Curso “Ciudadanía y Derechos Humanos en la era digital”

Módulo 1. Violencia digital de género
Documento de contenido

Docentes: Cielito Saravia y Lu An Méndez

1. Objetivo de aprendizaje

Identificar qué es la violencia digital de género, las formas de respuesta y comprender la seguridad digital holística desde una perspectiva feminista.

2. Programa del curso

1. ¿Qué es violencia digital de género?
2. Violencias digitales de género más comunes.
3. ¿Qué es seguridad digital?
4. Estrategias para afrontar la violencia digital.

3. Marco teórico

3.1. ¿Qué es la violencia digital?

> *“Internet es una de las plataformas más poderosas y ofrece grandes oportunidades para compartir ideas y construir comunidad, pero las mujeres son silenciadas con demasiada frecuencia y censuradas, lo qué es una grave amenaza para los avances en materia de igualdad de género. Cuando las mujeres tienen menos espacio en línea, tienen menos espacio en las salas de redacción, las salas de reuniones y los pasillos donde se toman las decisiones políticas.”*
>
> *(Tech Policy Design Lab: Online Gender-Based Violence and Abuse.*
>
> *World Wide Web Foundation - 2021)*[1]

La violencia de género traspasa el entorno físico y se expresa también en el entorno digital, a esto se le llama violencia digital de género. Es importante recordar que la violencia de género es consecuencia de la desigualdad que persiste en las relaciones entre hombres y mujeres, que está definida por los roles que socialmente se han construido sobre lo femenino y lo masculino.

La Asociación de Comunicaciones para el progreso (APC) una organización internacional de sociedad civil, define a la violencia digital de género como:

> *“La violencia digital de género o en línea se refiere a actos de violencia de género cometidos instigados o agravados, en parte o totalmente, por el uso de las Tecnologías de la Información y la Comunicación (TIC), plataformas de redes sociales y correo electrónico. Estas violencias causan daño psicológico*

[1] https://techlab.webfoundation.org/ogbv/overview

y emocional, refuerzan los prejuicios, dañan la reputación, causan pérdidas económicas y plantean barreras a la participación en la vida pública y pueden conducir a formas de violencia sexual y otras formas de violencia física."

Este concepto es bastante completo y nos brinda herramientas para tener una mejor comprensión de las violencias digitales, en primer lugar nos dice que esta violencia no solo se la ejerce en el mundo digital, también ocurre cuando se utiliza las tecnologías de información y comunicación para incitar a ejercer violencia fuera o dentro de Internet, por ejemplo cuando en Internet se publica información difamatoria sobre una persona y se invita a las y a los usuarios a salir a las calles y ejercer violencia en ese espacio. Por otro lado, la violencia de género puede empezar en el mundo físico como la violencia física o psicológica y agravarse en Internet, por ejemplo cuando en una relación de noviazgo violenta, uno de los integrantes publica la imagen íntima de la otra persona sin su consentimiento.

En ese sentido, es común leer o escuchar "*lo virtual es real"* para referirse a que las violencias digitales son reales y lo que pasa en Internet también lo es, se tiende a pensar el mundo físico y el mundo digital como algo separado, sin embargo no existe tal división, lo que pasa en uno afecta al otro y viceversa.

Las violencias digitales no son un nuevo tipo de violencia sino que representan la violencia histórica que mujeres, niñas, adolescentes, poblaciones indígenas y otras poblaciones enfrentan hasta la actualidad. Estas violencias encontraron una nueva forma y espacio para expresarse en Internet. A continuación, una breve explicación de las formas en que distintas poblaciones enfrentan las violencias digitales:

- Según el Estudio Conectadas y Seguras (2021) de Plan Internacional Bolivia[2], 7 de cada 10 niñas en Bolivia manifestaron que sintieron acoso en línea en algún momento de su vida. La misma cantidad refiere que piensa dos veces antes de expresar sus opiniones en línea por temor a ser víctimas de violencia o juzgadas. En relación a esto, la investigación "Los retos de las niñas y mujeres de la tercera edad para sobrevivir a la brecha digital en tiempos de pandemia en el departamento de La Paz"[3] menciona que las niñas y adolescentes han generado cierta desconfianza con el uso de la tecnología, las niñas y adolescentes entrevistadas para este estudio consideran que este espacio no es seguro para ellas, por experiencias de acoso que enfrentaron mientras usaban Internet, mencionan que el gusto y la motivación con la que se conectan y navegan por Internet para resolver sus tareas y aprender cosas nuevas se pone en juego cuando enfrentan ciberacoso, también reconocen que existen otros tipos de peligros en Internet y que las niñas y adolescentes se encuentran en riesgo por estar conectadas. Esta relación de desconfianza con las tecnologías generada por las violencias digitales afecta el desempeño escolar, reduce el interés y deseo de querer formar parte del mundo de la ciencia y tecnología, generando una sensación desgastante de que al igual que fuera de Internet las niñas tienen la sensación de tener que cuidarse todo el tiempo.

---

2 https://plan-international.org/bolivia/noticias/2021/10/06/siete-de-10-ninas-en-bolivia-sintieron-acoso-en-linea-en-algun-momento-de-su-vida/

3 https://internetbolivia.org/actividades/publicaciones/los-retos-de-ninas-y-mujeres-de-la-tercera-edad-para-sobrevivir/

- Sobre la experiencia de las mujeres adultas y las violencias digitales, el año 2019 la Fundación Internet Bolivia.org realizó un sondeo sobre violencia digital, participaron 1.123 mujeres mujeres de las cuales casi 900 recibieron mensajes molestos de forma repetitiva en medios digitales, 337 recibieron insultos en redes por su identidad sexual, 813 dijeron que hubo un intento de "hackeo" a sus cuentas personales y 300 mujeres dijeron que en algún momento se publicó información personal sin su consentimiento como: nombre completo, número de celular, correo electrónico, entre otros.
- Las violencias digitales también impiden que las comunidades LGBTQI+ utilicen y se beneficien de Internet. La desigualdad estructural, la discriminación y patriarcado también se reproducen en el mundo digital y la comunidad LGBTQI+ se enfrenta a estereotipos de género, vigilancia, discursos de odio, contenido transfóbico, homofóbico, entre otros tipos de violencia cuando se conectan a Internet, lo que genera que las personas disidentes sexuales y de género se alejen de estas tecnologías y dejen de beneficiarse de ellas. [4]

3.1.1. Características de la violencia digital

Si bien la violencia digital tiene la misma raíz que las violencias de género que es la desigualdad estructural, las violencias digitales tienen características propias, revisamos algunas.

- **Espacio geográfico:** No es necesario que la persona agresora se encuentre en el mismo espacio físico para hacer daño, es decir la persona que ejerce violencia digital puede estar en cualquier lugar del mundo.
- **Anonimidad:** La anonimidad en Internet es un derecho nos permite expresar nuestras opiniones sin temor a represalias, históricamente el anonimato ha sido uno de los garantes de la libertad de expresión y fuera y en Internet.[5] Sin embargo, también se utiliza la anonimidad para ejercer violencia en Internet.
- **Se interrelaciona con otras violencias:** La violencia digital no actúa sola, muchas veces las personas que ejercen violencia digital no solamente están enfrentando un tipo de violencia digital, si no que enfrentan varios tipos de violencia al mismo tiempo.

3.1.2. Efectos de la violencia digital.

La violencia digital de género vulnera y castiga el derecho de las mujeres a la libre expresión de la sexualidad, especialmente en el caso de extorsión sexual y la difusión de imágenes íntimas sin consentimiento (esto ocurre cuando una persona publica una imagen íntima de otra persona sin el permiso de quien sale en la foto, o pide dinero o algún otro tipo de solicitud con la condición de no subir el contenido íntimo). Por medio de la impunidad y la culpa, muchas mujeres se ven obligadas a aceptar la violencia como una situación inevitable y las deja sintiéndose abrumadas, aisladas y solas.[6]

4

[5] https://www.derechosdigitales.org/6173/el-anonimato-es-un-derecho/
[6] https://hiperderecho.org/wp-content/uploads/2020/12/Informe-1_Despue%CC%81s-de-la-ley.pdf

Otros efectos que pueden experimentar quienes enfrentan violencias digitales son:

- Sensación de desconfianza y miedo al usar tecnología. Como Internet es parte de nuestras vidas, se enfrentan ante la necesidad de superar ese temor para que puedan desarrollar sus actividades diarias.[7]
- Muchas de las personas que ejercen violencia digital utilizan datos personales de las mujeres y población LQBTQI+ para este fin, esto tiene un impacto sobre la integridad física de las mujeres, y sobre su capacidad para moverse y emitir sus opiniones libremente sin temor a ser vigiladas/es o acosadas/es.[8]
- La violencia que sucede a través del uso de la tecnología ocasiona daño psicológico y emocional, daños en la reputación, pérdidas económicas ya que dificulta a la víctima la obtención de empleo o su conservación. Inclusive, puede frenar la búsqueda de oportunidades laborales. También genera grandes barreras para el normal desarrollo de la vida pública de la persona quienes enfrentan violencias digitales recurren a retirarse de la vida pública, familiar y social, se experimenta una pérdida de confianza en la red de contactos y en las comunidades donde se originó la relación con el agresor.

Según el estudio Conectadas y Seguras situación de las niñas en Bolivia elaborado por Plan Internacional Bolivia el 2020[9]:

- 5 de cada 10 niñas nunca le contaron a nadie que enfrentaron violencia digital.
- 4 de cada 1.000 niñas ha denunciado la violencia digital que enfrentaba en la policía o la defensoría.
- Las niñas prefieren contar a algún amigo o amiga que estén enfrentando violencias digitales.

Estos datos reflejan algunos efectos de la violencia digital como el autocastigo, la vergüenza, la ridiculización, la culpa, la creencia de que son las únicas personas que están enfrentando estas agresiones. Estos efectos hacen que las personas que enfrentan violencia digital no expresan lo que les está pasando o cómo se sienten al respecto en sus círculos de apoyo (amistades, familia, etc.) y enfrentan la violencia digital de forma solitaria por miedo a ser juzgadas.

3.2. Violencias digitales de género más frecuentes.

Las violencias digitales de género no son un fenómeno nuevo, son violencias estructurales reflejadas en otro espacio: la tecnología. Los tipos de violencias más comunes que atraviesan las mujeres, solo por el hecho de ser mujeres, según las estadísticas del Centro S.O.S Digital[10] son: el acoso, abuso de información personal usando las TIC y abuso sexual relacionado a las TIC.

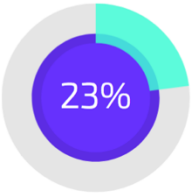
---

[7] Ídem.
[8] Ídem.
[9] https://plan-international.org/bolivia/noticias/2021/10/06/siete-de-10-ninas-en-bolivia-sintieron-acoso-en-linea-en-algun-momento-de-su-vida/
[10] Reporte de violencias digitales más frecuentes del 2021 registrados https://sosdigital.internetbolivia.org/reporte-sos/ El Centro S.O.S. Digital, de la Fundación InternetBolivia.org es una organización de sociedad civil que atiende a denunciantes que están pasando por una violencia de género facilitadas por las tecnologías de información y comunicación en Bolivia

Violencias digitales
MÁS FRECUENTES

ACOSO

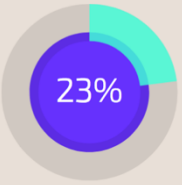
Conductas de carácter reiterado públicos y privados donde se reciben contenidos no solicitados (material sexualizado, insultos, amenazas, expresiones discriminatorias) que resultan **molestas e intimidantes.**



- Acoso sistemático con insultos: casos donde son desde 6 meses, 1 año y 3 años.
- Amenazas de agresión física, violación muerte o violencia a un familiar o persona cercana.
- Envío de contenido a familiares o personas cercanas:en menos cantidad pero con agravante.
- Mensajes con insultos y amenazas de perfiles falsos.
- Amenazas sistemáticas.
- En menor cantidad, realizan denuncias en la FELCV que no son aceptadas.

ABUSO DE INFORMACIÓN PERSONAL USANDO LAS TIC

Robo, obtención, pérdida, control o modificación de información personal no consentida



- Acoso sistemático
- Desprestigio, algunas usando imágenes manipuladas.
- Publicación de datos personales, nombres, contratos, usuarios de twitter con afinidad política.

Las violencias digitales de género son múltiples y se experimentan de manera simultánea sobre todo en mujeres que ejercen un rol público o político con el objetivo de excluirlas de la esfera pública. En el 2016, la Unión Interparlamentario sacó un reporte[11] sobre mujeres parlamentarias en cinco regiones. Según ese reporte, el 82% de las parlamentarias denunció haber experimentado algún tipo de violencia sexual durante su mandato por medios y redes sociales. La violencia sexual en línea se manifestaba con comentarios, gestos e imágenes de naturaleza sexista o sexualmente humillante, amenazas y acoso laboral. El 44% denunció haber recibido amenazas de muerte, violación, agresión o secuestro dirigidas contra ellas o sus familias. El 65% había sido objeto de comentarios sexistas, principalmente por parte de parlamentarios[12] los tipos de violencias digitales de género motivadas por la actividad política más comunes son: el acoso y la violencia política digital, la difamación virtual, discursos de odio, acecho y violación de datos personales.

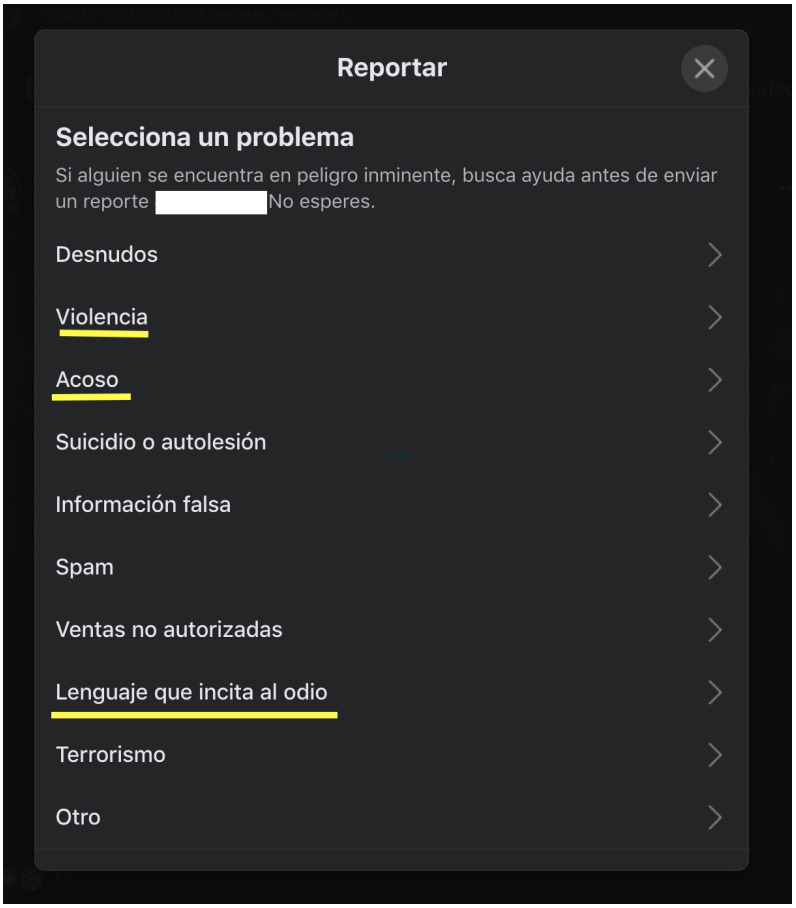
Las violencias digitales han cobrado fuerza e interés en los últimos años por la virtualización de actividades a causa del confinamiento, y porque las violencias en línea son novedosas, sobre todo para personas que recién están comenzando su relación con la tecnología. Es por esto que es invisibilizada, ya que se desconocen los riesgos, formas en las que se realiza la violencia y el impacto que puede tener en la vida de una persona o comunidad.

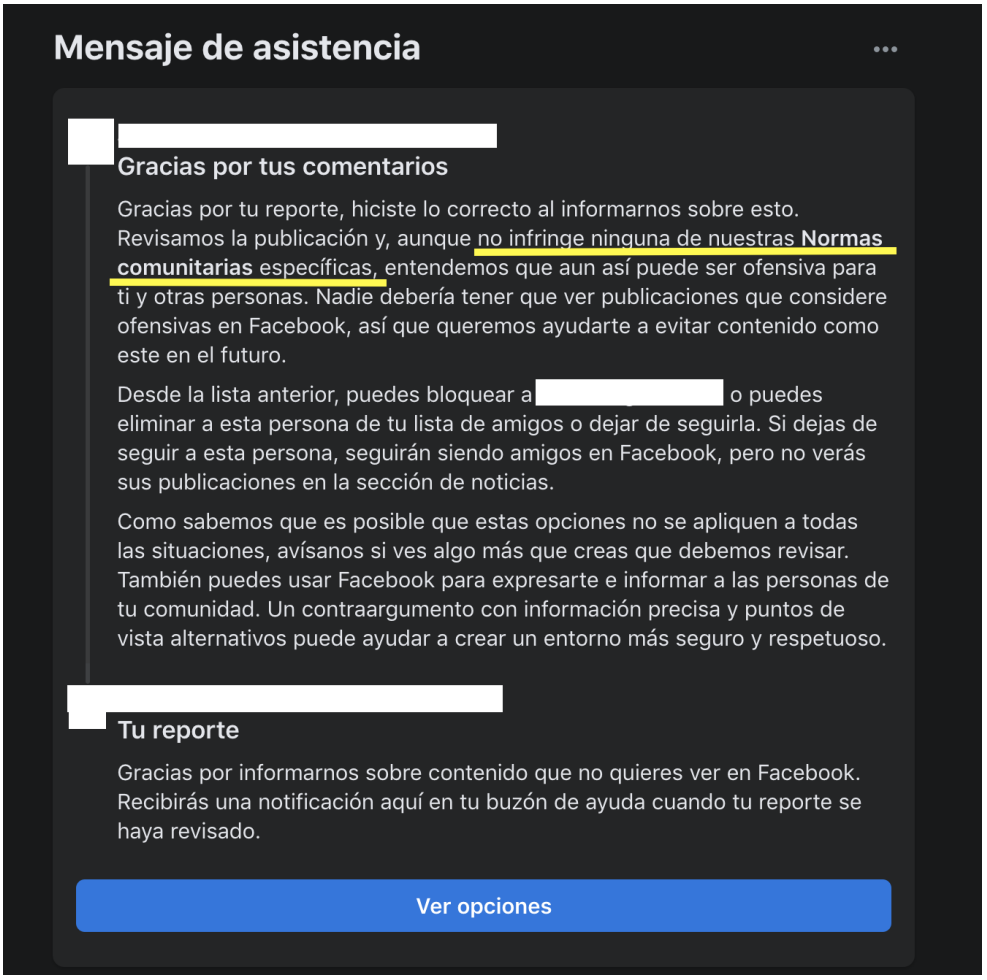
Esta característica alimenta una **cultura de la impunidad en torno a las violencias digitales**. Que si bien, es común en el sistema judicial donde las mujeres se vean disuadidas de denunciar a las personas que comenten actos violentos, también es común la

[11] Unión Interparlamentaria (2016). Sexismo, acoso y violencia contra las mujeres parlamentarias, pág. 3

[12]

impunidad en las plataformas digitales que tienden a tener una respuesta poca proporcional a un acto violento. Uno de los casos que mejor ejemplifica esta característica de impunidad por parte de las plataformas digitales se da cuando se denuncia un perfil falso que usa fotos reales de una menor de edad o una mujer. Estas fotos y contenido en general son robadas de un perfil real, es decir, es un perfil que ha robado la identidad de una mujer. Es común que la plataforma digital (Facebook, Instagram, TikTok) no identifique que se haya cometido una infracción a sus Normas o Lineamientos Comunitarios por lo tanto, no tome ninguna acción (eliminar el perfil o contenido, dar una advertencia al usuario, poner una limitación a la cantidad de personas que llegan sus contenidos o como comúnmente se lo conoce “ponerle en la cárcel” por incumplir las normas).





En un contexto de minimización de las violencias, escasa concientización en funcionarios y funcionarias públicas lo que ocasiona una falta de eficacia en la atención ante violencias digitales, carencia en la regulación de delitos digitales, datos insuficientes de casos de violencia digital, ausencia de un sujeto punible por el anonimato –que retrasa el proceso judicial- y el analfabetismo digital, entre otras, es que la atención a las violencias digitales recae en la víctima/denunciante y las personas que la acompañan en la denuncia –que generalmente son su familia, amigas o alguna especialista de sociedad civil- de la violencia y sus habilidades digitales para poder prevenir y resistirlas. Estas habilidades que se refuerzan o van generando, son conocidas como estrategias de seguridad digital.

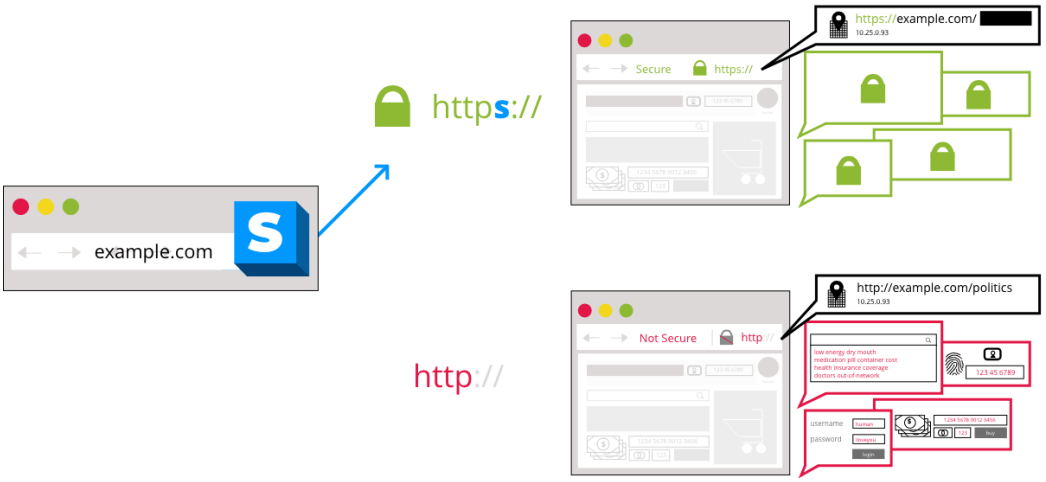
3.3. ¿Qué es seguridad digital?

La seguridad digital holística brinda estrategias y herramientas para hacer frente a la creciente hostilidad en Internet. Se puede resistir a las violencias digitales desde:

a) La prevención y reacción **tecnológica.**
b) El conocimiento sobre la **normativa nacional** que concierne a las agresiones en Internet.
c) Y el acompañamiento a mujeres denunciantes de estas violencias con la **contención psicológica**.

Al mismo tiempo, estas acciones son divididas en estrategias de prevención y reacción. En la prevención, esto hace referencia a:

- Conocer qué **derechos tienen las personas en Internet** para identificar con mayor facilidad alguna vulneración.
- Mapear a las personas y **organizaciones que puedan brindar ayuda** en caso de incidentes de seguridad. Esto es de mucha ayuda en el momento de una crisis, ya que permite una reacción rápida.
- Generar **hábitos digitales** para proteger los datos personales, comunicaciones y privacidad mientras habitamos las redes sociales e Internet en general, como ser:
    - Solo ingresar a páginas que tienen un protocolo de seguridad (HTTPS) que cifra la información. Lo que se busca es evitar conectarse a páginas que solo tienen HTTP ya que no cuentan con la protección necesaria. Para esto se puede instalar el complemento de navegador HTTPS *everywhere* que te muestra un mensaje grande cuando ingresan a una página que no tiene cifrado.



Fuente: HTTPS Everywhere - https://www.eff.org/https-everywhere

    - Tener contraseñas seguras, que contengan mayúsculas, minúsculas, símbolos y números. Con preferencia deberían tener 8 caracteres y deber ser cambiadas cada 6 meses. Para administrar las contraseñas se recomienda usar un gestor de contraseñas[13].
    - Generar respaldos de la información importante y guardarla en un lugar seguro (USB, DVD, disco duro u otro que tenga disponible). Se recomienda hacer una limpieza cada 3 ó 6 meses de archivos (fotos, videos, documentos,

[13]Los gestores de contraseñas son aplicaciones que sirven para almacenar usuarios y contraseñas en una base de datos cifrada mediante una contraseña principal. De este modo, se puede gestionar los usuarios y contraseñas memorizando únicamente una contraseña principal. Se recomienda explorar esta herramienta: KeyPassXC https://keepassxc.org/

apps, etc.) de los dispositivos que se tienen, es decir, eliminar los archivos o aplicaciones que no son de utilidad.
- Evitar ingresar a enlaces desconocidos.
- Cuidar la información personal al llenar formularios o ingresar nuestros datos en plataformas desconocidas.
- Evitar agregar a perfiles desconocidos en redes sociales.
- Activar la verificación/autenticación en 2 pasos.
- En general, familiarizarse con los procesos de personalización de seguridad. Para facilitarlo, se recomienda aprender a reconocer los símbolos que las empresas de tecnología usan para señalar las opciones de seguridad y privacidad.

Elaboración: Cielito Saravia G.

En la reacción, puede ser:

- Conocer el aspecto **legal** (normativa, delitos, procesos de denuncia) que tiene relación con las violencias digitales para realizar una denuncia a las instancias pertinentes[14], lo que se verá con mayor detalle en el caso de niñez y mujeres en el tema Estrategias para afrontar la violencia digital hacia la niñez y mujeres.
    - Hay países en América del Sur que no cuentan con normativa que permite la sanción penal de agresores que perpetúan crímenes en línea como la suplantación de identidad, ciberacoso, amenazas en línea, difusión de imágenes íntimas sin consentimiento e ingreso a cuentas sin consentimiento, entre otras. Sin embargo, es importante notar que tomar la vía política, y

[14] El proceso de denuncia de mujeres que están en una situación de violencia digital no es la misma que el de una menor de edad u hombre.

pensar que detrás de lo jurídico hay amarres, arreglos y alianzas que no le favorecen a las mujeres es complejo[15]

- También puede ser contar con **protocolos** o acciones comunitarias que puedan ser desplegadas en caso de una violencia digital, como mandar el enlace de un perfil agresor a grupos de confianza para que denuncien el contenido. Esto si bien es conocido, de manera anecdótica, como un método para bajar perfiles, no hay confirmación por parte de las empresas de tecnología (Facebook, Google, etc.) que sea una práctica eficaz ya que algunos de sus procesos internos de moderación de contenidos son desconocidos.
- Llamar a una reunión para generar un grupo **autocuidado** o medidas para poder acompañar a la/las personas afectadas por la violencia digital. Estos espacios resultan ser importantes, no solo para la contención, sino sobre todo porque ayuda a identificar patrones, posibles riesgos e incluso podría llegar a identificar agresores sin tener que contar con herramientas sofisticadas tecnológicas.
    - En caso de conocer a una persona que está pasando por una situación violenta en Internet se puede acompañarla con la escucha activa, respetando lo que la persona nos cuenta y los sentimientos que tiene en ese momento. Esto se complementa con la habilidad de ponernos en el lugar de la persona para entender que se encuentra frente a verdaderos peligros físicos y psicológicos. La falta de empatía puede generar una actitud negativa al responsabilizar a la persona que se quiere acompañar re victimizándola y no así a las personas que le agreden, quienes son las únicas culpables. Estas estrategias son conocidas como los PAP (Primero auxilios psicológicos) que tienen como objetivo acompañar a personas a procesar su crisis, a encontrar sentido y a cultivar su resiliencia.

- **Acciones que tomamos para recobrar control sobre nuestra información personal o reportar contenido que nos violenta en línea.** Ya que la mayor parte de las agresiones en línea se dan en redes sociales, es común que la interacción que tengamos sea con Facebook, Instagram o Twitter. Estas plataformas tienen procedimientos y formularios que permiten la denuncia de contenido, perfiles o grupos que violan sus normas comunitarias. Las denuncias son analizadas por las empresas, de manera manual y automática, para decidir si se quita el contenido, si se da una sanción a la persona agresora o se elimina el perfil, contenido o grupo.

3.3.1. Perspectiva feminista de la seguridad digital.

Las perspectivas feministas de la seguridad digital tienen un enfoque holístico y de género. Estas perspectivas nacen en un entorno donde las violencias digitales son abordadas por comunidades de ingenieros y tecnólogos. Son agrupaciones mayormente conocidas como CSIRT (*Computer Security Incident Response Team*) por sus siglas en inglés que significa: Equipo de respuesta a incidentes de seguridad informática.

Estos equipos tienden a considerar los impactos en los sistemas (celulares, computadoras, servidores, redes internas, Internet etc.) y mejorar los niveles de seguridad en dichos

[15] Hacks de Vida: https://caracolazul.espora.org/hacks-de-vida/

sistemas. La seguridad digital con perspectiva de género propone, además de la mejora de seguridad informática –que pone al centro a la tecnología-, trabajar en:

- Procesos de **alfabetización digital** (conocer qué es Internet, usos de dispositivos, reconocimiento de simbología en Internet, etc.),
- **Cuidado colectivo** (que los procesos y hábitos de seguridad sean adoptados por todas y todos de una comunidad –la cadena de la seguridad es tan fuerte como su eslabón más débil-),
- **Impactos** de las violencias (que tienen efectos psicológicos, físicos, en la comunidad, etc),
- El **rol** de las empresas de tecnología, academia, Estado y organizaciones que definen estándares y políticas de tecnología e Internet como la Corporación para la Asignación de Nombres y Números en Internet (ICANN)[16], Consorcio de la World Wide Web (W3C)[17], Unión Internacional de Telecomunicaciones (UIT)[18], entre otros.
- **Evitar procesos de culpabilización y revictimización** (comentarios como “no deberías haber publicado esa foto/comentario” “Pero acaso te ha pegado?” “Bloquealo no más” “Seguro tú has apretado algo y por eso se ha arruinado”, etc.)

Es decir, ponen al centro a las personas y su relación con la tecnología. Esta perspectiva permite tener un análisis crítico de los procesos de tomas de decisión relacionados a Internet, como ser:

- La moderación de contenidos: qué tipo de contenidos (publicaciones en redes sociales, comentarios, etc.) deberían ser quitados y porqué, quienes son las personas que toman esta decisión, la implementación de procesos automatizados -cuando la solicitud de eliminar un perfil o contenido es definido por la inteligencia artificial de la red social-, entre otras.
- Políticas públicas o legislación relacionada a la tecnología: cómo proteger ciudadanos, definir delitos digitales, tener protocolos de seguridad implementados en caso de un incidente, etc.
- Definición de nombres de dominios (.com .org .net .bo .gob) quienes deciden crear nuevos dominios, cuándo y dónde se reúnen, cuales son las consideraciones técnicas para proteger la privacidad, en qué idiomas se dan estas conversaciones, cual es el rol de sociedad civil, empresas y Estado en estos espacios, etc.

El enfoque holístico se refiere al tratamiento de la seguridad digital, el bienestar psicosocial y los procesos de seguridad organizacional, como procesos integrados y destaca su

[16] ICANN es s una corporación de beneficio público, sin fines de lucro, con participantes de todo el mundo dedicados a mantener una Internet segura, estable e interoperable. https://www.icann.org/

[17] W3C es un consorcio internacional que genera recomendaciones y estándares que aseguran el crecimiento de la World Wide Web a largo plazo https://www.w3.org

[18] La UIT es un organismo especial de Naciones Unidas que está comprometida para conectar a toda la población mundial https://www.itu.int/

interrelación[19]. El autocuidado, el bienestar, la seguridad digital y la seguridad de la información son consideradas dentro de las prácticas tradicionales de gestión de la seguridad.

El autocuidado es una parte esencial de la práctica de seguridad digital holística que contempla procesos de reflexión e introspección. Sus prácticas son variadas y cambiantes de acuerdo a cada persona que las realiza. Cada una puede construir sus propias definiciones de autocuidado, por ejemplo:

- Revisar las configuraciones de seguridad y privacidad de las redes sociales y cuentas en Internet regularmente.
- Poner límites a horarios de conexión.
- Buscar redes de apoyo en línea.
- Cerrar los ojos y meditar después de estar 3 horas frente a una pantalla.
- Explorar terapias alternativas con propiedades relajantes: aromaterapia, meditación, etc.

La seguridad de la información desde una perspectiva feminista apuesta por la autonomía tecnológica. Es decir, recobrar control sobre la información y comunicaciones intercambiadas en las TIC para no depender de empresas que replican modelos patriarcales, capitalistas y extractivistas en Internet. Esto nace de un concepto de trabajar con la tecnología desde una perspectiva feminista que no se limita al uso de las TIC pero tiene una reflexión filosófica, sociológica y política sobre la adopción de software libre y nuestra agencia en la toma de decisiones sobre las estrategias y herramientas más adecuadas a usar para protegernos.

3.3.2. Las estrategias de seguridad digital feminista se plantean desde 4 líneas de acción[20]:

- **Reducir.** Menos es más. Los datos que no se crean no pueden ser recogidos, analizados, almacenados o vendidos. Esta estrategia se basa en la premisa de que cuantos menos datos produzcamos es mejor. Esto se puede poner en práctica al limitar la cantidad de información entregada en Internet, por ejemplo, no es necesario rellenar todos los campos de los formularios de registro. También se puede eliminar las aplicaciones del dispositivo móvil que ya no utiliza, borrar imágenes, correos electrónicos y mensajes que estén desactualizados. Por otro lado, se puede instalar complementos al navegador usados para para impedir que las *cookies*[21] y otros *scripts*[22] de terceros se ejecuten y recojan datos, como *Privacy Badger*[23].

[19] Holistic Security: https://holistic-security.tacticaltech.org/

[20] Yo y mi sombra: https://myshadow.org/es

[21] Las cookies son pequeños fragmentos de texto que los sitios web envían al navegador. Permiten que los sitios web recuerden información sobre las visitas, lo que puede hacer que sea más fácil volver a visitar los sitios y hacer que estos resulten más útiles.

[22] Un script es un programa insertado dentro del documento html y que es interpretado y ejecutado por el navegador del usuario o usuario. El navegador hace cosas en la página según le diga el programa insertado en ella.

[23] Privacy Badger es una extensión para el navegador que evita que los anunciantes y otros rastreadores de terceros rastreen secretamente adónde va y qué páginas ve en la web. https://privacybadger.org/

- **Camuflar.** Confundir a las empresas, esto implica crear mucha información falsa de una misma para que las empresas, los gobiernos u otras personas no entiendan qué datos son verdaderos y cuáles son falsos. Se puede realizar creando perfiles falsos en redes sociales con nombres o imágenes similares. Se puede instalar *Adnausium*[24], una herramienta que crea ruido digital haciendo clic en anuncios aleatorios de manera automática. Se puede también usar una VPN (*Virtual Private Network* o red privada virtual) esta herramienta disfraza la identidad en línea cambiando la dirección IP[25], esto dificulta hacer un seguimiento de las actividades en línea de una persona.
- **Diversidad de Perfiles.** Fuera de la red tenemos diferentes personas en diferentes situaciones sociales: en el trabajo o en la escuela podemos ser una versión diferente de nosotras/os mismas/os que en casa, en el bar o en el trabajo. Esta estrategia consiste en gestionar múltiples personas en línea, separando las diferentes redes sociales, intereses, comportamientos, información e identidades. Se puede usar diferentes navegadores para ciertos conjuntos de actividades en línea; diferentes aplicaciones de mensajería para diferentes círculos sociales; aislar los datos valiosos o personales almacenándolos en un dispositivo diferente que permita desvincular la vida laboral de la vida social así se tiene diferentes cuentas de correo electrónico y número de celular para cada una.
- **Fortificar**
  Crear barreras, restringir el acceso y la visibilidad. Esta estrategia es para mantener los datos a salvo de miradas indiscretas a través de la generación de contraseñas seguras, bloquear dispositivos y señales que no se usan (apagar el Bluetooth o usar una bolsa Faraday), cubrir la cámara web con un sticker y asegurar que te conectas a páginas con el protocolo de seguridad HTTPS.

La seguridad digital feminista reconoce que no existen fórmulas mágicas, ni estrategias que apliquen a las necesidades, habilidades y realidades de todas, todos y todes[26]. Es por eso que es una práctica en constante crítica y reconfiguración para ajustarse a las condiciones de las personas que la requieran. Este concepto responde a los principios feministas de Internet, que plantean un espacio libre, plural y seguro.

3.4. Estrategias para afrontar la violencia digital.

Existe desconocimiento sobre cómo proceder cuando una persona está enfrentando violencia digital el Centro S.O.S. Digital[27] brinda algunas estrategias:

- Es importante recordar que la persona que enfrenta violencia digital no es culpable de lo que le está ocurriendo, la culpa siempre será de la persona agresora.

---

[24] AdNauseam es una extensión de navegador gratuita diseñada para ofuscar los datos de navegación y proteger a los usuarios del seguimiento de las redes publicitarias https://adnauseam.io/

[25] Una dirección IP es una dirección única que identifica a un dispositivo en Internet o en una red local.

26 Cyberwomen: https://cyber-women.com/en/

27 https://sosdigital.internetbolivia.org/

- Es importante que la persona que enfrenta violencia digital recurra a su círculo de apoyo para expresar cómo se siente.
- Muchas veces las personas que ejercen violencia digital solicitan el envío de fotos íntimas o envío de dinero, es importante no responder a estos mensajes.
- Sacar capturas de pantalla a los mensajes, perfiles, publicaciones y guárdalos en un lugar seguro es importante cuando una persona enfrenta violencia digital, las pruebas en Internet desaparecen rápido.
- Si la persona que enfrenta violencia digital tiene los mensajes en su celular o en sus cuentas de redes sociales, es importante no eliminarlos.

3.4.1. ¿Cómo denunciar violencias digitales ?

En la normativa boliviana no existen delitos específicos sobre violencia digital, sin embargo, a continuación se mostrarán algunos tipos de violencias digitales que se pueden denunciar usando figuras legales que se encuentran en la normativa nacional. Estos delitos no se encuentran tipificados de manera específica como digitales o informáticos, pero por el medio utilizado para la realización del delito pueden ser determinados como tales.[28]

Violencia digital	Definición	Figura legal según Código Penal u otro cuerpo legal	Definición
Ciberacoso	Conductas frecuentes que resultan hostigantes, molestas, intimidantes y perturbadoras. Ejem: Patricia es candidata a diputada, recibe mensajes insultantes, haciendo referencia hacia su aspecto físico y vida personal en WhatsApp.	Acoso sexual: Art. 312 quater. Acoso político contra mujeres: Art. Artículo 148 Bis	Las personas que valiéndose de una posición jerárquica o poder de cualquier índole hostigue, persiga, amenace(...)con producirle un daño(...) u obligue por cualquier medio a otra persona a mantener una relación o realizar actos o tener comportamientos de contenido sexual. Quien o quienes realicen actos de presión, persecución, hostigamiento y/o amenazas en contra de una mujer electa, designada o en el ejercido de la función político - pública y/o de sus familiares, durante o después del proceso electoral, que impida el ejercicio de su derecho político(...)
Difamación	Descalificación de la trayectoria credibilidad o imagen pública de una persona en medios digitales	Difamación Art. 282	El que de manera pública, tendenciosa y repetida, revelaré o divulgaré un hecho, una calidad, o una conducta capaces de afectar la reputación de una persona individual o colectiva, incurrirá en prestación de trabajo

[28] https://internetbolivia.org/actividades/guia-para-ciberbrigadistas/

	Ejem: Marcela es candidata, en redes sociales se está compartiendo noticias falsas sobre ella, en las publicaciones mencionan que se alió con el partido contrario.		de un mes a un año o multa de veinte a doscientos cuarenta días.
Difusión de imágenes íntimas sin consentimiento	Compartir o publicar sin consentimiento imágenes íntimas. Ejem: Carla es una autoridad en su municipio y está denunciando públicamente una vulneración de derechos humanos para amedrentarla se han publicado fotos íntimas de ella en redes sociales	Pornografía Art. 323 Bis	Quien procure, obligue, facilite o induzca por cualquier medio, por sí o tercera persona a otra que no dé su consentimiento a realizar actos sexuales o de exhibicionismo corporal con fines lascivos con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o de comunicaciones, sistemas informáticos, electrónicos o similares, será sancionada con pena privativa de libertad de diez (10) a quince (15) años. Igual sanción será impuesta cuando el autor o partícipe reproduzca o almacene, distribuya o venda material pornográfico
Amenazas	Mensajes con contenido agresivo que manifiestan una intención de hacer daño a la persona, a sus familiares o bienes. Ejem: Una mujer política comienza a recibir Amenazas en sus redes sociales, las amenazas hacen referencia de hacer daño a su familia si ella no renuncia a su cargo.	Amenazas Art.293°.	Que mediante amenazas graves alarmar o amedrentar a una persona, será sancionado con prestación de trabajo de un mes a un año y multa hasta de sesenta días.
Grooming	Acoso ejercido por un adulto hacia una niña, niño y adolescente y se	Art. 342 Engaño a personas incapaces	Artículo 342°.- (Engaño a personas incapaces). El que para obtener para sí o para otros algún provecho, abusando de las

	refiere a acciones realizadas deliberadamente para establecer una relación y control emocional con el fin de concluir con un abuso sexual” Ejem: Cuando una persona adulta se hace pasar por un adolescente en Internet para contactarse con niñas y adolescentes, ganarse su confianza y solicitarle fotos intimas.	Artículo 323° Bis.- Pornografía de niñas, niños o adolescentes y de personas jurídicamente incapaces	necesidades, de las pasiones o de la inexperiencia de una persona menor de dieciocho años o abusando del estado de enfermedad o deficiencia psíquica de una persona, aunque no esté en interdicción o inhabilitada, la indujere a realizar un acto que implique algún efecto jurídico perjudicial para ella o para otros, incurrirá en privación de libertad de tres a ocho años. Comete el delito de pornografía de Niñas, Niños o Adolescentes y de Personas Jurídicamente Incapaces, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de cinco a diez años de presidio.
Cyberbulling	El cyberbullying, también denominado acoso escolar, tendrá lugar “(...) cuando una persona, de forma intencionada y repetida, ejerce su poder o presión sobre otra con ayuda de medios electrónicos y de forma maliciosa, con comportamientos agresivos, tales como insultar, molestar, el abuso verbal, las	Art 151. Código niña, niño y adolescente.	g) Violencia Cibernética en el Sistema Educativo. Se presenta cuando una o un miembro de la comunidad educativa es hostigada u 45 hostigado, amenazada o amenazado, acosada o acosado, difamada o difamado, humillada o humillado, de forma dolosa por otra u otras personas, causando angustia emocional y preocupación, a través de correos electrónicos, videojuegos conectados al internet, redes sociales, blogs, mensajería instantánea y mensajes de texto a través de internet, teléfono móvil o cualquier otra tecnología de información y comunicación.

	amenazas, humillaciones, etc. Ejem: Cuando un adolescente por medio de perfiles falsos escribe a su compañero de curso mensajes insultantes y amenazantes.		II. Los tipos de violencia descritos en el presente Artículo, serán considerados infracciones mientras no constituyan delitos.

Fuente: elaboración propia.

3.4.2. ¿Dónde denunciar violencia digital?

Si la persona es mayor de edad puede acercarse al Servicio Legal Integral Municipal (SLIM) se recomienda ir en compañía de una persona de confianza, puede ser algún familiar, amigo o amiga. El SLIM es una instancia promotora de denuncia de violencia contra las mujeres, su objetivo es brindar atención, presentar la denuncia ante las instancias correspondientes y realizar acompañamiento. La persona que recibe la denuncia debe generar un registro de los datos y de los hechos y programará la evaluación psicológica y social. Los SLIM brindan apoyo psicológico, social y legal de forma gratuita.

- Apoyo Psicológico: El o la psicóloga brindan contención emocional. Si es necesario, derivarán a terapia psicológica, realizarán una evaluación psicológica y elaborarán un informe para que se pueda recibir apoyo social.
- Apoyo Social: La o el trabajador social brindará apoyo y orientación social. Realizará una valoración de niveles de riesgo y recomendará la aplicación de medidas de protección. Elaborará un informe para recibir apoyo legal.
- Apoyo Legal: El o la abogada con los informes psicológico y social, realizará análisis del caso. orientará e informará sobre los procedimientos legales aplicables. Promoverá la denuncia de violencia digital ante la Policía Nacional o el Ministerio Público.

También se puede realizar una denuncia en:

- La Policía donde se presenta la denuncia de forma verbal en plataforma de la Policía Boliviana, quien toma la denuncia debe entregarte una copia. La policía, dentro de las 24 horas debe informar al fiscal para iniciar la investigación.
- En él Ministerio Público donde la denuncia de forma escrita a través de una denuncia o una querella. La o el Fiscal inicia la investigación, debiendo informar al juez de instrucción en materia penal.

Si la persona que enfrenta violencia digital es menor de edad puede realizar la denuncia en las oficinas de la Defensoría de la Niñez y Adolescencia, esta instancia brinda un servicio gratuito, tienen la misión de prevenir, proteger y defender los derechos de las niñas, niños y

adolescentes cuando sus derechos son vulnerados. Las Defensorías de la Niñez y Adolescencia brinda apoyo legal, psicológico y social al igual que el SLIM, con los informes psicológico y social, el equipo de la Defensoría de la Niñez y Adolescencia decidirá promover una denuncia ante el Juzgado de Niñez y Adolescencia o la firma de una acta de compromiso con la persona agresora para que no vuelva a ejercer este tipo de violencia. El abogado o abogada de la defensoría de la niñez y adolescencia determinará si el tipo de violencia ejercido corresponde a una infracción o delito.

Una infracción es la violencia que no es considerada un delito, por ejemplo si alguien dentro de un colegio está molestando a través de mensajes por redes sociales a otro estudiante. Si se trata de un delito la Defensoría de la Niñez y Adolescencia promoverá la denuncia ante la Policía o el Ministerio Público.

4. Bibliografía.

- Acciones de acompañamiento ante violencias digitales: https://internetbolivia.org/actividades/guia-para-ciberbrigadistas/
- Apps para comunicaciones seguras: https://protege.la/apps-para-comunicaciones-seguras-y-privadas/
- Centro S.O.S. Digital - Protocolos de seguridad digital holística: https://sosdigital.internetbolivia.org/protocolo/
- Ciberseguras: https://ciberseguras.org/
- Guía de Seguridad Digital para Feministas Autogestivas: https://es.hackblossom.org/cybersecurity/
- Kit de primeros auxilios digitales: https://digitalfirstaid.org/es/index.html
- Mujeres Libres en Política: https://internetbolivia.org/publicacion/mujeres-libres-en-politica-guia-para-combatir-el-acoso-y-la-violencia-politica-digital-avp/
- Prevención de violencia sexual en Internet https://www.cuidadosdigitales.com/
- Ruta de atención y de denuncia de violencias digitales: https://drive.google.com/drive/folders/1e5OvOLc3c3jg6j1a0-pq0tRgerkIGIMy?usp=sharing
- Tutoriales sobre seguridad digital https://sosdigital.internetbolivia.org/videos/
- Yo y mi sombra: https://myshadow.org/es

Fundación InternetBolivia.org
Telf. 76767044
www.internetbolivia.org
Twitter: @internetbo_org

La Paz-Bolivia, 2022