COFEM



## Ficha de consejos 1:

# Protección digital

# Puntos principales

La violencia digital no es un problema privado. Se suele usar para silenciar, intimidar y excluir de la vida pública a las mujeres.

Una protección digital eficaz empieza por entender cuáles son sus riesgos. Pregúntese qué está protegiendo, de quién y qué consecuencias habría si se expusiera la información.

Contraseñas robustas, autentificación de dos pasos, comunicaciones seguras y configuraciones de privacidad siguen siendo algunas de las medidas más efectivas contra el daño digital.

La seguridad digital es una responsabilidad colectiva. Prácticas organizacionales compartidas, procedimientos de respuesta claros y redes de apoyo contribuyen a proteger a equipos y movimientos.

La protección digital y el bienestar van de la mano. Responder al daño *online* requiere apoyo técnico, legal, psicológico y emocional.

El objetivo no es retirarse de espacios digitales, sino participar en ellos de forma segura, con confianza y en nuestros propios términos.

# Las políticas de estar en línea

Lo extraordinario de estar en línea es la rapidez con la que se mueven las personas, las ideas y la información. Los espacios digitales nos permiten movernos. Nos movemos entre comunidades, lenguas, países y conversaciones. Movemos ideas, evidencia e historias. Nos encontramos, entablamos relaciones, desafiamos las narrativas dominantes y nos movilizamos colectivamente a través de las fronteras.

Pero el movimiento nunca tiene que ver solo con lo que ganamos. Los mismos espacios digitales que posibilitan la conexión, la visibilidad y la acción colectiva también puede exponernos a nuevas formas de vigilancia, acoso y daño. Hace tiempo ya que feministas de todo el mundo vienen diciendo que la violencia contra las mujeres no es un asunto privado, sino una violación sistémica de los derechos humanos, una posición que se refleja en marcos normativos internacionales como la Declaración de las Naciones Unidas sobre la Eliminación de la Violencia contra la Mujer, el protocolo de Maputo y la resolución general 35 de la CEDAW. El movimiento #MeToo se basó en este legado. Iniciado en 2006 por la activista Tarana Burke como una iniciativa liderada por sobrevivientes, logró visibilidad global cuando el hashtag se hizo viral en redes sociales en 2017. En cuestión de semanas, millones de personas de aproximadamente 85 países habían compartido sus historias online, lo que demuestra de qué manera los espacios digitales pueden conectar las experiencias individuales con la acción colectiva y el cambio social.[1]

En Argentina, el movimiento #NiUnaMenos surgió en 2015 tras el asesinato de Chiara Páez, de 14 años, un caso que provocó la indignación pública generalizada contra el femicidio. Un tuit de la periodista Marcela Ojeda que convocaba a las mujeres a alzar su voz contra los asesinatos por cuestiones de género rápidamente ganó tracción entre activistas, figuras de la cultura y los medios. Con el lema #NiUnaMenos, el mensaje se difundió con prontitud a través de Twitter y Facebook, lo que ayudó a movilizar a cientos de miles de personas en lo que se convirtió en una de las manifestaciones feministas más grandes de la historia de América Latina. Como el #MeToo, #NiUnaMenos demostró cómo los espacios digitales pueden transformar las experiencias individuales de violencia en acción colectiva y presión política en pos del cambio.

Estos ejemplos revelan algo importante: los espacios digitales no son nunca neutrales. Las mismas tecnologías que posibilitan la organización y la acción colectiva feministas están determinadas por el poder, la política e intereses contrapuestos. A medida que el mundo se vuelve más conectado, movernos en los espacios digitales también nos exponen a nuevas formas de daño. Las mismas tecnologías que permiten que las ideas feministas circulen también pueden posibilitar el acoso, la vigilancia, la desinformación y el abuso . La misma visibilidad que nos ayuda a construir movimientos puede convertirnos en blanco. Las mismas redes que nutren las conexiones también pueden convertirse en canales por los cuales viaja la violencia.

Para las feministas que trabajamos para poner fin a la violencia contra mujeres y niñas, la circulación de la información, las historias y los recursos es una de nuestras mayores fortalezas. Podemos documentar la injusticia, apoyar a sobrevivientes, aprender unas de otras y organizarnos colectivamente a través de las fronteras. Pero esta transmisión digital de conocimiento también nos exige que pensemos con cuidado sobre la protección, la privacidad y los riesgos. ¿Cómo, entonces, podemos usar el poder digital intencionalmente? ¿Cómo aprovechamos las posibilidades que crean los espacios digitales pero minimizando los riesgos que comportan? ¿Cómo seguimos siendo visibles sin convertirnos en vulnerables? ¿Cómo nos protegemos a nosotras mismas, a nuestras organizaciones y a las personas con las que trabajamos mientras seguimos participando plenamente en la vida pública?

Esta ficha de consejos explora algunas respuestas prácticas a estas preguntas. Empieza por entender la violencia digital como una cuestión política y pasa a evaluar el riesgo, implementar protecciones prácticas, fortalecer la seguridad colectiva y responder al daño cuando ocurre.

[1] Sweeney J 2020

[2] https://8am.media/eng/ni-una-menos/

[3] Amnesty International, May 2021 Azerbaijan: Stop the Vicious Campaign of Gendered Smears and Reprisals against Women Activists. London: Amnesty International. Available at: https://www.amnesty.org

En foco

### El caso de Narmin Shahmarzadeh[4]

El 8 de marzo de 2021, la activista azerbaiyana por los derechos de las mujeres Narmin Shahmarzadeh estuvo involucrada en la organización de la marcha por el Día Internacional de las Mujeres en Baku. La mañana siguiente se despertó solo para descubrir que su cuenta de Facebook había sido hackeada. Los atacantes usaron su cuenta para publicar conversaciones inventadas y contenido pornográfico. Lograron acceso a sus documentos de identidad, que usaron para bloquearla de su propia cuenta, y le robaron la tarjeta de crédito para pagar avisos que promovían el contenido abusivo. En Telegram, los perpetradores crearon un canal que atribuía falsamente imágenes pornográficas a Narmin. En un breve período, el canal había atraído a más de 1600 suscriptores y miles de visualizaciones.

El ataque fue digital, pero el propósito era político. Narmin se convirtió en un blanco porque era visible. Había organizado, había alzado su voz y había desafiado el poder. Los atacantes transformaron las mismas herramientas que le permitieron llevar adelante su activismo en armas para usar en su contra. Su experiencia ilustra una realidad cada vez más común para las defensoras de los derechos humanos de las mujeres y las activistas feministas. La violencia digital suele estar diseñada no solo para intimidar a los individuos, sino también para dañar reputaciones, socavar la credibilidad, interrumpir las iniciativas de organización y crear condiciones para el miedo. Las consecuencias pueden empezar en línea, pero rara vez se quedan allí.

# El costo de la visibilidad

El de Narmin no es un caso aislado. Ilustra un patrón más amplio en el que la violencia digital se usa para castigar la visibilidad, interrumpir el activismo y restringir la participación de las mujeres en la vida pública. Cada vez más, el abuso online no está confinado a los espacios digitales; se derrama al mundo físico y afecta la seguridad, el bienestar y el sustento de las mujeres, así como también su capacidad para involucrarse en la vida pública y política.

El impacto del daño digital en las mujeres que se desempeñan en la esfera pública es generalizado y viene en subida. Un estudio de ONU Mujeres de 2025 que involucraba a más de 640 mujeres de 119 países descubrió que el 70 % de las defensoras de los derechos humanos de las mujeres, las activistas, las periodistas y las comunicadoras habían experimentado violencia en línea en el curso de su trabajo. Y las consecuencias no se quedan *online*. El 41 % denunció haber sufrido daño *offline*, como ataque físico, acecho y acoso verbal, que ellas vinculan directamente con la violencia que empezó en los espacios digitales. Entre defensoras de los derechos humanos y activistas, esa cifra ascendía al 44 %. La trayectoria de la violencia *online* a la offline también se está acelerando. En el caso de periodistas y trabajadoras de medios, la proporción que conecta la violencia *online* con el daño en el mundo físico creció más del doble entre 2020 y 2025, del 20 % al 42 %. Casi un cuarto de todas las encuestadas habían experimentado violencia online asistida por IA; y el 28 % de las defensoras de los derechos humanos de las mujeres y las activistas denunciaron el uso de tecnologías de inteligencia artificial en el abuso del que fueron blanco. El informe es inequívoco sobre el propósito para el cual está diseñada esta violencia: es un instrumento estratégico empleado para suprimir la libertad de expresión de las mujeres, obstruir su participación democrática y retrotraer su derecho a la igualdad de género con efectos que son, en palabras quienes lo escribieron, cualquier cosa menos virtuales.[5]

Pero reconocer estos riesgos no debería llevarnos a retirarnos de los espacios digitales o aceptar la violencia como el precio de participar. Las mujeres, las niñas y las personas de género diverso tienen derecho a ser visibles, a expresarse con libertad, a construir comunidad, a organizarse, a crear y vivir la alegría *online* sin miedo a sufrir abuso. El objetivo no es hacernos más pequeñas o menos presentes en los espacios digitales, sino transformar esos espacios para que todas las personas puedan participar de forma segura, igualitaria y digna. Protegernos en línea por ende tiene que ver no solo con reducir el daño, sino también con defender la internet como un espacio de expresión, solidaridad, creatividad y posibilidades feministas.

[4] Ibid
[5] Posetti et al., UN Women, December 2025

# Evalúe su riesgo

Si bien la principal responsabilidad de crear entornos digitales más seguros es de Gobiernos, compañías tecnológicas y plataformas digitales, las protecciones y los mecanismos de rendición de cuentas actuales son desparejos. En este contexto, organizaciones y activistas feministas pueden dar pasos prácticos para contribuir a minimizar el riesgo. Estas medidas no pueden eliminar el daño y tampoco deberían quitarles la responsabilidad a quienes ejercen la violencia, pero pueden fortalecer nuestra capacidad para navegar los espacios digitales en nuestros propios términos.

*No todas las amenazas se aplican a todas las activistas, organizaciones o movimientos. Una investigadora feminista que trabaja con testimonios de sobrevivientes enfrenta riesgos diferentes a los de una organizadora de campañas en redes sociales. Una defensora de derechos humanos que documenta la violencia estatal tiene desafíos distintos a los de una proveedora de servicios que dirige un grupo de apoyo local. En lugar de preguntar ¿Qué es lo más seguro que se puede hacer?, un planteo más útil es: ¿Qué estoy tratando de proteger y de quién?*

Para algunas organizaciones, la respuesta puede ser información de las sobrevivientes, archivos de casos o base de datos de contactos. Para otras, la prioridad puede ser proteger la identidad del personal, asegurar las comunicaciones o salvaguardar las cuentas de redes sociales. Las activistas individuales pueden estar preocupadas por el doxeo, el acecho, el acoso en línea o la exposición de información personal que podría ponerlas a ellas o su familia en riesgo. No hay un enfoque único que es correcto para todas. Las evaluaciones del riesgo son más efectivas cuando reflejan el contexto, las prioridades y el nivel de visibilidad pública de cada persona, lo que permite tomar decisiones informadas sobre cuáles son las medidas de protección adecuadas. La experiencia de Narmin Shahmarzadeh ilustra con qué rapidez un ataque digital puede escalar cuando entran en riesgo la información personal, los documentos de identidad y las cuentas de redes sociales. Entender qué información, qué relaciones y qué cuentas son más importantes para proteger es por lo tanto un punto de partida útil para reducir la vulnerabilidad y minimizar el riesgo.

Una evaluación de riesgo simple puede empezar con cuatro preguntas:[6]

- ¿Qué información o activos estoy tratando de proteger?
- ¿Quién puede querer acceder?
- ¿Qué métodos podrían usar?
- ¿Cuáles serían las consecuencias si se expusiera esa información?

La mayoría de las organizaciones no tienen tiempo, dinero o conocimientos técnicos ilimitados para prepararse para todas las amenazas posibles. En cambio, el objetivo es tomar decisiones informadas sobre los riesgos que más importan en el propio contexto y priorizar los esfuerzos en función de eso. Una vez que entiende sus riesgos, se vuelve mucho más fácil identificar las medidas prácticas que marcarán la gran diferencia.

[6] Estas preguntas se basan en abordajes establecidos para el modelado de amenazas, adaptadas para la práctica de protección digital feminista. Ver por ejemplo, Slupska et al's *Participatory Threat Modelling*, 2021



# Asegurar sus cuentas y dispositivos

El punto de entrada más común para un daño digital grave es la usurpación de una cuenta: alguien logra acceso a su correo electrónico, red social u otra cuenta a través de una contraseña robada, adivinada o reutilizada. Una vez que una cuenta de email está en riesgo, todas las demás cuentas vinculadas se vuelven vulnerables. Para activistas feministas, investigadoras y defensoras de los derechos humanos, las consecuencias pueden extenderse mucho más allá del inconveniente personal, ya que se exponen fuentes, sobrevivientes, colegas y comunicaciones sensibles. La experiencia de Narmin Shahmarzadeh ilustra con qué rapidez puede escalar la situación cuando una cuenta entra en riesgo. Los atacantes lograron acceder a su red social, usaron su identidad para distribuir contenido inventado y la dejaron afuera de su propio perfil. Lo que empezó como una intrusión digital rápidamente se convirtió en un ataque reputacional y psicológico.

La buena noticia es que algunas de las medidas de protección más efectivas son también las más simples:

Usar una contraseña fuerte y exclusiva para cada cuenta y guardarla en un sistema gestor de contraseñas confiable como Bitwarden o 1Password. Los gestores de contraseña generan y recuerdan claves complejas para que nosotras no tengamos que hacerlo, lo que elimina la práctica común y riesgosa de reutilizar la misma contraseña en muchas plataformas.

Combine esto con la autentificación en dos pasos (2FA) en todas las cuentas que la permitan. Cuando sea posible, use una aplicación autentificadora en lugar de la verificación por SMS, que puede ser vulnerable a ataques de intercambio de SIM. Preste particular atención a su cuenta de correo electrónico. Es la llave maestra de su vida digital y debería tratarla como la mayor prioridad.

La seguridad de los dispositivos también es importante. Mantenga actualizados sus sistemas operativos, navegadores y aplicaciones, dado que las actualizaciones emparchan vulnerabilidades que los atacantes explotan de forma activa. Habilite la cifrado de todo el disco en las portátiles y use antivirus confiables cuando corresponda. Tenga cuidado con enlaces, adjuntos o solicitudes de inicio de sesión inesperados. El *phishing* sigue siendo una de las formas más efectivas de robar credenciales o de instalar un *malware*.

Las anteriores recomendaciones brindan un punto de partida práctico, pero la seguridad digital no es una lista de verificación de un solo uso. Es una práctica continua que evoluciona junto con los cambios en las tecnologías y las amenazas. Un número de organizaciones feministas han desarrollado guías accesibles a medida de las experiencias de mujeres, niñas y personas de género diverso. Algunas de ellas son Digital Security Resources for Young Women de FRIDA, Gitbook, Seguridad en internet: guía práctica para mujeres y niñas de ONU Mujeres y Youth Guide to End Online Gender-based Violence. Estos recursos ofrecen consejos más detallados para fortalecer el bienestar digital, responder al abuso *online* y crear prácticas digitales más seguras.



# Manejar su huella digital y su privacidad

Cada foto, etiqueta de ubicación, actualización de perfil y posteo de red social contribuyen a su huella digital. Para activistas feministas y defensoras de los derechos humanos de las mujeres, estas informaciones aparentemente pequeñas pueden revelar mucho más de lo querido. Manejar la propia huella digital no quiere decir volverse invisible. Tiene que ver con ser consciente. Empiece revisando qué información pone a disposición públicamente. Restrinja los controles de privacidad en las redes sociales, prestando particular atención a quién puede etiquetarla, buscarla o ver su contenido. Revise estos controles con regularidad, dado que las plataformas cambian sin avisar con frecuencia las opciones por defecto.

Piense con cuidado en la información sobre la ubicación. Registraciones en tiempo real, fotos geoetiquetadas y posteos que revelan dónde viven, trabajan o pasan el tiempo usted y su familia pueden hacer que sea más fácil que otras personas rastreen sus movimientos. Las fotos tomadas con teléfonos inteligentes suelen contener metadatos por defecto, que deberían eliminarse antes de compartir públicamente imágenes sensibles.

Para comunicaciones sensibles, use herramientas diseñadas teniendo la privacidad en mente:

- Signal sigue siendo una de las opciones más confiadas para cifrar mensajes y llamadas.
- Para el correo electrónico, proveedores enfocados en la privacidad como Proton Mail suelen ofrecer protecciones adicionales en comparación con servicios convencionales.
- Revisar los permisos de las aplicaciones con regularidad y eliminar accesos innecesarios a ubicación, micrófono, cámara y contactos.
- Al trabajar en espacios públicos, evite acceder a información sensible en redes de Wi-Fi inseguras y evalúe usar una VPN de confianza si es inevitable.

Ninguna de estas medidas es particularmente complicada. No obstante, cuando se aplican con constancia, pueden reducir considerablemente la exposición al riesgo.

# Protección colectiva y organizacional

La protección digital suele presentarse como una responsabilidad individual. Sin embargo, dentro de las organizaciones y los movimientos feministas, una cuenta comprometida puede exponer las comunicaciones, los contactos y el trabajo de todo un equipo. Una contraseña débil en una plataforma compartida puede crear vulnerabilidades para todas las personas que colaboran. La seguridad digital, por ende, tiene que ser entendida como una forma de cuidado colectivo y no como un asunto de competencia individual. Esto empieza estableciendo prácticas compartidas. Se debe acordar qué herramientas se usarán para las comunicaciones sensibles, fijar expectativas mínimas en relación con contraseñas y autentificación en dos pasos y asegurarse de que las cuentas organizacionales no dependan del dispositivo o el perfil de una sola persona.

Cuando el personal deja la organización, debe eliminarse su acceso a cuentas compartidas con celeridad y como parte de la rutina establecida. Igual de importante es crear estructuras de soporte antes de que se las necesite. Identificar personas de confianza dentro de sus redes que puedan brindar asistencia técnica, legal o psicosocial si usted o alguna persona conocida se convierten en blanco. Desarrolle procedimientos internos simples para responder a incidentes como hackeo, doxeo o una cuenta en riesgo. Saber quién hará qué durante una crisis puede reducir drásticamente la confusión y el daño. Como rutina, las organizaciones feministas invierten en la seguridad física y el bienestar de su personal y sus comunidades. La protección digital merece la misma atención.

# Responder a incidentes y priorizar el bienestar

Los ataques digitales y el acoso online suelen ser más dañinos cuando no se tiene un plan de respuesta. Tener un marco básico para responder ante un incidente hace una gran diferencia.

## Documentación

Cuando hay acoso o una cuenta se ve en riesgo, lo primero es documentarlo. Haga captura de pantallas, guarde las URL, registrar nombres de usuario y preservar las pruebas antes de que el contenido sea borrado o eliminado. Esta documentación puede ser crítica para denunciar ante las plataformas, tomar acciones legales o hacer una denuncia policial.



## Denuncia

Hay que saber dónde buscar ayuda. Los mecanismos de denuncia de las plataformas son imperfectos, pero siguen siendo un importante primer paso; en particular, en casos que involucran amenazas de violencia, suplantación, acecho o abuso basado en la utilización de imágenes. Muchos países tienen organizaciones que brindan asistencia legal, psicosocial o técnica a activistas que sufren daño digital. Conozca estos recursos antes de que ocurra una crisis y tenga la información de contacto en un lugar que sea de fácil acceso.

## Cuidado

El impacto emocional del daño digital es considerable. El abuso sexualizado, el contenido inventado, las campañas de acoso coordinadas y las amenazas sostenidas, todo esto está diseñado para agotar, aislar e intimidar. Sus efectos son reales, acumulativos y con frecuencia invisibles para el resto. Por esta razón, la planificación de la protección digital debería incluir siempre el cuidado. Hable con colegas de confianza. Tómese un descanso de las redes sociales cuando sea necesario. Use las funciones de silenciar, bloquear y restringir sin disculparse. Busque ayuda profesional si el impacto se hace abrumador. La seguridad digital y el bienestar no son temas separados. Son dos partes del mismo compromiso: asegurar que las activistas, las organizaciones y los movimientos feministas puedan seguir con su trabajo de forma segura, sostenible y en sus propios términos.

# Visibilidad, protección y poder

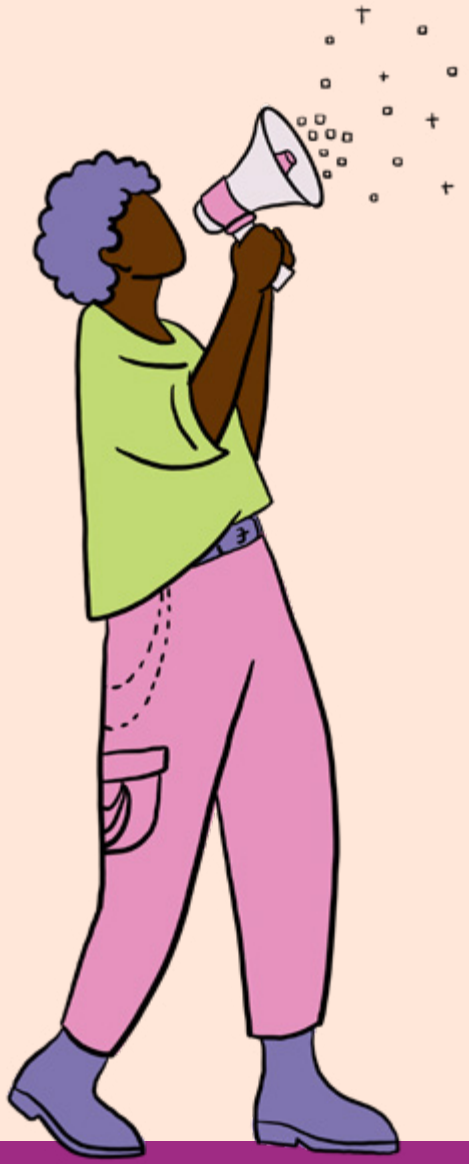
La protección digital tiene que ver con participar de la vida pública en nuestros propios términos. Los movimientos feministas siempre han tenido que adaptarse a los cambios del escenario político buscando nuevas formas de organizarse, comunicar y crear poder. Hoy, los espacios digitales son parte de ese escenario. Nos permiten compartir conocimiento, apoyar a sobrevivientes, desafiar la injusticia y conectarnos a través de las fronteras de un modo que no habríamos podido imaginar hace una generación. Sin embargo, también crean nuevos riesgos que exigen atención, preparación y cuidado.

El objetivo es tomar decisiones informadas sobre el riesgo, fortalecer la protección colectiva y crear la confianza para poder seguir participando en espacios digitales de forma segura y estratégica. Así, la protección digital es al mismo tiempo una cuestión técnica y un asunto del movimiento. Cuando las activistas feministas, las organizaciones y las comunidades pueden comunicarse con seguridad, protegerse mutuamente y responder de forma efectiva ante el daño, son más capaces de sostener el trabajo de promover los derechos, apoyar a las sobrevivientes y crear el cambio. Nuestros movimientos dependen de la conexión. La protección digital nos asegura que esas conexiones sigan siendo una fuente de fortaleza y no de vulnerabilidad.

# Recursos

Las siguientes organizaciones y recursos brindan asistencia práctica y gratuita para la protección digital:

| Recurso | Qué ofrece |
|---|---|
| Línea de ayuda para la seguridad digital de Access Now (Access Now Digital Security Helpline) | Asistencia gratuita y confidencia para la seguridad digital para activistas, periodistas y personas defensoras de los derechos humanos en todo el mundo, incluida Sudáfrica. |
| Coalizão contra a violência Online (Coalition Against Online Violence (CAOV)) | Recursos y asistencia específicamente para el acoso *online* por cuestiones de género para mujeres que ejercen el periodismo. |
| Manual contra el acoso en línea de PEN America (PEN America Online Harassment Field Manual) | Guía práctica integral sobre cómo responder al acoso *online*, gratuita y en línea. |
| Cyber Civil Rights Initiative | Apoyo a sobrevivientes del abuso de imágenes íntimas no consentidas; recursos legales y guías para denunciar ante las plataformas. |
| Electronic Frontier Foundation (EFF) — Surveillance Self-Defence | Guías de seguridad prácticas y gratuitas para activistas y periodistas, organizadas por nivel de amenaza. |
| Front Line Defenders | Asistencia para la protección y la seguridad digital para activistas de derechos humanos de todo el mundo. |
| Feminist Tech Exchange | Recursos sobre tecnología y seguridad digital creados específicamente para organizaciones feministas. |



# Agradecimientos

Este texto fue escrito por Joy Watson y revisado por Jennifer Chinoye Amadi, Leah Goldmann, Lauren Messina e integrantes del equipo de violencia contra las mujeres de ONU Mujeres. Contó con el diseño de Mara Ayuningtyas y Léa Drougard y las ilustraciones de Sarah Imran. Esta publicación fue producida por COFEM en el marco de la iniciativa ACTUEMOS para poner fin a la violencia contra las mujeres y las niñas creada por ONU Mujeres con financiamiento de la Unión Europea. Su contenido es responsabilidad exclusiva de COFEM y no necesariamente reflejan las visiones de la Unión Europea o de ONU Mujeres.

# Cita sugerida

Coalición de Feministas para el Cambio Social. Ficha de consejos 2: Protección digital, Bytes de resistencia: Abordaje de la violencia de género facilitada por la tecnología (2026).

# Referencias

Amnesty International (2021) Azerbaijan: Stop the vicious campaign of gendered smears and reprisals against women activists. London: Amnesty International. Available at: https://www.amnesty.org

Andreasen, M.B. (2020) 'Feminist/activist responses to online abuse', in The International Encyclopaedia of Gender, Media, and Communication. Hoboken: Wiley.

Andreasen, M.B. (2024) 'Evidentiary activism in the digital age: on the rise of feminist struggles against gender-based online violence', in Edited volume title. London: Routledge.

Bansal, V., Eruyar, S., Wang, S. & Wessells, M. (2024) 'A scoping review of technology-facilitated gender-based violence in low- and middle-income countries across Asia', Trauma, Violence, & Abuse, online.

Bennett, L. and Livingston, S. (2020) 'The #MeToo movement, digital media and the public sphere', in Digital Media and the Public Sphere. London: Routledge.

Koch, L., Russo Riva, M.P. & Steinert, J.I. (2025) 'Technology-facilitated gender-based violence against politically active women: A systematic review of psychological and political consequences and women's coping behaviours', Trauma, Violence, & Abuse, online.

Loney-Howes, R. and Mendes, K. (2023) 'It's a global #MeToo: A cross-national comparison of social media responses to sexual violence', Feminist Media Studies, 24(7), pp. 1032–1050.

Posetti J, Hellmueller L, Williams K, Renaud P, Aboulez N and Shabbir N 2025 *Tipping Point: The Chilling Escalation of Online Violence Against Women in the Public Sphere*, UN Women, New York.

UN Women (2025) AI and anonymity: Digital violence against women in the age of online backlash. New York: UN Women.

VAWG Helpdesk (2017) Cyber VAWG: Violence against women and girls and information and communications technology. VAWG Helpdesk Research Report No. 211. London: UK Aid.

Slupska J, Dawson S, Ma L and Neff G (2021) Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity. Proceedings of the ACM on Human-Computer Interaction.

Sweeney J 2020 The *#Me Too Movement in Comparative Perspective, Journal of Gender, Social Policy and the Law*, Volume 29, Issue 1, 2020

Organized Crime and Corruption Reporting Project (OCCRP) (2023) 'How revenge porn is used to silence dissidents in Azerbaijan', OCCRP, 3 April. Available at: https://www.occrp.org/en/feature/how-revenge-porn-is-used-to-silence-dissidents-in-azerbaijan