

La violencia de género en línea contra las mujeres y niñas

Manual práctico de seguridad digital y estrategias de respuesta



Créditos

Luis Almagro

Secretario General

Organización de los Estados Americanos

Arthur Weintraub

Secretario de Seguridad Multidimensional

Organización de los Estados Americanos

Alison August Treppel

Secretaria Ejecutiva

*Comité Interamericano contra el Terrorismo
(CICTE)*

Alejandra Mora Mora

Secretaria Ejecutiva

Comisión Interamericana de Mujeres (CIM)

Equipo Técnico de la OEA

Programa de Ciberseguridad

Kerry-Ann Barrett

Mariana Cardona

Gabriela Montes de Oca Fehr

Comisión Interamericana de Mujeres /

Mecanismo de Seguimiento de la Convención de Belém do Pará

Luz Patricia Mejía Guerrero

Alejandra Negrete Morayta

Autora

Katya N. Vera Morales

Diseño y Diagramación

Michelle Felguérez

Con el apoyo financiero del Gobierno de Canadá 

OAS Cataloging-in-Publication Data

La violencia de género en línea contra las mujeres y niñas : Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta / [Preparado por la Secretaría General de la Organización de los Estados Americanos].

v. ; cm. (OAS. Documentos oficiales ; OEA/Ser.D/XXV.25)

ISBN 978-0-8270-7306-7

1. Girls--Violence against. 2. Women--Violence against. 3. Computer security. 4. Computer crimes. 5. Girls--Crimes against. 6. Women--Crimes against. I. Title: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta. II. Inter-American Commission of Women. III. Inter-American Committee against Terrorism. IV. OAS/CICTE Cyber Security Program. V. Organization of American States. Secretariat for Multidimensional Security. VI. Vera Morales, Katya N. VII. Series. OEA/Ser.D/XXV.25

Índice

Introducción	05
Parte 1. Conceptos básicos. Reconocer la violencia digital es el primer paso para combatirla	06
A. ¿Qué es la violencia de género en línea contra las mujeres?	07
B. ¿Qué consecuencias sufren las mujeres y las niñas que son víctimas de violencia en línea?	14
C. ¿Quiénes son los agresores?	18
Parte 2. Un recorrido por los tipos de violencia de género contra las mujeres y las niñas facilitada por las nuevas tecnologías	21
A. Creación, difusión, distribución o intercambio digital de fotografías, videos o audioclips de naturaleza sexual o íntima sin consentimiento	25
B. Acceso, uso, control, manipulación, intercambio o publicación no autorizada de información privada y datos personales	28
C. Suplantación y robo de identidad	29
D. Actos que dañan la reputación o la credibilidad de una persona	30
E. Vigilancia y monitoreo de una persona	31
F. Ciberhostigamiento o ciberacecho	32
G. Ciberacoso	33
H. Ciberbullying	36
I. Amenazas directas de daño o violencia	37
J. Violencia física facilitada por las tecnologías	38
K. Abuso, explotación y/o trata de mujeres y niñas por medio de las tecnologías	39
L. Ataques a grupos, organizaciones o comunidades de mujeres	40
Parte 3. Manual de autoprotección y respuesta: herramientas de seguridad digital frente a la violencia de género en línea	41
A. Recomendaciones básicas para tu seguridad digital: medidas preventivas	42
B. Consejos para la seguridad digital de mujeres víctimas de violencia doméstica o de pareja	52
C. ¿Qué puedo hacer si estoy siendo víctima de actos de violencia digital?	55
D. Para explorar más	60
Glosario de términos	62
Bibliografía	66

Esta publicación se realizó gracias al apoyo brindado por el Departamento de Estado de los Estados Unidos, bajo los términos del Proyecto No. SLMQM20GR2380. Las opiniones expresadas en este documento pertenecen a los autores y no reflejan necesariamente las opiniones del Departamento de Estado de los Estados Unidos.

Introducción



La violencia de género facilitada por las nuevas tecnologías es un fenómeno que de forma creciente afecta la privacidad y seguridad de las mujeres dentro y fuera del ciberespacio. Investigaciones sobre el tema indican que **las mujeres son víctimas de ciertos tipos de ciberviolencia de manera desproporcionada en comparación con los hombres** (REVM-ONU, 2018; EIGE, 2017). De acuerdo con un estudio publicado en 2015 por la Comisión de la Banda Ancha para el Desarrollo Sostenible, de las Naciones Unidas, 73% de las mujeres habían vivido alguna forma de violencia de género en línea, mientras que 61% de los atacantes eran hombres (UNBC, 2015). Otras fuentes señalan que 23% de las mujeres han experimentado acoso en línea al menos una vez en su vida, y se estima que una de cada diez mujeres ya había sufrido alguna forma de ciberviolencia desde los 15 años de edad (REVM-ONU, 2018, párr. 16; EIGE, 2017: 3; AI, 2017).

Además, como lo han comprobado múltiples fuentes¹, esta violencia se ha agravado con las restricciones de la movilidad y el confinamiento impuestos a raíz de la pandemia de COVID-19: a medida que más mujeres y niñas se vuelcan a los espacios digitales, la ciberviolencia de género en su contra se incrementa (ONU Mujeres; CIM, 2020; Derechos Digitales, 2020).

Este fenómeno se observa en un escenario con múltiples retos. La información sobre la ciberviolencia contra las mujeres es aún escasa. Es muy poco lo que se sabe sobre el porcentaje real de víctimas y la prevalencia de los daños que provoca (EIGE, 2017). Además, hasta la fecha no hay una definición acordada a escala regional o internacional de la violencia de género en línea ni una terminología precisa². Hay una gran disparidad entre las respuestas de los Estados y los organismos internacionales y, en general, una falta de marcos jurídicos adecuados para proteger a las víctimas.

Ante la necesidad de visibilizar este fenómeno y de contar con herramientas para fortalecer la seguridad digital de las mujeres, el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE), en alianza con la Comisión Interamericana de Mujeres (CIM), ha elaborado este manual práctico en el cual se presentan conceptos básicos para entender la violencia de género

en línea, recomendaciones, medidas preventivas y estrategias de protección frente a agresiones y actos de ciberviolencia de género.

Con esta publicación se busca contribuir al empoderamiento digital de las mujeres y las niñas. Se basa en la premisa de que estas pueden adquirir las habilidades necesarias para protegerse de forma individual y colectiva en sus interacciones en línea y crear espacios propios en la virtualidad donde estén libres de violencia, a fin de que la internet sea para ellas puente y no barrera en el desarrollo de su proyecto de vida.

Este manual forma parte de la publicación *La violencia de género en línea contra las mujeres y niñas. Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta*, cuya consulta es recomendable para conocer más acerca de los últimos desarrollos en la materia en la región latinoamericana así como algunas de las medidas que pueden tomar las autoridades para prevenir y combatir esta forma de violencia.

¹ ONU Mujeres (2020). Online and ICT facilitated violence against women and girls during COVID-19. Disponible en: <https://www.unwomen.org/en/digital-library/publications/2020/04/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19> Véase también: Comisión Interamericana de Mujeres (CIM) (2020) COVID-19 en la vida de las mujeres. *Razones para reconocer los impactos diferenciados*. Disponible en: <http://www.oas.org/es/cim/docs/ArgumentarioCOVID19-ES.pdf>

² Como señaló la Relatora Especial de las Naciones Unidas sobre la violencia contra la mujer, todavía no hay consenso sobre la terminología para denominar esta forma de violencia. La expresión “violencia contra las mujeres facilitada por la tecnología de la información y las comunicaciones (TIC)” quizá sea la más incluyente, ya que abarca la vasta gama de conductas que esta forma de violencia puede adoptar. Sin embargo, siguiendo el uso común, en esta publicación se utilizarán indistintamente las expresiones “violencia facilitada por las TIC”, “violencia en línea contra las mujeres”, “violencia digital” y “ciberviolencia contra las mujeres”.

Parte *uno*

Conceptos básicos:

RECONOCER LA

VIOLENCIA DIGITAL

ES EL PRIMER PASO PARA

COMBATIRLA





¿Qué es la violencia de género en línea contra mujeres y niñas?

Elementos básicos de la violencia en línea en contra de las mujeres:

01

No es algo nuevo. Forma parte de un contexto de discriminación de género y violencia sistémica contra las mujeres que se da en todos los ámbitos de su vida.

No está desconectada de la violencia “fuera de internet”: es parte de la serie de formas múltiples, interrelacionadas y recurrentes de violencia contra las mujeres y las niñas que ahora fluye por el mundo *online-offline* y lo atraviesa.

02

03

Conlleva diversas violaciones de los derechos humanos de las mujeres y las niñas.

Es una expresión dinámica que abarca prácticas muy diversas de violencia facilitadas o reconfiguradas por las tecnologías de la información y las comunicaciones (TIC).

04

05

Causa en las víctimas daños y sufrimientos psicológicos, físicos, sexuales y/o económicos, y tiene efectos familiares, sociales y colectivos.

La violencia en línea contra las mujeres no es un fenómeno aislado, sino que **se localiza en un contexto social más amplio de desigualdad y discriminación de género contra las mujeres y las niñas**. Por ello, para entender la violencia digital, es crucial que nos detengamos primero a analizar qué es la violencia de género, puesto que las agresiones y los ataques que viven las mujeres en sus interacciones en línea no son más que una extensión de la violencia que por muchos años las ha afectado en todas las esferas de su vida.

¿Qué es la violencia de género contra las mujeres y las niñas?

De acuerdo con la Convención de Belém do Pará, se entiende como violencia contra la mujer “cualquier acción o conducta, basada en su género, que cause muerte, daño o sufrimiento físico, sexual o psicológico a la mujer, tanto en el ámbito público como en el privado” (artículo 1).

La violencia por razón de género es “**la violencia dirigida contra la mujer porque es mujer o que la afecta en forma desproporcionada**” (Comité CEDAW, Recomendación General 19, párr. 6).



La violencia de género contra las mujeres tiene su origen en estereotipos y prejuicios acerca de los atributos y las características que poseen hombres y mujeres y en expectativas de las funciones sociales que ambos supuestamente deben desempeñar (por ejemplo, que las mujeres son las únicas encargadas de las labores domésticas, que no tienen suficiente autoridad para ocupar cargos directivos o que son débiles por naturaleza). Estos patrones socioculturales colocan a las mujeres en una **posición inferior o subordinada respecto de los hombres** y propician su discriminación, elementos que son los principales impulsores de la violencia dirigida hacia ellas (MESECVI, 2017, párr. 37).

Es importante subrayar que la violencia opera en sinergia con la desigualdad de género y no solo como una consecuencia de ésta última, sino como mecanismo social que busca mantener a las mujeres en una situación de desventaja. Esto significa que la violencia se usa en muchos casos para “castigar” o “corregir” a mujeres cuyas actitudes o actividades supuestamente van en contra de lo que la sociedad espera de ellas (MESECVI, 2017, párr. 36).

Las Naciones Unidas han señalado que la violencia contra las mujeres es un problema omnipresente en todos los países del mundo y una violación sistemática y generalizada de los derechos humanos, con alto grado de impunidad.



Las mujeres y las niñas experimentan violencia de género a lo largo de los años en todos los espacios *offline* y *online* donde concurren y participan, ya sea en el hogar, la escuela, el trabajo, la vía pública, la política, los medios de comunicación, el deporte, las instituciones públicas o al navegar en redes sociales (Comité CEDAW, Recomendación General 35). Esta violencia no tiene fronteras, está dirigida contra todas las mujeres por el simple hecho de que son mujeres e **incide más en ciertos grupos de mujeres debido a que sufren formas de discriminación interseccional**, como es el caso de las mujeres indígenas, migrantes, con discapacidad, lesbianas, bisexuales y transgénero, entre otras (MESECVI, 2017).

Uno de los logros más importantes para las mujeres ha sido el reconocimiento de que **la violencia cometida en su contra no es un problema privado**, sino que constituye un asunto de interés público y una violación de los derechos humanos reconocida en instrumentos internacionales y legislaciones nacionales que prescriben la obligación de los Estados de prevenirla, atenderla, investigarla, repararla y sancionarla (Edwards, 2010). En el caso del sistema interamericano, el derecho de las mujeres a vivir una vida libre de violencia está reconocido en la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Convención de Belém do Pará), el primer tratado en la materia que elevó el combate de la violencia de género contra las mujeres al rubro de problema de interés regional³.

¿Qué es la violencia de género en línea contra las mujeres?



En el ámbito de la Organización de las Naciones Unidas (ONU), la Relatora Especial sobre la Violencia contra la Mujer definió en 2018 la violencia en línea contra las mujeres como “todo acto de violencia por razón de género contra la mujer cometido, con la asistencia, en parte o en su totalidad, del uso de las TIC, o agravado por este, como los teléfonos móviles y los teléfonos inteligentes, Internet, plataformas de medios sociales o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada” (REVM-ONU, 2018, párr. 23).

Los datos y estudios pertinentes han demostrado que, en la mayoría de los casos, la violencia en línea no es un delito neutro en cuanto al género (REVM-ONU, 2018).

La violencia en línea contra las mujeres puede estar facilitada por algoritmos y dispositivos tecnológicos tales como teléfonos móviles e inteligentes, tabletas, computadoras, sistemas de geolocalización, dispositivos de audio, cámaras o asistentes virtuales.



Esta violencia puede verificarse en una gran variedad de plataformas de internet; por ejemplo, redes sociales (*Facebook, Twitter, Tik Tok*), servicios de correo electrónico, aplicaciones de mensajería instantánea (*WhatsApp*), aplicaciones para citas (*Tinder, Grindr, Hinge, Match.com*), videojuegos en línea, sitios donde se intercambia contenido (*Reddit*), foros de discusión en línea (en las secciones de comentarios de los periódicos) o plataformas generadas por los usuarios (blogs, sitios para intercambio de imágenes y videos).

³ Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer. Disponible en: <https://www.oas.org/juridico/spanish/tratados/a-61.html>

La ciberviolencia de género es un concepto en constante cambio. Como lo reconoció la Relatora Especial sobre Violencia contra las Mujeres de las Naciones Unidas, **las rápidas transformaciones tecnológicas influyen en la violencia en línea**, y surgen nuevas y diferentes manifestaciones de violencia a medida que los espacios digitales se transforman y trastocan la vida fuera de internet (REVM-ONU, 2018, párr. 24).

La violencia en línea ha variado desde los orígenes de la internet, y seguramente seguirá transformándose a medida que las plataformas digitales y las herramientas tecnológicas sigan avanzando e interrelacionándose más y más en nuestra vida.

El proceso continuo online-offline de la violencia: nuevas formas de la misma violencia

La violencia en línea se manifiesta en una serie de formas múltiples, recurrentes e interrelacionadas de violencia por razón de género contra las mujeres (REVM-ONU, 2018).

No debemos caer en el error de considerar que la violencia en línea es un fenómeno separado de la violencia en el mundo “real”, pues forma parte de las manifestaciones continuas e interconectadas de violencia que las mujeres ya vivían fuera de internet.



Estamos hablando de un viejo sistema de dominación y violencia de género que ahora usa una nueva plataforma para replicarse.

En 1989, Liz Kelly llamó la atención por primera vez sobre el hecho de que los diferentes tipos de violencia y abuso de género pueden ser conceptualizados como un **proceso continuo de violencia (*continuum de violencia*) en la vida y las experiencias de las mujeres en todo el mundo** (y no solo como sucesos esporádicos o anormales), que abarca desde actos expresamente reconocidos como delitos hasta conductas de control y dominación tan comunes que han llegado a normalizarse (Kelly, 1989).

Todos los tipos de violencia de género contra las mujeres tienen algo en común: son formas de coerción, abuso o agresión que se usan para controlar, limitar o constreñir la vida, el estatus, los movimientos y las oportunidades de las mujeres y para facilitar y asegurar los privilegios de los hombres (Kelly, 1989).

Por lo tanto, en el contexto actual, en el cual el ciberespacio y la vida fuera de internet están cada vez más interrelacionados, la violencia contra las mujeres ha llegado al mundo digital como una extensión más de esa serie continua de sucesos de violencia que se presentan en la experiencia diaria de mujeres y niñas (Kelly, 1988; Powell, Henry y Flynn, 2018).

Así observamos que, en la era digital, las formas de violencia de género persisten o se amplifican con el uso de nuevas tecnologías y que están surgiendo nuevas formas de sexismo y misoginia en línea, las cuales pueden salir del ciberespacio para convertirse en agresiones físicas contra las mujeres. La violencia contra las mujeres puede, por ejemplo, comenzar como acoso sexual en la vía pública, como violencia “por motivos de honor” en una comunidad o como agresiones físicas perpetradas por una pareja sentimental y convertirse y reubicarse por medio de la tecnología en la distribución no consensuada de imágenes íntimas, en actos de ciberacoso, en discurso de odio sexista en redes sociales, en el monitoreo por medio del celular, etc. En sentido inverso, la violencia puede comenzar como intercambios en las redes sociales por una menor de edad con supuestos nuevos amigos y culminar en encuentros donde se cometen actos de violencia sexual o secuestros. Todos estos actos nuevos inciden en la interacción de las mujeres no solo en línea sino en todos los espacios de su vida *offline*.

En muchos casos, la violencia de género se ha intensificado dado que los espacios digitales ofrecen una muy conveniente anonimidad y el abuso puede cometerse desde cualquier lugar, a través de una amplia gama de nuevas tecnologías y plataformas que los perpetradores de violencia tienen a su alcance y con una rápida propagación y permanencia del contenido digital.

Algunos aspectos de las nuevas TIC que han contribuido a la transformación de la violencia de género contra las mujeres son su rápida expansión, la permanencia en línea de contenidos que dejan un registro digital indeleble, su replicabilidad y alcance global, y la posibilidad de localizar fácilmente a personas e información sobre ellas, lo cual facilita el contacto de los agresores con las víctimas y su victimización secundaria (REVM-ONU, 2018).



Bajo la lupa:

La estrecha relación entre la violencia de pareja y las nuevas tecnologías

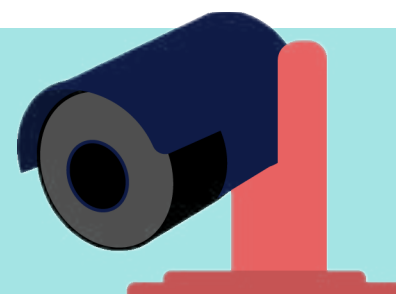


Desde hace varios años, las TIC están desempeñando un papel muy importante en el surgimiento de nuevas estrategias de abuso y control por los perpetradores de actos de violencia doméstica y de pareja (Dragiewicz, 2019). Varios estudios han revelado que **77% de las víctimas de ciberacoso han sufrido también alguna forma de violencia física o sexual a manos de una pareja íntima** (FRA, 2014) y que conocían por lo menos a la mitad de los agresores en línea (APC, 2015).

A medida que las nuevas tecnologías se han ido incorporando en prácticamente todas las actividades diarias de las personas, los agresores se han aprovechado, extendiendo e intensificando comportamientos abusivos, posesivos y controladores que antes no eran posibles (Woodlock, 2017). En consecuencia, las mujeres ahora experimentan esta violencia sin límites de espacio y tiempo y con la sensación de que el agresor es omnipresente (Harris, 2018), lo cual tiene efectos graves en su salud mental⁴.

Aunque la investigación en la materia es aún incipiente, varios estudios iniciales indican que algunas tecnologías se usan más que otras para cometer abusos y ejercer cibercontrol en contextos de violencia doméstica o de pareja. Ese es el caso de los mensajes de texto, redes sociales o software para monitorear la ubicación de las víctimas por medio de sus celulares (Dragiewicz, 2019).

No obstante, las manifestaciones del abuso y la vigilancia digital de las mujeres y de la intrusión en su vida cambian constantemente y abarcan desde incidentes de robo de identidad por la pareja o expareja para hacer compras por internet hasta el uso por los agresores de dispositivos inteligentes instalados en los hogares, como termostatos, cámaras, micrófonos, bocinas o cerraduras, para generar estrés psicológico en las víctimas.



Se ha observado también en parejas jóvenes **nuevos comportamientos que se han normalizado en el actual contexto online-offline, disfrazados con ideas y mitos del amor romántico, pero que en el fondo buscan el cibercontrol y la limitación de la vida digital de las mujeres.** Algunos de ellos son los siguientes:



Exigir a la pareja las contraseñas y claves personales y espiar el teléfono móvil.

Interferir en las relaciones digitales con otras personas.



Tratar de controlar las interacciones en redes sociales, censurar fotos o publicaciones y revisar los contactos, las conversaciones o los comentarios en línea.



Exigir que la pareja muestre su geolocalización constantemente.



Obligarla a enviar imágenes íntimas.

⁴ Alexandra Topping (2013). "How domestic violence spreads online: I felt he was watching me". *The Guardian*. Disponible en: <https://www.theguardian.com/society/2013/sep/03/domestic-violence-spreads-online-watching>

En el caso específico de las víctimas de violencia doméstica y de pareja, la violencia en línea puede disuadirlas de abandonar la relación, dado que muchas veces se sienten atrapadas en una situación de la cual no pueden escapar. Se ha documentado también que, en muchos casos, la violencia digital aumenta en el momento de la separación (no solo contra las víctimas sino también contra sus hijas o hijos, familiares, amistades o parejas sentimentales). Parecería incluso que cortar abruptamente toda comunicación o interacción digital con cierto tipo de agresores puede incrementar el riesgo para las sobrevivientes y su familia (Dragiewicz, 2019).

A esto se suma el **aumento exponencial en todo el mundo de la violencia física y el abuso sexual contra mujeres y niñas durante la pandemia de COVID-19** (ONU Mujeres, CIM, 2019). Con las medidas de confinamiento, se han visto obligadas a permanecer encerradas con sus agresores, y para ellas la tecnología se ha convertido en una herramienta indispensable para comunicarse con el exterior, pedir ayuda y tener acceso a los servicios de atención.

En este contexto, apoyar a víctimas y sobrevivientes de violencia doméstica y de pareja para que sepan reconocer el cibercontrol, proteger su seguridad e integridad digital y **utilizar la tecnología como un medio de apoyo para salir del círculo de violencia** es algo esencial que ahora debe formar parte de los modelos ecológicos de prevención, atención y sanción de la violencia contra las mujeres, que implican un trabajo con familias, comunidades e instituciones.





¿Qué consecuencias sufren las mujeres y las niñas que son víctimas de violencia en línea?

La violencia en línea contra las mujeres produce daños reales

Como consecuencia de la violencia en línea, las mujeres y las niñas sufren graves daños psicológicos, físicos, sexuales, emocionales, económicos, laborales, familiares y sociales (REVM-ONU, 2018).

Las manifestaciones y las repercusiones de esta violencia pueden ser muy variadas dependiendo de la forma que tome; por ejemplo, sentimientos de depresión, ansiedad, estrés, miedo o ataques de pánico en casos de ciberhostigamiento, intentos de suicidio por parte de mujeres afectadas por la distribución no consensuada de imágenes sexuales, daños físicos contra las víctimas de *doxing*⁵ o perjuicios económicos ante la pérdida del empleo como consecuencia de actos en línea que desprestigian (Pew Research Center, 2017; Kwon et al., 2019; AI, 2017).



Se ha comprobado que, como parte del proceso continuo de violencias de género, los daños causados por actos en línea no difieren de los efectos que tiene la violencia fuera de internet, sino que inciden a corto y a largo plazo en todos los ámbitos del desarrollo individual de las mujeres, como su autonomía, privacidad, confianza e integridad (Van Der Wilk, 2018).

Desafortunadamente, persiste una comprensión inadecuada de la seriedad de las consecuencias y los daños que la violencia en línea causa en las mujeres, daños que muchas veces se considera que “no son reales” porque se verificaron en internet. Esto refleja un entendimiento erróneo del proceso continuo *online-offline* en que ahora se desarrolla nuestra vida, así como de las características de la serie de formas múltiples e interrelacionadas de violencias que viven mujeres y niñas en sus interacciones sociales.

⁵ *Doxxing* o *doxing* es un ciberataque que consiste en obtener información personal sobre alguien y hacerla pública en línea.

Se ha observado además que **las características de ciertas tecnologías hacen que la magnitud del daño de algunos actos de violencia se incremente exponencialmente** y se extienda más allá del acto original (como su rápida propagación, alcance, anonimidad y permanencia) (APC, 2017), dado que las mujeres son juzgadas con mayor severidad que los hombres por sus actitudes en línea. Tal es el caso de incidentes de distribución no consentida de imágenes sexuales, en los que se ha visto que mujeres y niñas son estigmatizadas por el ejercicio de su sexualidad y, después de ver sus imágenes distribuidas, tienen que vivir en un contexto de humillación y vergüenza permanente en su entorno social, lo cual en muchos casos las ha empujado al suicidio.

Las mujeres afectadas a menudo se responsabilizan a sí mismas por acciones que pudieran haber causado la violencia y se retiran de los espacios digitales, se autocensuran o se aíslan socialmente (Citron, 2014). Además, es muy común que sean revictimizadas por familiares, autoridades y medios de comunicación, que con frecuencia les atribuyen la responsabilidad de protegerse, en vez de recalcar la conducta ilícita de los agresores, y de esta forma normalizan y minimizan esta violencia (REVM-ONU, 2018, párr. 25).



Aunado a los efectos individuales, **la violencia en línea conlleva daños colectivos e intergeneracionales** y tiene costos directos e indirectos para las sociedades y las economías, dado que las víctimas y sobrevivientes no solo requieren atención médica y servicios judiciales y sociales, sino que también pueden ver disminuida su productividad y sus interacciones en la comunidad (UNBC, 2015). Asimismo, **esta violencia tiene un efecto silenciador**, puesto que es una amenaza directa a la libertad de expresión de las mujeres (AI, 2017) y afecta su acceso y participación en línea como ciudadanas digitales activas, lo cual crea un déficit democrático al impedir que las voces de las mujeres se escuchen libremente en los debates digitales (REVM-ONU, 2018, párr. 29).

Las investigaciones en la materia indican que 28% de las mujeres que fueron objeto de violencia perpetrada por medio de las TIC han reducido deliberadamente su presencia en línea (REVM-ONU, 2018, párr. 26) y se autocensuran por temor a que su privacidad o su seguridad se vean vulneradas (AI, 2017). Para peor, a las sobrevivientes con frecuencia les aconsejan “alejarse” o “retirarse” de las tecnologías tras un incidente de violencia.

Por último, tampoco debemos olvidar que esta violencia **contribuye a la perpetuación de estereotipos de género nocivos y a la reproducción de la violencia sistémica** en el nuevo mundo *online-offline*, al propiciar el desarrollo de tecnologías con sesgos de género.

¿Hay mujeres que están siendo atacadas en línea más que otras?

Al analizar la violencia digital es importante no caer en generalizaciones a partir de una supuesta experiencia común de las mujeres. En cada caso deben tomarse en cuenta las especificidades de las distintas experiencias en línea vividas por las mujeres y las diversas identidades partir de las cuales se definen.

Si bien la violencia en línea es un fenómeno común entre mujeres y niñas que navegan el mundo digital, lo cierto es que también **afecta a las mujeres de forma diferente dependiendo de otras formas de discriminación** que enfrentan en su vida cotidiana por motivos de raza, origen étnico, orientación sexual, identidad de género, clase social o nacionalidad.

Según Amnistía Internacional, las mujeres que enfrentan discriminación fuera de internet debido a rasgos específicos de su identidad con frecuencia encuentran que la violencia y el abuso en línea contra ellas están dirigidos a esos mismos rasgos (AI, 2018). Estas mujeres son particularmente vulnerables a la victimización mediante una combinación de abusos que reflejan creencias racistas, sexistas, estereotipos, prejuicios sociales e ideas sobre un supuesto orden de género.

Asimismo, la Relatora Especial sobre Violencia de Naciones Unidas señaló en su informe de 2018 que ciertos grupos de mujeres son especialmente objeto de violencia en línea, como las parlamentarias, las periodistas, las mujeres jóvenes o que tienen una participación en el debate digital y las mujeres de minorías étnicas o de la comunidad LGBTIQ+ (REVM-ONU, 2018; Van Der Wilk, 2018; UNBC, 2015; EIGE, 2017; Henry y Powell, 2016). Por lo general, la violencia digital contra ellas toma la forma de ataques a su visibilidad, a su sexualidad, a su libertad de expresión y a su participación política. Es evidente que uno de los objetivos de la violencia digital es mantener a las mujeres en silencio y en condiciones de subordinación en la sociedad.



¿Sabías que...?



En varios informes se señala que las mujeres de 18 a 24 años se encuentran en particular riesgo de violencia digital, con una probabilidad 27% mayor de ser víctimas de ciberabuso en comparación con los hombres (APC, 2001; UNBC, 2015). El *Pew Research Center* informó también que estas mujeres son particularmente vulnerables al ciberacoso (*Pew Reserach Center*, 2014 y 2017).

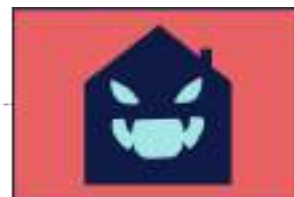
Se ha observado que el simple hecho de ser mujer y ser una figura pública o participar en la vida política conlleva ser blanco de comentarios extremadamente misóginos, violencia sexual y amenazas de violencia física y femicida en línea (Rawlison, 2018). Las mujeres que participan en debates públicos en internet o que escriben sobre temas de género son, de manera desproporcionada, víctimas de acoso en línea con el fin de silenciarlas e intimidarlas y suelen ser el blanco de campañas masivas de abuso y violencia verbal sexualizada, con discurso de odio y amenazas de abuso y violación sexual (REVM-ONU, 2018, párr. 25). De acuerdo con Amnistía Internacional, 88% de las mujeres sufren abusos y ciberacoso tras la publicación de contenidos feministas (AI, 2018).



Bajo la lupa:

mujeres propensas a ser el blanco de ciertos tipos de violencia digital⁶

Mujeres en una relación íntima o víctimas de violencia doméstica o de pareja.



Defensoras de derechos humanos, periodistas, mujeres que participan en actividades políticas, participantes activas en el debate digital o mujeres que tienen un perfil público.

Estas mujeres son frecuentemente objeto de ciberacoso y ciberhostigamiento en internet, incluso de amenazas en línea y abuso verbal de naturaleza misógina y sexual.

Mujeres lesbianas, bisexuales, transgénero o intersex, mujeres con discapacidad, mujeres de una minoría étnica o racial, mujeres indígenas o de grupos marginados. Estas mujeres suelen ser blanco de discurso de odio y abuso en línea con connotaciones homofóbicas, racistas o sexistas.



Las mujeres jóvenes son también un blanco frecuente de violencia sexual en línea, que reproduce formas de hostigamiento, acoso y abuso sexual.

⁶ Association for Progressive Communications (APC). *From impunity to justice. Exploring corporate and legal remedies for technology-related violence against women 2012-2015*. Disponible en: <https://genderit.org/onlinevaw/>



¿Quiénes son los agresores?

Se ha observado que los agresores y los responsables de la violencia de género en línea contra las mujeres tienen por lo general una identidad masculina (Van Der Wilk, 2018, 34-37). Estos agresores pueden ser una persona que la víctima no conoce (como un acosador sexual en línea que dirige sus ataques sistemáticamente hacia diversas mujeres o sujetos que practican el *grooming* o ciberengaño pederasta)⁷ o un integrante del círculo familiar, profesional o una amistad. Algunos estudios indican, por ejemplo, que entre **40% y 50% de las víctimas conocían a sus agresores en línea** (una expareja sentimental, un miembro de la familia, un amigo o un colega) y que, **en un tercio de los casos, los agresores tenían o habían tenido una relación íntima con la persona atacada** (Pew Research Center, 2017; APC, 2015).

Pueden identificarse dos tipos de responsables de la violencia en línea contra las mujeres (Abdul, 2017):

El perpetrador original:

La persona que comete el acto inicial de violencia o abuso digital o que crea, manipula o publica por primera vez información dañina, datos personales o imágenes íntimas sin el consentimiento de la víctima.

El perpetrador o los perpetradores secundarios:

Persona o grupo de personas que participan en la continuación y propagación de un acto de violencia en línea al reenviar, descargar, volver a publicar o compartir información dañina, datos personales o imágenes íntimas obtenidas sin el consentimiento de la víctima.

¿Qué buscan los agresores con la violencia en línea contra las mujeres y las niñas?

El objetivo de la violencia es crear un ambiente hostil en línea para las mujeres a fin de avergonzarlas, intimidarlas, denigrarlas, menospreciarlas o silenciarlas por medio de la vigilancia, el robo o la manipulación de información o el control de sus canales de comunicación (AI, 2018).



Bajo la lupa:

La violencia en línea como violación de los derechos humanos de las mujeres

Como subraya la Relatora Especial sobre la Violencia contra la Mujer de las Naciones Unidas en su informe de 2018, los derechos humanos de las mujeres amparados por tratados internacionales deben estar protegidos en internet, “en particular mediante la prohibición de la violencia por razón de género en formas facilitadas por las TIC y en línea” (REVM-ONU, 2018, párr. 17).

⁷ El *grooming* o ciberengaño pederasta consiste en actos deliberados de un adulto para acercarse a un menor a fin de establecer una relación y un control emocional que le permita cometer abusos sexuales, entablar relaciones virtuales, obtener pornografía infantil o practicar la trata de menores.

Por su parte, el Consejo de Derechos Humanos de las Naciones Unidas reconoció que la violencia en contextos digitales impide “a las mujeres y las niñas disfrutar plenamente de sus derechos humanos y libertades fundamentales” reconocidos en el derecho internacional, lo que obstaculiza su participación plena y efectiva en los asuntos económicos, sociales, culturales y políticos (HRC, 2018, párr. 3).

Algunos de los derechos humanos de las mujeres que la violencia en línea puede violar son los siguientes (REVM-ONU, 2018; Vela y Smith, 2016; APC, 2017):

- **Derecho a la igualdad y no discriminación.**
- **Derecho a una vida libre de violencia.**
- **Derecho a la integridad personal.**
- **Derecho a la autodeterminación.**
- **Derecho a la libertad de expresión, al acceso a la información y al acceso efectivo a internet.**
- **Derecho a la libertad de reunión y asociación.**
- **Derecho a la privacidad y a la protección de los datos personales.**
- **Derecho a la protección del honor y la reputación.**
- **Derechos sexuales y reproductivos de las mujeres.**



Es importante tener presente que “la prohibición de la violencia de género se ha reconocido como un principio del derecho internacional de los derechos humanos” (REVM-ONU, 2018, párr. 17). Eso implica que los Estados tienen obligaciones de debida diligencia de prevenir y combatir la violencia en línea contra las mujeres cometida tanto por agentes estatales como por agentes no estatales (Abdul, 2017).



Bajo la lupa:

El Internet de las Cosas (IoT) y la violencia doméstica

El Internet de las Cosas (*Internet of Things* o IoT por sus siglas en inglés) se refiere a la red de dispositivos inteligentes conectados a internet que pueden compartir datos entre sí. El IoT va más allá de la conectividad entre computadoras, teléfonos celulares y tabletas, e incluye dispositivos como televisiones, relojes, frigoríficos, sistemas de calefacción, cámaras o cerraduras inteligentes.

Se dice que estos dispositivos son “inteligentes” porque pueden recolectar y analizar datos, comunicarse entre ellos y ejecutar acciones sin intervención humana directa. Por ejemplo, por medio del IoT se puede controlar el sistema de seguridad de una casa desde una aplicación instalada en el teléfono celular, mediante comandos de voz dirigidos a asistentes virtuales, o se pueden activar o desactivar remotamente cámaras o sistemas de iluminación.

El IoT tiene muchos beneficios al facilitar cuestiones prácticas de la vida cotidiana, pero puede conllevar potenciales riesgos para la privacidad y la seguridad porque los dispositivos asumen que todas las personas usuarias confían entre sí. Por ejemplo, en el caso de violencia doméstica, un agresor puede utilizar el IoT para monitorear a una víctima o impedirle abrir las cerraduras de su casa, o un *hacker* puede controlar de forma remota una cámara de seguridad para grabar sin consentimiento imágenes o videos íntimos directamente en el hogar de una víctima.

De acuerdo con el proyecto de investigación “Género e Internet de las Cosas” (*Gender and Internet of Things*) de *University College London (UCL)*, el IoT facilita tres formas de violencia en línea:

- Ciberhostigamiento.
- Comportamientos coactivos y controladores, incluyendo amenazas de daño o abuso para atemorizar a una víctima. Por ejemplo, denegando el control de la calefacción, la iluminación o de las cerraduras de la casa.
- *Gaslighting* digital, que es una forma de abuso psicológico realizado mediante la manipulación de la realidad de la víctima, con lo cual se busca que se cuestione su cordura, su memoria o su percepción.

Cómo puede afectar el IoT a víctimas de violencia doméstica y violencia sexual



Implicación:

Los perpetradores pueden explotar las funcionalidades del IoT para monitorear, controlar y / o prevenir que las víctimas usen dispositivos.

Consideración:

Es importante que los servicios de apoyo sean conscientes de las funcionalidades del IoT, dado que pueden informar sobre las evaluaciones y la planificación de la seguridad de las víctimas.

Mitigación:

No existe una estrategia de mitigación única para todos cuando se produce el abuso de tecnología habilitada por IoT. Conocer sus funcionalidades comunes puede ayudar a la hora de buscar el apoyo de profesionales como la policía.

Información:

Dado que los dispositivos de IoT y sus funcionalidades evolucionan constantemente, en el sitio web de STEaPP se proporcionan más recursos e información actualizada sobre el tema.

Parte DOS

UN RECORRIDO POR LOS TIPOS

DE VIOLENCIA DE GÉNERO

CONTRA LAS MUJERES Y LAS NIÑAS
FACILITADA POR LAS NUEVAS
TECNOLOGÍAS





Es importante no perder de vista que la violencia de género en línea contra las mujeres es una expresión que abarca una amplia variedad de prácticas y comportamientos dañinos u ofensivos y contextos *online-offline* que se transforman a la par de los avances tecnológicos.

Aquello que entendemos como violencia en línea contra las mujeres son, de hecho, prácticas y conductas muy diversas que pueden constituir ciberdelitos o actos ilícitos que conllevan responsabilidad administrativa, civil o penal de acuerdo con el derecho de cada país (IGF, 2015; REVM-ONU, 2018; APC, 2017).

Hasta la fecha persiste una gran disparidad en cuanto a la terminología utilizada para hacer referencia a los diversos tipos de violencia en línea contra las mujeres y sus manifestaciones, con constantes variaciones entre las expresiones usadas por los Estados, los organismos internacionales, las organizaciones no gubernamentales y el sector académico (Van Der Wilk, 2018). Desafortunadamente, eso ha sembrado la confusión en torno a la clasificación de estas conductas y, en muchos casos, ha dado lugar a referencias imprecisas en la legislación nacional.

En un esfuerzo por clarificar este escenario, **a continuación se presenta una guía descriptiva de las conductas y ataques en línea o facilitados por las TIC que podrían calificarse como formas específicas de violencia contra las mujeres y niñas basada en su género**, con miras a facilitar la identificación de experiencias personales y, a partir de ello, saber qué medidas se pueden tomar para fortalecer la seguridad digital de las víctimas (véase tercera parte de esta guía).

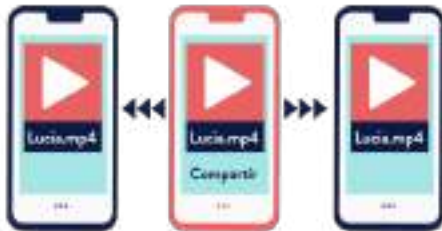
Este catálogo se conformó sobre la base de una revisión bibliográfica y no debe considerarse como algo fijo o estático, puesto que la violencia digital está en constante transformación paralelamente a la tecnología y surgen otras manifestaciones de violencia a medida que aparecen nuevas herramientas tecnológicas (UNBC, 2015).

Asimismo, como se observará en este apartado, es importante tener en cuenta que puede haber casos en que dos o más formas de violencia digital se ejerzan de forma simultánea, sean interdependientes (por ejemplo, amenazas en línea seguidas de la distribución no consensuada de imágenes íntimas) o estén acompañadas de otras formas de violencia fuera de internet (como sucede a menudo en casos de violencia doméstica).

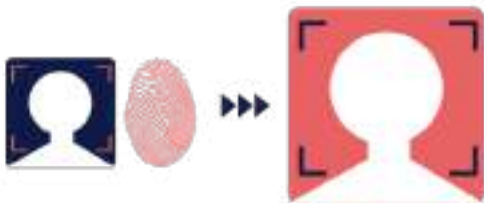
En todo caso, debe tenerse presente que estos ciberataques y actos en línea serán considerados como violencia de género al dirigirse contra una mujer por el mero hecho de ser mujer (es decir, por su identidad de género) o porque la afectan en forma desproporcionada.



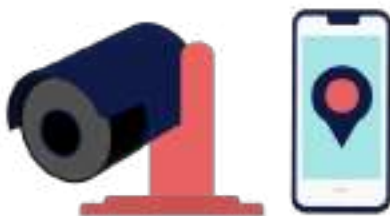
Tipos de violencia de género contra mujeres y niñas facilitada por las nuevas tecnologías:



Acceso, uso, manipulación, intercambio o distribución no autorizados de datos personales.



Actos que dañan la reputación o la credibilidad de una persona.



Ciberhostigamiento.

01

Creación, difusión, distribución o intercambio digital de fotografías, videos o audioclips de naturaleza sexual o íntima sin consentimiento.

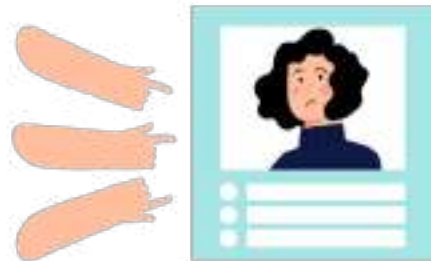
02



03

Suplantación y robo de identidad.

04

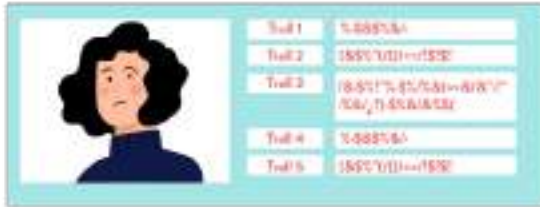


05

Actos que implican la vigilancia y el monitoreo de una persona.

06





Ciberintimidación.



Violencia física facilitada por las tecnologías.



Ataques a grupos, organizaciones o comunidades de mujeres.

07

Ciberacoso.



08

Amenazas directas de daño.



10

Abuso, explotación de mujeres y niñas a través de las tecnologías.



11

12



Creación, difusión, distribución o intercambio digital de fotografías, videos o audioclips de naturaleza sexual o íntima sin consentimiento

Las mujeres son las principales víctimas de esta forma de violencia digital, que las afecta de manera desproporcionada en todo el mundo. En varios estudios se ha comprobado que 90% de las personas afectadas por la distribución digital de imágenes íntimas sin consentimiento son mujeres (REVM-ONU, 2018; *Cyber Civil Rights Initiative*).



Consiste en crear, compartir o difundir en línea, **sin consentimiento**, material, imágenes o videos íntimos o sexualmente explícitos obtenidos con o sin el consentimiento de una persona, con el propósito de avergonzarla, estigmatizarla o perjudicarla (REVM-ONU, 2018, párr. 41).

Esta forma de violencia puede ocurrir en una gran variedad de contextos y relaciones interpersonales: en una relación íntima y de confianza en la cual estas imágenes son enviadas de forma voluntaria por una persona a su pareja o expareja sentimental (quizás por *sexting*), como parte de esquemas de ciberhostigamiento o ciberacoso por amistades, conocidos o desconocidos, o cuando el material se obtiene mediante *hackeo*⁸ o acceso físico a dispositivos.

Abarca también los siguientes actos:

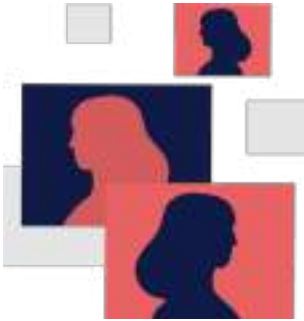
- 01 Grabar y distribuir imágenes de abuso sexual.
- 02 Tomar, sin consentimiento, fotografías o videos de partes íntimas del cuerpo de las mujeres en espacios públicos y compartirlos en línea (por ejemplo, fotografías tomadas por debajo de la falda o por arriba de la blusa, actos que se denominan *upskirting*, *downblousing* o *creepshots*).
- 03 **Crear imágenes sexualizadas, editadas con fotomontaje, o videos *deepfake***, en cuyo caso las imágenes o los videos de las mujeres pueden ser tomados de sitios en línea o cuentas de redes sociales y superpuestos en el cuerpo de otras personas para simular escenas sexuales o contenido pornográfico con el objetivo de dañar la reputación de la víctima.

⁸ El *hackeo* es el uso de técnicas y procedimientos por un hacker para introducirse sin autorización en sistemas informáticos ajenos con el fin de manipularlos o de obtener información o por diversión. El *cracking* es una práctica relacionada con el hackeo, pero implica entrar en sistemas ajenos con fines delictivos para violar la intimidad de la persona afectada o la confidencialidad de la información o dañar la información o los soportes físicos.



¿Qué es un *deepfake* (video ultra falso)?

Desde 2017 existen programas de *software* que utilizan técnicas de aprendizaje automático para intercambiar la cara de una persona con la de otra (Knight, 2019). Estos programas se están usando para crear videos pornográficos falsos y publicarlos en línea (Farokhmanesh, 2018). Con estos videos se ha atacado en particular a mujeres que participan en la vida política; sin embargo, se prevé que su uso se extenderá puesto que esta tecnología se ha vuelto más accesible para usuarios que no son expertos (*Deeptrace*, 2019). Además, dado que los videos *deepfakes* utilizan técnicas de aprendizaje automático, a la larga podría ser difícil distinguir entre un video falso y uno real sin la ayuda de herramientas forenses (Maras y Alexandrou, 2018).



La producción de fotografías o videos íntimos sin consentimiento **puede estar acompañada de extorsión o amenazas de distribuirlos** o efectuarse sin el conocimiento de las víctimas en grupos cerrados de redes sociales en los cuales varios hombres difunden imágenes de mujeres desnudas sin su consentimiento para gratificación sexual de los otros miembros o como parte de esquemas de enriquecimiento en los cuales los agresores compilan y venden enlaces con archivos o “paquetes” de imágenes sexuales de mujeres obtenidas por diversas vías sin su consentimiento (archivos que, en países como México y Chile, se han denominado *packs*)⁹.

También **es muy común filtrar datos personales de las mujeres que aparecen en esas imágenes o videos**, muchas de las cuales se ven obligadas a abandonar la escuela, el trabajo, el hogar y su comunidad para evitar la humillación constante (Henry, Powell y Flynn, 2017).



Para recordar...

Esta forma de violencia en línea se ha denominado comúnmente “*pornovenganza*”. Sin embargo, no es un término correcto, y su uso es problemático puesto que no refleja la diversidad de motivaciones de los perpetradores, que se extienden más allá de la venganza y van desde una reafirmación de su masculinidad hasta la extorsión económica o la gratificación sexual. Este término también minimiza el daño que se causa a las víctimas, oculta el componente no consensual de la conducta y pone énfasis en la imagen en lugar del comportamiento abusivo de los perpetradores (Powell, Henry y Flynn, 2018).



¿Qué es el *sexting* o sexteo?

El *sexting* o sexteo es una práctica que implica la generación e intercambio de material sexualmente explícito (UNDOC, 2019; *Interagency Working Group*, 2016). Puede incluir la creación y envío de imágenes de forma consensuada o la creación consensuada de imágenes que se distribuyen sin consentimiento (Salter, Crofts y Lee, 2013, p. 302).

En varios estudios se ha comprobado que es una práctica común entre jóvenes de ambos sexos, quienes están utilizando las tecnologías como una herramienta de expresión sexual. Se ha constatado, sin embargo, que el *sexting* se presenta en contextos en los cuales las jóvenes y las niñas están sometidas a una mayor presión social que los jóvenes para compartir imágenes sexuales y degradantes de su cuerpo, mientras que los jóvenes y los niños se ven presionados para solicitar imágenes, recibirlas y compartirlas con sus amigos a fin de reafirmar su heterosexualidad (Walker, Sanci y Temple, 2013).

⁹ Monserrat Peralta (2019). “El oscuro negocio de los packs”. *El Universal*. Disponible en: <https://www.eluniversal.com.mx/nacion/el-oscuro-negocio-de-los-packs-fotos-intimas-desde-un-peso-en-la-red>



Bajo la lupa:

Algunos aspectos importantes del sexting y la distribución de imágenes y videos íntimos sin consentimiento:

01

Aunque exista consentimiento para intercambiar fotos íntimas con alguien o para grabar actos sexuales (incluso en presencia de otras personas), **este consentimiento no implica un permiso para almacenar, publicar, reproducir o difundir estos contenidos.** Haber consentido a la grabación no significa que se haya otorgado consentimiento para otra etapa en el proceso. Quien lo haga estará violando la intimidad de la persona que participó en la práctica de *sexting*. Esto es una forma grave de violencia de género, una violación de los derechos humanos, un acto ilícito, y ya está tipificado como delito en muchos países.

No se debe estigmatizar la práctica del sexting. Todas y todos tenemos derecho a usar la tecnología para expresar nuestra sexualidad. No obstante, al hacerlo es muy importante tener presente que hay riesgos y que, por consiguiente, es necesario **considerar la seguridad digital.**

02

03

Los Estados tienen la obligación de adoptar medidas apropiadas para prevenir, investigar, sancionar y reparar los daños causados por esta forma de violencia. Asimismo, las plataformas de internet están obligadas a evitar la difusión de imágenes y videos íntimos sin consentimiento, a retirar ese contenido y a reducir o mitigar los riesgos.

En el sitio [Acoso.online](https://acoso.online) se puede encontrar información sobre esta forma de violencia digital, así como consejos para denunciar un caso ante plataformas de internet, además de detalles sobre las distintas leyes en países de América Latina en las que puede basarse una denuncia. El sitio de la organización [Without my Consent](https://withoutmyconsent.org) también tiene una gran variedad de recursos para apoyar a las sobrevivientes de esta forma de violencia¹⁰. Además, en la página 51 de esta guía se pueden encontrar algunas recomendaciones y consejos adicionales.

Se destaca que la provisión de estos recursos no representa un respaldo por parte de la OEA o de sus Estados Miembros al contenido o a las organizaciones aquí nombradas. Estos recursos se presentan a modo de ejemplo de aquellas organizaciones, guías, herramientas, etcétera, que están disponibles en la región para que las personas lectoras puedan ampliar la información relacionada con la temática de esta publicación.

¹⁰ Acoso.online, *Pornografía no consentida. Cinco claves para denunciar y resistir su publicación*. Disponible en: <https://acoso.online/ar>; Without my Consent. *Tools to fight online harassment, Resources*. Disponible en: <https://withoutmyconsent.org/resources/>



Acceso, uso, control, manipulación, intercambio o publicación no autorizada de información privada y datos personales



Según Amnistía Internacional, una cuarta parte de las mujeres usuarias de internet han sido víctimas de *doxing* al menos una vez en su vida (AI, 201).

Esta forma de violencia se manifiesta en forma de **ataques a cuentas en línea o dispositivos** de una persona (teléfonos móviles, computadoras, tabletas, etc.) para obtener, manipular y/o publicar información de manera no autorizada mediante el robo de contraseñas, instalación de programas espías, robo de equipo o registradores de teclas¹¹ (APC, 2017). Puede involucrar también el acceso no autorizado y control total de cuentas o dispositivos de una persona.

Doxing o doxxing:

El término proviene de la frase en inglés *dropping docs* y consiste en **la extracción y la publicación no autorizadas de información personal** —como el nombre completo, la dirección, números de teléfono, correos electrónicos, el nombre del cónyuge, familiares e hijos, detalles financieros o laborales— como una forma de intimidación o con la intención de localizar a la persona en “el mundo real” para acosarla (APC, 2017; *Women’s Media Center*, 2019). También se ha observado que la información personal puede ser publicada en sitios pornográficos junto con el anuncio de que la víctima está ofreciendo servicios sexuales.

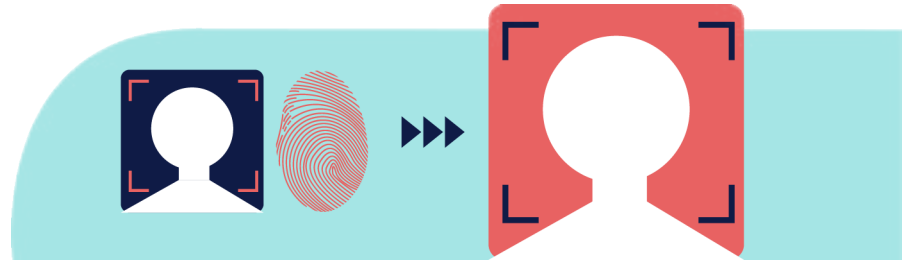


¹¹ El registrador de teclas o *keylogger* es un programa malicioso que se instala entre el teclado y el sistema operativo para interceptar y registrar información de cada tecla pulsada en el dispositivo sin que la persona usuaria lo sepa.

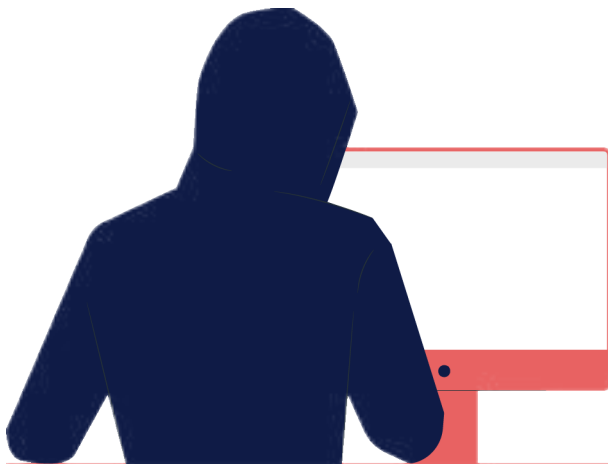


Suplantación y robo de identidad

Una investigación realizada por la Universidad Nacional de Australia reveló que las mujeres tienen 50% más de probabilidades que los hombres de ser víctimas de robo de identidad¹².



Es una actividad malintencionada que consiste en **hacerse pasar por otra persona en línea usando sus datos personales con el fin de amenazarla o intimidarla** (*Women's Media Center*, 2019). Esto puede hacerse mediante la creación de perfiles o cuentas falsas en redes sociales o la usurpación de cuentas de correo o números de teléfono que puedan ser utilizados para contactar amistades, familiares, colegas o conocidos de la víctima con el propósito de entablar comunicación y tener acceso a información sobre ella (APC, 2017; Barrera, 2017).



El caso del ciberatacante de toda una familia

En un conocido caso en Chile, un agresor cibernético extranjero acosó durante 13 años a una familia completa y su círculo de amistades (al menos 50 personas), robando información personal y suplantando su identidad, incluido el robo de contraseñas, correos electrónicos y perfiles de redes sociales, así como fotos personales para enviar mensajes obscenos y hacer publicaciones a gran escala en páginas pornográficas. El agresor, que se sospecha que era la expareja sentimental de una de las integrantes de la familia, realizó numerosos actos de ciberviolencia contra toda persona relacionada con la víctima original y su familia o que tuviera contacto con ella (Paz Peña, 2017).

En casos de violencia doméstica es frecuente la suplantación y el robo de identidad de las víctimas a través de distintos mecanismos, como la utilización de sus datos personales para el uso ilícito de sus tarjetas de crédito o el control de los bienes, para controlar las comunicaciones que entablan con otras personas, o hacerse pasar por familiares o amistades en redes sociales para vigilarlas a través de esos perfiles.

¹² Australian Communications Consumer Action Network, "Identity Theft and Gender". Disponible en: https://accan.org.au/files/Grants/ANU%20ID%20theft/ANU%20ID%20theft%20infographic_Gender.pdf



Actos que dañan la reputación o la credibilidad de una persona



En una investigación mundial de la UNESCO, 41% de las encuestadas señaló haber sido blanco de ataques que parecían estar relacionados con campañas de desinformación dirigidas específicamente a desacreditar mujeres periodistas.

Esta forma de violencia afecta a las mujeres en general. Por ejemplo, de acuerdo con el estudio *Conocer para resistir. Violencia de género en línea en Perú*¹³, 15% de las víctimas entrevistadas señalaron haber sido afectadas por la difusión de información falsa, manipulada o fuera de contexto.

Esta forma de violencia consiste en **crear y compartir información personal falsa con la intención de dañar la reputación de una persona**. Por ejemplo, crear perfiles falsos en redes sociales o cuentas en línea; hacer fotomontajes o imágenes manipuladas de contenido sexual a partir de fotografías obtenidas de redes sociales; publicar avisos en sitios de citas o pornográficos con fotos íntimas; difundir comentarios o publicaciones ofensivos o falsos o memes en foros de discusión, redes sociales o páginas de internet (incluidos los actos de vandalismo en *Wikipedia*) y realizar actos de calumnia y manipulación (APC, 2017; Barrera, 2017).



¿Qué es el *slutshaming*?

Es una forma de violencia que consiste en señalar públicamente a una mujer por su supuesta actividad sexual con el fin de avergonzarla, dañar su reputación y regular su sexualidad. Puede implicar el uso de fotografías y/o videos y lenguaje denigrante.

Caso Camila Zuluaga

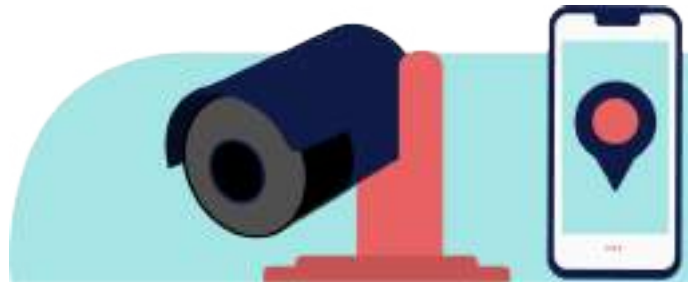
Diversas organizaciones de la sociedad civil han documentado a lo largo de la región un aumento en la comisión de actos en línea que buscan dañar la reputación y credibilidad de mujeres periodistas, políticas y defensoras de derechos humanos (Peña, 2017; Luchadoras, 2017; Cuellar y Chaher, 2020). En un caso en Colombia, la periodista Camila Zuluaga fue atacada en septiembre de 2019 de forma coordinada y masiva luego de que el portal *Los Irreverentes* publicó, sin presentar prueba alguna, que había recibido 35 millones de pesos de una persona implicada en un escándalo de corrupción. Los ataques se concentraron en las etiquetas #CamilaEstásPillada y #CamilitaEstásPillada, que alcanzaron hasta 10 mil menciones en un día. Investigaciones en el tema encontraron evidencias de automatización en estos ataques coordinados y la operación de un grupo de WhatsApp en el cual se daban las instrucciones para realizar los ataques a fin de desprestigiar su trabajo periodístico (Cuellar y Chaher, 2020).

¹³ UNESCO y el Centro Internacional para Periodistas (ICFJ) (2021). Violencia en línea: La nueva línea de combate para las mujeres periodistas - #JournalistsToo. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000375136_spa; Carlos Guerrero y Miguel Morachimo (2018). Conocer para resistir. Violencia de Género en Línea en Perú. Disponible en: https://hiperderecho.org/tecnore resistencias/wp-content/uploads/2019/01/violencia_genero_linea_peru_2018.pdf



Actos que implican la vigilancia y el monitoreo de una persona

Se ha documentado que, por lo menos en 29% de los casos de violencia doméstica o íntima, la pareja o expareja ha usado algún tipo de programa espía o equipo de geolocalización instalado en las computadoras o los celulares de las mujeres afectadas (*Women's Aid*, 2014).



El monitoreo y la vigilancia constantes de las **actividades de una persona en línea y fuera de internet** o de su ubicación constituyen formas de violencia que pueden realizarse con la intervención de diferentes tecnologías (APC, 2017).

- Se pueden realizar con un *spyware* instalado en el celular de la víctima para monitorearla clandestinamente o robar su información.
- También se efectúan con dispositivos de geolocalización ubicados en automóviles o en bolsas de mano, juguetes, cámaras de vigilancia, asistentes virtuales o dispositivos inteligentes conectados.



¿Qué es el *spyware*?

Es un tipo de *software* malicioso que se instala en los dispositivos de una persona para registrar todo lo que hace, incluidos los mensajes de texto, los correos electrónicos, las fotografías o hasta todas las teclas pulsadas. Con ciertos tipos de *software* malicioso, los agresores pueden encender de forma remota la cámara o el micrófono del teléfono móvil, rastrear la ubicación de la víctima, monitorear el uso de aplicaciones o interceptar llamadas.





Ciberhostigamiento o ciberacecho



Varios estudios sobre el tema han demostrado que el ciberhostigamiento y el ciberacoso son ciberdelitos con una importante connotación de género y que las mujeres y las niñas tienen una mayor probabilidad de ser víctimas de estas formas de violencia (Reyns, Henson y Fisher, 2011).

Hasta la fecha no hay una definición única del ciberhostigamiento, ya que abarca una gran variedad de comportamientos digitales abusivos. En términos generales puede definirse como una actividad intencional y reiterada realizada mediante computadoras, teléfonos celulares y otros dispositivos electrónicos, que puede constituir o no actos inofensivos por separado, pero que, en conjunto, constituye un patrón de conductas amenazantes que socavan la sensación de seguridad de una persona y le provocan miedo, angustia o alarma (EIGE, 2017: 4; PRC, 2018; Maras, 2016). Esta actividad puede estar dirigida también contra familiares, amistades o la pareja sentimental de la víctima.

A diferencia del ciberacoso, el ciberhostigamiento implica un patrón y la comisión de más de un incidente a lo largo de un tiempo usando las TIC, con el objetivo reiterado de hostigar, acechar, molestar, atacar, humillar, amenazar, asustar u ofender a una persona o abusar verbalmente de ella (UNODC, 2015). Puede consistir en correos electrónicos, llamadas, mensajes de texto, chat en línea o el envío constante de comentarios obscenos, vulgares, difamatorios o amenazantes por internet. Algunas de las conductas que puede abarcar son:



Espiar, obsesionarse o compilar información en línea sobre alguien y entablar comunicación con la persona sin su consentimiento; enviar constantemente solicitudes de amistad en redes sociales; unirse a todos los grupos en línea de los que esta forma parte; dar seguimiento a las notas publicadas por la víctima en redes sociales por medio de conocidos que tengan en común, colegas, amistades o familiares, o ver constantemente su perfil para que ella lo note (UNODC, 2019).



Llamar o enviar correos, mensajes de texto o de voz de forma repetitiva, incluso mensajes amenazantes o que busquen mantener el control sobre la víctima.



Formular proposiciones sexuales indeseadas y reiteradas, enviar fotos sexuales no solicitadas (fotos de los genitales masculinos de los agresores) o monitorear y vigilar constantemente la ubicación de una persona o sus actividades y comunicaciones diarias (Henry y Powell, 2016).



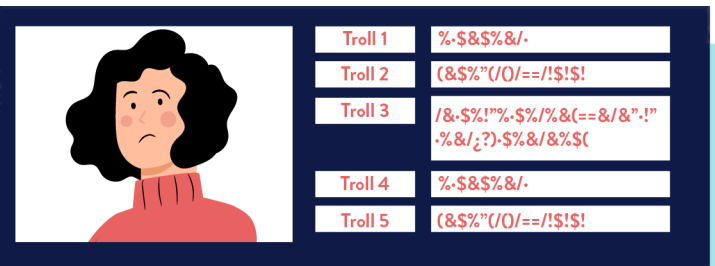
Publicar constantemente información falsa, maliciosa u ofensiva sobre una persona en sus páginas, blogs o redes sociales.

Los perpetradores de ciberhostigamiento pueden ser parejas íntimas o sexuales, exparejas, conocidos, amistades, familiares o extraños. También es importante destacar que **esta táctica es particularmente frecuente en contextos de violencia doméstica o de pareja.**



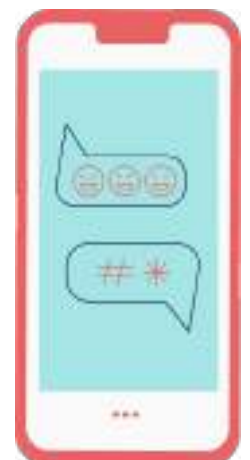
Ciberacoso

En un estudio publicado en 2018 por Amnistía Internacional se señaló que 23% de las mujeres encuestadas habían experimentado por lo menos una vez algún tipo de abuso u hostigamiento en redes sociales (AI, 2018).



El ciberacoso implica el **uso intencional de las TIC para humillar, molestar, atacar, amenazar, alarmar, ofender o insultar a una persona** (Maras, 2016). A diferencia del ciberhostigamiento, en el que hay un patrón de comportamientos amenazantes, en el caso del ciberacoso basta con un solo incidente, aunque puede implicar también más de uno (UNODC, 2019).

El ciberacoso **puede adoptar numerosas manifestaciones y estar asociado a otras formas de violencia en línea.** Por ejemplo, puede incluir el envío de mensajes no deseados e intimidantes por correo electrónico, texto o redes sociales; insinuaciones inapropiadas u ofensivas en redes sociales o salas de chat; violencia verbal y amenazas en línea de violencia física o muerte; discurso de odio; el robo o la publicación de información personal, imágenes y videos, y la difusión de información falsa o rumores para dañar la reputación de una persona (EIGE, 2017; APC, 2017, UNODC, 2019).

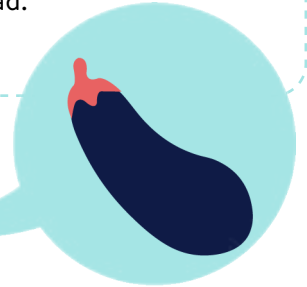




¿Qué es el discurso de odio?

Es el uso de un lenguaje que denigra, insulta, amenaza o ataca a una persona a causa de su identidad y otras características, como su orientación sexual o discapacidad.

El ciberacoso puede abarcar también la revelación de información personal de la víctima (*doxing*) con invitaciones a su violación sexual, lo cual ha propiciado situaciones de revictimización en las cuales los acosadores y agresores van al domicilio de la mujer bajo ataque.



El ciberacoso, que afecta de forma desproporcionada a las mujeres en todo el mundo, tiene connotaciones sexuales (Li, 2006; Henry y Powell, 2017, p. 212). Puede implicar amenazas de violación, femicidio, violencia física sexualizada o incitación a la violencia física y sexual dirigida contra la víctima o sus familiares, y ataques verbales sexistas u ofensivos asociados a la condición de género o a la apariencia física de las mujeres. Incluye el envío indeseado de materiales sexualmente explícitos, contenido que deshumaniza a las mujeres y las presenta como objetos sexuales, *slutshaming* o comentarios misóginos, explícitamente sexuales y abusivos (Jane, 2016).



¿Sabías que...?

Varios estudios revelan que las mujeres tienen más del doble de probabilidades que los hombres de ser blanco de ciberacoso sexual (Reid, 2016).

Una forma común de ciberacoso sexual es el *cyberflashing* o envío de fotos obscenas a una mujer sin su consentimiento (por ejemplo, fotografías de los genitales del acosador) con el objetivo de molestarla, intimidarla o incomodarla.



Los perpetradores de ciberacoso pueden ser *trolls*, que publican comentarios extremadamente ofensivos y virulentos para provocar una reacción emocional y una respuesta de otras personas usuarias de internet. Este comportamiento se denomina *troleo* (Maras, 2016).

El troleo de género es la publicación de mensajes, imágenes o videos, así como la creación de *hashtags*, con el propósito de molestar a mujeres y niñas o incitar a la violencia contra ellas (REVM-ONU, 2018; Mantilla, 2013)

El ciberacoso también puede ser grupal (a lo que se ha llamado *raiding*), cuando dos o más personas se organizan y se coordinan para acosar en línea de forma repetida a una persona, muchas veces de manera sostenida a lo largo del tiempo y con una estrategia. Estos grupos pueden estar formados por miembros de comunidades, foros o alianzas digitales, donde se han encontrado ciertos tipos de masculinidades particularmente violentas (Jane, 2017). El ciberacoso puede realizarse también a través de *bots* y/o cuentas falsas (llamadas marionetas o *sockpuppets*) que buscan pasar como usuarios reales para difundir información sesgada, desinformar o atacar.

Están proliferando en América Latina los ataques de grupos coordinados por medio de redes de trolles y hackers, como la “Legión Holk” (originada en Colombia y Perú) o la “Secta 100tifka”, que realizan ataques y acoso en masa con el fin de generar confrontación y polémica, generar tendencias y fomentar la discriminación, el racismo y la misoginia. Estos grupos suelen atacar a mujeres que son activas en redes sociales, que tienen un perfil público o que son feministas. Es común la difusión de fotomontajes sexualizados, la suplantación de su identidad en redes sociales con fines difamatorios y la circulación de contenidos degradantes (Peña, 2017; Barrera, 2017).



Algunos de estos ataques se han vuelto desproporcionados: se forman ciberturbas (denominadas *cybermobs*) integradas por grupos organizados en línea que publican contenido ofensivo o destructivo de forma masiva con la intención de avergonzar a alguien o de lograr el retiro de su perfil de redes sociales (Citron, 2014).

Caso Ana Gabriela Guevara

Un caso emblemático de ataques coordinados en México fue el de la ex deportista y senadora Ana Gabriela Guevara, quien, en diciembre de 2016, después de haber hecho públicas en redes sociales las agresiones físicas que sufrió en la vía pública, fue atacada por grupos organizados de *trolls* y *hackers* con cuentas falsas que hicieron virales *hashtags* con referencias a la violencia de género. Se utilizaron *hashtags* tales como #MujerGolpeadaEsMujerFeliz o #GolpearMujerEsFelicidad, los cuales se convirtieron en *trending topics* en diversos países hispanohablantes (Peña Ochoa, 2017; Barrera, 2017).



Ciberbullying



Según una investigación a nivel mundial realizada por IPSOS¹⁴ en 2018, 1 de cada 5 progenitores señaló que su hija/o había sido víctima de *ciberbullying*. También se identificó que Perú, Argentina y México eran los países con los niveles más altos de *ciberbullying* en redes sociales.

El *ciberbullying* o ciberintimidación es el uso de tecnologías por menores de edad para humillar, molestar, alarmar, insultar o atacar a otra/o menor de edad o difundir información falsa o rumores sobre la víctima, así como para amenazarla, aislarla, excluirla o marginarla (Maras, 2016; Hinduja y Patchin, 2014; UNODC, 2015).

Puede realizarse a través de mensajes de texto, correos electrónicos, encuestas virtuales, blogs, publicaciones de redes sociales, videojuegos en línea o sitios de realidad virtual, y puede producir daños muy graves a la salud emocional y física de las personas bajo ataque, quienes pueden incluso autolesionarse o suicidarse.

En la mayoría de los países se considera que, **en los casos de *ciberbullying*, los niños y las niñas son responsables y víctimas de esta forma de violencia** (Duggan et al., 2015). En otros, como Australia y Nueva Zelandia, el *ciberbullying* puede involucrar a personas adultas.



¿Sabías que...?

Hay diversas opiniones sobre si el género de las personas es un factor determinante del *ciberbullying* (Navarro y Jasinski, 2013; Smith, 2012; Fanti, Demetriou y Hawa, 2012; Livingstone et al., 2011; Calvete et al., 2010). A reserva de ello, es claro es que los daños y las consecuencias que sufren las niñas y los niños son diferentes en función de los estereotipos de género que enfrentan: es común que las niñas víctimas de *ciberbullying* sean atacadas con comentarios ofensivos y violentos sobre su cuerpo o su sexualidad.

¹⁴ Ipsos Public Affairs (2018). *Cyberbullying. A Global Advisory Survey*. Disponible en: https://www.ipsos.com/sites/default/files/ct/news/documents/2018-06/cyberbullying_june2018.pdf



Amenazas directas de daño o violencia

En 2019, Amnistía Internacional publicó la investigación *Corazones Verdes: Violencia online contra las mujeres durante el debate por la legislación del aborto en Argentina*¹⁵, en la cual identificó que 1 de cada 3 mujeres encuestadas había sufrido violencia en redes sociales, de las cuales 26% recibió amenazas directas y/o indirectas de violencia psicológica o sexual.



Este tipo de violencia consiste en el envío o la publicación de comunicaciones o contenido (mensajes orales o escritos, imágenes, videos) por medio de tecnologías para expresar la **intención de cometer un daño** físico o violencia sexual (APC, 2017; Barrera, 2017).

Incluye la extorsión digital, la cual ocurre cuando una persona ejerce presión sobre otra para forzarla a actuar de un cierto modo con amenazas, intimidación o agresiones, con la finalidad de doblegar su voluntad o controlarla emocionalmente. Puede tomar la forma de amenazas de publicar en línea o enviar a conocidos de la víctima información privada, sexual o íntima como chantaje sexual.



La sextorsión consiste en amenazar a una persona con difundir imágenes o videos íntimos con la finalidad de obtener más material sobre actos sexuales explícitos, mantener relaciones sexuales o sonsacar dinero (REVM-ONU, 2018, párr. 32). Esta forma de violencia afecta desproporcionadamente a mujeres y, con pocas excepciones, es perpetrada por lo general por personas que se identifican como hombres (Kelley, 2019).

Esta forma de violencia ha tenido un crecimiento exponencial durante los últimos años y puede llevarse a cabo de múltiples formas: desde *hackers* que envían correos en los que exigen dinero para no publicar imágenes y videos íntimos supuestamente tomados de forma remota activando la cámara de un dispositivo hasta parejas o exparejas íntimas que hacen sextorsión para su propia gratificación sexual. En un informe de 2018 del Centro de Quejas sobre Delitos Cibernéticos del FBI, se señaló que se había producido un incremento de 242% de los correos electrónicos con amenazas de extorsión, que en su mayoría son sextorsivos (FBI-ICC, 2018).

¹⁵ Amnistía Internacional (2019). *Corazones Verdes. Violencia online contra las mujeres durante el debate por la legalización del aborto en Argentina*. Disponible en: https://amnistia.org.ar/corazonesverdes/files/2019/11/corazones_verdes_violencia_online.pdf

Caso #GamerGate

En 2014 tuvo lugar una de las primeras campañas de ataques masivos en línea denominada #GamerGate¹⁶ dirigida en contra de varias mujeres de la industria de los videojuegos, incluidas las desarrolladoras Zoe Quinn, Brianna Wu y la comunicadora Anita Sarkeesian, luego de que se pronunciaron en torno al sexismo y la desigualdad de género en los videojuegos. Los partidarios del #GamerGate manifestaron su oposición a la influencia del feminismo en la cultura de los videojuegos, organizándose en plataformas en línea tales como 4Chan, Twitter y Reddit para coordinar ataques a gran escala que incluyeron actos de ciberacoso, *doxing* y amenazas de violación y de muerte. Estas tres mujeres denunciaron ataques de *doxing* con amenazas que escalaron a tal magnitud que tuvieron que huir de sus casas. En particular, los ataques en contra de Anita Sarkeesian alcanzaron proporciones altamente agresivas que incluyeron amenazas de bomba cuando se le nominó para recibir un premio en San Francisco y amenazas terroristas cuando se anunció que participaría en una conferencia en la Universidad de Utah.



Violencia física facilitada por las tecnologías



En la investigación de la UNESCO y ICFJ titulada *Violencia en línea: La nueva línea de combate para las mujeres periodistas - #JournalistsToo*¹⁷ se documentó que 20% de las mujeres encuestadas habían sido atacadas *offline* en conexión con la violencia que experimentaron en línea.

Esta forma de violencia puede tener diversas manifestaciones, como ataques sexuales organizados o planificados por medio de las TIC o violencia sexual a partir de la publicación en línea de los datos personales de la víctima después de localizarla (*doxing*).

También puede presentarse cuando un agresor entabla amistad en línea con una persona para conocerla y después abusar sexualmente de ella (como puede ocurrir con aplicaciones de citas) o cuando un agresor obliga a una persona a entablar relaciones sexuales bajo la amenaza de publicar información íntima o sexual (sextorsión) (Henry y Powell, 2018).

¹⁶ Eliana Dockterman (2014). "What is #GamerGate and why are women being threatened about video games?" *Time*. Disponible en <https://time.com/3510381/gamergate-faq/>

¹⁷ UNESCO y el Centro Internacional para Periodistas (ICFJ) (2021). *Violencia en línea: La nueva línea de combate para las mujeres periodistas - #JournalistsToo*. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000375136_spa



Abuso, explotación y/o trata de mujeres y niñas por medio de las tecnologías

Algunas encuestas indican que las nuevas tecnologías facilitan la trata mundial de personas (cuyas víctimas son mujeres en 80% de los casos y en 95% de los casos de explotación sexual) con un nuevo *modus operandi* digital, en el cual se usa la internet para el reclutamiento, la venta, el anuncio y la explotación de mujeres y niñas (Van Der Wilk, 2018).



Esta forma de violencia en línea implica la intermediación de las tecnologías para el ejercicio de poder sobre una persona a partir de la explotación sexual de su imagen o de su cuerpo contra su voluntad (Barrera, 2017). Algunas de las conductas incluidas en esta forma de violencia son las siguientes:

- El uso de tecnologías para seleccionar y enganchar mujeres y niñas con fines de abuso sexual o trata, obligarlas a aceptar situaciones de trata y abuso sexual, ejercer poder y control sobre ellas o impedirles que se liberen del abuso, incluso con amenazas de revelar información privada (REVM-ONU, 2018, párr. 32).
- El *grooming* o ciberengaño pederasta, es decir, actos deliberados de un adulto para acercarse a una persona menor de edad (posiblemente cultivando una conexión sentimental) con el objetivo de establecer una relación y un control emocional que le permita cometer abusos sexuales, entablar relaciones virtuales, obtener pornografía infantil o traficar al o la menor (*Women's Media Center*, 2019).
- La publicación de imágenes sexuales sin el consentimiento de una persona para fines de comercialización y prostitución.



Ataques a grupos, organizaciones o comunidades de mujeres



Diversos estudios han documentado que entre quienes enfrentan un riesgo más alto de ser víctimas de violencia de género en línea se encuentran las defensoras de derechos humanos y de la igualdad de género, mujeres identificadas como feministas y mujeres activistas trabajando en el ámbito de la salud sexual y reproductiva (APC, 2017; Barrera, 2018; REVM-ONU, 2018)

Consisten en actos intencionales para censurar y dañar a organizaciones de mujeres, incluso con ataques a sus canales de expresión (Barrera, 2018), como tener acceso a ellos sin consentimiento y *hackear* páginas de internet, redes sociales o cuentas de correo para afectar el desarrollo de sus funciones, lograr que se dé de baja al perfil o a las redes sociales de la organización mediante el uso de normas comunitarias para denunciar contenido que la plataforma considera sensible, ataques de denegación de servicio (DDoS)¹⁸, restricciones de uso de dominio o robo de dominio, y *blakouts* o apagones de internet durante una reunión o protesta (APC, 2017).

Abarcan la vigilancia y el monitoreo de las actividades de las integrantes de comunidades o grupos, amenazas directas de violencia contra ellas, el ciberacoso mediante contenido sexualmente explícito, la publicación de información confidencial (como direcciones de refugios para mujeres sobrevivientes de violencia) o el acoso reiterado a un grupo completo.



Casos de ataques a grupos feministas

En América Latina se han registrado múltiples ataques a sitios web, perfiles o cuentas de grupos feministas o defensoras de los derechos humanos de las mujeres con el fin de bloquear o poner fuera de línea sus contenidos de forma temporal o permanente. Se han denunciado casos como el de la colectiva feminista mexicana Las Hijas de la Violencia y la organización feminista colombiana Mujeres Insumisas, y constantes ataques coordinados contra activistas y grupos de mujeres feministas negras y transfeministas en Brasil (Lyons et al., 2016; Peña, 2017).

¹⁸ Ataque en línea que consiste en movilizar personas para que envíen una gran cantidad de solicitudes al servidor de un sitio web a fin de saturarlo y que sea inaccesible.

Parte *tres*

Manual de Autoprotección y Respuesta:

HERRAMIENTAS DE SEGURIDAD

DIGITAL

FRENTE A LA VIOLENCIA DE GÉNERO EN LÍNEA





Recomendaciones básicas de seguridad digital: medidas preventivas



Tomar medidas para reforzar la seguridad digital es la primera línea de defensa contra amenazas, ataques y actos de violencia en línea. Por supuesto, no todas las mujeres tienen las mismas prioridades o se ven amenazadas de la misma manera, y las medidas pueden variar según el caso. Es importante recordar que la ciberseguridad es un proceso personal que puede desarrollarse al propio ritmo y que se puede alcanzar con un poco de paciencia y una planificación apropiada.

A continuación, se presentan algunas recomendaciones básicas para navegar con seguridad y controlar las interacciones digitales, así como recursos adicionales para saber más sobre el tema. Toda esta información puede resultar abrumadora en una primera lectura. Sin embargo, **este manual busca desmitificar el proceso de fortalecimiento de la ciberseguridad de las mujeres.** Es importante recordar que se puede avanzar poco a poco con estas recomendaciones, y en el camino seguramente se revelará que fortalecer la seguridad digital es mucho más sencillo de lo que parece.

Es importante destacar que la provisión de los siguientes recursos no representa un respaldo por parte de la OEA o de sus Estados Miembros a su contenido o a las organizaciones nombradas. Los recursos se presentan a modo de ejemplo de las organizaciones, guías, herramientas, etcétera, que están disponibles en la región para que las personas lectoras puedan ampliar la información relacionada con la temática que aborda esta publicación.

01 Utilizar contraseñas seguras como protección frente al *hackeo* o la suplantación de identidad.

Usar contraseñas fuertes y seguras es crucial para proteger la información en línea, puesto que son la puerta de entrada a nuestras cuentas y, con ello, a los pormenores de nuestra vida personal.





Es muy común que elijamos contraseñas personales y fáciles de recordar (por ejemplo, 12345), pero esto nos pone en riesgo, ya que alguien conocido o un *hacker* podría adivinarlas fácilmente. Para una protección efectiva deben emplearse **contraseñas únicas: no usar la misma contraseña o contraseñas muy similares** en las diferentes páginas y cuentas (por ejemplo, simplemente agregando un 1 o reciclándolas) y, de ser posible, utilizar un nombre de usuario diferente en cada cuenta (por ejemplo, una contraseña y un nombre de usuario para el correo electrónico, otros para la cuenta bancaria, otros para redes sociales, etc.).



Cambiar las contraseñas constantemente (de preferencia cada 90 días), en particular las de cuentas más confidenciales. Sobre todo, cambiarlas si se recibe un correo legítimo y verificado (cerciorándose que no sea un intento de *phishing*) en el cual se informa que la cuenta de un servicio ha sido comprometida.



Crear contraseñas complejas. Para brindar una protección efectiva, las contraseñas tienen que ser largas, únicas, aleatorias y difíciles de predecir e incluir una combinación de por lo menos 12 letras mayúsculas y minúsculas, números y símbolos. En este sitio de *Autoprotección Digital contra la Vigilancia* es posible consultar una [guía para crear contraseñas seguras](#)¹⁹.



Activar la **verificación en dos pasos** (autenticación de dos factores)²⁰ del correo electrónico y las redes sociales. Esta opción pide a la usuaria que se identifique con una combinación de dos métodos de autenticación, es decir, solicita la contraseña y un código único enviado por SMS o generado por una aplicación, el cual se debe introducir para ingresar a la cuenta desde una computadora, un teléfono o un navegador nuevo o no registrado. Es posible consultar más información sobre la [autenticación de dos factores](#) en el sitio de *Electronic Frontier Foundation*²¹ así como directamente en [Facebook](#)²², [Instagram](#)²³, [Twitter](#)²⁴, [Gmail](#)²⁵ y [Apple](#)²⁶.



Para mayor facilidad, se puede utilizar un **generador automático o administrador de contraseñas en línea**, que crean contraseñas aleatorias y seguras para cada una de las cuentas. Si se elige esta opción, lo único que tiene que recordarse es la contraseña maestra para desbloquear las demás. Algunos ejemplos de administradores son [1Password](#), [LastPass](#), [Password Generator](#) y [KeePassXC](#)²⁷. Puede consultarse un [video](#) con más información en el sitio de *Surveillance Self-Defense*²⁸.

¹⁹ *Surveillance Self-Defense. Creando contraseñas seguras.* Disponible en: <https://ssd.eff.org/es/node/23/>

²⁰ Disponibles en: <https://twofactorauth.org/>; <https://ssd.eff.org/es/module/c%C3%B3mo-habilitar-la-autenticaci%C3%B3n-de-dos-factores>

²¹ *Electronic Frontier Foundation. The 12 Days of 2FA: How to Enable Two-Factor Authentication for Your Online Accounts.* Disponible en: <https://www.eff.org/deeplinks/2016/12/12-days-2fa-how-enable-two-factor-authentication-your-online-accounts>

²² *Facebook. ¿Qué es la autenticación en dos pasos y cómo funciona en Facebook?* Disponible en: <https://www.facebook.com/help/148233965247823>

²³ *Instagram. Garantizar la seguridad en Instagram.* Disponible en: <https://help.instagram.com/1372599552763476>

²⁴ *Twitter. Cómo usar la autenticación de dos factores.* Disponible en: <https://help.twitter.com/es/managing-your-account/two-factor-authentication>

²⁵ *Google. Verificación en dos pasos.* Disponible en: <https://www.google.com/intl/es-419/landing/2step/>

²⁶ *Apple. Autenticación de doble factor para el ID de Apple.* Disponible en: <https://support.apple.com/es-es/HT204915>

²⁷ Disponibles en: <https://1password.com/>; <https://www.lastpass.com/es/>; <https://passwordsgenerator.net/>; y <https://keepassxc.org/>

²⁸ *Surveillance Self-Defense. Visión animada. Uso de gestores de contraseñas para estar seguro en línea.* Disponible en: <https://ssd.eff.org/es/node/85/>

Utilizar las preguntas de seguridad en los sitios que ofrecen esta opción, pero sin responderlas con información real (por ejemplo, el nombre de una mascota o de la calle del domicilio personal). Las respuestas deben ser difíciles de adivinar y no contener datos que puedan encontrarse en internet o en redes sociales (el apellido de la abuela, por ejemplo). Es posible guardar también las respuestas en un administrador de contraseñas.

Nunca compartir las contraseñas a través de una conexión que no sea segura, como mensajes de texto o SMS.

No guardar las contraseñas en la configuración del navegador, en la nube²⁹ o en un documento poco seguro en la computadora o el teléfono, puesto que son fáciles de encontrar si *hackean* el dispositivo. Pueden guardarse en un documento encriptado en un dispositivo físico seguro o anotarlas y guardarlas en un lugar donde pueda eliminarse fácilmente su rastro. Se puede consultar más información sobre el cifrado de archivos en [Windows](#) en el sitio de *Microsoft* y en el sitio de [Apple](#) para el sistema operativo iOS³⁰.

Para aprender más acerca del fortalecimiento de contraseñas, se puede consultar también la publicación [Alfabetización y Seguridad Digital](#), de la OEA y Twitter³¹.

02 Usa direcciones de correo electrónico distintas

Una medida de seguridad útil es **tener diferentes correos electrónicos para cada una de nuestras cuentas** en internet y para fines diversos; por ejemplo, una para comunicaciones personales, otra para el trabajo, otra para el perfil público, otra para las redes sociales, otra para juegos en línea y otra para recibir promociones. Con esto se evita que alguien que logre entrar en una de las cuentas tenga acceso automáticamente a las demás.



²⁹ La nube es un sistema de almacenamiento de datos, como Google Drive, Dropbox o iCloud, que no está en los dispositivos personales.

³⁰ *Microsoft*. *Cómo cifrar un archivo*. Disponible en: <https://support.microsoft.com/es-es/windows/c%C3%B3mo-cifrar-un-archivo-1131805c-47b8-2e3e-a705-807e13c10da7>; *Apple*. *Información general sobre la seguridad de iCloud*. Disponible en: <https://support.apple.com/es-es/HT202303>

³¹ Organización de los Estados Americanos y Twitter (2019). *Alfabetismo y Seguridad Digital: Mejores Prácticas en el uso de Twitter*. Disponible en: <https://www.oas.org/es/sms/cicte/docs/alfabetizacion-y-seguridad-digital.pdf>



Para recordar: precauciones básicas al navegar
La precaución es tu mejor arma cuando estás en línea.

- Borrar siempre correos electrónicos, publicaciones o mensajes que parezcan sospechosos.
- Conectarse únicamente por medio de redes *Wi-Fi* confiables. En caso de conectarse en una red pública, limitar la información que se envía o consulta.
- Utilizar una VPN (*virtual private network* o red virtual privada)³², la cual es una tecnología de red que protege de ciberataques cuando se realiza la conexión a internet por medio de una red *Wi-Fi* pública, ya que dificulta el robo de información confidencial por terceros. Es posible [descargar una VPN gratuita o paga](#), lo cual es un proceso relativamente sencillo como se explica en este [video](#).
- Navegar siempre en modalidad segura: cerciorándose de que el sitio web comience con `https://` (y no `http://`); eso significa que la información transita cifrada.
- Cuando se utilicen dispositivos ajenos, navegar siempre de forma privada o en modo incógnito para evitar que queden registradas las contraseñas.
- Descargar aplicaciones solo de sitios oficiales para asegurarse de que sean seguras.

03 Proteger los dispositivos electrónicos (computadora de escritorio, computadora portátil, teléfono móvil o tableta)



¿Qué es el malware?

Es un *software* malicioso que ejecuta acciones no solicitadas en los dispositivos para infiltrarse y dañar una computadora o un sistema de información.



No olvidar actualizar el *software* en los dispositivos. Actualizar el *software* regularmente no solo ayuda a que el dispositivo sea más rápido, sino que además brinda mayor seguridad, puesto que puede proteger de amenazas y resolver vulnerabilidades de las versiones anteriores.



Usar un programa antivirus. Si bien los antivirus no pueden detectar todos los programas maliciosos, ofrecen una capa de protección adicional a los dispositivos. Hay una gran variedad de antivirus en el mercado, pudiendo elegirse aquel que resulte más acorde a nuestras necesidades. En este sitio de *Reason Security* es posible consultar algunas [recomendaciones](#) para elegir un antivirus para la computadora³³.

³² Avast Blog. Por qué y cómo configurar una VPN en un iPhone o un Android. Disponible en: <https://blog.avast.com/es/por-que-y-como-configurar-una-vpn-en-un-iphone-o-un-android>; We Live Security. ¿Qué es una VPN y cómo funciona para la privacidad de la información? Disponible en: <https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/>

³³ Reason security. Which antivirus is best for laptops? Disponible en: <https://blog.reasonsecurity.com/2020/01/12/which-antivirus-is-best-for-laptops/>

Verificar las aplicaciones (apps). A fin de reforzar la seguridad de los dispositivos, se recomienda revisar qué aplicaciones están instaladas en el celular (pueden verse en el menú de configuraciones). Si se encuentra una *app* que no se usa o que no resulte conocida, buscar en internet para qué sirve. Si no se reconoce o no es del sistema operativo del celular, es preferible desinstalarla para mayor seguridad. En los siguientes enlaces es posible consultar cómo eliminar aplicaciones en *Android* y *Apple*³⁴.

Protección frente al software malicioso (malware). Algunos atacantes pueden tratar de acceder al dispositivo para extraer información o espiar por medio de ataques de *phishing*, es decir, instalando programas disfrazados en adjuntos a correos o mensajes que parecen inocentes, pero que en realidad contienen un *software* malicioso. Estos programas pueden encender el micrófono o la cámara del dispositivo, transmitir conversaciones, ver lo que se escribe, copiar archivos o mensajes, monitorear movimientos o robar contraseñas. La mejor estrategia para prevenirlo es **desconfiar siempre al recibir un correo electrónico extraño**, examinar el remitente del archivo **y no abrir los archivos adjuntos a esos correos** extraños. No hacer clic en enlaces poco confiables ni descargar archivos con esas características.

Proteger los teléfonos móviles. Los teléfonos portátiles son ventanas abiertas a nuestra vida. En ellos se encuentra y se enlaza gran parte de nuestra información personal y de nuestras interacciones sociales. Además, suelen estar sincronizados con otros dispositivos. Por ello es importante tomar algunas medidas básicas para proteger este instrumento tan cercano a nuestra vida *online* y *offline*:

- Colocar una **contraseña de bloqueo** en el teléfono para que no se pueda usar sin introducir un código (preferentemente una combinación de palabras y números) en caso de robo o extravío.



¿Qué es cifrar o encriptar una información?

Significa ocultarla a simple vista para hacerla más segura y confidencial. Es un proceso para convertir datos digitales en códigos, que hacen la información ilegible excepto para la persona que posee la clave para descifrarlo. Se pueden cifrar dispositivos, archivos, datos, mensajes de texto o cualquier tipo de información que lo requiera.

¿Qué es el phishing?

Es una técnica mediante la cual se trata de conseguir información confidencial de forma fraudulenta (contraseñas, datos bancarios, etc.) a través de una comunicación electrónica engañosa (correo electrónico, mensaje de texto, etc.). Por lo general se suplanta la personalidad de una persona o empresa para que quien recibe la comunicación electrónica facilite datos privados. Estos mensajes también pueden infectar el dispositivo con un programa informático espía para vigilar o robar información.

³⁴ Google support. Eliminar o inhabilitar aplicaciones en Android. Disponible en: <https://support.google.com/googleplay/answer/2521768?hl=es>; Apple support. Eliminar apps en el iPhone, el iPad y el iPod touch. Disponible en: <https://support.apple.com/es-es/HT207618>

- Procurar **no guardar información sensible en el teléfono** y, cuando sea necesario, utilizar la función para encriptar o cifrar la información. En los siguientes enlaces se incluyen instructivos para cifrar los datos en [dispositivos Apple](#) y en [dispositivos Android](#)³⁵. También se puede bloquear el acceso a aplicaciones para proteger la información e interacciones en ellas con aplicaciones como [Smart App Lock](#)³⁶.
- Si se requiere borrar información sensible, es importante recordar que no basta con borrarla del celular, puesto que en muchos casos esa **información pudo haber subido de forma automática a la nube, por lo que también es necesario borrarla allí**. *Android* no sube la información a la nube de forma automática, pero los dispositivos *Apple* lo hacen, así que se tiene que desactivar esta opción manualmente. La guía para [desactivar la sincronización automática con iCloud](#) puede ser consultada en este el centro de ayuda de *Apple*³⁷.
- **Verificar qué aplicaciones están instaladas en el celular**. Si una no resulta conocida o parece sospechosa, buscar información en internet sobre sus características y, si no es necesaria, desinstalarla. También desinstalar las aplicaciones que no se usen, porque pueden ser una fuente de vulnerabilidad. Tener instalado solo lo necesario aumenta la protección digital.



¿Sabías que...?

La persona media hace clic y desliza en su teléfono más de 2.600 veces al día.

- Cada paso que damos en internet queda registrado, y con el tiempo el navegador que usamos en el teléfono o la computadora se convierte en un gran libro de nuestras vidas. Para reforzar la privacidad y proteger la identidad digital es **recomendable borrar el historial del navegador**.

- Nuestra ubicación revela mucho sobre nuestras actividades y nuestros hábitos, y las aplicaciones instaladas en el teléfono pueden registrar nuestros movimientos constantemente sin que nos demos cuenta y proporcionar información a agresores. Es recomendable **verificar y desactivar los permisos de localización** en el teléfono para que las aplicaciones no lo localicen innecesariamente.



¿Qué son los metadatos de fotos o imágenes?

Son parámetros informativos incorporados en todas las fotografías digitales que se almacenan en un dispositivo. Muestran, entre otras cosas, detalles sobre la geolocalización y el día y la hora en que se tomaron.

Antes de publicar o enviar tus fotos es importante considerar que esta información quedará incrustada en ellas. Si es necesario, elimina los metadatos para no comprometer información sensible.

³⁵ Microsoft. Cifrado del dispositivo Android. Disponible en: <https://docs.microsoft.com/es-es/mem/intune/user-help/encrypt-your-device-android>; [Apple Support](#). Acerca de los respaldos encriptados en el iPhone, iPad o iPod touch. Disponible en: <https://support.apple.com/es-mx/HT205220>

³⁶ Smart AppLock (App Protect). Disponible en: <https://play.google.com/store/apps/details?id=com.thinkyeah.smartlockfree&hl=en>

³⁷ Apple Support. Cambiar la configuración de iCloud. Disponible en: <https://support.apple.com/es-es/HT207689>

Seguridad de la cámara. Cubrir la **webcam** del teléfono móvil o la computadora cuando no se usa (con un *post-it* o una cubierta especial), con lo cual se evitará que alguien pueda grabar o tomar fotografías si tiene acceso remoto al dispositivo.



Para recordar: Protección frente al doxxing

Nuestra información está esparcida por toda la web. Datos como nuestro nombre completo, dirección, teléfono, correo electrónico, el nombre de familiares y amistades o nuestro número de seguridad social pueden encontrarse en diversos sitios de internet, y un acosador que quiera *doxxearnos* puede recopilarlos.

Se puede consultar con *data brokers* qué información nuestra está en internet y pedir que la borren. Algunos de estos *data brokers* son *White Pages*, *Instant Check Mate*, *Axiom* o *Spokeo*³⁸. Otros servicios como *DeleteMe* o *Privacy Duck* pueden monitorear sitios para asegurar que la información se mantenga eliminada.

También se puede hacer una búsqueda inversa de nuestra información en Google, colocando dirección, correo electrónico o teléfono, o una *búsqueda inversa de imágenes* con *Google Images* o en sitios como *Tineye* o *Bing*³⁹.

04 Seguridad en las redes sociales







Las redes sociales se han convertido en un medio indispensable para navegar y expresarnos en la nueva realidad *online-offline* y nos permiten mantenernos en contacto con familiares, amistades, el trabajo, intereses, aficiones, etc. Sin embargo, no debemos perder de vista que pueden ser un medio para cometer ciberataques o actos de ciberviolencia. Pueden ser una puerta a nuestra vida para desconocidos, por lo que es crucial asegurarnos de que estemos compartiendo información personal solo con quienes así lo decidamos.



Como primer paso, es importante preguntarnos: ¿qué información queremos mantener privada? La información y las fotos que publicamos en línea dejan una huella indeleble. Por eso es importante preguntarnos qué queremos que esté al alcance del público y evaluar los riesgos y beneficios de que esa información sea pública. Debemos tener presente que un acosador podría aprovecharse de datos tales como nuestra ubicación, ciudad o la fecha de nacimiento o de fotografías publicadas en perfiles públicos.

³⁸ *White Pages*. Disponible en: <https://www.whitepages.com/suppression-requests>; *Instant Checkmate*. Disponible en: <https://www.instantcheckmate.com/opt-out/>; *Axiom*. Disponible en: <https://isapps.axiom.com/optout/optout.aspx#section8>; *Spokeo*. Disponible en: <https://www.spokeo.com/optout/>; *Delete Me*. Disponible en: <https://joindeleteme.com/>; *Privacy Duck*. Disponible en: <https://www.privacyduck.com/>

³⁹ *Digital Inspiration. Reverse Image Search*. Disponible en: <https://www.labnol.org/reverse/>; *Google. Ayuda de Búsqueda de Google*. Disponible en: <https://support.google.com/websearch/answer/1325808?co=GENIE.Platform%3DAndroid&hl=es> *TinEye*. Disponible en: <https://tineye.com/> *Microsoft Bing*. Disponible en: <https://www.bing.com/?setlang=es>

-  Para evitar ser identificada fácilmente, puede considerarse el **uso de seudónimos** y de fotografías de perfil que no muestren rasgos físicos.
-  **Conocer y configurar las opciones de privacidad y seguridad** de redes sociales. Es importante tomarse el tiempo para ver qué información nuestra está expuesta en las redes (por ejemplo, quién puede ver nuestro perfil o publicaciones, qué contenido nuestro pueden agregar o dónde nos pueden etiquetar), lo cual se puede revisar y controlar con las opciones de configuración de privacidad. Se pueden consultar guías útiles para explorar las configuraciones de privacidad en la publicación [Alfabetización y Seguridad Digital](#), de la OEA (pág. 17)⁴⁰, el sitio *Dominemos la Tecnología*⁴¹ o directamente en *Facebook*, *Twitter*, *Instagram* y *Tik Tok*⁴².
-  **Desactivar la geolocalización** en las aplicaciones que no necesiten ubicación para funcionar, así como la etiqueta de localización en redes sociales como *Facebook* o *Instagram*. Esta es una medida de prevención importante porque siempre que se publica algo en redes sociales se graban los datos de geolocalización, lo cual puede usarse para encontrar nuestro domicilio o sitios que frecuentamos.
-  En caso de que familiares o amistades estén compartiendo fotos nuestras o actualizaciones en sus redes sociales con nuestra información y se considere que, por seguridad, es mejor mantener en privado esta información, se les puede pedir que desactiven la geolocalización o la etiqueta de ubicación en sus publicaciones.
-  Verificar **qué dispositivos están conectados a las redes sociales**. Si hay alguno desconocido, es recomendable desconectarlo, pues podría significar que clonaron el teléfono y que otra persona tiene acceso a las aplicaciones (e información) desde otro celular o computadora.
-  Pueden consultarse directamente los servicios de ayuda y soporte técnico de las distintas redes sociales (*Facebook*, *Twitter*, *Instagram* y *Tik Tok*) para plantear dudas o preguntas específicas sobre sus funciones o problemas que surjan durante las interacciones⁴³.


⁴⁰ Organización de Estados Americanos y Twitter (2021). *Alfabetización y Seguridad Digital: La importancia de mantenerse seguro e informado*. Disponible en: <https://www.oas.org/es/sms/cicte/docs/alfabetizacion-y-seguridad-digital.pdf>


⁴¹ Dominemos la Tecnología. *Privacidad en las redes sociales*. Disponible en: <https://www.takebackthetech.net/es/privacidad-en-las-redes-sociales>


⁴² Facebook. *¿Cómo puedo modificar la configuración de privacidad de Facebook?* Disponible en: <https://www.facebook.com/help/193677450678703>; Twitter. *Privacidad*. Disponible en: <https://help.twitter.com/es/safety-and-security#ads-and-data-privacy>; Instagram. *Configuración de la privacidad e información*. Disponible en: <https://www.facebook.com/help/instagram/196883487377501>; TikTok. *Ajustes de privacidad de la cuenta*. Disponible en: <https://support.tiktok.com/es/account-and-privacy/account-privacy-settings>.

⁴³ Facebook. *Servicio de ayuda*. Disponible en: <https://www.facebook.com/help>; Twitter. *Centro de ayuda*. Disponible en: <https://help.twitter.com/es>; Instagram. *Servicio de ayuda*. Disponible en: <https://help.instagram.com/>; TikTok. *Centro de ayuda*. Disponible en: <https://support.tiktok.com/en/>

05 Seguridad en los juegos en línea

 No usar información o fotos de perfil que revelen detalles personales.

 Para mayor seguridad, utilizar *gamertags*⁴⁴ únicas y nombres diferentes en cada plataforma. Con esto se evita que, si una cuenta de juego se ha comprometido, se puedan ubicar fácilmente las otras.

 Conocer y **cambiar las configuraciones de privacidad** de los sistemas de juego en línea para controlar la información que se hace pública (por ejemplo, quién puede ver el perfil o nombre real, quién puede ver la lista de amistades o enviar mensajes, quién puede ver cuando se está en línea o videos).



Tip

Se pueden encontrar más consejos sobre la forma de jugar en línea de manera segura en la guía del sitio *Feminist Frequency*⁴⁵.

06 Sexting con seguridad

Las tecnologías han abierto nuevos canales para la expresión de la intimidad y la sexualidad. No obstante, ante la lógica de violencia y discriminación de género que ha permeado los espacios digitales, es importante **conocer los riesgos conexos y asumir el control de las herramientas tecnológicas** para protegerse, sabiendo que el proceso nunca es completamente seguro. La plataforma [Acoso.online](https://acoso.online) propone preguntas muy útiles para guiar a las personas en tres etapas claves de este proceso (R.A.P.)⁴⁶:




- 1. Registrar:** ¿Quién lo registrará y dónde? ¿En qué dispositivo? ¿Este dispositivo guarda una copia automática en la nube? ¿Se mostrará el rostro o alguna característica física que pueda facilitar la identificación?
- 2. Almacenar:** ¿Quién almacenará el material y dónde (en la nube, en el teléfono, en la computadora)? ¿Quién tendrá acceso a ese registro? ¿Por cuánto tiempo? ¿Qué medidas de seguridad digital se adoptarán para que un tercero no tenga acceso al material?
- 3. Publicar:** ¿Se tiene pensado difundir o publicar el material? ¿Hay certeza de que el material desaparecerá si se quiere borrar posteriormente? ¿Qué opciones tiene la plataforma de internet para proteger la seguridad y la privacidad de las personas usuarias?


⁴⁴ Un *gamertag* es un identificador de personas que juegan y comparten contenido en la comunidad de la plataforma digital de *Microsoft Xbox Live*. Se crea a partir de un alias, un avatar o una imagen e información sobre las preferencias de la o el jugador.


⁴⁵ *Feminist Frequency. Speak Up & Stay Safe(r): A Guide to Protecting Yourself from Online Harassment*. Disponible en: <https://onlinesafety.feministfrequency.com/en/>


⁴⁶ *Acoso.online. Resiste y toma control sobre la tecnología*. Disponible en: <https://acoso.online/mx/4-resiste-y-toma-control-sobre-la-tecnologia/>


Recomendaciones básicas:


 **¿Existe confianza?** Es crucial sentirse segura con la persona que recibirá la imagen o video, porque tendrá también la responsabilidad de proteger la privacidad de quienes participan en el intercambio.


 **El consentimiento es fundamental.** Llegar a un acuerdo sobre la forma de compartir fotos y los tipos de detalles que puede contener la foto.

 Buscar ángulos seguros y **procurar no mostrar rasgos físicos o lugares que revelen la identidad.**

 **Editar el contenido** de ser necesario (por ejemplo, con *emojis* que cubran rasgos que puedan revelar la identidad).

 **No olvidar los metadatos** de las imágenes, los cuales pueden proporcionar información que permite identificar a la persona que registró la foto. Además, procurar que el registro se haga siempre en un dispositivo propio, conocer y controlar su configuración y desactivar las etiquetas de ubicación automática.

 **Elegir bien el medio.** No compartir imágenes íntimas en *Wi-Fi* públicas. Además, cuando se usan aplicaciones de mensajería como *WhatsApp*, se corre el riesgo de que las imágenes o los videos puedan ser retransmitidos o difundidos, ya que, a pesar de que cifran los mensajes de extremo a extremo, el contenido queda guardado en los dispositivos. *Snapchat* permite hacer publicaciones efímeras que se borran después de un tiempo, pero el receptor puede hacer una captura de pantalla de la imagen recibida y guardarla en su dispositivo.

 **Borrar periódicamente las fotos almacenadas** en la memoria del dispositivo (y de la nube) para que nadie pueda robarlas.



Tip

Es crucial **no consentir en nada** hasta estar segura de qué pasará con la imagen o video. Nunca permitir que alguien grabe o tome fotografías sin tener claridad absoluta de ese proceso.



Tip

Para una mayor protección, se pueden utilizar aplicaciones⁴⁷ como *Signal*, que ofrece la opción de borrar mensajes en conversaciones, *Confide*, que tiene mensajes cifrados que se autodestruyen (en los dispositivos y en los servidores) una vez que han sido vistos, además de bloquear intentos de captura de pantalla, o *Wickr* que tiene la opción de detectar y enviar una notificación si la persona que recibió la imagen tomó una captura de pantalla.



Tip

En este el sitio de *Ciberpatrulla*⁴⁸ se puede consultar un [tutorial](#) para revisar y borrar los metadatos de imágenes en *Windows*, *Mac*, *iOS* y *Android*.

También se pueden usar [programas para eliminar los metadatos](#), como *Nectar*, *MedialInfo*, *Metanull* y *Get-Metadata*.

⁴⁷ *Signal*. Disponible en: <https://signal.org/es/>; *Confide*. Disponible en: <https://getconfide.com/>; *Wickr*. Disponible en: <https://wickr.com/>

⁴⁸ *Ciberpatrulla*. ¿Qué son los Metadatos de fotos e imágenes? Cómo puedes utilizar los datos EXIF en tus investigaciones (y de paso aprender a borrarlos para no dejar huella). Disponible en: <https://ciberpatrulla.com/metadatos-de-fotos/> Tekcrispy. 4 programas para extraer los metadatos de archivos multimedia. Disponible en: <https://www.tekcrispy.com/2018/04/22/extraer-metadatos-audiovosuales/>



Consejos para la seguridad digital de mujeres víctimas de violencia doméstica o de pareja

Es cada vez más frecuente en relaciones abusivas que el agresor trate de ejercer control y extender la violencia por medio de nuevas tecnologías, especialmente los teléfonos celulares, los cuales son el medio por excelencia para mantener la conectividad en nuestro cotidiano *online-offline*. Cuando esto sucede, podríamos pensar que nuestra pareja o expareja es un *hacker* o gran conocedor de la tecnología porque siempre logra saber dónde estamos, qué hacemos, los mensajes que enviamos, las cosas que buscamos en internet o con quién nos comunicamos. Sin embargo, en varios estudios se ha constatado que **la mayoría de los agresores tienen conocimientos muy básicos de tecnología que simplemente saben utilizar a su favor.**



Por supuesto, no todas las experiencias, amenazas y riesgos que enfrentan las víctimas son las mismas. Sin embargo, es importante tener presente que **todas las mujeres puede aprender técnicas muy sencillas para cuidarse, reforzar su seguridad digital**, proteger sus comunicaciones e incluso recurrir a la tecnología para estar conectadas con contactos de confianza, pedir ayuda o documentar la violencia.

A continuación, presentamos algunos consejos que podrían adoptarse en caso de que la violencia doméstica de una pareja o expareja sentimental se haya extendido al teléfono móvil. Algunos de ellos retoman las recomendaciones publicadas por las organizaciones Derechos Digitales y MaríaLab en su [Guía de precauciones digitales para mujeres víctimas y sobrevivientes de violencia](#) durante la pandemia de COVID-19⁴⁹.




Sin embargo, antes de tomar cualquiera de estas medidas, es muy importante evaluar los propios riesgos y **hacer solo aquello que genere seguridad o comodidad**. No hay fórmulas únicas para enfrentar este tipo de situaciones, y la seguridad digital es un proceso personal que cada persona desarrolla a su ritmo y conforme a sus propias circunstancias.

Primero, para considerar bien las opciones y la seguridad, es importante preguntarse: ¿Fue el agresor quien proporcionó el teléfono móvil o tuvo acceso al mismo durante un tiempo? ¿Tiene acceso permanente al teléfono sin poder evitarlo?

Si la respuesta es afirmativa, es posible que el agresor tenga acceso al celular a través de un software espía (*spyware*), por lo que es recomendable desconectar el dispositivo de internet, revisar su configuración y, en la medida de lo posible, dejar de utilizarlo y buscar otro teléfono para comunicarse.



⁴⁹ Goldsman y Natansohn (2020). *Cuidados durante la pandemia: ¿Cómo denunciar la violencia doméstica?* Derechos Digitales y MaríaLab. Disponible en: <https://www.derechosdigitales.org/wp-content/uploads/covid-violencia-domestica.pdf>

-  Se puede **verificar si el teléfono tiene un programa espía** (por medio del cual se pueden ver fotos, chats, ubicación o llamadas) usando aplicaciones como [Root Verifier](#) para *Android*⁵⁰.
-  Además, **muchas veces los agresores utilizan aplicaciones que podrían parecer inofensivas**, pero que en realidad revelan la ubicación de la víctima, como las aplicaciones para encontrar el dispositivo en caso de pérdida o robo que muchos teléfonos tienen instaladas (por ejemplo, *Find my Phone*). Si se encuentra esta aplicación y no se reconoce la cuenta de acceso, es posible que la estén usando para rastrear el teléfono, por lo que es recomendable desactivarla. En estos enlaces se puede consultar cómo desactivar aplicaciones en [Android](#) y cómo desactivar [Find my iPhone](#)⁵¹.
-  También se puede [verificar si alguna de las aplicaciones del teléfono tiene un permiso de superusuario](#)⁵², ya que puede tratarse de un *spyware*⁵³.
-  Es importante recordar que mucha de nuestra información se almacena en la nube, por lo que es crucial **cambiar la contraseña de la cuenta de Google o iCloud en el teléfono**. Asimismo, se recomienda iniciar sesión en un dispositivo que se considere seguro y cambiar las contraseñas de todas las cuentas. En los sitios web de *Google* y *Apple* se puede consultar la forma de cambiar la contraseña de la cuenta en un dispositivo [Android](#) y del [ID de Apple](#)⁵⁴.
-  Si a pesar de haber hecho lo anterior aún existe la sospecha de que hay un *spyware*, se puede volver a la configuración original de fábrica, lo cual desactivará todos los programas instalados. Se debe tener presente que esto borrará también las **fotos**, información y contactos, por lo que es importante hacer una copia de ellos antes⁵⁵. En los siguientes enlaces se puede consultar una [guía para respaldar la información](#)⁵⁶ y cómo restaurar la configuración de fábrica de un [Android](#) y un [iPhone](#)⁵⁷.
-  Si se prefiere una revisión mucho más completa, se sugiere desconectar el dispositivo de internet, dejar de usarlo inmediatamente y llevarlo a una persona experta en seguridad digital, que podrá descubrir más detalles sobre el posible *spyware*.



Es importante tener una contraseña de bloqueo segura en el teléfono. Si eso no es viable dada la presión del agresor (por ejemplo, si ello pudiera tornarlo violento), puede instalarse una aplicación que simule un error en el teléfono en caso de que alguien trate de usar las aplicaciones sin contraseña.

⁵⁰ Google Play. *Root Verifier*. Disponible en: https://play.google.com/store/apps/details?id=com.abcdj.rootverifier&hl=en_US

⁵¹ Ayuda de Google Play. *Eliminar o inhabilitar aplicaciones en Android*. Disponible en: <https://support.google.com/googleplay/answer/2521768?hl=es>; Actualidad iPhone. *Como desactivar buscar mi iPhone*. Disponible en: <https://www.actualidadiphone.com/desactivar-buscar-mi-iphone/>

⁵² Los permisos de súperusuario, o acceso root en el sistema *Android*, le permiten a la persona usuaria tener privilegios elevados para sobrepasar las limitaciones que impone el fabricante y hacer cambios profundos dentro del sistema operativo del dispositivo, incluyendo la posibilidad de reemplazar aplicaciones del sistema o ejecutar *software* especializado.

⁵³ Betech. *Cómo quitar permisos a una app en Android y en iOS*. Disponible en: https://as.com/meristation/2020/02/12/betech/1581547469_996131.html

⁵⁴ Google Support. *Cambiar o recuperar tu contraseña*. Disponible en: <https://support.google.com/mail/answer/41078?co=GENIE.Platform%3Dandroid&hl=es>; Apple Support. *Cambiar la contraseña del ID de Apple*. Disponible en: <https://support.apple.com/es-es/HT201355>

⁵⁵ Mayores conectados. *Cómo pasar fotos del celular a la computadora*. Disponible en: <https://mayoresconectados.com.ar/descargar-fotos-del-celular-a-la-computadora>

⁵⁶ ESET-LA. *Guía de Backup*. Disponible en: <https://www.welivesecurity.com/wp-content/uploads/2017/03/guia-backup.pdf>

⁵⁷ Google Support. *Restablecer los datos de fábrica de un dispositivo Android*. Disponible en: <https://support.google.com/android/answer/6088915?hl=es>; Apple Support. *Restaurar el iPhone, iPad o iPod a los ajustes de fábrica*. Disponible en: <https://support.apple.com/es-es/HT201252>



Puede suceder también que el agresor revise frecuentemente el teléfono celular sin poder evitarlo. En estos casos, es posible hacer lo siguiente:



Si se está pensando en solicitar ayuda, **recordar no dejar rastros en el teléfono** que puedan ser identificados por el agresor: eliminar fotos, videos, mensajes o el historial de visitas o búsquedas en internet que puedan darle pistas de que se está pensando en pedir ayuda.



Es importante recordar que toda la información que se busca en internet o los sitios web que se visitan quedan registrados en el celular o la computadora. Si se ha buscado información sensible que se quiera mantener oculta (por ejemplo, números de emergencia o servicios de apoyo para casos de violencia), se puede **borrar el historial de búsquedas de navegación**⁵⁸ y usar el modo incógnito o privado para no dejar rastro.

Puede acordarse un “**código secreto**” con **personas de confianza** para pedir ayuda por medio de *emojis* específicos. Por ejemplo, uvas (emoji) 🍇 = me está atacando. Memorizar estos códigos y eliminar el mensaje después de enviarlo.

Procurar **borrar el historial de mensajes de chats** y utilizar los códigos de comunicación acordados con la red de apoyo.

No guardar en el teléfono nombres que puedan darle indicios al agresor de que se está pidiendo ayuda. Por ejemplo, en vez de escribir “refugio”, escribir “Señora Martínez”.

Escribir en un papel los números de teléfono de contactos de confianza y guárdalo en un lugar seguro. Esto servirá en caso de que el agresor impida usar el celular.



⁵⁸ Google Support. Eliminar el historial de navegación de Chrome. Disponible en: <https://support.google.com/chrome/answer/95589?co=GENIE.Platform%3DDesktop&hl=es>



¿Qué puedo hacer si estoy siendo víctima de actos de violencia digital?

Cada mujer y cada niña tienen necesidades y experiencias únicas y viven de forma distinta la violencia en línea, por lo que es importante no generalizar cuando se abordan estrategias para prevenir la violencia. Tomando en cuenta esta diversidad, a continuación, se presentan algunos consejos prácticos que podrían ser de utilidad a la hora de enfrentar un contexto de violencia digital.

Hacer una pausa y recordar: NO es culpa de quien es víctima de violencia



Si se reciben ataques, acoso, amenazas o son publicadas imágenes o videos íntimos en internet, debe recordarse que nunca será culpa de la víctima, incluso si no se tomaron las precauciones digitales necesarias.

La violencia en línea que vive una mujer o niña **no es su culpa**, independientemente de que haya o no tomado precauciones antes de los hechos o de que haya compartido imágenes íntimas en el marco de una relación de confianza. **La responsabilidad recae siempre en el agresor y no en la víctima.**

En situaciones como estas, emprender una práctica personal de autocuidado o limpieza digital puede ser de gran ayuda para la sobreviviente de violencia. Es aconsejable hacer una pausa, dar un paseo o dejar descansar los ojos, conversar con una amiga o desintoxicarse de las redes sociales. La violencia en línea puede ser abrumadora, y darse un momento para cuidar de una misma puede ayudar a navegar mejor las redes y la situación.

Documentar

Si se es sobreviviente de algún tipo de violencia en línea, es recomendable **documentar, registrar y guardar de forma segura y ordenada toda prueba de violencia** que pueda ser pertinente (correos electrónicos, mensajes recibidos en redes sociales, mensajes SMS, mensajes de audio o llamadas telefónicas). Esto no solo puede ayudar a sentirse en control de la situación, sino que también será útil en caso de que se decida acudir a las autoridades o reportar ante las plataformas de internet. Se puede hacer manualmente, guardando los hipervínculos de los sitios web donde aparece el material, o haciendo capturas de pantalla de la violencia recibida mediante las funciones de *Windows* o *Mac* o con aplicaciones como *Snapfiles* o *Evernote*⁵⁹.



Durante este proceso, una herramienta de apoyo de utilidad es el [cuadro de evidencias](#) elaborado por Acoso.online.

⁵⁹ Microsoft Support. Cómo tomar y anotar capturas de pantalla en Windows 10. Disponible en: <https://support.microsoft.com/es-es/windows/c%C3%B3mo-tomar-y-anotar-capturas-de-pantalla-en-windows-10-ca08e124-cc30-2579-3e55-6db63e36fbb9>; Apple Support. Realizar una captura de pantalla en el Mac. Disponible en: <https://support.apple.com/es-es/HT201361>; Snapfiles. SnapDraw Free. Disponible en: <https://www.snapfiles.com/get/alphascreenshot.html>; Evernote. Disponible en: <https://evernote.com/intl/es/features/webclipper>.

Es importante guardar las pruebas de forma ordenada y cronológica en carpetas. También hay que tomar precauciones para guardar las pruebas de forma segura, ya sea en formato digital con contraseña o incluso en forma impresa.



Si se es víctima de distribución no consentida de contenido íntimo o sexual, es importante conservar y respaldar las pruebas antes de borrar el material: realizar capturas de pantallas de los sitios web donde aparezca el material, de los mensajes de texto o de los correos electrónicos que se reciban (con la hora y fecha y los miembros del grupo) y, en su caso, descargar el video y guárdalo.

Si se es víctima de violencia doméstica perpetrada por una pareja o expareja sentimental, puede ser muy importante documentar los hechos de violencia a la hora de denunciar a las autoridades. Para ello se puede recurrir al celular y a diversas aplicaciones para guardar grabaciones y videos, tomar fotos, hacer capturas de pantallas de violencia en redes sociales o registrar mensajes de texto hostiles. Sin embargo, antes de hacerlo, **es crucial determinar si ello podría significar en mayor riesgo** (por ejemplo, si la pareja o expareja tiene acceso al dispositivo). Si se percibe riesgo, podría ser más conveniente no hacer el registro o considerar la posibilidad de enviar las pruebas a una persona de confianza o a un familiar para que las guarde (y, después de enviarlas, borrarlas del teléfono y de la nube). Es importante también anotar la hora, el día y el lugar del incidente. Se puede encontrar más información sobre la documentación en la [Guía de Derechos Digitales y MariaLab](#).

Bloquear o denunciar la violencia en redes sociales

Bloquear agresores y ciberacosadores en redes sociales puede ser de ayuda para protegerse de conductas dañinas, indeseadas e inapropiadas, especialmente si el grado de ciberviolencia está causando mucha ansiedad o sentimientos negativos. No obstante, la **decisión de bloquear o no a alguien es exclusivamente personal**, y dependerá de cada contexto.

- **Bloquear y silenciar en *Twitter*.** Como señaló Amnistía Internacional, *Twitter* es la red social con el mayor volumen de ciberacoso y ciberhostigamiento contra mujeres. En este contexto es importante saber usar esta red social de manera segura; por ejemplo, saber cómo [bloquear y silenciar posibles acosadores](#) o [compartir listas de bloqueo](#)⁶⁰. La publicación [Alfabetismo y Seguridad Digital](#), de la OEA, contiene también recomendaciones sobre herramientas para navegar por *Twitter* de forma segura y denunciar tuits, mensajes, cuentas y violaciones a las reglas.
- Se puede consultar también la forma de bloquear agresores en los sitios de [Facebook](#), [Instagram](#) y [Tik Tok](#).

Las redes sociales también tienen **herramientas específicas para denunciar información o comportamientos** dañinos, abusivos o perjudiciales o amenazas violentas, y tienen la obligación de analizar la denuncia y tomar las medidas necesarias, desde una advertencia al usuario responsable hasta la suspensión permanente de su cuenta. Si bien queda mucho por hacer para mejorar la respuesta de las plataformas de internet ante casos de violencia, lo cierto es que denunciar incidentes permite documentar patrones de agresión y contribuye a visibilizar la violencia digital que afecta a millones de mujeres en línea.

⁶⁰ *Twitter Centro de Ayuda. Información sobre la situación de bloqueo.* Disponible en: <https://help.twitter.com/es/using-twitter/someone-blocked-me-on-twitter>; *Twitter blog. Compartir listas bloqueadas convierte a Twitter en un espacio más seguro.* Disponible en: https://blog.twitter.com/es_es/a/es/2015/compartir-listas-bloqueadas-convierte-a-twitter-en-un-espacio-m-s-seguro.html#:~:text=Para%20exportar%20o%20importar%20las,cuentas%20que%20se%20quieren%20exportar.

Si se decide denunciar la violencia, por lo general se tendrá que **describir el incidente o el tipo de amenaza o enviar una captura de pantalla** con el contenido violento o un enlace. En plataformas como *Twitter* o *Facebook* también se puede denunciar un contenido directamente haciendo clic en la parte superior derecha del artículo en el momento en que aparece. Se pueden consultar las guías para hacer denuncias en [Tik Tok](#), [Instagram](#), [Twitter](#), [Facebook](#) y [YouTube](#)⁶¹.

Buscar apoyo

Si se es víctima de violencia en línea o se sospecha que se podría ser víctima, es recomendable pedir ayuda a familiares, amistades o personas de confianza. En caso de encontrarse en una situación de gran estrés, se puede incluso pedir a un amigo o una amiga que monitoree las actualizaciones en redes sociales o las publicaciones abusivas, para no tener que hacerlo directamente.

Se puede encontrar también en internet una gran **red de apoyo y prácticas colectivas de seguridad digital** que las mujeres han creado para apoyarse mutuamente en casos de violencia facilitada por la tecnología. Varias organizaciones cuentan con números de emergencia a los que se puede llamar en caso de ser víctima de la distribución no consensuada de imágenes íntimas, y pueden ayudar a hacer denuncias ante plataformas de internet, a rastrear imágenes o videos que estén circulando en línea y a pedir que sean retirados (se encontrará una lista de algunas de estas organizaciones más adelante).

Es importante también procurar acercarse a servicios de salud mental. La violencia digital puede ser abrumadora y tener graves consecuencias psicológicas, desde sentimientos de angustia y depresión hasta tendencias suicidas, por lo que no hay que subestimar el apoyo emocional y psicológico durante este proceso.

Algunas organizaciones que pueden brindar asesoría:

[Acoso.online](#)

[SocialTIC](#)

[Fundación Activismo Feminista Digital](#) (Argentina)

[MariaLab](#) (Brasil)

[SOS Digital](#) (Bolivia)

[Fundación Karisma](#) (Colombia)

[Datos Protegidos](#) (Chile)

[Ciberfeministas](#) (Guatemala)

[Frente Nacional para la Sororidad y Defensoras](#)

[Digitales](#) (México)

[TEDIC](#) (Paraguay)

[Hiperderecho](#) (Perú)

La provisión de estos recursos no representa un respaldo por parte de la OEA o de sus Estados Miembros a su contenido o a las organizaciones nombradas. Los recursos se presentan a modo de ejemplo de aquellas organizaciones, guías, herramientas, etcétera, que están disponibles en la región para que las personas lectoras puedan ampliar la información relacionada con la temática que aborda esta publicación.

⁶¹ Facebook Servicio de Ayuda. ¿Qué es el bloqueo de Facebook y cómo bloqueo a alguien? Disponible en: <https://www.facebook.com/help/168009843260943>; Instagram. Servicio de ayuda. Bloquear personas. Disponible en: <https://help.instagram.com/426700567389543>; TikTok. Centro de ayuda. <https://support.tiktok.com/en>; Internet Matters. Configuración de Privacidad de TikTok. Disponible en: <https://www.internetmatters.org/es/parental-controls/social-media/tiktok-privacy-and-safety-settings/#:~:text=A%20bloquear%20o%20informar%20a,opciones%2C%20seleccione%20bloquear%20o%20informar.>

¿Se debe responder al agresor?

No existe una respuesta correcta o una fórmula única que se aplique a las interacciones con acosadores y perpetradores de violencia en línea, y mantener o no el contacto dependerá por completo de las prioridades de cada persona y de lo que la haga sentir más cómoda y segura.

Por ejemplo, en casos de violencia doméstica facilitada por las nuevas tecnologías, quizá se considere que la falta de respuesta pueda llevar a una intensificación de la violencia física por parte de la pareja o expareja sentimental, en cuyo caso se podrían mantener las interacciones en línea o, por el contrario, se podría sentir la suficiente seguridad para bloquear toda comunicación digital con él. Como se dijo anteriormente, todas las experiencias son distintas y, en la medida de lo posible, es mejor ponderar las opciones disponibles en el contexto personal.

En otros casos de violencia en línea, como en incidentes de ciberacoso, puede determinarse cuáles son las prioridades. Si, por ejemplo, es prioritario protegerse en el plano psicológico y emocional, quizá lo mejor sea no interactuar con el agresor o los agresores para evitar que se intensifiquen los ataques. Por otro lado, si resulta importante exponer el acoso o encarar a los agresores

y se puede aceptar el riesgo de recibir más ataques o ciberacoso, una opción viable es escribir directamente a los agresores, retuitear sus comentarios o reenviarlos a amistades, activistas, organizaciones o periodistas para hacerlos públicos y virales. En la [guía de PEN América](#) y en el sitio de [Ciberseguras](#) se pueden encontrar algunos consejos para responder de forma segura a los acosadores⁶².

Otra técnica es “contestar a conciencia” a los ataques, usando una comunicación activa y no violenta para dar visibilidad al sexismo y la violencia de género de los agresores (por ejemplo, incorporando la ironía o el humor en las respuestas).

En suma, no hay una respuesta única para esta pregunta; dependerá en gran medida de lo que cada persona considere que es mejor para su integridad física y emocional.

Denuncia la agresión a las autoridades

Las mujeres y las niñas tienen derecho a vivir una vida libre de violencia dentro y fuera de internet, y a recibir justicia cuando se vulnera este derecho. Denunciar ante las autoridades puede permitir que los actos de violencia digital queden registrados y debidamente documentados, y agilizar el retiro de contenido dañino por parte de las plataformas de internet, sobre todo en casos de ciberacoso, *doxxing* o distribución no consensuada de imágenes íntimas.

Números de emergencia para solicitar ayuda:

Argentina (144) / 1127716463 (WhatsApp)	El Salvador (2510-4300)
Belice (0800-A-WAY-OUT / 672-9628 (WhatsApp))	Guatemala (1572)
Brasil (180)	México (911)
Bolivia (800 14 0348)	Nicaragua (118)
Chile (1455)	Panamá (5006172)
Colombia (155)	Paraguay (137),
Costa Rica (911)	Perú (100)
Ecuador (09 992 8032)	Uruguay (0800 4141 o *4141 desde celular)



⁶² Pen America. *You're not Powerless in the Face of Online Harassment*. <https://onlineharassmentfieldmanual.pen.org/fight-back-write-back/>; Ciberseguras. *Machitrol y autodefesa feminista*. Disponible: <https://ciberseguras.org/machitrol-y-autodefesa-feminista/>

Además, en casos de denuncias de violencia íntima o doméstica, dado el uso recurrente de la tecnología para extender los alcances del abuso y el control, podría resultar importante notificar a las autoridades todos los eventos de violencia digital ocurridos durante la relación o con posterioridad, a fin de que puedan considerarlos en su análisis del caso y, de ser necesario, emitir órdenes de protección.

Por su parte, a partir de lo previsto en la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Convención de Belém do Pará), los Estados tienen la obligación de prevenir, investigar, sancionar y reparar la violencia de género en línea cometida en contra de mujeres y las niñas con la debida diligencia.

Si bien resta mucho por hacer para mejorar la atención y el seguimiento de la violencia en línea por parte de las autoridades, lo cierto es que se han registrado avances en la región, con recientes esfuerzos de capacitación del funcionariado público e incluso con la creación en muchos países de leyes y unidades especiales de ciberseguridad.

Asimismo, es importante tener presente que, aun ante conductas que pudieran resultarnos “nuevas”, los marcos jurídicos vigentes (incluso aquellos en los que no se han creado normas o no se han tipificado estos delitos) permiten encuadrar diversos actos de violencia en línea contra las mujeres en leyes contra la ciberdelincuencia, leyes sobre la violencia contra la mujer, leyes penales y leyes sobre privacidad y protección de datos, así como investigarlos, enjuiciarlos y sancionarlos. Esto quizá requiera un conocimiento un poco más avanzado de conceptos y técnicas jurídicas, pero no significa que las sobrevivientes de violencia digital no puedan hacerlo si reciben la orientación debida. Las organizaciones indicadas más adelante han realizado un trabajo al respecto que podría consultarse en caso de decidir acudir a las autoridades.



Crear comunidad

Platicar, compartir y socializar la experiencia puede ser de gran utilidad. Al visibilizar esta forma de violencia podemos contribuir a que se hable sobre el tema y a la implementación de herramientas de apoyo para las víctimas y sobrevivientes.

Enfrentarse a violencia en línea puede ser también una oportunidad para aprender más sobre tecnología y medidas de seguridad digital. Aunque parecieran cosas muy distantes la una de la otra, la ciberseguridad, la igualdad de género y la prevención de la violencia son componentes íntimamente interrelacionados en la era digital, y al aprender a proteger nuestra identidad y compartir esos aprendizajes con otras mujeres y niñas, estamos contribuyendo a que la internet sea un espacio más incluyente para todas.



Para explorar más

La provisión de los siguientes recursos no representa un respaldo por parte de la OEA o de sus Estados Miembros a su contenido o a las organizaciones nombradas. Los recursos se presentan a modo de ejemplo de aquellas organizaciones, guías, herramientas, etcétera, que están disponibles en la región para que las personas lectoras puedan ampliar la información relacionada con la temática que aborda esta publicación.

Organizaciones, sitios de internet y líneas de apoyo:

[Acoso.online](#) (sitio que brinda herramientas e información útil en casos de publicación no consentida de imágenes y videos íntimos)
[Asociación para el Progreso de las Comunicaciones](#) (APC)
[Ciberfeministas Guatemala](#)
[Ciber Civil Rights Initiative](#)
[Ciberseguras](#)
[Cl4ndestina](#) (Brasil)
[Coding Rights](#) (Brasil)
[Crash Override Network](#)
[Datos Protegidos](#) (Chile)
[Datysoc](#) (Uruguay)
[Derechos Digitales](#) (América Latina)
[Dominemos la Tecnología](#)
[Feminist Frequency](#)
[Frente Nacional para la Sororidad y Defensoras Digitales](#)
[Fundación Datos Protegidos](#)
[Fundación Activismo Feminista Digital](#)
[Fundación InternetBolivia.org](#) (Bolivia)
[Fundación Karisma](#) (Colombia)
[GenderIT.Org](#)
[HeartMob](#)
[Hiperderecho](#) (Perú)
[Internet es Nuestra](#)
[InternetLab](#) (Brasil)
[La <clika> libres en línea](#)
[Luchadoras](#) (México)
[MariaLab](#) (Brasil)
[Nodo Común](#)
[ONG Amaranta](#) (Chile)
[R3D](#) (México)
[Safernet](#) (Brasil)
[SocialTIC](#)
[SOS Digital](#) (Bolivia)
[TEDIC](#) (Paraguay)
[The Atlas of Online Harassment](#)
[Without My Consent](#)

Guías:

[A First Look at Digital Security](#). *Access Now*.

[Alfabetización y Seguridad Digital: La Importancia de Mantenerse Seguro e Informado](#) (2021). Organización de los Estados Americanos y Twitter.

[Alfabetismo y Seguridad Digital. Mejores Prácticas en el uso de Twitter](#). Organización de los Estados Americanos, 2019.

[Alza la voz y ten cuidado: Guía para protegerte del acoso online](#). *Feminist Frequency*.

[Ciberseguridad de las mujeres durante la pandemia de COVID-19: Experiencias, riesgos y estrategias de autocuidado en la nueva normalidad digital](#). Organización de los Estados Americanos, 2021.

[Cuidados durante la pandemia: ¿Cómo denunciar la violencia doméstica?](#) Derechos Digitales y MariaLab.

[Cuidar nuestro@ cuerpo@ digital. Reflexiones de un equipo virtual](#). Fondo de Acción Urgente.

[Data Detox x Youth](#). *Tactical Tech*.

[Guía de Seguridad Digital para Feministas Autogestivas](#). *Hackblossom*.

[Guía breve para la cobertura periodística de la violencia de género online \(2020\)](#). *Acoso.online*.

[Guía práctica para tratar casos de pornografía no consentida en recintos educacionales \(2018\)](#). *Acoso.online*.

[Netizens Online Security Guide](#).

[Online Harassment Field Manual](#). (2019) PEN America.

[Security in a Box \(2020\)](#). *Tactical Tech, Front Line Defenders*.

[Surveillance Self-Defense](#). *Electronic Frontier Foundation*.

Reportes:

[Cyber Violence against Women and Girls. A World-Wide Wake-up Call. United Nations Broadband Commission for Digital Development \(UNBC\). Working Group on Broadband and Gender \(2015\).](#)

[\(In\)Seguras Online. Experiencias de niñas, adolescentes y jóvenes en torno al acoso online \(2020\).](#) Plan Internacional.

[Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos \(2018\).](#) Relatora Especial de las Naciones Unidas sobre la Violencia contra la Mujer, sus Causas y Consecuencias.

[La ciberviolencia contra mujeres y niñas \(2017\).](#) Instituto Europeo de la Igualdad de Género.

[Online and ICT facilitated violence against women and girls during COVID-19 \(2020\).](#) ONU Mujeres.

[Reporte de la Situación de América Latina sobre la Violencia de Género Ejercida por Medios Electrónicos \(2017\).](#) Paz Peña Ochoa (ed).

[Ser periodista en Twitter. Violencia de Género digital en América Latina \(2020\).](#) Sentiido-Colombia, Comunicación para la Igualdad y el Programa Internacional para el Desarrollo de la Comunicación de la Organización de las Naciones Unidas para la Educación, Ciencia y la Cultura (UNESCO).

[Toxic Twitter - A Toxic Place for Women \(2018\).](#) Amnistía Internacional.

[Violencia en línea: La nueva línea de combate para las mujeres periodistas - #JournalistsToo \(2021\).](#) UNESCO y el Centro Internacional para Periodistas (ICFJ).

Eventos TED y Documentales:

[How Online Abuse of Women Has Spiraled Out of Control.](#) Ashley Judd. TEDTalk, 2016.

[Anita Sarkeesian at TEDxWomen 2012.](#)

[The problem with “Don’t Feed the Trolls”.](#) Steph Guthrie, TEDxToronto.

[Grooming, el acoso ¿virtual?.](#) Sebastián Bortnik, TEDxRíodelaPlata, 2016.

[Netizens.](#) Cynthia Lowen, 2019.

Glosario de Términos

Aplicación (también llamada *app*). Es un programa informático creado para llevar a cabo o facilitar un conjunto de tareas determinadas (profesionales, de ocio, educativas, etc.) que se ejecuta en teléfonos inteligentes, tabletas u otros dispositivos móviles. Existen aplicaciones gratuitas y de paga, y por lo general se encuentran disponibles en plataformas de distribución específicas o a través de las compañías propietarias de los sistemas operativos de los dispositivos electrónicos.

Blackout o apagón de internet. Una interrupción de la internet causada por un ataque a un sitio web, a un proveedor de servicio de internet (ISP) o al sistema de nombres de dominios de internet (DNS). También puede ser una interrupción debido a una configuración incorrecta de la infraestructura del servidor web.

Blog. Es un sitio web que permite la creación y publicación de artículos cortos sobre temas específicos o libres.

Brecha de género: Se refiere a cualquier disparidad entre la condición o posición de las mujeres y hombres en la sociedad (diferencias en el acceso a recursos, derechos y oportunidades).

Bot. Cuenta controlada por un algoritmo que usualmente se utiliza para coordinar una acción *online*.

Chat. Método de comunicación digital en tiempo real que se realiza entre varias personas usuarias cuyas computadoras están conectadas a una red.

Cybermobs o ciberturbas. Acción de grupos organizados en línea que publican contenido ofensivo o destructivo de forma masiva con la intención de avergonzar a alguien o lograr el retiro de su perfil de redes sociales.

Cifrado de información. Es un proceso para convertir datos digitales en códigos, los cuales hacen la información ilegible excepto para la persona que posee la clave para descifrarlos.

Cortafuegos (*Firewall*). Sistema físico o digital que tiene el objetivo de permitir o prohibir el acceso desde o hacia una red a fin de asegurar que todas las comunicaciones entre la red e internet se realicen conforme a las políticas de seguridad de una organización o corporación.

Creepshot. Se refiere a una foto tomada por un hombre a una mujer o niña en público sin su consentimiento. Las fotos suelen centrarse en los glúteos, las piernas o el escote de la víctima.

Cyberflashing. Envío de fotografías obscenas a una mujer sin su consentimiento con el objetivo de molestarla, intimidarla o incomodarla.

Deepfake o video ultra falso. Técnica de inteligencia artificial que permite editar videos falsos de personas que aparentemente son reales mediante el uso de algoritmos de aprendizaje y videos o imágenes ya existentes.

Denegación de servicio. Ciberataque que tiene por objeto saturar con peticiones de servicio a un servidor a fin de impedir que personas usuarias legítimas puedan utilizarlo. Un método más sofisticado es el ataque de Denegación de Servicio Distribuido (DDoS), mediante el cual las peticiones son enviadas de forma coordinada entre varios equipos.

Discurso de odio. Es el uso de un lenguaje que denigra, insulta, amenaza o ataca a una persona a causa de su identidad y/u otras características, como su orientación sexual o discapacidad.

Discriminación por razón de género. Toda distinción basada en el sexo que tenga por objeto o por resultado menoscabar o anular el reconocimiento, goce o ejercicio por la mujer, independientemente de su estado civil, sobre la base de la igualdad del hombre y la mujer, de los derechos humanos y las libertades fundamentales en las esferas política, económica, social, cultural y civil o en cualquier otra esfera [Fuente: Artículo 1 de la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer].

Downblousing. Registro sin consentimiento de fotografías tomadas por arriba de la blusa de una mujer.

Doxxing o doxing. El término proviene de la frase en inglés *dropping docs*, y consiste en en la extracción y la publicación en línea no autorizadas de información personal.

Emoji. Pequeña imagen o icono digital que se usa en las comunicaciones electrónicas para representar una emoción, un objeto, una idea, etc.

Estereotipos de género. Es una opinión o un prejuicio generalizado acerca de atributos o características que hombres y mujeres poseen o deberían poseer o de las funciones sociales que ambos desempeñan o deberían desempeñar [Fuente: OHCHR, *Estereotipos de género y su utilización*].

Gamertag. Identificador de personas que juegan y comparten contenido en la comunidad de la plataforma digital de Microsoft Xbox Live. Se crea a partir de un alias, un avatar o una imagen e información sobre las preferencias de la o el jugador.

Gaslighting. Es una forma de abuso psicológico realizado mediante la manipulación de la realidad de la víctima, con lo cual se busca que se cuestione su cordura, su memoria o su percepción.

Geolocalización. Es la capacidad para obtener la ubicación geográfica real de un objeto, como un radar, un teléfono móvil o un ordenador conectado a internet.

Género. Se refiere a los roles, comportamientos, actividades, y atributos que una sociedad determinada en una época determinada considera apropiados para hombres y mujeres. El género también hace referencia a las relaciones entre mujeres y las relaciones entre hombres. Estos atributos, oportunidades y relaciones son construidos socialmente y aprendidos a través del proceso de socialización [Fuente: ONU Mujeres, *OSAGI Gender Mainstreaming - Concepts and definitions*].

Grooming o ciberengaño pederasta. Son actos deliberados de un adulto para acercarse a una persona menor de edad con el objetivo de establecer una relación y un control emocional que le permita cometer abusos sexuales, entablar relaciones virtuales, obtener pornografía infantil o traficar a la o al menor de edad.

Hackeo. Uso de técnicas y procedimientos por un *hacker* para introducirse sin autorización en sistemas informáticos ajenos con el fin de manipularlos o de obtener información o por diversión. El *cracking* es una práctica relacionada con el *hackeo*, pero implica entrar en sistemas ajenos con fines delictivos para violar la intimidad de la persona afectada o la confidencialidad de la información o dañar la información o los soportes físicos.

Hacker. Persona que obtiene acceso no autorizado a un sistema informático.

Hashtag o etiqueta. Cadena de caracteres que inician con el símbolo #. Se utiliza en redes sociales para indicar la temática de una conversación o de un mensaje. Además, permite la creación automática de un hipervínculo que brinda acceso a todos los contenidos que incluyan el *hashtag* en cuestión.

HTTPS. Corresponde a las siglas en inglés de *Hypertext Transfer Protocol Secure* y consiste en un protocolo de red destinado a la transferencia segura de datos cifrados.

Internet de las Cosas (Internet of Things o IoT por sus siglas en inglés). Se refiere a la red de dispositivos y objetos cotidianos conectados a la internet que pueden compartir datos entre sí.

Igualdad de género. Se refiere a la igualdad de derechos, responsabilidades y oportunidades de las mujeres y los hombres y de las niñas y los niños [Fuente: ONU Mujeres, *OSAGI Gender Mainstreaming - Concepts and definitions*].

Keylogger o registrador de teclas. Es un *software* malicioso que se coloca entre el teclado y el sistema operativo para interceptar y registrar información de cada tecla pulsada en el dispositivo sin que la persona usuaria lo sepa.

Malware o programa malicioso. El término nace de la unión de las palabras en inglés *malicious software* y hace referencia a un tipo de *software* que tiene como objetivo infiltrarse y/o dañar un sistema de información sin el consentimiento de la persona usuaria.

Metadatos. Son datos sobre datos, es decir, es información que se usa para describir los datos contenidos en un archivo, documento, fotografía, una página web, etc.

Nube. Designa la red mundial de servidores diseñados para almacenar y administrar datos, ejecutar aplicaciones o entregar contenido o servicios.

Outing. Revelación en línea de la identidad o preferencia sexual de una persona.

Packs. Conjunto de imágenes de mujeres de naturaleza íntima o sexual obtenidas y/o distribuidas sin su consentimiento.

Perspectiva de género. Mecanismo de análisis que consiste en observar el impacto del género en las oportunidades, roles e interacciones sociales de las personas [Fuente: ONU Mujeres, *OSAGI Gender Mainstreaming - Concepts and definitions*].

Phishing o ataque de pesca de información. Es una estafa cometida a través de una comunicación electrónica engañosa y aparentemente oficial (correo electrónico, mensaje de texto o telefónicamente) mediante la cual el estafador o *phisher* suplanta la personalidad de una persona o empresa de confianza para que la persona receptora facilite información confidencial (contraseñas, datos bancarios, etc.). Se denomina *smishing* cuando la estafa se realiza vía SMS y *vishing* cuando se realiza recreando una voz automatizada.

Pornovenganza. Término utilizado de forma incorrecta para referirse a la distribución no consensuada de imágenes o videos íntimos.

Raiding o troleo colectivo. Ataque coordinado de una gran cantidad de cuentas en contra de una persona usuaria específica para producir un impacto significativo.

Red Privada Virtual. También referida como VPN por sus siglas en inglés (*Virtual Private Network*), es una tecnología de red de ordenadores que establece una extensión segura de una red de área local (LAN) sobre una red pública o no controlada, permitiendo que el ordenador en la red envíe y reciba datos sobre redes públicas como si fuera una red privada (consiguiendo que esta conexión sea segura gracias al cifrado de la información).

Red Social. Servicio de la sociedad de la información que ofrece a las persona usuarias una plataforma de comunicación a través de internet para que generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación, de modo que las personas usuarias pueden interactuar mediante mensajes, compartir información, imágenes o videos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todas las personas de un grupo [Fuente: Real Academia Española].

Roles de género. Normas sociales y de conducta que, dentro de una cultura específica, son ampliamente aceptadas como socialmente apropiadas para las personas de un sexo específico. Suelen determinar las responsabilidades y tareas tradicionalmente asignadas a hombres, mujeres, niños y niñas [Fuente: UNICEF, UNFPA, PNUD, ONU Mujeres. *Gender Equality, UN Coherence and you*].

Sexo (biológico). Se refiere a las características biológicas que definen a los seres humanos como mujeres y hombres.

Sexting o sexteo. Es una práctica que implica la generación e intercambio de material sexualmente explícito entre dos personas. Puede incluir la creación y envío de imágenes de forma consensuada o la creación consensuada de imágenes que se distribuyen sin consentimiento.

Sextorsión. Consiste en amenazar a una persona con difundir imágenes o videos íntimos con la finalidad de obtener más material sobre actos sexuales explícitos, mantener relaciones sexuales u obtener dinero.

Slutshaming. Es una forma de violencia que consiste en señalar públicamente a una mujer por su supuesta actividad sexual con el fin de avergonzarla, dañar su reputación y regular su sexualidad. Puede implicar el uso de fotografías y/o videos y lenguaje denigrante.

Sockpuppet o cuenta marioneta: Cuentas falsas no automatizadas que buscan pasar como usuarios reales para desinformar o difundir contenido sesgado sobre temas específicos.

Software. Conjunto de programas, instrucciones y reglas informáticas que permiten a los dispositivos electrónicos realizar determinadas tareas.

Spyware o software espía. Un tipo de programa maligno que infecta un dispositivo y graba secretamente y sin consentimiento datos de navegación, información personal, ubicación del dispositivo, registro de llamadas o mensajes, entre otros datos personales.

Trending topic. Hace referencia a la palabra o frases más repetidas en redes sociales en un momento determinado.

Troll o trol. Persona con identidad desconocida que publica en línea mensajes con la intención de molestar, provocar una respuesta emocional por parte de las personas usuarias o alterar las conversaciones en línea.

Troleo de género. Publicación de mensajes, imágenes o videos, así como la creación de *hashtags* (etiquetas), con el propósito de molestar a mujeres y niñas o incitar a la violencia contra ellas.

Upskirting. Registro sin consentimiento de fotografías tomadas por debajo de la falda de una mujer o niña.

URL. Por las siglas en inglés *Uniform Resource Locator*, se refiere a la dirección específica que se asigna a cada uno de los recursos disponibles en la red (páginas, sitios, documentos) con la finalidad de que puedan ser localizados o identificados.

Violencia contra la mujer. Cualquier acción o conducta basada en su género que cause muerte, daño o sufrimiento físico, sexual o psicológico a la mujer, tanto en el ámbito público como en el privado [Fuente: Artículo 1 de la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer].

Violencia de género en línea o ciberviolencia de género contra la mujer. Todo acto de violencia por razón de género contra la mujer cometido, con la asistencia, en parte o en su totalidad, del uso de las Tecnologías de la Información y la Comunicación, o agravado por este, como los teléfonos móviles y los teléfonos inteligentes, internet, plataformas de medios sociales o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada [Fuente: Relatora Especial sobre Violencia de la Organización de las Naciones Unidas].

Virus. Es un programa informático auto propagado que tiene por objeto alterar el funcionamiento normal de un dispositivo electrónico. Los virus se diferencian de otros tipos de programa maligno en que se replican automáticamente, es decir, son capaces de copiarse de un archivo o un ordenador a otro sin el consentimiento de la persona usuaria.

Wi-Fi. Es una red de dispositivos inalámbricos interconectados entre sí y generalmente también conectados a la internet a través de un punto de acceso inalámbrico.

Bibliografía

- Abdul Aziz, Z (2017). [Due Diligence and Accountability for Online Violence against Women](#). APC Issue Papers, Consultado el 9 de septiembre de 2020.
- Agencia de los Derechos Fundamentales de la Unión Europea (FRA) (2014). [Violencia de género contra las mujeres: una encuesta a escala de la UE](#). Consultado el 9 de septiembre de 2020.
- Amnesty International (2018). [Toxic Twitter-A Toxic Place for Women](#). Consultado el 9 de septiembre de 2020.
- (2017). [Amnistía revela alarmante impacto de los abusos contra las mujeres en Internet](#). Consultado el 9 de septiembre de 2020.
- Amnistía Internacional (2019). Corazones Verdes. Violencia online contra las mujeres durante el debate por la legalización del aborto en Argentina. Disponible en: https://amnistia.org.ar/corazonesverdes/files/2019/11/corazones_verdes_violencia_online.pdf
- Association of Progressive Communications (APC) (2017). *Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences*.
- (2015). [Briefing paper on VAW](#). APC Women's Rights Programme. Consultado el 9 de septiembre de 2020.
- Barrera, L. (coord) (2017). *La Violencia en Línea contra las Mujeres en México*. Informe para la Relatora Especial sobre la violencia contra la mujer. Luchadoras, México.
- Citron, D. (2014). *Hate Crimes in Cyberspace*. Massachusetts: Harvard University Press.
- Comité para la Eliminación de la Discriminación contra la Mujer de las Naciones Unidas (Comité CEDAW) (2017). CEDAW/C/GC/35. [Recomendación general núm. 35 sobre la violencia por razón de género contra la mujer, por la que se actualiza la recomendación general núm. 19](#). Consultado el 9 de septiembre de 2020.
- (1992). A/47/38. [Recomendación General No. 19. La Violencia contra la Mujer](#). Consultado el 9 de septiembre de 2020.
- Comisión Interamericana de Mujeres (CIM) (2020). [COVID-19 en la vida de las mujeres. Razones para reconocer los impactos diferenciados](#). Consultado el 9 de septiembre de 2020.
- Cuellar, L y Sandra Chaher (2020). [Ser periodista en Twitter. Violencia de género digital en América Latina](#). Fundación Sentiido, Comunicación para la Igualdad Ediciones, UNESCO.
- Deeptrace (2019). [The State of Deepfakes: Landscape, Threats and Impact](#). Consultado el 9 de septiembre de 2020.
- Derechos Digitales América Latina (2020). *COVID-10 and the increase of domestic violence against women in Latin America: A digital rights perspective*. Documento presentado por Derechos Digitales a la Relatora Especial de las Naciones Unidas sobre la violencia contra la mujer, sus causas y consecuencias.
- Dragiewicz, H., Woodlock et. al (2019) *Domestic violence and communication technology: Survivor experiences of intrusion, surveillance, and identity crime*. Brisbane: Queensland University of Technology.
- Edwards, A. (2010). "Feminist Theories on International Law and Human Rights". En *Violence against Women under International Human Rights Law*, 36-87. Cambridge: Cambridge University Press.
- Fanti K., A. G. Demetriou, y V. Hawa. (2012). "A longitudinal study of cyberbullying: Examining risk and protective factors". En *European Journal of Developmental Psychology*, Vol. 9(2), 168-181.
- Federal Bureau of Investigation. Internet Crime Complaint Center (FBI-ICC) (2018). [Internet Crime Report](#). Consultado el 9 de septiembre de 2020.
- Fondo de las Naciones Unidas para la Infancia (UNICEF) (2017). [Access to the Internet and Digital Literacy](#). Consultado el 9 de septiembre de 2020.
- Freed, D., J, Palmer, D. Minchala, et al. (2017). "Digital technologies and intimate partner violence: a qualitative analysis with multiple stakeholders". En *Proceedings ACM Human-Computer Interaction*, Vol. 1, 46:1- 46:22.

- Goldsman, F. y G. Natansohn (2020). *Cuidados durante la pandemia: ¿Cómo denunciar la violencia Doméstica?* Derechos Digitales y María Lab.
- Henry, N. y A. Powell (2018). "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research". En *Trauma, Violence, & Abuse*, Vol. 19 (2), 195-208.
- Henry, N. y A. Powell (2017). "Sexual Violence and Harassment in the Digital Era". En Antje Deckert y Rick Sarre (eds.). *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice*. Palgrave Macmillan.
- Henry, N. y A. Powell (2016). "Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law". En *Social & Legal Studies*, Vol. 25 (4), 397-418.
- Henry, N., A. Powell y F., Asher (2018). "[AI can now create fake porn, making revenge porn even more complicated](#)". En *The Conversation*.
- (2017). [Not just "revenge pornography": Australians' experiences of image-based abuse: A summary report](#). Gender Violence and Abuse Research Alliance (GeVARA). Centre for Global Research, Centre for Applied Social Research.
- Harris, B. (2018). "Spacelessness, spatiality and intimate partner violence: Technology-facilitated abuse, stalking and justice". En K. Fitz-Gibbon, S. Walklate, J. McCullough, y J. Maher (eds.), *Intimate partner violence, risk and security: Securing women's lives in a global world* (pp. 52-70). Londres: Routledge.
- Hinduja, S., y J. W. Patchin (2014). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying* (Second edition). Thousand Oaks, California: Corwin.
- Hinson L., J. Mueller, L. O'Brienn-Milne, N. Wandera (2018). *Technology-facilitated gender-based-violence: What is it, and how to we measure it?* Washington D.C., International Center for Research on Women.
- Interagency Working Group (2016). "[Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse](#)". En *ECPAT International and ECPAT Luxembourg*, Luxembourg. Consultado el 9 de septiembre de 2020.
- Internet Governance Forum (IGF) (2015). [2015: Best Practice Forum \(BPF\) on Online Abuse and Gender-Based Violence against Women](#). Consultado el 9 de septiembre de 2020.
- Instituto Europeo de la Igualdad de Género (EIGE) (2017). [La ciberviolencia contra mujeres y niñas](#). Consultado el 9 de septiembre de 2020.
- Jane, E. (2017). *Misogyny Online. A Short (and Brutish) History*. Londres: Sage Publications.
- Jane E. (2016). "Online Misogyny and Feminist Digilantism". En *Continuum. Journal of Media & Cultural Studies*, Vol. 30 (3), 284-297.
- Kelly, L. (1988) *Surviving Sexual Violence*. Cambridge: Polity.
- Knight, W. (2018). "[The Defense Department has produced the first tools for catching deepfakes](#)". En *MIT Technology Review*. Consultado el 9 de septiembre de 2020.
- Kwon, M., Y. S. Seo, S. S. Dickerson, E. Park, y J. A. Livingston (2019). "Cyber Victimization and Depressive Symptoms: A Mediation Model Involving Sleep Quality". En *Sleep*, 42(Supplement_1), A322-A322.
- Qing Li (2006). "Cyberbullying in schools: a research of gender differences". En *School Psychology International*, Vol. 27(2), 157-170.
- Mantilla. K. (2013). "Gendertrolling: misogyny adapts to new media". En *Feminist Studies*, Vol. 39(2), 563-570.
- Maras, M. (2016). *Cybercriminology*. Oxford University Press.
- Maras, M., y A. Alexandrou (2018). "Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos". En *International Journal of Evidence and Proof*, Vol. 23(3), 255-262.
- Mecanismo de Seguimiento de la Convención de Belém do Pará (MESECVI). Comisión Interamericana de Mujeres (2017). [Tercer Informe Hemisférico sobre la Implementación de la Convención de Belém do Pará](#). Consultado el 9 de septiembre de 2020.
- Salter M., T. Crofts y M. Lee (2013). "Beyond Criminalisation and Responsibilisation: Sexting, Gender and Young People". En *Current Issues in Criminal Justice*, Vol. 24 (3), 301-316.

Navarro, J. y J. L. Jasinski (2012). "Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences". En *Sociological Spectrum*, Vol. 32(1), 81-94.

Neiris, N., J. Ruiz y M. Valente (2018). [Enfrentando Disseminação Não Consentida de Imagens Íntimas: Uma análise comparada](#). InternetLab. Consultado el 9 de septiembre de 2020.

Oficina de Naciones Unidas para la Droga y el Delito (UNODC) (2015). [Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children](#). Consultado el 9 de septiembre de 2020.

--- (2019). University Module Series. Cybercrime. [Module 12. Interpersonal Crime](#).

Organización de las Naciones Unidas. Asamblea General (2018). [Intensificación de los esfuerzos para prevenir y eliminar todas las formas de violencia contra las mujeres y las niñas: el acoso sexual](#). A/C.3/73/L.21/Rev.1. Consultado el 9 de septiembre de 2020.

---. Consejo de Derechos Humanos (2018). [Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales](#). A/HRC/38/L.6. Consultado el 9 de septiembre de 2020.

---. Comisión de la Banda Ancha para el Desarrollo Sostenible (UNBC-UN) (2015). Working Group on Broadband and Gender. [Cyber Violence against Women and Girls. A World-Wide Wake-up Call](#). Consultado el 9 de septiembre de 2020.

Organización de Estados Americanos (OEA) (2019). [Media Literacy and Digital Security: Twitter Best Practices](#). Consultado el 9 de septiembre de 2020.

Peña Ochoa, P. (ed) (2017). *Reporte de la Situación de América Latina sobre la Violencia de Género Ejercida por Medios Electrónicos*. Presentación para la Relatora Especial sobre la violencia contra la mujer.

Pew Research Center (2014). [Online Harassment 2014](#). Consultado el 9 de septiembre de 2020.

--- (2017). [Online Harassment 2017](#). Consultado el 9 de septiembre de 2020.

Powell, A., N. Henry, y F. Asher (2018). "Image-based Sexual Abuse". En Walter DeKeseredy and Molly Dragiewicz (eds.) *Handbook of Critical Criminology*. Nueva York: Routledge.

Relatora Especial de las Naciones Unidas sobre la Violencia contra la Mujer, sus Causas y Consecuencias (REVM-ONU) (2018). A/HRC/38/47. *Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos*. Consultado el 9 de septiembre de 2020. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/Documents/A_HRC_38_47_EN.docx

Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (RELE) (2018). *Mujeres periodistas y libertad de expresión: Discriminación y violencia basada en el género contra las mujeres periodistas por el ejercicio de su profesión* (OEA/Ser.LV/II), párr. 48. Disponible en: <http://www.oas.org/es/cidh/expresion/docs/informes/MujeresPeriodistas.pdf>

Reyns, Bradford, Billy Henson y Bonnie S. Fisher (2011). "Being pursued online. Applying Cyberlifestyle-Routine activities theory to cyberstalking victimization". En *Criminal Justice and Behavior*, Vol. 38(11), 1149-1169.

Salter, M. y T. Crofts y M. Lee (2013). "Beyond Criminalisation and Responsibilisation: Sexting, Gender and Young People". En *Current Issues in Criminal Justice*, Sydney Law School Research Paper No. 13/38, Vol. 24(3), 301-316.

Segrave, M., y L. Vitis (2017), *Gender, Technology and Violence*. Oxon y Nueva York: Routledge.

Smith, Peter K. (2012). "Cyberbullying and cyber aggression". En S.R. Jimerson, A.B. Nickerson, M.J. Mayer, y M.J. Furlong. (eds). *Handbook of school violence and school safety: International research and practice* (pp. 93-103). Routledge.

Van Der Wilk, A. (2018). *Cyber violence and hate speech online against women*. Estudio encargado por el Departamento Temático de Derechos de los Ciudadanos y Asuntos Constitucionales del Parlamento Europeo. Bruselas: Parlamento Europeo.

Vela, E. y E. Smith. ["La violencia de género en México y las tecnologías de la información"](#). En *Internet en México: Derechos Humanos en el entorno digital*. Ed. Juan Carlos Lara. México: Derechos Digitales, 2016. Consultado el 9 de septiembre de 2020.

Walker, Shelley, Sanci, Lena y Temple-Smith Meredith (2013). "Sexting: Young women's and men's views on its nature and origins". En *Journal of Adolescent Health*, Vol. 52, 697-701.

Web Foundation (2018a). [Advancing Women's Rights Online: Gaps and Opportunities in Research and Advocacy](#). Consultado el 9 de septiembre de 2020.

Web Foundation (2018b). [Measuring the digital divide: Why we should be using a women-centered analysis](#). Consultado el 9 de septiembre de 2020.

Women's Aid (2014). *Virtual World, Real Fear. Women's Aid report into online abuse, harassment and stalking*.

Women's Media Center (2019). [Online Abuse 101](#). Consultado el 9 de septiembre de 2020,

Woodlock D (2017). "The abuse of technology in domestic violence and stalking". En *Violence Against Women*, Vol. 23(5), 584-602.

La violencia de género en línea contra las mujeres y niñas

Manual práctico de seguridad digital y estrategias de respuesta

ISBN 978-0-8270-7306-7

