para el control parental

1. Fomentar el diálogo y llegar a acuerdos con los NNA basados en la confianza, es indispensable para establecer formas de acceso y uso de los dispositivos, así como para limitar el tiempo que pasan en internet. Habla con ellos y ellas sobre los riesgos digitales a los que están expuestos para que puedan desarrollar criterios propios y aprender a seleccionar contenidos adecuados a su edad. También es crucial enseñarles sobre la importancia de NO compartir imágenes íntimas o información sensible.

2. Si han decidido abrir un perfil infantil en algún juego o aplicación, asegúrate de configurar la privacidad y, en la medida de lo posible, mantener los perfiles en privado. Oculta su identidad utilizando un nombre distinto y evita publicar datos personales.

3. Explora herramientas de control parental, ya que la supervisión de los contenidos digitales es esencial para garantizar experiencias seguras y educativas. Las herramientas de monitorización llevan un registro de las páginas visitadas y el tiempo de navegación, mientras que las de filtro de contenidos bloquean y restringen el acceso a sitios inadecuados. Además, es importante mantener actualizado el antivirus y las aplicaciones en el dispositivo.

4. Controla su participación en foros, videojuegos y chats en línea para asegurarte de que sean seguros y adecuados para su edad. Fomenta actividades fuera de línea como juegos de mesa, deportes y lectura en familia.

5. Anima a los NNA a reflexionar sobre su tiempo en pantalla y a hablar sobre cómo se sienten. Enséñales a verificar la autenticidad de la información en línea y cómo identificar noticias falsas y contenidos engañosos.

6. Si bien el control parental es útil, también es necesario complementarlo con la enseñanza de habilidades como el pensamiento crítico, la confianza y la resiliencia. Genera confianza para que te alerten sobre interacciones incómodas o riesgosas y para prevenirles sobre riesgos y delitos cometidos en internet.

4. Agenda de taller

UNIDAD UNO: PRESENTACIÓN Y DINÁMICA		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Preséntate y expón el objetivo del taller. 2. Realiza una dinámica de acuerdo al público objetivo, procure que esta permita al grupo distenderse. 3. Elabora acuerdos comunes y escríbalos en una pizarra o papelotes.	▪ Recuerde que el primer momento le permitirá contar con un grupo distendido y abierto al aprendizaje. ▪ Genere confianza y tranquilidad en el grupo. ▪ Use tarjetas con los nombres, esto facilitará la relación durante el taller. ▪ Haga que los acuerdos sean participativos y úselos a lo largo del taller.	▪ Etiquetas para los nombres. ▪ Marcadores. ▪ Papelotes. ▪ Cinta adhesiva.

UNIDAD DOS: CONTENIDO		
ROLES Y SIMULACIONES DE SITUACIONES EN LÍNEA		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. Diseña una serie de roles o personajes relacionados con situaciones de riesgo en línea, como un acosador en redes sociales, un amigo que comparte información privada sin permiso, un niño o niña que es víctima de ciberbullying. 2. Divide a las y los participantes en grupos pequeños y asigna a cada grupo un rol diferente. Entrega las descripciones de los roles a cada grupo y explícales que tendrán que actuar la situación que se les asignó. 3. Indica a los grupos que actúen la situación, pueden hacerlo a través de una dramatización, una exposición, una entrevista periodística o mediante otra actividad que facilite la participación lo que permitirá identificar las posibles consecuencias de estos riesgos. 4. Pregunta a las y los participantes sobre sus observaciones, cómo se sintieron al actuar esos roles y qué aprendieron sobre los riesgos a niñas, niños y adolescentes.	▪ Observa la capacidad de las y los participantes para comprender las diferentes perspectivas y roles relacionados con la seguridad en línea de NNA. ▪ Evalúa la participación activa y las contribuciones durante la actuación de los roles y la discusión posterior. ▪ Refuerza la comprensión de las y los participantes sobre los riesgos digitales a los que están expuesto NNA y prácticas de seguridad digital.	▪ Descripciones de roles o personajes relacionados con situaciones en línea. ▪ Espacio para las actuaciones y la discusión grupal.

PRESENTACIÓN DE TÍTERES		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
1. En esta actividad, se realizará una presentación de títeres basada en el guion proporcionado titulado “Un cuento para no caer en cuentos”. El objetivo principal es educar y concienciar a los NNA sobre los riesgos digitales que pueden enfrentar en línea, en este caso relacionado a los riesgos de la Trata de Personas. 2. La metodología de esta actividad se puede implementar a través de la creación de nuevas historias que aborden los diferentes riesgos y necesidades educativas y de información de niñas, niños y adolescentes.	La evaluación de esta actividad se realizará de la siguiente manera: ■ Participación de la audiencia: Se evaluará el nivel de participación e interacción de los NNA durante la presentación ■ Comprensión del mensaje: Se evaluará si los participantes comprendieron los mensajes y consejos relacionados con la seguridad digital transmitidos durante la presentación. ■ Impacto emocional: Se evaluará el impacto emocional de la presentación en los participantes, especialmente en cuanto a la comprensión de situaciones de riesgo y cómo abordarlas.	■ Dos títeres de personajes. ■ Escenografía con telón negro y cortinas amarillas. ■ Juguetes variados adecuados para diferentes edades. ■ Promotor/a o moderador/a para la interacción con la audiencia. ■ Música de fondo para la presentación. ■ Espacio adecuado para la presentación con buena visibilidad para la audiencia.
UNIDAD TRES: HÁBITOS DE UNA CULTURA DIGITAL RESPONSABLE Y CIERRE		
ACTIVIDAD	**RETROALIMENTACIÓN**	**MATERIALES**
■ Moderar un diálogo abierto y participativo para intercambiar recursos y experiencias que contribuyan a la prevención de riesgos digitales.	■ ¿Qué aprendí y cómo lo aplicaré en mi vida? ■ ¿Cuál es mi compromiso con la prevención de riesgos digitales?	Dinámica de cierre.

5. Guión de títeres

UN CUENTO PARA NO CAER EN CUENTOS:

Sami y Mai ante los retos peligrosos

Acto A: ¡La bienvenida!

Moderador o moderadora: ¡Hola amiguitas y amiguitos! Hoy les vamos a presentar una historia llamada "Un cuento para no caer en cuentos: Sami y Mai ante los retos peligrosos". Vamos a hablar sobre los peligros en internet y cómo podemos protegernos. ¿A quién le gusta navegar en internet? (Interacción con la audiencia). ¡Genial! Vamos a conocer a unos amigos y amigas que tienen una historia muy importante que contarles.

(El telón se abre y los títeres aparecen en el teatrino)

Títere animal (Sami): (Cantando y bailando al ritmo de la canción "Chu Chu Ua") ¡Eh! ¡Eh! ¡Eh! "Chu chu ua, chu chu ua, ua, ua" Un viaje sideraaaal que en tu computadora puedes realizaaaar

https://www.youtube.com/watch?v=Asl3wa6OFo0

Títere persona (Mai): (Se encuentra en la esquina del teatrino apenada)

Sami: ¿Qué te pasa, Mai? ¿Por qué estás triste?

Mai: Sami, no sé si deba contarte... (lo dice de manera tímida y un poco temerosa).

Sami: Cuéntame, tranquila, recuerda que somos amigos y estamos siempre para apoyarnos.

Mai: Tienes razón, es un espacio seguro.

Moderador o moderadora: (En voz baja pregunta a la audiencia) ¿Niños y niñas, es un espacio seguro? (Interacción con las y los participantes).

Mai: Oh, buenos días/tardes, qué gusto verlos y verlas, yo me llamo Mai y él es Sami.

Sami: Yo soy Sami, pero ya lo saben (sonríe). Pero bueno, cuéntanos, Mai, ¿Qué pasa? ¿Por qué estás triste?

Mai: Estoy triste porque me metí en un reto en internet y ahora me siento muy mal.

Sami: Oh no, Mai. ¿Qué pasó? ¿Qué reto era? (preocupada)

Mai: Era el reto de la Tonina o del Delfín Rosado. Al principio parecía un juego divertido, pero después se puso muy peligroso.

Sami: ¿Tonina o El Delfín Rosado? ¿Qué es eso?

Mai: Es un reto que tiene muchos niveles. Al principio, te piden hacer cosas sencillas, pero luego se vuelve muy peligroso y te hacen hacer cosas que pueden lastimarte.

Moderador o moderadora: Estatuas (Dice a la audiencia y a los títeres). ¿Ustedes han escuchado del reto del Delfín Rosado o Tonina? ¿Saben qué es? (Interacción con el público y explicación de ser necesaria).

Sami: ¡Oh no, Mai! ¿Qué te hicieron hacer?

Mai: Primero me pidieron que viera una película de miedo a medianoche. Luego me dijeron que tenía que cortarme el cabello. Me dio mucho miedo y no sabía a quién contarle.

Sami: ¡Eso suena terrible, Mai! Los retos como esos son muy peligrosos y pueden hacer mucho daño físico y psicológico.

Moderador o moderadora: Niños y niñas, ¿qué piensan de lo que le pasó a Mai? ¿Es algo seguro? (Interacción con la audiencia).

Mai: Realmente fue muy difícil. No solo me asusté, sino que también me sentí muy sola y preocupada.

Sami: Mai, ¿por qué seguiste el reto si era tan peligroso?

Mai: Porque me dijeron que, si no lo hacía, algo malo le pasaría a mi familia. Me sentí atrapada y no sabía qué hacer.

Moderador o moderadora: Niños y niñas, ¿ustedes qué harían en una situación así? (Interacción con la audiencia).

Sami: Mai, hay mucha información falsa y peligrosa en internet. Siempre debemos hablar con un adulto de confianza si algo nos preocupa o asusta.

Mai: Sí, ahora sé que debería haber hablado con mi padre, madre o con un maestro. Es muy importante buscar apoyo en alguien de confianza.

Sami: Así es, Mai. Además, hay personas en internet que te pueden pedir información personal, como tu nombre, dirección o fotos. Nunca debemos dar esa información a personas que no conocemos.

Mai: Sí, una vez me pidieron que enviara una foto y me dio miedo, pero ahora sé que debo decirle a una persona adulta cuando algo así pase.

Sami: Y si no sabes a quién acudir, siempre puedes buscar ayuda en InfoPa'Lante (en tono entusiasmado).

Moderador o moderadora: Niños y niñas, ¿han escuchado hablar de InfoPa'Lante? (Interacción con el público participante).

Mai: Les cuento amiguitas y amiguitos que InfoPa'Lante es un servicio que nos da información confiable y segura. Podemos preguntar si algo es peligroso y hay alguien que nos puede guiar.

Sami: Sí, sí. InfoPa'Lante es muy importante porque allí siempre puedes encontrar

ayuda y orientación sobre los peligros en internet.

Mai: ¡En serio! No sabía de esto, pero ahora se lo voy a contar a toda mi familia.

Sami: Sí**,** y no te olvides de siempre pedir ayuda si no estás segura de algo que ves en internet. Juntos y juntas, podemos encontrar una solución.

Mai: Gracias, Sami. Y gracias a ustedes, amiguitos y amiguitas, por escucharme.

Moderador o moderadora: Ahora que Mai ha compartido su historia, es muy importante que también escuchemos a las personas adultas responsables. (Dirigiéndose a las personas adultas presentes). Queridas y queridos cuidadores, ¿cómo pueden ustedes ayudar a los niños y niñas a estar seguros en internet? (Interacción con las personas adultas).

(Posibles respuestas de las personas adultas: supervisar el uso de internet, hablar abiertamente sobre los peligros, establecer reglas claras, etc.)

Moderador o moderadora: ¡Exactamente! Es muy importante que las personas adultas estén atentos y hablen con los niños sobre lo que hacen en internet. También pueden usar recursos como InfoPa'Lante para encontrar guías y ayuda en estos casos. Recuerden que es un canal de orientación en línea que está disponible en *Facebook, WhatsApp, Instagram, TikTok* y su página *web*.

Mai: Sí, es importante que los adultos estén siempre presentes y dispuestos a escuchar.

Sami: Y recuerden, siempre busquen apoyo de una persona adulta de confianza y, si necesitan más ayuda, InfoPa'Lante está allí para ustedes.

Acto B: ¡La despedida!

Mai: ¡Uf, uf! ¡Qué cansada estoy! Me la pasé muy bien compartiendo mi experiencia con ustedes, gracias por ser un espacio seguro. Y tú, Sami, ¿Cómo la pasaste?

Sami: Yo la pasé estupendo. Me gustó mucho estar con ustedes y

espero que hayan aprendido algo muy importante hoy. Yo aprendí mucho sobre lo importante que es estar seguros en internet.

Moderador o moderadora: ¿Qué fue lo que más les gustó? ¿Qué aprendieron hoy? (Interacción con la audiencia).

Mai: ¡Qué bueno escuchar todo lo que aprendieron! Espero que sigan siendo cuidadosos en internet y siempre hablen con un adulto de confianza.

Sami: Recuerden siempre buscar ayuda de una persona de confianza si algo en internet les preocupa. Y cuidadores, es importante estar atentos y atentas al consumo de información en redes sociales de los niños y niñas.

Moderador o moderadora: Es muy importante que entiendan qué es un delito. Un delito es cuando alguien hace algo muy malo y peligroso que está prohibido por la ley. Los retos peligrosos en internet pueden llevar a cometer delitos o a ser víctimas de ellos. Por ejemplo, pedir información personal y usarla para hacer daño es un delito. (Explica más si es necesario).

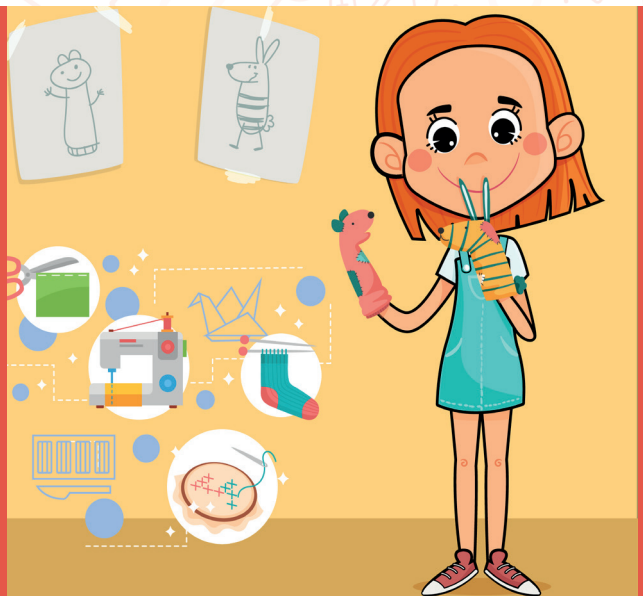
Mai: Me alegra haber podido contar mi experiencia en este espacio seguro. Espero que les haya sido de ayuda y que nadie más se una a estos retos peligrosos.

Sami: Recuerden que InfoPa'Lante es un lugar donde pueden encontrar guías y ayuda para estos casos. No duden en usarlo.

Mai: Sí, juntos y juntas podemos protegernos y estar seguros en el mundo digital.

Sami y Mai: ¡Gracias y hasta pronto! (suena la canción del inicio)

Recuerda que puedes elaborar tú mismo los títeres[63], puedes para ello utilizar material reciclado como un calcetín y hacerlo junto con las niñas y niños, aquí unas ideas, lo más importe es, ¡tu creatividad!



63 Como hacer un Títere con un calcetín - Manualidades para todos (youtube.com)

Bibliografía

Anderson, D. R., & Loomis, M. K. (2012). The effectiveness of puppetry and digital media in promoting science concepts in young children. Journal of Educational Psychology, 104(1), 239-254.

Amnistía Internacional, Educación en Derechos Humanos (EDH). (2017.) Los peligros de las redes sociales para NNA. Recuperado de https://www.amnistia.org/ve/blog/2017/05/2705/los-peligros-de-las-redes-sociales-para-ninos-ninas-y-adolescentes#:~:text=El%20mal%20uso%20de%20las,alguien%20que%20no%20desea%20recibirlos

Agencia de Regulación y Control de las Telecomunicaciones, Consejo Nacional para la Igualdad Intergeneracional. (2022). Recomendaciones para configuración del control parental. Recuperado de https://cnt-media.boxqos.com/legals/Informaci%C3%B3n%20al%20p%C3%BAblico/recomendaciones-para-configuracion-del-control-parental.pdf

Asamblea Nacional. (05 de febrero de 2018). Reglamento Ley Orgánica Integral para Prevenir y Erradicar la Violencia Contra las Mujeres en Ecuador. Modificado Quito. Ecuador. https://oig.cepal.org/sites/default/files/2018_ecu_reglamento-general-de-la-ley-organica-integral-para-prevenir-y-erradicar-la-violencia-contra-las-mujeres.pdf

Asamblea Nacional. (2021). Ley Orgánica Integral para Prevenir y Erradicar la Violencia Contra las Mujeres en Ecuador. Última Reforma del Registro Oficial 30 de agosto de 2021. Quito. Ecuador. https://biblioteca.defensoria.gob.ec/bitstream/37000/3366/1/Ley%20Violencia%20contra%20las%20mujeres%20%2830-08-2021%29.pdf

Buckingham, D. (2019). Medios digitales en la vida cotidiana infantil: Una visión crítica. Comunicar, 27(58), 7-16.

Coomeva. (2021). *El Violentómetro*. Coomeva. https://www.coomeva.com.co/en_equidad/publicaciones/171816/el-violentometro/#:~:text=As%C3%AD%20lo%20indica%20el%20Violent%C3%B3metro,y%20Ciencias%20de%20la%20Educaci%C3%B3n

Diego, M., Córdova Páez, A., Godoy, S., & Paz, P. (2020). *Diagnóstico de Violencia de Género Digital en Ecuador*. CC Creative Commons.

EDUC.AR Portal.(2020). Cuidados y seguridad al utilizar redes sociales: Instagram y TikTok

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. Communications of the ACM, 59(7), 96-104.

Gaptain. (s.f). CONTACTOS PELIGROSOS EN REDES SOCIALES. Recuperado de https://gaptain.com/contactos-peligrosos-redes-sociales/

González, J. L. (2010). Learning and instructional technologies for the 21st century: Visions of the future. Springer Science & Business Media.

Hidalgo, N. (2023) Deepfakes: violencia basada en género en la era de la inteligencia artificial. Recuperado de https://blogs.iadb.org/igualdad/es/deepfakes-violencia-basada-en-genero-inteligencia-artificial/

Hobbs, R. (2010). Digital and media literacy: A plan of action. Aspen Institute.

International Rescue Committee (2023). Manos que cuidan. Recuperado de https://www.rescue.org/primera-infancia-desarrollo-economico-ecuador

Livingstone, S. (2004). Media literacy and the challenge of new information and communication technologies. The Communication Review, 7(1), 3-14.

Livingstone, S., & Helsper, E. (2008). Parental mediation of children's internet use. Journal of Broadcasting & Electronic Media, 52(4), 581-599.

Medina, V. (2022). 10 motivos para prohibir los smartphone a niños menores de 12 años. Guía Infantil. Recuperado de https://www.guiainfantil.com/articulos/educacion/nuevas-tecnologias/10-motivos-para-prohibir-los-smartphone-a-ninos-menores-de-12-anos/

Organización Mundial de la Salud. (2021). Temas de Salud. Obtenido de Violencia: https://www.who.int/topics/violence/es/

Organización de las Naciones Unidas (2001). Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. Asamblea General, resolución 55/25, Anexo II. Nueva York, NY, Asamblea General de las Naciones Unidas.

Smith, S. W., & Duncan, T. E. (2005). Puppetry as an educational tool: Theory into practice. Springer Science & Business Media.

Telos 123. Inteligencia artificial. Fundación Telefónica (2023)

UNESCO. (2022). Declaración Universal de la Inteligencia Artificial

UNICEF. (2020). Fake news and misinformation: Recommendations for action. Recuperado de https://www.unicef.org/reports/fake-news-and-misinformation#_ftn1

UNICEF (2017) ESTADO MUNDIAL DE LA INFANCIA.

Vaccaro, S (2021). Violencia vicaria: un golpe irreversible contra las madres. Asociación de Mujeres Psicólogas Feministas, España.

Glosario

Ciberactivismo: Ejercicio de la ciudadanía y del compromiso social mediante la participación activa en redes sociales de personas naturales o jurídicas creando dinámicas de información, sensibilización, educación y movilización social usando la web.

***Ciberbullying*:** Acoso realizado entre usuarios y usuarias de edad similar y contexto social equivalente, mediante medios digitales como lo pueden ser las redes sociales, videojuegos, etc.

Ciber-relaciones: Relaciones o contactos que se mantienen a través de la internet, que pueden resultar peligrosas en ciertos momentos debido a la anonimidad que se encuentra en los perfiles en línea.

Control parental: Herramienta que busca monitorear, restringir o bloquear el acceso de NNA a sitios web cuyo contenido sea inapropiado o ponga en riesgo su integridad.

***Deepfakes*:** Archivos de vídeo, imagen o audio manipulados mediante un *software* de Inteligencia Artificial de modo que parecen originales, auténticos y reales.

***Fake News*:** En Español, "noticias falsas" se utiliza para promover ampliamente la desinformación en cualquier ámbito, por lo general las redes sociales son el mecanismo perfecto para la difusión de las mismas.

***Grooming*:** Práctica en la que una persona adulta se hace pasar por un menor en internet e intenta establecer contacto con NNA buscando una relación de confianza y pasando después al control emocional y chantaje con fines sexuales.

***Hacking*:** En español se puede definir como pirateo, método en el que una persona ingresa a un sistema digital sin el conocimiento del dueño o dueña y extrae datos de forma ilegal para beneficio personal.

Huella digital: Cada uno de nosotros y nosotras somos responsables de nuestros propios dispositivos. Cualquier información publicada en nuestras redes sociales o enviada desde nuestro móvil u ordenador es responsabilidad nuestra, aunque no la enviáramos nosotros y nosotras.

Un Viaje Seguro por la Red

Metodologías para prevenir los riesgos digitales y fortalecer el acceso a información segura

Descargo de Responsabilidad

Financiado por la Unión Europea. Sin embargo, las opiniones y puntos de vista expresados son únicamente de los autores y no reflejan necesariamente los de la Unión Europea o IRC. Ni la Unión Europea ni la autoridad otorgante pueden ser considerados responsables por ellos.

UN VIAJE SEGURO POR LA RED

Metodologías para prevenir los riesgos digitales y fortalecer el acceso a información segura

InfoPa'lante Ecuador es una iniciativa dedicada a la promoción de derechos y al acceso a información segura y veraz para toda la comunidad. Mediante metodologías participativas y un enfoque inclusivo, empodera a personas de todas las edades en la prevención de riesgos digitales, fomentando un entorno digital seguro y consciente para todos y todas.

Quito - Ecuador
2024

Alas de Colibrí FUNDACIÓN
INTERNATIONAL RESCUE COMMITTEE
InfoPa'lante ECUADOR
Financiado por la Unión Europea Ayuda Humanitaria