PROTOCOLO DE ATENCIÓN PARA CASOS DE VIOLENCIA DIGITAL EN UNIDADES EDUCATIVAS

Fundación Machaqa Amawta

Protocolo de atención para casos de violencia digital en unidades educativas

Elaboración:
Eloisa Larrea
Camilo Morales

Edición:
María Acho Marquez

Diseño y diagramación:
José Cusicanqui Aguirre

Depósito legal: 4-2-5475-2026

© 2026, Fundación Machaqa Amawta

Impreso en:
Diseño Innova

La Paz - Bolivia
2026

Financiado por:

AEXCID cooperación extremeña JUNTA DE EXTREMADURA

BOSCO GLOBAL ONGD SALESIANA

Usar la tecnología con conciencia es el primer paso para construir un futuro sostenible.

PROTOCOLO DE ATENCIÓN PARA CASOS DE VIOLENCIA DIGITAL EN UNIDADES EDUCATIVAS

Contenido

Introducción

1. Objetivos del protocolo 7
   1.1. Objetivo general 7
   1.2. Objetivos específicos 7

2. Alcance y Ámbito de Aplicación 8

3. Marco Conceptual y Enfoques Transversales 9
   3.1. ¿Qué es la violencia digital? 9
   3.2. Tipos de violencia digital más frecuentes en el ámbito escolar 9
   3.3. Enfoques que guían el protocolo 13

4. Principios Rectores para la Actuación. 14
   4.1. El interés superior es la niñez y adolescencia 14
   4.2. No revictimizar 14
   4.3. Confidencialidad 14
   4.4. Escucha activa y empática 15
   4.5. Actuación oportuna 15
   4.6. Autonomía y consentimiento 15
   4.7. Acompañamiento a las familias 15

5. Identificación y Detección de Situaciones de Violencia Digital 16
   5.1. Señales de alerta 16
   5.2. ¿Cómo abordar la sospecha? 17
   5.3. Canales de denuncia internos 17

6. Ruta de Actuación (pasos concretos) 18
6.1. Paso 1: Recepción del caso y contención emocional 18
6.2. Paso 2: Evaluación inicial y preservación de evidencia 19
6.3. Paso 3: Notificación interna y activación del Equipo de Respuesta Rápida 20
6.4. Paso 4: Medidas de protección inmediata 27
6.5. Paso 5: Derivación a instancias externas 28
6.6. Paso 6: Registro, seguimiento y evaluación del caso 30

7. Roles y Responsabilidades Específicas (por actor) 31
7.1. Directora o director 31
7.2. Maestras y maestros 31
7.3. Maestra/maestro referente en violencia digital (mediante elección participativa o designación de dirección) 32
7.4. Personal administrativo 32
7.5. Junta escolar (MAPAC) 32

8. Anexos 33
Anexo 1: Formato de registro de caso de violencia digital 33
Anexo 2: Flujograma de la ruta de atención 34
Anexo 3: Lista de verificación para preservación de evidencia digital 35
Anexo 4: Glosario de términos básicos 36

Introducción

Actualmente, el uso de Internet y de plataformas digitales es parte de la vida cotidiana de niñas, niños, adolescentes y jóvenes. Estas herramientas ofrecen grandes oportunidades para el aprendizaje, la comunicación y la expresión. Sin embargo, también pueden ser utilizadas para ejercer violencia: burlas, amenazas, difusión de imágenes íntimas sin permiso, suplantación de identidad, acoso, captación para trata de personas o grooming, entre otras formas de agresión que se trasladan a la vida real.

Este tipo de violencia, que llamamos violencia digital, ocurre dentro y fuera de la escuela, y afecta profundamente la autoestima, la salud emocional, el rendimiento académico e incluso la integridad física y sexual de estudiantes. Por eso, las unidades educativas no pueden permanecer en silencio e inactivas ante esta realidad. Aunque la agresión ocurra en una red social o en el ámbito digital, sus consecuencias se sienten en el aula, en el recreo, en la vida de las personas y en la comunidad educativa.

Si bien, el Ministerio de Educación cuenta con un protocolo general para atender la violencia física, psicológica y sexual en las escuelas, la violencia digital tiene características propias: es difícil de eliminar, puede mantenerse en el tiempo, la persona agresora puede actuar de forma anónima y la víctima puede ser violentada de forma permanente y escalonada. Es así que, se presenta esta propuesta de “Protocolo de atención para casos de violencia digital en unidades educativas”.

El propósito de este documento es brindar una guía clara y práctica (paso a paso) para la actuación de directivos, maestras, maestros, personal administrativo y juntas escolares ante una situación de violencia digital en estudiantes. Cada persona adulta en la escuela debe ser un espacio seguro, que ofrezca apoyo efectivo sin juzgar ni revictimizar.

Esta iniciativa se encuentra en el marco del proyecto “Ciberdefensa juvenil: protegiendo derechos con tecnología crítica y seguridad digital en Achachicala (La Paz, Bolivia)”, la misma que cuenta con el apoyo de la Agencia Extremeña de Cooperación Internacional para el Desarrollo y Bosco Global.

1. Objetivos del Protocolo

1.1. Objetivo general

Establecer un procedimiento claro, inmediato y articulado de identificación y atención de casos de violencia digital en el ámbito escolar para garantizar la protección integral de la niñez y adolescencia, bajo el principio del interés superior.

1.2. Objetivos específicos

- Definir roles y responsabilidades de cada actor adulto responsable de la comunidad educativa ante una situación de violencia digital.
- Asegurar la contención emocional y no revictimización de la persona afectada durante el proceso.
- Orientar la preservación de evidencia digital y la derivación a instancias externas cuando sea necesario (Defensoría de la Niñez y Adolescencia, FELCV, FELCC).
- Promover entornos protectores y seguros para la niñez y adolescencia, en coordinación con la comunidad educativa.

2. Alcance y Ámbito de Aplicación

Este protocolo está dirigido a:

- Directoras y directores
- Maestras y maestros de todas las áreas
- Personal administrativo
- Junta escolar (madres, padres, cuidadoras y cuidadores - MAPAC)

Se aplica en todas las situaciones de violencia digital que afecten a estudiantes, sin importar la edad o si el hecho ocurrió dentro del horario escolar o fuera de él, siempre que tenga impacto en el bienestar integral de las personas y en la convivencia socio-educativa.

También es una guía cuando la persona agresora es adulta (del plantel docente, personal administrativo o externa) o cuando el caso involucra a estudiantes de otras unidades educativas.

3. Marco Conceptual y Enfoques Transversales

Para entender y actuar correctamente, es necesario conocer conceptos vitales.

3.1. ¿Qué es la violencia digital?

> Es cualquier acto de violencia que se comete, apoya o amplifica mediante el uso de teléfonos, Internet, redes sociales, aplicaciones de mensajería, correo electrónico, videojuegos en línea u otras tecnologías de la información y la comunicación. Si bien, se puede realizar por medio de una computadora, celular o tableta, la intención es humillar, asustar, controlar o dañar a las personas.

La violencia digital es tan grave como la violencia física. Muchas veces, el contenido violento permanece en Internet por largo tiempo y la víctima siente que no puede liberarse de esa exposición.

3.2. Tipos de violencia digital más frecuentes en el ámbito escolar

La violencia digital se presenta de muchas formas. A continuación, se detallan algunas de las más frecuentes:

Tabla 1. Tipos de violencia digital en el ámbito escolar

Tipo	¿En qué consiste?	Ejemplo cotidiano
Ciberbullying	Acoso entre estudiantes por medios digitales. Incluye insultos, burlas repetidas, exclusión, difusión de información personal, falsa y/o estigmatizante, entre otros.	Alguien crea un grupo de chat para burlarse y compartir memes ofensivos de un estudiante. Se hacen estíqueres de WhatsApp haciendo mofa del físico del estudiante.
Suplantación de identidad	Crear una cuenta falsa con el nombre y/o fotos de otra persona para dañar su imagen.	Alguien abre un perfil de Instagram falso, usando la foto de una compañera y publica mensajes groseros como si fuera ella.
Difusión no consentida de imágenes íntimas	Compartir fotos o videos con contenido íntimo sin permiso de la persona implicada.	Una pareja termina la relación y el exnovio envía, a todo el curso, fotos íntimas que ella compartió, en confianza, durante la relación.
Grooming	Una persona adulta se hace pasar por menor de edad para ganarse la confianza de una niña, niño o adolescente y luego ejercer manipulación, violencia, abuso sexual y/o violación.	Un hombre de 35 años crea un perfil falso con una foto de alguien de 15 y empieza a hablar a diario con una estudiante, pidiéndole fotos íntimas.

Tipo	¿En qué consiste?	Ejemplo cotidiano
Sextorsión	Amenazar a alguien con difundir imágenes o videos íntimos si no entrega dinero, más contenido sexual u otro requerimiento.	Una persona desconocida gana la confianza de una o un adolescente, obtiene fotos íntimas y luego le pide dinero, más imágenes o tiene otras exigencias, bajo amenaza de difundir el contenido ya obtenido.
Acecho o stalking digital	Vigilar constantemente las actividades en línea de una persona, enviarle mensajes repetitivos o seguirla acuciosamente en todas sus redes sociales.	Un estudiante revisa, cada hora, las historias de Instagram de otra estudiante, le envía mensajes y aparece en todos sus comentarios, aunque ella no responda.
Difamación o calumnia	Publicar información falsa para dañar la reputación de alguien.	Alguien escribe en un grupo de WhatsApp que una estudiante robó dinero en el curso, siendo una acusación falsa.
Robo de cuentas	Acceder sin permiso a las cuentas de correo, redes sociales o aplicaciones de una persona para realizar publicaciones a su nombre y ocasionar algún tipo de daño.	Un estudiante filtra o descubre la contraseña de un compañero y cambia su foto de perfil por una imagen ofensiva.

Tipo	¿En qué consiste?	Ejemplo cotidiano
Doxing	Publicar datos personales de alguien (dirección, teléfono, nombre de su madre y padre) sin su permiso.	La persona agresora difunde y escribe en una red social: “La casa de Martha está en la calle X, N° 12, su mamá trabaja en Y y su papá en Z”.

A menudo, una misma persona puede ser víctima de dos o más de estas formas de violencia digital.

La violencia digital afecta a la salud mental y física, así como deja huellas permanentes en la vida de las personas.



3.3. Enfoques que guían el protocolo

Enfoque de derechos humanos

Toda y todo estudiante tiene derecho a vivir sin violencia, fuera y dentro de Internet.

Enfoque de género

No obstante, los hombres también viven situaciones de violencia digital; las mujeres, niñas y adolescentes son ampliamente afectadas por este tipo de violencias, especialmente con la difusión de imágenes íntimas, acoso e incluso violación.

Enfoque de cultura de paz

La cultura de paz frente a la violencia digital debe ser integral: educar para prevenir; acompañar para proteger; normar y regular para respetar derechos; en suma, transformar la convivencia digital para una vida sin violencia.

Enfoque inclusivo

Garantiza que todas las personas –sin importar su género, identidad, condición social, cultural o discapacidad– accedan, participen y se expresen en entornos digitales de manera segura, respetuosa y sin violencia.

Enfoque de medio ambiente

A través de la promoción del uso responsable de la tecnología, reduciendo la basura electrónica y el consumo innecesario de dispositivos.

4. Principios Rectores para la Actuación

Los principios son las reglas de oro que toda persona adulta en la unidad educativa debe seguir al gestionar un caso de violencia digital. Facilita la acción responsable sin causar daño adicional.

4.1. El interés superior es la niñez y adolescencia

Se prioriza el bienestar de la niña, el niño o adolescente que experimenta violencia. Sus necesidades emocionales y de seguridad integral están por encima de cualquier otra consideración (por ejemplo, la reputación de la unidad educativa o el miedo a involucrar a las familias).

4.2. No revictimizar

No someter, innecesariamente, a la víctima a procedimientos reiterados que revivan el trauma del hecho violento (como contar varias veces lo sucedido a diferentes personas).

Asimismo, bajo ninguna circunstancia se debe culpabilizar a la víctima. La responsabilidad siempre es de quien ejecuta el hecho de violencia. Preguntas como: ¿por qué le enviaste esa foto?, ¿para qué tenías ese perfil público? o ¿por qué no te cuidaste?, solo empeoran el daño.

4.3. Confidencialidad

Todo lo que la persona afectada cuente o develе debe mantenerse en estricta reserva. Solo se compartirá la información indispensable

con quienes, rigurosamente, coadyuven en el proceso de apoyo (directora, director, familia, instituciones de protección u otro relevante). Nunca comentar el caso en una junta de maestras y maestros ni con estudiantes o en reuniones generales.

4.4. Escucha activa y empática

Cuando una o un estudiante decida contar su situación, se debe escuchar con mucha atención, sin interrumpir, sin juzgar y sin apuros. Mostrar con gestos y palabras que se le cree y que cuenta con apoyo.

Estas frases pueden ser útiles:

- "Gracias por confiar en mí"
- "Entiendo que esto es muy difícil para ti"
- "Voy a ayudarte"
- "No estás sola/solo".

4.5. Actuación oportuna

La violencia digital puede escalar rápidamente. No es responsable esperar a ver si el problema "se calma por sí solo"; se debe actuar, desde el primer momento, siguiendo los pasos de este protocolo.

4.6. Autonomía y consentimiento

Siempre que sea posible, se pregunta qué desea hacer. Por ejemplo: "¿Quieres que hable con tus papás?" o "¿Te sientes lista para ir a la Defensoría?". Se respeta su decisión, a menos que su vida o integridad se encuentre en peligro.

4.7. Acompañamiento a las familias

Madres, padres, cuidadoras y cuidadores tienen un rol fundamental; por tanto, se les debe informar con respeto y sin culpabilizar para cooperar, conjuntamente, en la protección de la o del estudiante.

5. Identificación y Detección de Situaciones de Violencia Digital

A veces, la o el estudiante puede no comunicar que vive una situación de violencia digital, pero se pueden observar señales de alerta.

5.1. Señales de alerta

- Cambio repentino en el rendimiento escolar (bajas notas, incumplimiento en la entrega de tareas).
- Pérdida de interés en actividades que antes le gustaban.
- Se aísla y no quiere participar en clases ni en los recreos.
- Muestra nerviosismo o tristeza cuando recibe un mensaje en el celular.
- No quiere ir a la escuela, pone excusas para faltar.
- Cambios en el estado de ánimo: irritabilidad, ansiedad, depresión profunda.
- Deja de usar sus redes sociales o, por el contrario, las revisa obsesivamente.
- Tiene problemas para dormir o pesadillas.
- Cambios en sus hábitos (académicos, de alimentación, gustos, consumo, sociabilidad, etc.).

5.2. ¿Cómo abordar la sospecha?

Si se percibe una o más de las señales, buscar un momento y espacio privado para hablar con la o el estudiante; no hacerlo frente a otras personas.

Frases sugeridas para empezar:

- "He notado que últimamente te ves un poco triste. Si quieres conversar, aquí estoy".
- "Todos atravesamos por situaciones difíciles, alguna vez. Si algo te está pasando, puedes contarme".
- "Antes te gustaba jugar básquet, ahora ya no lo haces. ¿Todo está bien en casa? ¿Hay algo que quisieras comentarme en confianza y confidencia?

Tener en cuenta que:

→ No se debe presionar o forzar respuestas.

→ Mostrar disponibilidad para hablar cuando lo necesite.

→ Si la sospecha persiste, consultar con la directora, el director, madre, padre o equipo de apoyo.

5.3. Canales de denuncia internos

Para que las y los estudiantes sientan seguridad al pedir ayuda, la unidad educativa debe habilitar, al menos, dos canales confidenciales de denuncia:

- Maestra/maestro referente en violencia/violencia digital.
- Buzón físico o correo electrónico para reportar situaciones de violencia digital de forma anónima (si se prefiere).

La comunidad educativa y, especialmente, las y los estudiantes deben recibir información sobre el funcionamiento de estos canales al comenzar el año escolar.

6. Ruta de Actuación (pasos concretos)

Pasos a seguir cuando una o un estudiante realice una denuncia o comunique que está viviendo una situación de violencia digital:

6.1. Paso 1: Recepción del caso y contención emocional

¿Quién hace la recepción?

- → Toda persona adulta de la unidad educativa (directora, director, maestra, maestro, personal administrativo).
- → Es ideal que exista una maestra o maestro de referencia con capacitación para el caso.

¿Cómo actuar?

- Conducir a la o al estudiante a un espacio privado, tranquilo y que no permita interrupciones, pensado y acondicionado para este tipo de ocasiones.
- Sentarse a su altura, mantener contacto visual cálido y una postura abierta y receptiva.
- Decir frases como: “Te escucho. Lo que me digas es confidencial. No te voy a juzgar”.
- Dejar que hable a su ritmo. No interrumpir ni pedir detalles íntimos innecesarios.

- No minimizar lo que siente. Evitar frases como: “No es para tanto” o “Ya se te pasará”.
- Validar sus emociones: “Es normal que te sientas así” “Cualquiera estaría asustada/asustado en tu lugar”.
- No prometer lo que no se puede cumplir (por ejemplo, “haré que expulsen al agresor”).
- Agradecerle la confianza depositada (“Hiciste bien en contarme”).

6.2. Paso 2: Evaluación inicial y preservación de evidencia

Antes de hacer cualquier denuncia ante instancias oficiales, es fundamental guardar la evidencia. Porque, si se reporta una cuenta o se eliminan mensajes, se pueden perder las pruebas.

¿Qué evidencia guardar?

- Capturas de pantalla de los mensajes, publicaciones, comentarios ofensivos u otras formas de agresión. Asegurarse de que se vea, claramente, la fecha, la hora y el nombre de la persona agresora.
- Guardar la dirección URL (enlace) de la publicación o del perfil falso y también realizar capturas de pantalla.
- Si son mensajes de WhatsApp o similar, no borrar la conversación. Hacer copia de seguridad antes de bloquear o reportar al usuario.
- Anotar fechas y horas de cada agresión.
- Grabar conversaciones de audio (llamadas), cuando sea posible.

¿Cómo guardar la evidencia sin exponer a la o al estudiante?

- Orientar la toma de capturas desde su teléfono. Enseñar el paso a paso, si no tiene información al respecto.
- Las capturas se guardan en una carpeta segura. No se comparten con nadie más que con las personas indicadas en su debido momento (autoridad educativa, instancia de protección, etc.).
- Si la víctima tiene miedo de perder el material, puede guardar un respaldo (copia) en una memoria USB, al cual tendrán acceso solo personal o autoridad competente.

6.3. Paso 3: Notificación interna y activación del Equipo de Respuesta Rápida

Una vez que se ha recibido el caso y guardado la evidencia, se debe informar inmediatamente a la directora o director de la unidad educativa quien activa el "Equipo de Respuesta Rápida".

El Equipo de Respuesta Rápida (puede estar compuesto por la dirección, maestra o maestro referente y un representante de la junta escolar), se conforma y se capacita a inicio de año. Igualmente, cuenta con un reglamento de funciones y medidas de atención.

Según el caso, el testimonio de la persona en situación de violencia digital y la evidencia encontrada, este equipo evalúa:

- → El nivel de riesgo: bajo, medio o alto.
- → Si la violencia implica un delito (difusión de imágenes íntimas, extorsión, amenazas graves, grooming, trata de personas u otro).
- → Si la persona agresora es mayor de edad.

- Si la persona agresora es estudiante de la misma unidad educativa o de otra.

Esta evaluación se realiza con el análisis detallado de los siguientes aspectos:

- Nivel de exposición y riesgo de la integridad física y psicológica de la persona en situación de violencia digital.
- Gravedad del daño causado.
- Amenazas o riesgo de escalamiento en el daño.
- Nivel de contacto y/o cercanía con la persona agresora.
- Acceso a datos sensibles por parte de la persona agresora.

Nivel de riesgo



Alto

Medio

Bajo

A efectos de determinar si el hecho constituye delito, la siguiente tabla resumen vincula algunos de los tipos de violencia relevantes con un tipo penal:

Tabla 2. Tipos de violencia digital vinculados a tipos penales e instancias competentes

Tipo de violencia	¿Constituye delito?	Ley / Tipo penal (referencia)	Instancia competente
Ciberbullying o acoso cibernético (si no conlleva expresiones de racismo, ni amenazas graves o difusión de material íntimo)	No (pero es una falta administrativa)	• Ley N° 548 (Código Niña, Niño y Adolescente) • Medidas socioeducativas	DNA
Difusión no consentida de imágenes íntimas	Sí	• Código Penal – Art. 323 Bis (Pornografía)	FELCC + DNA
Suplantación de identidad	Sí	Código Penal: • Art. 363 Bis (Manipulación informática) • Art. 363 Ter (Alteración, acceso y uso indebido de datos informáticos)	FELCC

Tipo de violencia	¿Constituye delito?	Ley / Tipo penal (referencia)	Instancia competente
Expresiones racistas, discriminatorias y/o estigmatizantes	Sí	Código Penal: • Art. 281 Quinquies (Racismo) • Art. 218 Sexies (Discriminación) • Art. 218 Septies (Difusión e incitación al racismo o a la discriminación) • Art. 218 Octies (Organizaciones o asociaciones racistas o discriminatorias) • Art. 218 Nonies (Insultos y otras agresiones verbales por motivos racistas o discriminatorios)	FELCC + DNA
Sextorsión	Sí	• Código Penal – Art. 333 (Extorsión)	FELCC

Tipo de violencia	¿Constituye delito?	Ley / Tipo penal (referencia)	Instancia competente
Grooming	Sí	Código Penal: • Art. 312 Quinquies (Contacto con niñas, niños o adolescentes con fines sexuales a través de tecnologías de la información y comunicación) • Art. 312 Sexies (Abuso sexual de niñas, niños o adolescentes por medios digitales) • Art. 318 Bis (Exposición a contenido sexual a niñas, niños o adolescentes) • Art. 323 Ter (Producción de material de abuso sexual de niña, niño o adolescente) • Art. 323. Quater (Posesión o comercialización de material de abuso y explotación sexual de niña, niño o adolescente)	FELCV + DNA

Tipo de violencia	¿Constituye delito?	Ley / Tipo penal (referencia)	Instancia competente
Captación para trata de personas (explotación laboral, sexual, matrimonio servil, etc.)	Sí	• Código Penal – Art. 281 Bis (Trata de personas)	FELCC + DNA
Reclutamiento para ejercicio de trabajo sexual	Sí	• Código Penal – Art. 321 (Proxenetismo)	FELCC + DNA
Pago para mantener relaciones sexuales con un o una menor de edad	Sí	• Código Penal – Art. 322 (Violencia sexual comercial)	FELCC + DNA

Tipo de violencia	¿Constituye delito?	Ley / Tipo penal (referencia)	Instancia competente
Robo de cuenta o acceso indebido	Sí	Código Penal: • Art. 363 Bis (Manipulación informática) • Art. 363 Ter (Alteración, acceso y uso indebido de datos informáticos)	FELCC
Doxing (publicación de datos personales sin consentimiento)	Sí (si causa daño)	Código Penal: • Art. 363 Bis (Manipulación informática) • Art. 363 Ter (Alteración, acceso y uso indebido de datos informáticos)	FELCC
Difamación o calumnia	Sí	Código Penal: • Art. 282 (Difamación) • Art. 283 (Calumnia) – Aplicable a medios digitales	FELCC

Artículos 312 Quiquies, 312 Sexies, 318 Bis, 323 Ter y 323 Quáter del Código Penal, incorporados por la Ley N° 1636. Artículo 323 Bis del Código Penal, modificado por la Ley N° 1636.

6.4. Paso 4: Medidas de protección inmediata

Mientras se define la derivación externa, se toman estas medidas de protección, según corresponda:

- Separar a la persona afectada de la agresora dentro del centro educativo (por ejemplo, cambiar de aula), sin que esto implique un castigo para quien sufrió violencia digital.
- Acompañamiento emocional inicial. Si la unidad educativa cuenta con una persona profesional en psicología, esta debe realizar la evaluación y consiguiente contención a la víctima. Si no es así, se contacta a la Defensoría de la Niñez y Adolescencia (DNA) para acceder al servicio.
- Informar a la familia. La dirección o maestra/maestro referente cita a madre, padre, cuidadora o cuidador de la víctima. En un ambiente privado, se les explica la situación, las medidas tomadas y los pasos a seguir. Nunca se les culpa. Se brinda orientación y se pide colaboración.
- No contactar directamente a la persona agresora sin la presencia de la persona adulta responsable y/o profesional del sistema de protección y sin seguir el procedimiento establecido, especialmente cuando se trate de un delito.

6.5. Paso 5: Derivación a instancias externas

Según el tipo de violencia digital, el caso se deriva a determinadas entidades del sistema de protección. La dirección, junto al Equipo de Respuesta Rápida, coordina dichas derivaciones y acompaña a la familia.

Tabla 3. Derivación y acciones de instancias externas

Tipo de violencia	Instancia externa principal	¿Qué hace?
Ciberbullying entre estudiantes (sin delito)	DNA	Realiza una intervención psicosocial, cita a las familias, aplica medidas de protección y, si la persona agresora es menor de edad, activa una intervención en la familia.
Difusión de imágenes íntimas, sextorsión, grooming, amenazas graves	FELCV + DNA	La FELCV investiga el delito y, si la persona agresora es menor de edad, informa a la DNA para la activación del Sistema Penal Juvenil e implementa medidas de protección para la seguridad de la víctima.

Suplantación de identidad, robo de cuenta, delitos informáticos	FELCC + DNA	La FELCC investiga el delito y, si la persona agresora es menor de edad, informa a la DNA para la activación del Sistema Penal Juvenil e implementa medidas de protección para la seguridad de la víctima.
Cuando la persona agresora adulta es alguien de la unidad educativa	DNA + FELCC o FELCV	La FELCC o FELCV investiga el delito y formaliza la denuncia ante el Ministerio Público; la DNA protege a la víctima y acompaña el proceso penal.

DNA: Defensoría de la Niñez y Adolescencia
FELCV: Fuerza Especial de Lucha Contra la Violencia
FELCC: Fuerza Especial de Lucha Contra el Crimen

IMPORTANTE:

La denuncia puede hacerse de forma oral o escrita. Las familias pueden acudir primero a la DNA, que colaborará en la redacción de la denuncia, y esta será derivada al Ministerio Público o a la Policía Boliviana.

La escuela debe acompañar a la familia en este proceso, pero no puede hacer la denuncia por la víctima (excepto en casos de violencia sexual, en los que la unidad educativa tiene la obligación de realizar dicha denuncia ante la instancia competente).

6.6. Paso 6: Registro, seguimiento y evaluación del caso

Cada caso debe quedar registrado en un libro o expediente confidencial de la unidad educativa. Dicho registro debe contener:

- Fecha de recepción
- Tipo de violencia
- Medidas asumidas
- Derivaciones realizadas
- Acuerdos con la familia
- Fecha de seguimiento

El seguimiento implica:

- **A los 3 días:** verificar que la víctima esté asistiendo a la unidad educativa (si corresponde), reciba atención psicoterapéutica y que las medidas de protección se cumplan a cabalidad.
- **A los 15 días:** evaluar si el hecho de violencia cesó o si existen nuevos episodios; así como hacer seguimiento al acompañamiento y protección de la víctima.
- **A los 30 días:** reunión con la familia para evaluar el proceso y determinar si se necesita apoyo psicológico continuo o mayores acciones en diferentes ámbitos, entre ellos el legal, cuando corresponda.

7. Roles y Responsabilidades Específicas (por actor)

7.1. Directora o director

- Activar el protocolo apenas se conozca un caso.
- Conformar y liderar el Equipo de Respuesta Rápida.
- Informar a la familia de la víctima y de la persona agresora (por separado) con respeto y confidencialidad.
- Coordinar con las instancias externas (DNA, FELCV, FELCC, etc.).
- Garantizar que no haya represalias contra la víctima.
- Llevar el registro oficial de casos.
- Hacer el seguimiento a los casos.

7.2. Maestras y maestros

- Detectar señales de alerta.
- Escuchar, activa y respetuosamente, a quien expresa que vive o sabe de una situación de violencia digital.
- Derivar el caso inmediatamente a la dirección o maestra/maestro referente (no intentar "resolver" el hecho de forma independiente).
- No exponer a la o al estudiante en público ni hacer comentarios frente a otras personas.

- Mantener la confidencialidad absoluta.
- Incorporar actividades de prevención de violencia digital en sus clases, de ser posible.

7.3. Maestra/maestro referente en violencia digital (mediante elección participativa o designación de dirección)

- Escuchar a la o al estudiante, en primera instancia (se respeta si prefiere hablar con otra persona).
- Ayudar a preservar la evidencia digital.
- Informar sobre el caso a la dirección y colaborar en la derivación correspondiente.
- Acompañar a la o al estudiante y su familia durante el proceso, sin asumir funciones de profesionales en psicología o abogacía.
- Capacitar al plantel docentes en el uso del protocolo.

7.4. Personal administrativo

- Mantener la confidencialidad absoluta.
- Apoyar en la gestión de citas con familias y derivaciones.
- Resguardar los registros de casos de violencia digital de la unidad educativa.

7.5. Junta escolar (MAPAC)

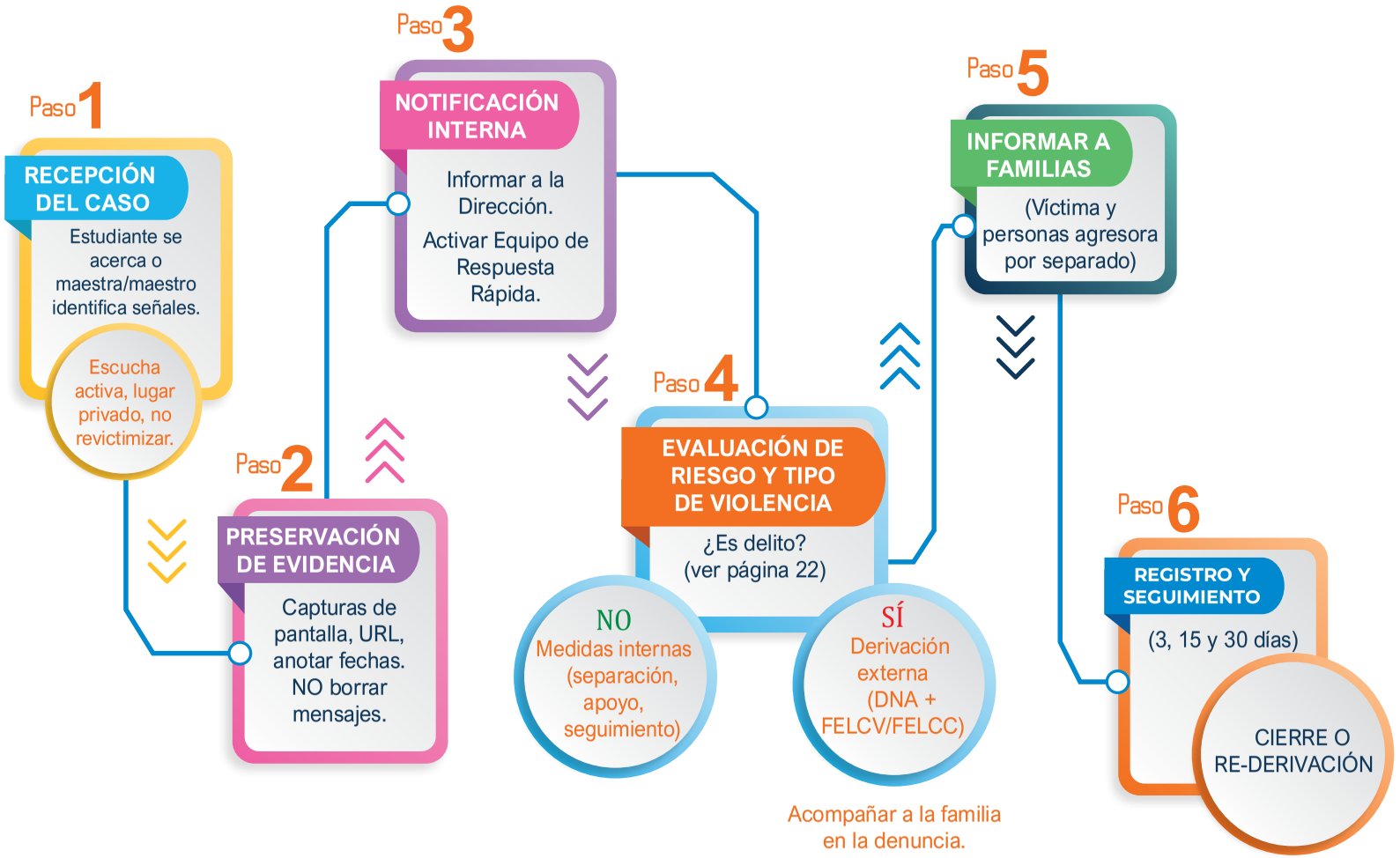
- Mantener un canal de confianza para las familias de estudiantes en situación de violencia digital.
- Colaborar en la difusión del protocolo entre padres, madres, cuidadoras y cuidadores.
- Participar en las reuniones de seguimiento cuando se requiera.
- Apoyar actividades de prevención (charlas, campañas, entre otros).

8. Anexos

Anexo 1: Formato de registro de caso de violencia digital

Campo	Descripción
N° de caso	[Año] - [N° correlativo]
Fecha de recepción	[dd/mm/aaaa]
Iniciales del/la estudiante (víctima)	
Edad	
Curso/grado	
Persona que recibe el caso	[Nombre y rol]
Fecha o periodo de los hechos	dd/mm/aaaa (o período)
Tipo de violencia digital (marcar o especificar)	☐ Ciberbullying ☐ Suplantación ☐ Difusión no consentida ☐ Sextorsión ☐ Grooming ☐ Acecho ☐ Robo de cuentas ☐ Difamación ☐ Doxing ☐ Otro: _____
Descripción breve de los hechos (referencial)	[máximo 5 líneas]
Evidencia preservada	☐ Capturas ☐ URL ☐ Registro de fechas ☐ Otro: _____
Medidas de protección inmediatas asumidas	☐ Separación de agresor/agresora ☐ Acompañamiento emocional ☐ Información a familia ☐ Otras: _____
Derivación externa	☐ Defensoría de la Niñez y Adolescencia ☐ FELCV ☐ FELCC ☐ Ninguna correspondía (seguimiento interno)
Personas que participaron	
Fecha de seguimiento a 3 días	Observaciones:
Fecha de seguimiento a 15 días	Observaciones:
Fecha de seguimiento a 30 días	Observaciones y cierre (si aplica)

Anexo 2: Flujograma de la ruta de atención



Anexo 3: Lista de verificación para preservación de evidencia digital

Paso	Acción	¿Hecho?
1	No borrar nada (mensajes, publicaciones, historial, fotos o videos).	☐
2	Tomar capturas de pantalla completas. Que se vea: fecha, hora, nombre de usuario, contenido.	☐
3	Si es video o audio, grabar desde otro dispositivo si es posible (sin alterar el original).	☐
4	Guardar URL o enlace directo a la publicación o perfil falso.	☐
5	Anotar fechas y horas de cada agresión (ayudar a la/al estudiante a recordar).	☐
6	No reportar ni bloquear a la persona agresora hasta después de guardar toda la evidencia (al reportar puede desaparecer el contenido).	☐
7	Hacer copia de seguridad de conversaciones (WhatsApp: ajustes > chats > copia de seguridad).	☐
8	Guardar capturas y archivos en una carpeta segura (en computadora o USB con acceso único de maestra/maestro referente o la dirección).	☐
9	No compartir la evidencia con estudiantes, personal no autorizado o redes sociales.	☐
10	Si el/la estudiante tiene miedo, sugerir que el dispositivo sea guardado por una persona adulta de confianza, mientras se realiza la denuncia.	☐

Recordatorio: La evidencia es fundamental para que la DNA o la policía puedan actuar. Sin pruebas, es muy difícil proteger y sancionar.

Anexo 4: Glosario de términos básicos

Término	Descripción
Violencia digital	Toda acción, a través del Internet y medios digitales (redes sociales, juegos en línea, mensajería o cualquier otra tecnología de información y comunicación), que tiene el objetivo de humillar, amenazar, agredir, controlar y dañar a las personas.
Ciberbullying o ciberacoso	Acoso, generalmente entre pares, por medio del uso de tecnologías digitales (redes sociales, juegos, mensajería y otras plataformas en línea) para intimidar, humillar o violentar a una persona de manera repetida y consciente. Implica insultos, burlas, difusión de mentiras, publicación de material íntimo y vergonzoso y exclusión, entre otros.
Suplantación de identidad	Crear un perfil falso con el nombre y fotos de otra persona para hacerse pasar por ella y ocasionar algún tipo de daño.
Difusión no consentida	Compartir información, datos, mensajes, fotos o videos íntimos sin permiso de la persona afectada. Es un delito.
Sextorsión	Amenazar con difundir mensajes o imágenes íntimas y personales si no se proporciona dinero, más contenido sexual u otro requerimiento.
Grooming	Una persona adulta se hace pasar por alguien de menor de edad para ganar confianza de una niña, un niño o adolescente y cometer abuso sexual o violación.
Acecho o stalking digital	Vigilar constantemente las actividades en línea de alguien, enviar mensajes repetitivos y acechar, aunque no responda.
Doxing	Publicar datos personales de alguien (dirección, teléfono, nombres de familiares) sin permiso y solo para exponerla.
Revictimización	Hacer que la víctima cuente su experiencia de violencia muchas veces, sin necesidad, hacerla sentir culpable e incrementar su sufrimiento.
Preservación de evidencia	Guardar pruebas (capturas, enlaces) antes de que desaparezcan, para que las autoridades puedan realizar la investigación correspondiente.
Interés superior de la niña, el niño y adolescente	Principio en el que la protección y bienestar de la niña, el niño o adolescente es lo más importante y está por encima de otros intereses.

Fundación
Machaqa
Amawta

Av. Arce Nº 2433
Edificio Torre de Las Américas - Of. 21
La Paz - Bolivia
Teléfonos: (591-2) 2141235 - 2442787

amawta@fmachaqa.org
www.fmachaqa.org
Fundación Machaqa Amawta
Protege sin diferencias
Fundación Machaqa Amawta
fmachaqa_org
Fundación Machaqa Amawta

Financiado por:

AEXCID
cooperación extremeña
JUNTA DE EXTREMADURA

BOSCO GLOBAL
ONGD SALESIANA