Curso corto virtual	Abordaje de la violencia de género facilitada por la tecnología en el entorno educativo

TEXTO GUÍA TÉCNICO-PEDAGÓGICO: ABORDAJE DE LA VIOLENCIA DE GÉNERO FACILITADA POR LA TECNOLOGÍA (VGFT) EN EL ENTORNO EDUCATIVO

Autora: Carla Menacho Gonzales

Proyecto Fomento de la Igualdad de Género - ProIgualdad

Implementada por:

Curso corto virtual	**La IA responsable y respuesta a violencias digitales en entornos educativos**

PRESENTACIÓN

1. MARCO CONCEPTUAL Y EJES DE ANÁLISIS

1.1. Derechos Digitales

1.2. Conceptualización de la Violencia Digital y la VGFT

1.3. El continuo de la violencia (Noción 1)

1.4. Ejes de análisis: Perspectiva de género e interseccionalidad (Noción 2)

A. Mecanismos de castigo e hiperfiscalización sobre las mujeres

B. Análisis Interseccional en el contexto boliviano

1.5. Propiedades y especificidades del entorno digital (Noción 3)

1.6. Mitos más comunes respecto a la violencia digital (Noción 4)

1.7. Principios del enfoque centrado en la víctima (Noción 5)

2. TIPOLOGÍAS DE VGFT Y ANÁLISIS DE CASOS

2.1. Matriz de tipologías de la VGFT

2.2. Análisis de caso: El caso de Sofía

3. PREVENCIÓN, DETECCIÓN Y PRIMERA RESPUESTA EN LA PRÁCTICA DOCENTE

3.1. Estrategias didácticas de prevención: Límites, consentimiento y conductas de riesgo

1. Enseñar el consentimiento digital (La regla del "paso de la privacidad")

2. Definición y reconocimiento de límites digitales y personales

3. Identificación de conductas de riesgo y manipulación en línea

4. Cuidado colectivo y desarticulación de la complicidad pasiva

3.2. Indicadores para la detección temprana en el aula

3.3. Decálogo de primera respuesta docente

REFERENCIAS BIBLIOGRÁFICAS Y CONCEPTUALES

ANEXO 1: RECURSOS DE AUTOAPRENDIZAJE Y MATERIAL COMPLEMENTARIO

Lecturas, recursos web y material complementario

ANEXO 2: SOLUCIONARIO Y ORIENTACIONES PARA EL ANÁLISIS DE CASOS

Solución al caso 2.2: El caso de Sofía

PRESENTACIÓN

El presente texto guía constituye un recurso didáctico para el autoaprendizaje de las y los futuros docentes de las Escuelas Superiores de Formación de Maestros (ESFM). Su objetivo central es desarrollar competencias conceptuales, analíticas y procedimentales para la prevención, detección temprana y primera respuesta frente a la Violencia de Género Facilitada por la Tecnología (VGFT) en las comunidades educativas.

A lo largo de este material formativo, la VGFT se analiza desde cinco nociones estructurales clave: (1) El continuo de la violencia, comprendiendo que la frontera entre lo presencial y lo digital es difusa o inexistente; (2) La perspectiva de género e interseccionalidad, visibilizando los mecanismos patriarcales de hiperfiscalización hacia las mujeres; (3) Las características técnicas intrínsecas del entorno digital; (4) Los mitos más comunes sobre el daño digital; y (5) Los principios del enfoque centrado en la víctima. Por otra parte, se encuentran ejemplos didácticos, pautas prácticas para llevarlas a cabo dentro de las aulas y materiales complementarios que pueden revisar para ampliar sus conocimientos en la temática.

1. MARCO CONCEPTUAL Y EJES DE ANÁLISIS

1.1. Derechos Digitales

Previo al abordaje de las violencias digitales, es importante comprender el concepto de Derechos Digitales. Este no se refiere a una nueva categoría de derechos, sino a la extensión de los Derechos Humanos al espacio digital. Toda persona tiene derecho al acceso universal a internet, a la libertad de expresión, a la privacidad, a la protección de datos personales, al anonimato y al ejercicio de una ciudadanía digital plena y segura (Asociación para el Progreso de las Comunicaciones [APC], 2015; Fondo de Población de las Naciones Unidas [UNFPA], 2021).

Reconocer la violencia digital desde el marco de los derechos digitales implica entender que cualquier acto de acoso, difusión no consentida de contenido íntimo o ciberacecho es una vulneración directa a los derechos fundamentales (UNFPA, 2021).

Garantizar un entorno digital libre de violencia es la condición necesaria para que las y los estudiantes ejerzan su derecho a la educación, la información, la participación y el desarrollo integral en la sociedad.

1.2. Conceptualización de la Violencia Digital y la VGFT

En el mismo sentido que los derechos digitales, la violencia digital se define como un acto perpetrado por uno o más individuos que se comete, asiste, agrava y amplifica parcial o totalmente mediante el uso de tecnologías de la información y la comunicación (TIC), hardware, software o espacios digitales por razón de género (UNFPA, 2021).

Por su parte, la VGFT se define como cualquier acto cometido, asistido, agravado o amplificado por el uso de tecnologías de información y comunicación (TIC) u otras herramientas digitales, que cause daño en diversos aspectos como físico, sexual, psicológico, social, político o económico a mujeres y niñas (Fundación InternetBolivia.org, AGETIC & ONU Mujeres, 2024). Esta conceptualización extiende los principios de prevención y protección integral hacia los entornos virtuales.

1.3. El continuo de la violencia (Noción 1)

Es fundamental resaltar que la VGFT es un continuo de la violencia estructural e histórica que afecta a mujeres y niñas, incluyendo violencia física, psicológica, sexual, política y económica; y asimismo, este tipo de violencia posee características distintivas que la diferencian de las formas tradicionales, requiriendo un mayor entendimiento de sus manifestaciones, efectos y herramientas de prevención y atención integral (Fundación InternetBolivia.org, AGETIC & ONU Mujeres, 2024).

Respecto al marco del continuo de la violencia (Kelly, 1988), este enfoque pretende desmitificar la noción errónea de que las agresiones digitales son hechos aislados, virtuales o desconectados de la realidad. El siguiente esquema muestra la articulación entre las estructuras de poder presenciales, los medios tecnológicos y el daño integral que resulta en la vida de las víctimas:

FASE DEL CONTINUO	ESPACIO / MEDIO	MANIFESTACIÓN O IMPACTO
Origen estructural (Kelly, 1988)	Espacio presencial / Físico	Relaciones asimétricas de poder, machismo normalizado y estereotipos de género.
Soporte de comisión	Medios digitales / Dispositivos	WhatsApp, TikTok, redes sociales, herramientas de Inteligencia Artificial, foros, etc.
Consecuencia tangible	Daño real e integral	Afectación psicológica, ansiedad, deserción escolar, aislamiento y vulneración de derechos fundamentales; y posibilidad del traspaso a daños físicos.

Fuente: Elaboración propia en base a Kelly (1988) y UNFPA (2021).

En ese sentido, lo digital constituye el medio o canal de comisión; el daño resultante es plenamente real, material y sistemático en la vida de las personas afectadas dentro del continuo de la violencia (Kelly, 1988; UNFPA, 2021).

Actualmente, la frontera entre el espacio presencial (físico) y el entorno digital es indefinida en la vida cotidiana. Las agresiones virtuales no nacen de la tecnología en sí misma, sino que representan la extensión y amplificación de relaciones asimétricas de poder, machismo normalizado y patrones patriarcales que operan históricamente en la sociedad.

1.4. Ejes de análisis: Perspectiva de género e interseccionalidad (Noción 2)

La Violencia de Género Facilitada por la Tecnología (VGFT) no se manifiesta de manera neutral ni aleatoria en la sociedad, sino que impacta de forma cualitativa y cuantitativamente distinta a niñas, adolescentes y mujeres de todas las edades, vulnerando las garantías de convivencia libre de violencia establecidas en el ámbito educativo (Ministerio de Educación de Bolivia, 2021). Para fundamentar esta asimetría, la evidencia de la realidad boliviana documentada en la Encuesta Nacional "Conectando Bolivia: Percepciones sobre género, violencia y uso de tecnologías de la información y la comunicación" (AGETIC, ONU Mujeres & Ipsos, 2024), la Investigación

"Cuerpos, pantallas y algoritmos: Sexualidad digital en adolescentes y jóvenes y su relación con la violencia digital en Bolivia" (Ciberwarmis, ChildFund Bolivia & UMSA, 2026) y el "Reporte estadístico quinquenal de atenciones por ciberviolencia de género y cibercrimen (2021-2025)" del Centro S.O.S. Digital (2025) demuestra la existencia de patrones estructurales de violencia basada en género:

A. Mecanismos de castigo e hiperfiscalización sobre las mujeres

Socialmente se juzga, hipersexualiza y sanciona a las mujeres por su imagen, su vestimenta, su sexualidad o sus opiniones en línea mediante la vergüenza pública, mientras que en los varones estas conductas suelen tolerarse o celebrarse (UNFPA, 2021). Esta desproporción se evidencia en los datos de la realidad boliviana:

- **Concentración del daño en la intimidad:** De acuerdo con la Investigación "Cuerpos, pantallas y algoritmos: Sexualidad digital en adolescentes y jóvenes y su relación con la violencia digital en Bolivia", el **75.9%** de los incidentes de agresión reportados por mujeres adolescentes y jóvenes se concentra en violencia sexual digital y acoso combinado (desglosado en un **41.8%** por recepción de contenido sexual no solicitado y **34.1%** por acoso sexual explícito) (Ciberwarmis, ChildFund Bolivia & UMSA, 2026).
- **Desproporción en solicitudes no consentidas:** En la etapa escolar y adolescente, las mujeres reciben hasta 7 veces más solicitudes no consentidas de fotografías íntimas que los varones (7.3% frente a 1.1%), conforme a la Investigación "Cuerpos, pantallas y algoritmos: Sexualidad digital en adolescentes y jóvenes y su relación con la violencia digital en Bolivia" (Ciberwarmis, ChildFund Bolivia & UMSA, 2026).
- **Prevalencia de violencias digitales en Bolivia:** Los datos oficiales de la Encuesta Nacional "Conectando Bolivia" señalan que entre las principales manifestaciones sufridas por mujeres destacan el **31%** por abuso de datos personales e invasión a la privacidad, el 27% por abuso sexual vinculado a las TIC (incluyendo un 22% con intentos directos de captación) y un 13% por acoso digital y hostigamiento continuado (AGETIC, ONU Mujeres & Ipsos, 2024).
- **Concentración de la asistencia especializada:** Los datos de atención directa documentados en el Reporte estadístico quinquenal de atenciones por ciberviolencia de género y cibercrimen (2021-2025) del Centro S.O.S. Digital revelan que la violencia sexual digital (28%) y el acoso digital continuado (19%) encabezan las denuncias recibidas de mujeres asistidas, donde más del 57% de las solicitudes responde explícitamente a violencia basada en género frente

a un porcentaje marginal de delitos puramente informáticos o económicos (Centro S.O.S. Digital, 2025).

- **Patrón de reincidencia y hostigamiento sistemático:** En Bolivia, el 58% de las víctimas de VGFT sufre agresiones reiteradas en el tiempo (de 2 a más de 5 veces), lo que demuestra un patrón de amedrentamiento continuado y no hechos aislados, conforme a la Encuesta Nacional "Conectando Bolivia" (AGETIC, ONU Mujeres & Ipsos, 2024).

B. Análisis Interseccional en el contexto boliviano

Las violencias digitales no operan de forma aislada, sino que se cruzan con variables socioestructurales que agravan la vulnerabilidad de las y los estudiantes:

- **Edad y etapa de desarrollo:** Las y los adolescentes poseen menor experiencia acumulada en gestión de crisis y configuración de privacidad, lo que incrementa su exposición ante dinámicas de chantaje o manipulación.
- **Origen etnolingüístico y territorio:** Estudiantes pertenecientes a pueblos indígenas originarios o de zonas rurales en contextos urbanos enfrentan una doble victimización por la intersección entre racismo y machismo digital, además de una marcada brecha digital (menor acceso y uso a dispositivos digitales e internet) en estos sectores.
- **Identidad y orientación sexual:** Estudiantes con identidades de género u orientaciones sexuales diversas enfrentan de forma desproporcionada campañas masivas de acoso, difamación, doxing e incitación al odio en entornos virtuales.

1.5. Propiedades y especificidades del entorno digital (Noción 3)

PROPIEDAD TÉCNICA	IMPACTO EN LA COMUNIDAD EDUCATIVA
Rápida expansión ("Lo viral")	La difusión opera de manera exponencial e instantánea en segundos, desbordando de inmediato el espacio del aula física hacia redes sociales ampliadas y comunidades familiares.
Persistencia y huella digital	El material digital permanece alojado indefinidamente en servidores externos y dispositivos locales, con riesgo de reactivarse en

PROPIEDAD TÉCNICA	IMPACTO EN LA COMUNIDAD EDUCATIVA
	distintos momentos, sometiendo a la víctima a una victimización recurrente.
Escalabilidad y replicabilidad	Copiar, duplicar, descargar y compartir material digital no genera costos ni degradación en la calidad del archivo, lo que imposibilita la restitución total de la privacidad original de la víctima.
Capacidad de búsqueda global	Los motores de indexación y algoritmos facilitan localizar el contenido abusivo asociándolo de forma persistente a los nombres o identidades de víctimas.
Anonimato y desinhibición en línea (Suler, 2004)	La distancia mediada por pantallas mitiga la empatía y favorece conductas hostiles que no se manifestarían de forma presencial; el uso de perfiles anónimos o falsos dificulta la sanción inmediata.

Fuente: Elaboración propia en base a Suler (2004) y APC (2015).

1.6. Mitos más comunes respecto a la violencia digital (Noción 4)

- **Mito 1: "Lo digital no es real; lo que pasa en internet se queda en internet."**
  Realidad material: El espacio presencial y digital están plenamente conectados. La violencia digital desencadena impactos materiales como la deserción escolar inmediata, aislamiento social, cuadros de ansiedad severa, depresión clínica e ideación o intentos de suicidio.
- **Mito 2: "Si no quieres que te afecte, solo apaga el teléfono o bloquea al agresor."**
  Realidad material: Minimiza la gravedad del daño y traslada la culpa hacia la víctima. Además, vulnera de manera arbitraria sus derechos humanos fundamentales a la educación, la comunicación, la información y la libre expresión en el entorno digital.
- **Mito 3: "La culpa o el error es de quien se tomó la fotografía íntima o la envió."**

Realidad material: Desplaza la responsabilidad del agresor. Compartir imágenes íntimas en relaciones de confianza es un ejercicio legítimo de la autonomía personal y sexual; la transgresión y el delito radican exclusivamente en quien rompe los acuerdos de confianza y difunde el material sin consentimiento.

- **Mito 4: "Es solo una broma entre compañeros o un juego de adolescentes."** *Realidad material:* Normaliza el acoso y la violencia sistemática a través de una supuesta cultura de la travesura. Las agresiones estructuradas por razones de género no pueden constituir humor ni juego, sino que son mecanismos disciplinadores de control patriarcal.

1.7. Principios del enfoque centrado en la víctima (Noción 5)

- **Credibilidad y presunción de verdad:** Otorgar valor probatorio inicial al testimonio de la víctima, sin que suponga sospechas sobre su conducta, vestimenta o estilo de vida digital.
- **No revictimización:** Evitar someter a la estudiante a múltiples interrogatorios, preguntas inquisitivas o juicios de valor moral respecto a sus decisiones íntimas.
- **Confidencialidad e intimidad:** Salvaguardar con estricta reserva los datos, identidades y evidencias del caso para evitar la filtración o rumores en la comunidad escolar.
- **Autonomía y participación:** Respetar el protagonismo de la víctima en la toma de decisiones sobre las medidas de protección y restitución a implementar y evitar imponer medidas punitivas o restrictivas sin su consentimiento.

2. TIPOLOGÍAS DE VGFT Y ANÁLISIS DE CASOS

2.1. Matriz de tipologías de la VGFT

CATEGORÍA	MANIFESTACIONES Y CONCEPTOS CLAVE
Violaciones a la intimidad sexual y los cuerpos	· **DNCII:** Difusión no consentida de imágenes o videos íntimos, así como la exigencia de dinero o nuevos contenidos bajo amenaza de divulgación.

CATEGORÍA	MANIFESTACIONES Y CONCEPTOS CLAVE
	· **Deepfakes / Contenido Sintético:** Manipulación de registros visuales mediante herramientas de inteligencia artificial para elaborar falsos desnudos. · **Ciberacecho:** Vigilancia sistemática, hostigamiento repetitivo o instalación de software de geolocalización sin consentimiento.
Hostigamiento, acoso colectivo y difamación	·**Ciberacoso / ciberbullying:** Ataques continuados orientados a descalificar, avergonzar o limitar la participación de la estudiante. · **Doxxeo (*Doxing*):** Divulgación no autorizada de datos personales confidenciales (dirección, teléfonos, documentos). · **Suplantación de Identidad:** Creación de perfiles paralelos con propósitos denigratorios o para generar conflictos dentro del centro educativo.
Captación y violencia estructural	· **Grooming:** Estrategia deliberada mediante la cual una persona adulta establece lazos de confianza con una persona menor de edad con fines de explotación o agresión sexual. · **Discursos de odio y linchamiento digital:** Convocatorias organizadas dirigidas a hostigar y deslegitimar a por ejemplo lideresas estudiantiles o educadoras.

Fuente: Elaboración propia en base a Ciberwarmis, ChildFund Bolivia & UMSA (2026), AGETIC, ONU Mujeres & Ipsos (2024), Centro S.O.S. Digital (2025) y UNFPA (2021).

2.2. Análisis de caso: El caso de Sofía

- **Contexto:** Sofía es delegada del centro de estudiantes de la ESFM y ha sido muy activa opinando sobre equidad de género en los talleres. Un grupo anónimo creó un perfil en TikTok usando Inteligencia Artificial para hacer un montaje de fotos de ella en ropa interior y publicando su número telefónico personal bajo el título: *"Busco atención, llámenme a este número"*. Sofía comenzó a recibir decenas de llamadas morbosas y amenazas de extraños.

- **Reacción docente inadecuada:** Al pedir ayuda, una docente le dice: *"Eso te pasa por exponerte tanto y meterte en temas polémicos en la institución. Mejor borra tu cuenta, cambia de número y mantén un perfil bajo para que se olviden de ti"*.
- **Preguntas de análisis:**
- ¿Qué tipos de violencia digital se observan?
  ¿Qué consecuencia pedagógica tiene la respuesta brindada por la docente?
    - A) Protege eficazmente la seguridad digital de Sofía.
    - B) Disciplina el comportamiento de los agresores anónimos.
    - C) Castiga el liderazgo de la estudiante y convalida la autocensura.
    - D) Es la única medida técnica realizable en entornos virtuales.

(Nota: Las soluciones y la fundamentación reflexiva de este caso se encuentran al final del documento, en la sección «ANEXO 2: SOLUCIONARIO Y ORIENTACIONES PARA EL ANÁLISIS DE CASOS».)

3. PREVENCIÓN, DETECCIÓN Y PRIMERA RESPUESTA EN LA PRÁCTICA DOCENTE

3.1. Estrategias didácticas de prevención: Límites, consentimiento y conductas de riesgo

Idealmente la prevención no debe ser entendida como una lista punitiva de "prohibiciones", en ese sentido el abordaje formativo en el aula debe ser dinámico, reflexivo, participativo y enraizado en situaciones cotidianas de la vida digital escolar.

1. Enseñar el consentimiento digital (La regla del "paso de la privacidad")

- **Concepto clave para el alumnado:** *El consentimiento digital no es universal ni permanente; es específico, voluntario, informado y revocable en cualquier momento.*
- **Estrategias didácticas en aula:**
    - **Análisis de escenarios hipotéticos ("¿Se puede o no se puede?"):** Plantear debates guiados con preguntas tipo: "Si una amiga te comparte una foto suya por chat privado, ¿tienes permiso implícito de subirla a tus historias o mandarla al grupo del curso?".

- **La regla del "pide permiso primero":** asentar el hábito reflexivo de que fotografiar, grabar video o realizar capturas de pantalla (screenshots) de conversaciones o contenidos privados para difundirlos exige la autorización explícita y previa de todas las personas involucradas.
- **Desmitificación del "si ya es público, puedo hacer lo que sea":** Establecer la clara distinción entre la decisión autónoma de una persona de publicar un contenido en sus redes y el derecho inexistente de terceros a reutilizar esa imagen para ridiculizarla, alterar su sentido, manipularla con IA o redistribuirla en otros entornos.

2. Definición y reconocimiento de límites digitales y personales

- **Concepto clave para el alumnado:** *Cada estudiante posee el derecho a fijar y exigir límites firmes sobre su tiempo, su cuerpo, sus datos personales, su imagen y su tranquilidad en el espacio digital.*
- **Estrategias didácticas en aula:**
  - **Mapeo interactivo "Espacios Seguros vs. Espacios de Presión":** Ejercicio de identificación colectiva sobre cuándo una interacción digital deja de ser lúdica o afectiva para convertirse en una dinámica de coacción (ej. exigencias de responder mensajes a altas horas de la noche, demandas de fotos para "demostrar amor o confianza", o exigencia de compartir contraseñas).
  - **Entrenamiento en asertividad digital:** Practicar en clase frases sencillas para establecer límites claros sin miedo al rechazo social.
    - *"No me siento cómodo/a enviando o compartiendo esto."*
    - *"Por favor elimina esa foto o comentario de inmediato; no autoricé su publicación."*
    - *"Prefiero salir de este grupo si van a dedicarse a denigrar o hablar mal de otras personas."*

3. Identificación de conductas de riesgo y manipulación en línea

- **Concepto clave para el alumnado:** *Desarrollar capacidad para detectar las "señales rojas" (red flags) y patrones de manipulación antes de que se concrete una situación de violencia, chantaje o abuso.*
- **Estrategias didácticas en aula:**

- **Desenmascarar la manipulación (Grooming y DNCII):**Enseñar a los estudiantes a reconocer patrones de persuasión y chantaje emocional que suelen usar agresores o adultos en la red:
  - *"Si me quisieras de verdad, me mandarías la foto."*
  - *"Es nuestro secreto, no le digas a nadie o me voy a enojar."*
  - *"Si no haces lo que te pido, voy a mostrar lo que me mandaste a tus papás/amigos."*
- **Evaluación de la huella digital y pérdida de control:** Ejercicio práctico para visualizar que todo lo enviado por canales digitales puede ser guardado o replicado en cuestión de segundos, independientemente de la confianza inicial.

4. Cuidado colectivo y desarticulación de la complicidad pasiva

- **Concepto clave para el alumnado:** *En el entorno digital, quien observa en silencio, celebra o reenvía un contenido violento no es un mero espectador neutro, sino un eslabón activo en la cadena de agresión.*
- **Estrategias Didácticas en Aula:**
  - **El rol del espectador/a activo/a:** Promover que el grupo escolar no sea un "público pasivo" frente al acoso. Enseñar 3 acciones concretas frente a un hecho de violencia en grupos de WhatsApp o redes:
    - **No ser megáfono:** No dar "like", no comentar con burlas y no reenviar contenido íntimo o difamatorio.
    - **Apoyar en privado:** Mandar un mensaje de respaldo a la persona agredida para que sepa que no está sola.
    - **Reportar y poner un alto:** Denunciar la publicación/cuenta en la plataforma y avisar a un adulto de confianza o profesor tutor.

3.2. Indicadores para la detección temprana en el aula

Las y los futuros maestros deben desarrollar una mirada atenta y sensible para detectar tempranamente las señales de alerta ante situaciones de violencia facilitada por la tecnología. Se debe prestar especial atención a los siguientes indicadores de comportamiento:

- **Indicadores emocionales y de conducta:**
  - Ansiedad o hipervigilancia excesiva al usar o recibir notificaciones en el teléfono celular durante clases (esconder la pantalla, sobresaltarse, revisar el dispositivo de forma obsesiva).

- Cambios drásticos de ánimo: tristeza repentina, llanto inmotivado, irritabilidad o expresiones de vergüenza extrema frente a sus pares.
- Aislamiento social repentino: dejar de juntarse con su grupo habitual, alejarse de los espacios comunes o evitar la participación en actividades grupales.

- **Indicadores académicos y de asistencia:**
  - Descenso brusco y notorio en el rendimiento escolar o en la entrega de tareas.
  - Ausentismo injustificado, faltas recurrentes los días posteriores a un fin de semana, o solicitudes constantes de ir al baño o enfermería para escapar del entorno escolar.
  - Autocensura: dejar de opinar en clases, apagar la cámara de forma permanente en clases virtuales o abandonar redes y plataformas digitales académicas donde solía participar.

3.3. Decálogo de primera respuesta docente

ACTUACIONES INADECUADAS (ERRORES FRECUENTES)	ACTUACIONES PERTINENTES (INTERVENCIÓN ÉTICA Y PROFESIONAL)
Culpabilizar o revictimizar: Emplear frases como "¿Por qué enviaste esas fotografías?".	**Escucha activa y validación:** Crear un ambiente seguro, privado y empático donde se ratifique que el daño vivido es legítimo.
Minimizar el hecho: Tratar el incidente como "juegos de adolescentes sin importancia".	**Desresponsabilizar a la víctima:** Dejar claro que la responsabilidad de la falta reside siempre en el agresor.
Imponer aislamiento: Exigir que la estudiante renuncie a sus redes sociales o suspenda su asistencia a clases.	**Preservar evidencias digitales:** Orientar en el guardado de capturas completas, enlaces web, fechas y perfiles infractores sin alterar los registros.

ACTUACIONES INADECUADAS (ERRORES FRECUENTES)	ACTUACIONES PERTINENTES (INTERVENCIÓN ÉTICA Y PROFESIONAL)
Eliminar el material de forma precipitada: Borrar las pruebas impide dar curso al debido proceso.	**Activar protocolos institucionales:** Canalizar la situación a las instancias internas conforme al Manual de Convivencia Pacífica y Armónica (Ministerio de Educación de Bolivia, 2021) y coordinar con los mecanismos de protección y bienestar estudiantil, garantizando reserva y discreción.
Filtrar información: Divulgar el caso entre el plantel educativo transformando la situación en rumor.	**Garantizar la permanencia escolar:** Asegurar el acompañamiento pedagógico y adaptaciones necesarias para que la formación académica no se interrumpa.

Fuente: Elaboración propia en base a UNFPA (2021) y Fundación InternetBolivia.org et al. (2024).

REFERENCIAS BIBLIOGRÁFICAS Y CONCEPTUALES

1. **Continuo de la violencia / Continuum of violence:**
    - Kelly, L. (1988). *Surviving Sexual Violence*. Polity Press.
2. **Violencia de Género Facilitada por la Tecnología (VGFT):**
    - APC - Asociación para el Progreso de las Comunicaciones (2015). *Violencia de género en línea: Respuestas para la libertad de expresión y la seguridad*. APC.
    - UNFPA - Fondo de Población de las Naciones Unidas (2021). *Mi cuerpo es mío: El derecho a la autonomía y la autodeterminación*. Informe sobre el Estado de la Población Mundial.
3. **Efecto de desinhibición en línea:**
    - Suler, J. (2004). *The Online Disinhibition Effect*. CyberPsychology & Behavior, 7(3), 321-326. (Fundamento teórico sobre cómo las pantallas y el anonimato/seudonimato reducen la empatía y facilitan la agresión).
4. **Datos e informes nacionales:**
    - AGETIC, ONU Mujeres & Ipsos. (2024). *Encuesta Nacional "Conectando Bolivia": Percepciones sobre género, violencia y uso de tecnologías de la información y la comunicación*. La Paz, Bolivia.
    - Ciberwarmis, ChildFund Bolivia & Observatorio de Políticas Públicas - UMSA. (2026). *Cuerpos, pantallas y algoritmos: Sexualidad digital en adolescentes y jóvenes y su relación con la violencia digital en Bolivia*. La Paz, Bolivia.
    - Centro S.O.S. Digital (2025). *Reporte estadístico quinquenal de atenciones por ciberviolencia de género y cibercrimen (2021-2025)*. La Paz, Bolivia.
5. **Marcos normativos y guías:**
    - Ministerio de Educación de Bolivia (2021). *Manual de Convivencia Pacífica y Armónica en Unidades Educativas y ESFM*. La Paz, Bolivia: Ministerio de Educación.
    - Fundación InternetBolivia.org, AGETIC & ONU Mujeres. (2024). *Guía de prevención y atención: Violencia de género facilitada por la tecnología*. La Paz, Bolivia.

ANEXO 1: RECURSOS DE AUTOAPRENDIZAJE Y MATERIAL COMPLEMENTARIO

Lecturas, recursos web y material complementario

Para profundizar en la temática, se recomienda la revisión de las siguientes investigaciones y plataformas web especializadas en derechos digitales y prevención de la VGFT:

Informes institucionales e investigación nacional:

- Encuesta Nacional "Conectando Bolivia: Percepciones sobre género, violencia y uso de tecnologías de la información y la comunicación" (AGETIC, ONU Mujeres & Ipsos, 2024).
- Ciberwarmis, ChildFund Bolivia & Observatorio de Políticas Públicas - UMSA. (2026). *Cuerpos, pantallas y algoritmos: Sexualidad digital en adolescentes y jóvenes y su relación con la violencia digital en Bolivia*. La Paz, Bolivia.
- Guía de prevención y atención: Violencia de género facilitada por la tecnología (Fundación InternetBolivia.org, AGETIC & ONU Mujeres, 2024).
- Reportes estadísticos anuales del Centro S.O.S. Digital (2025).

Plataformas y portales web de referencia nacional e internacional:

- **Centro S.O.S. Digital / Fundación InternetBolivia.org (Bolivia):** Plataforma de acompañamiento holístico, generación de datos empíricos y reportes sobre ciberviolencia de género y cibercrimen en el país (sosdigital.internetbolivia.org).
- **Asociación para el Progreso de las Comunicaciones - APC / Dominemos la Tecnología! (Global):** Campaña internacional con mapas de seguridad digital, investigación sobre violencia en línea e incidencia en derechos de las mujeres (takebackthetech.net / apc.org).
- **Derechos Digitales (América Latina):** Organización regional dedicada a la defensa, estudio y promoción de los derechos humanos en el entorno digital, con enfoque en privacidad y género (derechosdigitales.org).
- **Fondo de Población de las Naciones Unidas - UNFPA (#Bodyright):** Iniciativa global para la protección de la autonomía corporal y la intimidad frente al abuso en entornos digitales (unfpa.org).

ANEXO 2: SOLUCIONARIO Y ORIENTACIONES PARA EL ANÁLISIS DE CASOS

Solución al caso 2.2: El caso de Sofía

- **Respuesta correcta 1:** En este caso se observan los siguientes tipos de violencia:

  Difusión no consentida de imágenes o contenido íntimo (DNCII) / Manipulación sintética (Deepfakes):

  Se utilizan herramientas de Inteligencia Artificial para crear un montaje de las fotografías de Sofía en ropa interior sin su autorización ni consentimiento, con el fin de exponerla, vulnerar su intimidad y dañar su imagen.

  Doxing:

  Al publicar y difundir públicamente el número telefónico personal de Sofía en un entorno digital y sin su consentimiento, exponiéndola al hostigamiento masivo de terceros.

  Ciberacecho / Hostigamiento masivo:

  La publicación malintencionada desencadena una ola de llamadas morbosas y amenazas de extraños, lo que constituye hostigamiento digital que vulnera su seguridad y tranquilidad.

  Violencia basada en género con fines de disciplinamiento político:

  El ataque está dirigido específicamente contra Sofía debido a su rol activo como delegada y su participación opinando sobre equidad de género en los talleres, buscando castigarla, avergonzarla públicamente y silenciar su liderazgo.

- **Respuesta correcta 2:** C) Castiga el liderazgo de la estudiante y convalida la autocensura.

  Análisis reflexivo:

  La opción C es la correcta. La respuesta de la docente desplaza erróneamente la responsabilidad del ataque hacia la víctima (*victim-blaming*), institucionaliza la autocensura y castiga el ejercicio del liderazgo político de Sofía en la ESFM. Lejos de ofrecer protección, valida la impunidad de los agresores anónimos y restringe sus derechos a la libertad de expresión y a la educación.

Fundamentación:

Frente a una situación de esta naturaleza, el equipo docente debe actuar respetando el enfoque centrado en la víctima a través de los siguientes pasos:

1. **Contención empática e incondicional:** Escuchar a Sofía sin emitir juicios de valor moral, reafirmando que la culpa del ataque es exclusivamente de quienes vulneraron su intimidad.
2. **Preservación de evidencia digital:** Acompañar a la estudiante en el guardado metódico de capturas de pantalla de la cuenta de TikTok, las publicaciones, los números entrantes y las amenazas recibidas.
3. **Activación de la ruta institucional:** Derivar el caso de forma confidencial a la Dirección de la ESFM y a la comisión de convivencia/bienestar estudiantil para iniciar el abordaje correspondiente.
4. **Protección del derecho a la permanencia y participación:** Garantizar que Sofía mantenga su rol de delegada estudiantil y su asistencia regular sin que se le exija recluirse o cambiar sus dinámicas académicas ni personales.