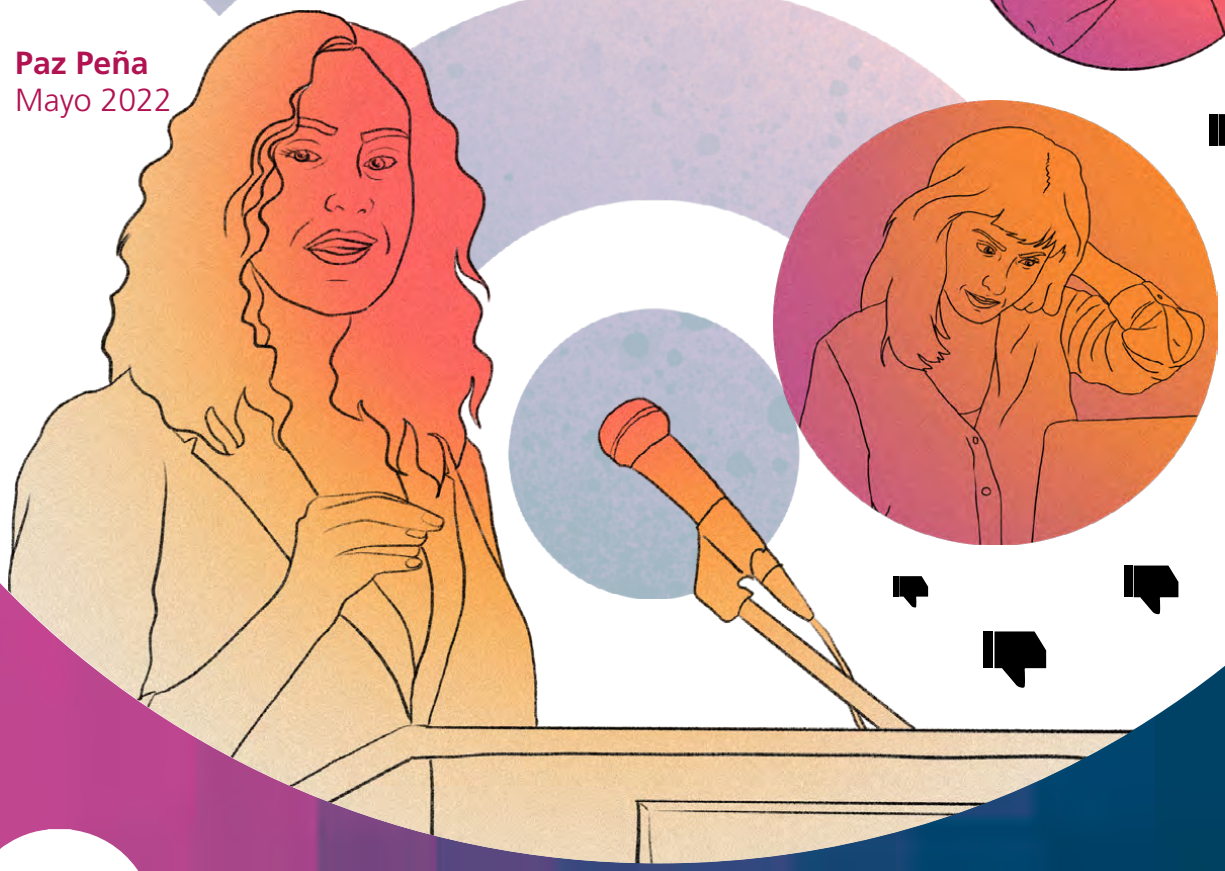
TRABAJO Y JUSTICIA SOCIAL

GUÍA PRÁCTICA CONTRA LA VIOLENCIA POLÍTICA DE GÉNERO DIGITAL

Paz Peña
Mayo 2022



FESMINISMOS

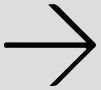
#TOMAPARTIDO

FRIEDRICH EBERT STIFTUNG

TRABAJO Y JUSTICIA SOCIAL

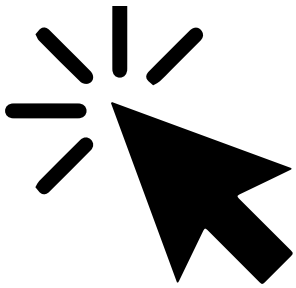
GUÍA PRÁCTICA CONTRA LA VIOLENCIA POLÍTICA DE GÉNERO DIGITAL

La violencia política contra las mujeres comprende todo acto de violencia basada en el género, o la amenaza de esos actos, que se traduce, o puede resultar en daños físicos, sexuales o psicológicos o sufrimiento, y está dirigida contra la mujer en la política por su condición de mujer.

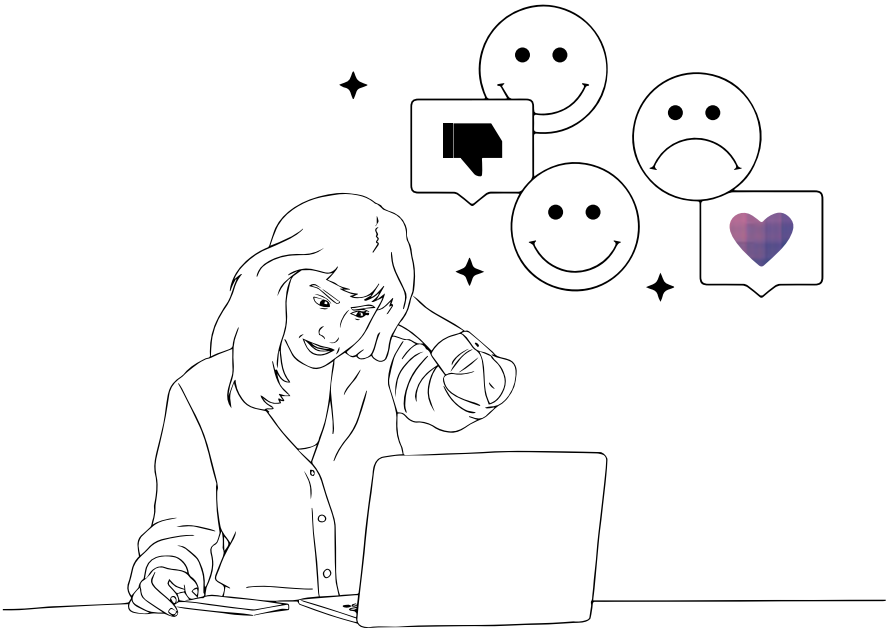


Esta es una guía de recomendaciones en seguridad digital y con enfoque feminista para las personas y organizaciones que enfrentan violencia política de género digital.

Es un trabajo que quiere reforzar la idea de que los hábitos de seguridad digital son importantes, pero que no pueden hacer frente como carta solitaria ante un problema estructural como es la violencia de género. En este sentido, este documento espera ser una guía de acompañamiento, pero también un catalizador de actividades colectivas que sirva para resistir y actuar sobre estos ataques.



Índice



Introducción

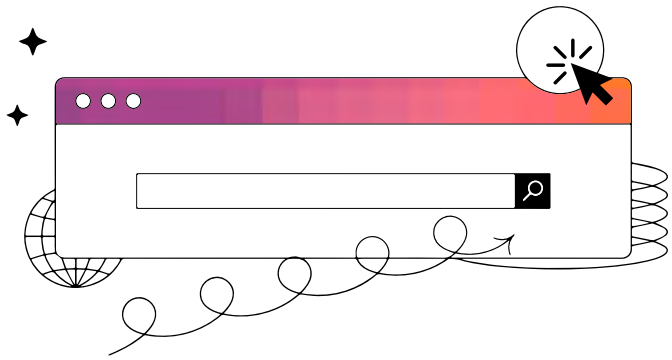
Esta es una guía que busca dar recomendaciones de amplia gama a las personas y organizaciones que enfrentan violencia política de género digital y, en particular, busca integrar recomendaciones de seguridad digital que, desde un punto de vista feminista, puedan hacer frente a estos ataques en particular. Al ser un tema de complejidad que necesita un enfoque de múltiples miradas, la guía se divide en dos. La primera parte está abocada, por un lado, a dar una mirada general de contextualización a la violencia política de género digital, la que no pretende ser una recolección acabada de evidencia, pero sí dar un repaso de lo que sabemos del problema, sobre todo en América Latina. Por otro, también se da uns revisión a las distintas respuestas que existen del problema, una amplia gama que va desde la seguridad digital feminista, la denuncia directa a las plataformas online donde ocurren los ataques, la denuncia legal, además de otras acciones de incidencia.

La segunda parte funciona como un anexo de la primera, en tanto se concentra en las acciones de seguridad digital que se pueden aplicar de acuerdo con la tipología de ataques más comunes que en ámbito digital se sufre por razones de género. Además, integra una serie de recursos externos que pueden ser de gran utilidad para las personas que quieran conocer más aspectos de seguridad digital en particular.

Con todo, esta guía busca reforzar la idea que los hábitos de seguridad digital son importantes, pero que no pueden hacer frente como carta solitaria ante un problema estructural como es la violencia de género. En este sentido, este documento espera ser una guía de acompañamiento, pero también un catalizador de actividades colectivas que sirva para resistir y actuar sobre estos ataques.

PRIMERA PARTE:

GUÍA PRÁCTICA CONTRA LA VIOLENCIA POLÍTICA DE GÉNERO DIGITAL



Definición

De acuerdo a la relatora especial de las Naciones Unidas (ONU) contra la violencia de la mujer en un informe especial sobre el tema,[1] la violencia política contra las mujeres comprende todo acto de violencia basada en el género, o la amenaza de esos actos, que se traduce, o puede resultar en daños físicos, sexuales o psicológicos o sufrimiento, y está dirigida contra la mujer en la política por su condición de mujer o afecta a las mujeres de manera desproporcionada, afectándolas en períodos eleccionarios pero incluso más allá de ellos.

Este tipo de violencia puede adoptar diversas formas que incluyen las perpetradas por medios digitales. En un informe específico sobre violencia online contra la mujer, la relatora especial de la ONU[2] ya había destacado que las mujeres en la política son víctimas periódicamente de la violencia en línea y la violencia facilitada por la tecnología de la información y las comunicaciones (TIC):

> Reciben amenazas en línea, generalmente de carácter misógino y a menudo sexualizadas. En última instancia, la violencia en línea contra la mujer en la política es un ataque directo a la participación plena de la mujer en la vida política y pública y al disfrute de sus derechos humanos. Aún no se ha comprendido cabalmente en qué medida los agentes estatales y no estatales utilizan esa violencia en línea para difundir desinformación encaminada a disuadir a las mujeres de participar en la política, apartar el apoyo popular de las mujeres políticamente activas e influir en la manera en que los hombres y las mujeres ven determinadas cuestiones.

Los medios digitales, en su amplitud, pueden ser espacios para la violencia de género online en contra de las mujeres políticas. No obstante, diversos estudios han demostrado cómo las redes sociales son, en particular, los espacios donde más se ejerce este tipo de violencia.[3] Hay sobrada evidencia de que las mujeres políticas experimentan un volumen de conversación significativamente mayor sobre su físico y la vida familiar en redes sociales, en comparación a sus homólogos masculinos.[4] Particularmente, un estudio en Chile muestra

---

1 A/73/301. 6 de agosto de 2018.

2 A/HRC/38/47. 18 de junio del 2018.

3 Ver Amnesty International (2018). TOXIC TWITTER - TRIGGERS OF VIOLENCE AND ABUSE AGAINST WOMEN ON TWITTER. Chapter 2. https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-2-3/

4 Barboni, E. (2016). (Anti)social media: the benefits and pitfalls of digital for female politicians; Chaturvedi, S., I Am a Troll: inside the Secret World of the BJP's Digital Army, Juggernaut

que la violencia política de género en Twitter se hace a través del desprestigio, el menosprecio de capacidades y alusiones al cuerpo o la sexualidad. Y se hace la advertencia de la necesidad de observar las agresiones desde la interseccionalidad de las víctimas. Por ejemplo, los ataques a candidatas indígenas de la Convención Constitucional chilena fueron, principalmente, racistas; por su lado, las disidencias sexuales fueron objeto de ofensas de alto calibre por su orientación sexual, identidad o expresión de género, así como las candidatas jóvenes (menores de 35 años) y las académicas enfrentan mayores niveles de menosprecio a sus capacidades.

Asimismo, la difusión de información errónea y noticias falsas es omnipresente en estas plataformas y con frecuencia se dirige a las candidatas en las elecciones parlamentarias, pero también a las mujeres políticas fuera de los ciclos electorales. Las investigaciones han demostrado que existe una correlación entre la difusión de información errónea relativa a las funciones, las campañas, las creencias y las acciones de las mujeres en la política, y el acoso y los abusos que se reciben como resultado.[5] En muchos casos, estas agresiones son producto de una colaboración colectiva, con presencia de bots y trolls para amplificar el número de mensajes violentos y sus efectos. La percepción de impunidad envalentona a los agresores y aumenta la sensación de inseguridad y violación de las mujeres, alejando a muchas de ellas de la participación política.[6]

Efectos

Las consecuencias de la violencia de género online muchas veces son relativizadas debido a la idea de que lo online "no es real", no obstante, los efectos en la vida de las víctimas son persistentes en diversos ámbitos. La relatora especial de la ONU ha reconocido que los actos de violencia en línea "pueden llevar a la mujer a abstenerse de usar Internet" (párrafo 26), como también a daños o sufrimientos psicológicos, físicos, sexuales o económicos.[7]
De acuerdo con el informe especial del 2021 para el Parlamento Europeo sobre el tema,[8] se reconoce el impacto directo que esta violencia tiene en las víctimas y advierte que tienen una dimensión interseccional que, además, debe observarse junto otras formas de discriminación y discursos de odio, como las que reciben las personas LGBTIQ+, así como grupos racializados, minorizados o de diferentes comunidades religiosas.

Además, el informe sostiene que el mayor impacto de la violencia de género online es a nivel mental, lo que se refleja en una mayor incidencia de depresión y trastornos de ansiedad, que repercute en una reducción de la calidad de vida. Asimismo, reconoce una serie de impactos económicos, como los costes derivados de la búsqueda de asistencia legal y sanitaria y los riesgos de pérdida de empleo o menor productividad.

5 Oates, Sarah and Gurevich, Olya and Walker, Christopher and Di Meco, Lucina, Running While Female: Using AI to Track how Twitter Commentary Disadvantages Women in the 2020 U.S. Primaries (August 28, 2019). SSRN: https://ssrn.com/abstract=3444200 or http://dx.doi.org/10.2139/ssrn.3444200

6 NDI (2018). #NOTTHECOST Stopping Violence Against Women in Politics. Submission by the National Democracy Institute to the United Nations Special Rapporteur on Violence Against Women. https://www.ndi.org/publications/submission-national-democratic-institute-united-nations-special-rapporteur-violence

7 A/73/301. 6 de agosto de 2018.

8 MEENAKSHI FERNANDES, NIOMBO LOMBA, Cecilia NAVARRA. 2021. Combating Gender based Violence: Cyber Violence. Study from the European Added Value. European Parliament. 17/03/2021 https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662621

Para el National Democracy Institute (NDI), existe una clara relación entre el troleo persistente y agresivo en línea y las agresiones físicas reales a las que se enfrentan algunas mujeres, lo que denomina "el efecto pasarela", y destaca el trágico ejemplo del asesinato de la parlamentaria británica Jo Cox a manos de Thomas Mair.[9] Este último, un terrorista de derecha con vínculos transnacionales con movimientos de supremacía blanca en Estados Unidos. Mair había acechado a Cox por Internet durante muchos meses antes de asesinarla mientras Cox visitaba su circunscripción electoral.[10]

A lo anterior, se suma el impacto social que tiene la violencia de género online, y que tiene efectos en los derechos económicos, sociales y culturales, además de los derechos humanos, de las personas afectadas. Así, se trata de un fenómeno que tiene efectos en los espacios laborales de las mujeres, como también en sus derechos cuando las víctimas se ven obligadas a retirarse de una plataforma como Internet que, como ha sido reconocido por organismos internacionales de derechos humanos,[11] es un medio fundamental para la realización de derechos fundamentales.

Particularmente, cuando esta forma de violencia de género es recibida por mujeres políticas, contribuye a generar un entorno hostil para el ejercicio pleno y en igualdad de condiciones de los derechos políticos de las candidatas en la contienda.[12] Así, algunos efectos en el debate público son:[13]

- Deslegitimar a las mujeres como líderes y cuestionar su derecho a desempeñar funciones políticas;
- Despersonalizar a las mujeres líderes, aumentando el coste de compartir información personal;
- Distraer intencionadamente a las líderes para que no se centren en el trabajo sustantivo, obligándolas a dedicar tiempo y energía a hacer frente a los abusos y las amenazas;
- Inculcar el temor por su seguridad física y la de sus familias, y obligarlas a aplicar nuevas medidas de seguridad; y
- Disuadir a las mujeres de presentarse a las elecciones o de participar en el debate político.

9 NDI (2018). #NOTTHECOST Stopping Violence Against Women in Politics. Submission by the National Democracy Institute to the United Nations Special Rapporteur on Violence Against Women. https://www.ndi.org/not-the-cost

10 Chan, S. (2016). Right-Wing Extremist Convicted of Murdering Jo Cox, a U.K. Lawmaker. New York Times. https://www.nytimes.com/2016/11/23/world/europe/thomas-mair-convicted-murder-jo-cox.html

11 A/HRC/17/27 (2011)

12 Lourdes V. Barrera, Anaiz Zamora, Érika Pérez Domínguez, Ixchel Aguirre, Jessica Esculloa (2018). Violencia política a través de las tecnologías en México. Luchadoras. https://iknowpolitics.org/sites/default/files/violencia_politica_a_traves_de_las_tecnologias_contra_las_mujeres_en_mexico_pags_web.pdf

13 Atalanta (2018). (Anti)Social Media The benefits and pitfalls of digital for female politicians. https://www.atalanta.co/news-insights/antisocial-media-the-benefits-and-pitfalls-of-digital-for-female-politicians/

Tipología de ataques comunes

Uno de los estudios en América Latina más completos sobre la violencia política de género digital, fue realizado por la Coalizão Direitos na Rede a través de su plataforma "Tretaqui!", que ha estudiado el fenómeno en Brasil durante diversas campañas electorales, recolectando evidencia desde su plataforma.[14] En ese contexto, hicieron una agrupación de seis tipos de ataques más frecuentes, con la aclaración de que estos tipos de ataques pueden estar perfectamente entrelazados los unos con los otros y que, muchas veces, tienen relación con ataques fuera de línea.[15]

TIPOLOGÍA DE ATAQUE	ACCIONES MÁS COMUNES
Desinformación	• Campañas de desprestigio (destinadas a desacreditar a la persona atacada). • Difusión de información falsa (a menudo vinculada a la sexualidad y el matrimonio).
Violaciones de la intimidad	• Exposición de datos personales (conocida como doxxing). • Filtración de datos personales, privados y de orientación sexual. • Datos de orientación sexual recopilados sin consentimiento o con consentimiento o con el consentimiento de un clic. • Compartir imágenes íntimas sin consentimiento (exposición de la intimidad). • Uso no consentido de materiales y fotos. • Robo de identidad.
Ofensas	• Discurso de odio. • Ciberacoso/ofensa. • Explotación de la imagen sexual y estereotipada. • Edición de imágenes y videos.

14 Ladyane Souza & Joana Varon (2020). INTERNET E ELEIÇÕES. Guia para proteção de direitos nas campanhas eleitorais. Coalizao Direitos Na Rede.

15 Hay diversas formas de clasificar la violencia política de género digital; se optó por esta solo porque es una de las más completas y usadas por organizaciones de la sociedad civil en el continente.

Amenazas	• Acoso sexual y psicológico. • Acoso a través de la bandeja de entrada en las redes sociales, con fotos y vídeos obscenos. • Hostigamiento. • Amenazas de violencia física.
Censura	• Ataques masivos y coordinados. • Manipulación de algoritmos. • Eliminación de contenidos. • Bloqueo de publicaciones, páginas y perfiles por denuncia o iniciativa de las redes sociales.
Desinformación	• Zoombombing (invasión de la videoconferencia o del evento en línea). • Acceso no autorizado a cuentas o dispositivos personales. • Hacking/Ataques a la seguridad de los sistemas.

En México, la organización Luchadoras logró detectar un patrón preocupante en las agresiones a las candidatas en Internet, que complejiza y profundiza el daño, y que revela una intención explícita del uso de tecnologías como herramienta de ataque. Se trata de lo que denominan una "cadena de agresiones", y que consiste en cuatro situaciones entrelazadas que suceden la una a la otra:

¿Quiénes provocan estos ataques?

Para las elecciones del año 2018, Luchadoras encontró en México que el 52% de los casos la agresión hacia una candidata proviene de alguien desconocido, siendo los principales agresores las y los usuarios de redes sociales, seguidos de integrantes de partidos políticos; advirtiendo que no se tuvo información suficiente para caracterizar a los agresores en el 33% de los casos.

También se puede encontrar evidencia de que los ataques son producidos en el contexto de las olas de autoritarismo, misoginia y racismo

en algunos países, en los que las redes sociales tienen un papel clave; incluso se apunta a que son producidos por grupos misóginos y racistas muchas veces organizados trasnacionalmente, como los llamados grupos Incel (del inglés involuntarily celibate, o célibe involuntario). Los agresores utilizan hábilmente las redes sociales y sus lógicas para priorizar el contenido que ven las personas, por lo que hasta se los consideran tech-savvy, es decir, que poseen un buen conocimiento de las tecnologías[16]. En países de América Latina también se ha visto el uso coordinado de las redes sociales en contra de la agenda feminista a través de discursos virulentos y estigmatizantes[17].

Con todo, la violencia que enfrentan las mujeres en Internet por su rol político no se trata de incidentes aislados, sino que son una muestra de la prevalencia de la misoginia y la hostilidad de género que encuentran las mujeres en la red, cada día[18].

¿Cuál es la responsabilidad de las plataformas?

A diferencia de otros tipos de violencia de género a nivel político, la que se produce a través de medios digitales se hace a través de un intermediario privado: las empresas dueñas de las plataformas. En el caso de las plataformas de redes sociales -pero también otras que ofrecen modelos gratuitos de uso-, es importante examinar su modelo de negocio, pues se basan en recolectar datos personales de las personas usuarias, para luego perfilarlas y comercializar esa información a terceros (con fines comerciales u otros, que puede ser perfectamente electorales, como demostró el caso de Cambridge Analítica)[19].

En particular, como los contenidos de las redes sociales son producidos por sus suscriptores, para que las empresas puedan obtener más datos y hacer un mejor perfilamiento de las personas, es necesario que éstas tengan la mayor atención en las plataformas (incluso al nivel de adicción)[20] e interacción posible. Para eso, las plataformas crean algoritmos de información que privilegien contenidos polémicos que obliguen a las personas a reaccionar.[21] En otras palabras, "los algoritmos que maximizan el engagement premian los contenidos incendiarios"[22]. Esta lógica fue rápidamente aprendida por grupos de extrema derecha[23],

16 Souza, L. & Varón, J. (2020) Violencia política de género en Internet. Policy paper América LAtina y el Caribe. Al Sur. https://www.alsur.lat/sites/default/files/2021-07/Violencia%20Pol%C3%ADtica%20de%20G%C3%A9nero%20en%20Internet%20ES.pdf

17 Chaher, S. (2021) ¿Es posible debatir en medio de discursos de odio?: activismo feminista y grupos antiderechos en el Cono Sur de América Latina. - 1a ed - Ciudad Autónoma de Buenos Aires: Comunicación para la Igualdad Ediciones.

18 Barker, K. (sin fecha). Violence Against Women in Politics (#VAWP) – The Antithesis of (Online) Equality. The Open University Law School. https://law-school.open.ac.uk/news/violence-against-women-politics-vawp

19 BBC Mundo (2018). 5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día. https://www.bbc.com/mundo/noticias-43472797

20 Al Jazeera (2021). Facebook products 'harm children, stoke division': Whistleblower https://www.aljazeera.com/news/2021/10/5/facebook-products-harm-children-stoke-divisions-whistleblower

21 Natasha Lomas. YouTube's recommender AI still a horror show, finds major crowdsourced study. TechCrunch. July 7, 2021. https://techcrunch.com/2021/07/07/youtubes-recommender-ai-still-a-horrorshow-finds-major-crowdsourced-study/

22 Karen Hao. How Facebook got addicted to spreading misinformation. MIT Technology Review. March 11, 2021 https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/

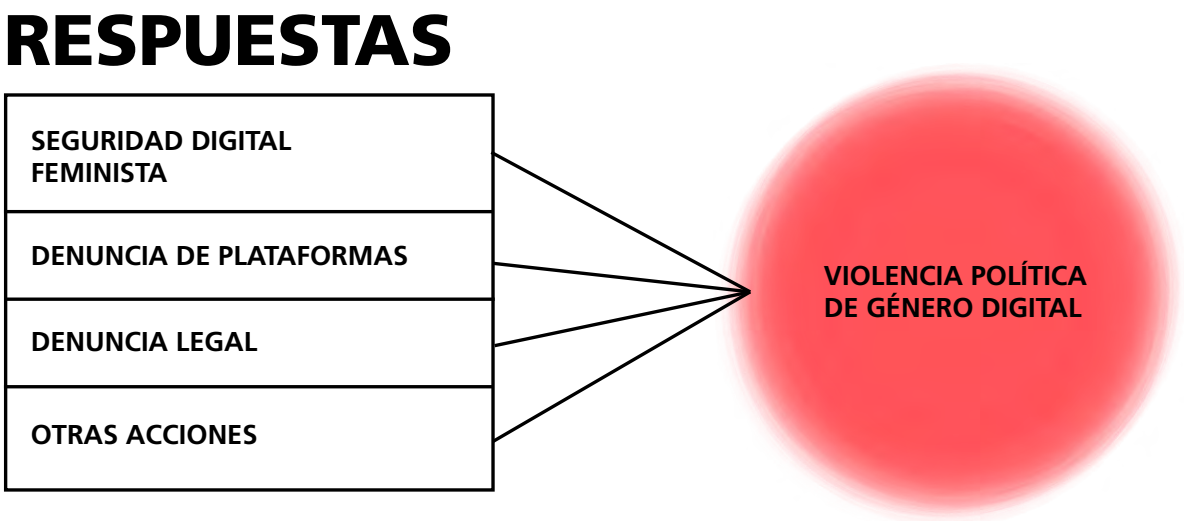
23 Souza, L. & Varón, J. (2020) Violencia política de género en Internet. Policy paper América Latina y el Caribe. Al Sur. https://www.alsur.lat/sites/default/files/2021-07/Violencia%20Pol%C3%ADtica%20de%20G%C3%A9nero%20en%20Internet%20ES.pdf

sobre todo al momento de diseñar campañas de desinformación[24]. Los costos de esta forma de ordenar la información son múltiples, y muchos de ellos los pagan las mujeres y otros grupos especialmente vulnerables, como ha sido revelado por las filtraciones del 2021 de Facebook[25].

A lo anterior, también debe ponderarse otra serie de factores, que van desde el uso de set de datos sesgados hasta la falta de diversidad en la industria tecnológica, que repercuten en el diseño de espacios que facilita diversos tipos de violencias, intencionadamente o no[26].

RESPUESTAS AL PROBLEMA

Como hemos visto, la violencia política de género digital se trata de un fenómeno altamente complejo, multicausal, del que recién se tiene más evidencia. La mirada sobre él debe ser compleja, en la que no pueden descartarse acciones individuales de prevención, como acciones colectivas políticas en múltiples frentes. A continuación, se propone un modelo de respuesta que incluye examinar cuatro frentes de acción ante la violencia política de género online:



24 Samuel Woolley. We're fighting fake news AI bots by using more AI. That's a mistake. MIT Technology Review. January 8, 2020 https://www.technologyreview.com/2020/01/08/130983/were-fighting-fake-news-ai-bots-by-using-more-ai-thats-a-mistake/

25 France24 (2021). "Facebook daña a los niños": las estruendosas revelaciones de Frances Haugen. https://www.france24.com/es/ee-uu-y-canad%C3%A1/20211005-frances-haugen-facebook-senado-da%C3%B1oscom/2021/07/07/youtubes-recommender-ai-still-a--horrorshow-finds-major-crowdsourced-study/

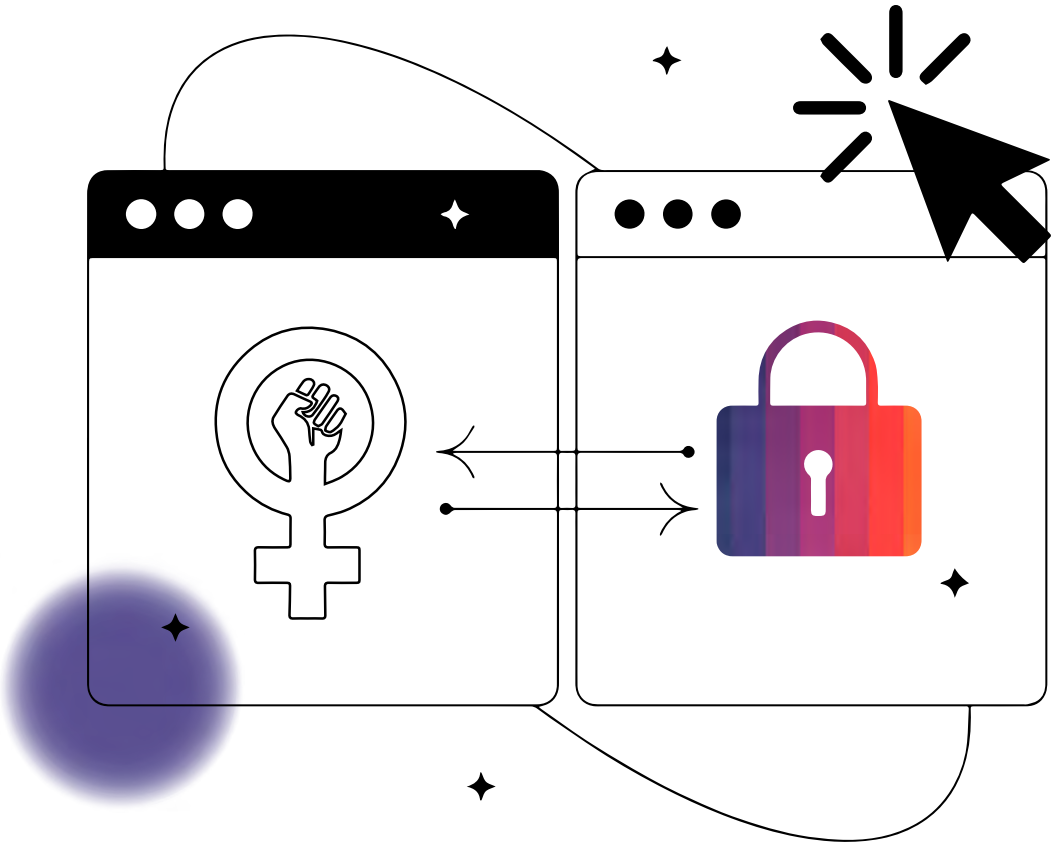
26 A/HRC/44/57 (2020)

SEGURIDAD DIGITAL FEMINISTA

Una respuesta a la violencia política de género digital es, justamente, la seguridad digital. Esta última debe entenderse como una herramienta de prevención de ataques como, también, de mitigación.

Una mirada feminista de la seguridad digital deja de lado la idea de centrarse solo en la adopción de tecnología segura y busca, más bien, centrarse en el bienestar de las personas a través del cuidado digital. Esto tiene diferentes implicancias concretas:

- La seguridad digital es entendida como el conjunto de hábitos y decisiones que tomamos para prevenir y mitigar los riesgos asociados al uso de la tecnología. En otras palabras, más que tecnologías, se enfoca en los hábitos. Y más que buscar comportamientos universales, se trata de definirlos localmente, de acuerdo con los diversos riesgos particulares de las personas y sus comunidades.
- Busca el bienestar de la persona, integralmente. Es decir, se sostiene una perspectiva holística, donde tres esferas están interconectadas: Seguridad física - Bienestar mental y de autocuidado - Seguridad digital.
- A diferencia de los enfoques individualistas, se trata también de un ejercicio colectivo, donde, en comunidad, las personas se fortalecen.
- El enfoque feminista integra cómo las mujeres, los cuerpos e identidades que no se rigen por la cisheteronormatividad experimentan riesgos específicos y más amenazas a través de las tecnologías.



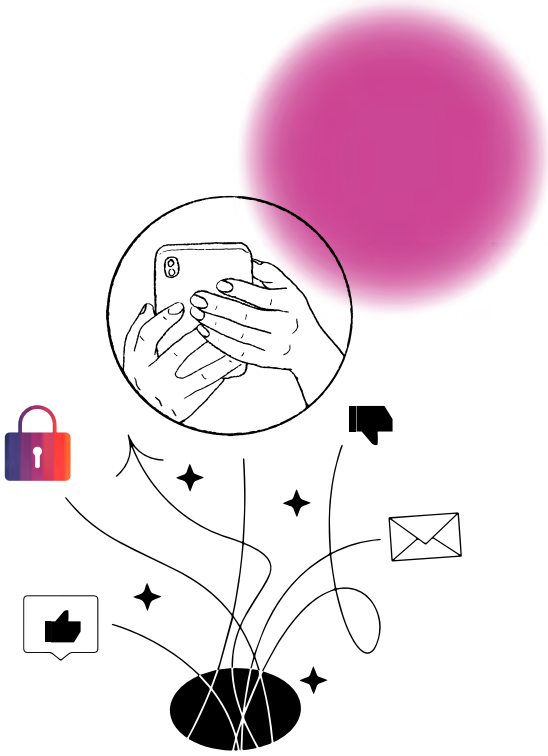
Modelo feminista para evaluar riesgos de seguridad digital

Un modelo de riesgos es una herramienta que te permite medir y evaluar las amenazas que vives en el ámbito digital, y poder así determinar el tipo de protección holística que necesitas para cuidar tu información, la de tu organización, como también lograr el bienestar individual y colectivo.

Se debe recordar que la seguridad digital es también parte de un modelo más grande, donde la seguridad física (los ataques pueden también manifestarse física y materialmente) y el bienestar psicosocial (los efectos de las violencias son reales sobre las personas, en múltiples dimensiones) debe acompañar cualquier modelo de seguridad digital.

Es importante hacer este ejercicio porque es la única forma de identificar de manera proactiva las amenazas a las que queremos darle prioridad, actualizar nuestros hábitos de seguridad y evitar riesgos, reduciendo las pérdidas de información y el estrés asociado. Pero también es un ejercicio importante que puede ser hecho colectivamente en comunidades afines, pues brinda coordinación y solidaridad.

Un modelo de evaluación de riesgos feminista toma tiempo y significa un compromiso organizacional importante; de hecho, hay organizaciones y profesionales especializadas que pueden ayudar a personas en particular riesgo.[27] Con todo, el siguiente modelo que presentamos es uno simplificado, que busca demostrar que, más que concentrarse en la adopción de complicadas herramientas técnicas, es necesario revisar nuestros hábitos cotidianos de seguridad digital, lo que muchas veces es mucho más simple y cercano para las personas.
La siguiente tabla muestra cinco pasos con reflexiones que necesitas hacer para priorizar las amenazas[28] y sus respectivas respuestas. No hay respuestas correctas universales. En la tabla, también, y a modo de ejemplo, se muestra una posible respuesta de una persona ficticia que se concentra solo en Twitter.



27 Por ejemplo, Digital Defenders Partnership o Front Line Defenders.

28 Recuerda: los incidentes son ataques que ya ocurrieron y, las amenazas, son los ataques que podrían ocurrir en un futuro.

1	2	3	4	5
Identifica activos que quieres proteger	**Identifica los adversarios (de quién quieres proteger tus activos) y sus capacidades**	**Identifica las amenazas**	**Mide el riesgo**	**Determina el impacto**
Activos: información que pondría en riesgo tu labor, tu organización, tu comunidad, tu bienestar.	Personas, organizaciones o comunidades que podrían buscar atacarte. Sus capacidades (bajas, medianas o altas) comprenden sus recursos económicos, sociales y tecnológicos. Recuerda, los adversarios pueden ser personas, organizaciones y Estados. También pueden ser contactos muy cercanos.	Ataques, incidentes o cualquier evento que tus adversarios podrían llevar a cabo. **Recuerda considerar que las interseccionalidades (género, raza, clase social, etc.) de una persona pueden ponerla en especial riesgo.**	Identifica la probabilidad de que esa amenaza ocurra y se convierta en realidad. Siendo 1 (muy baja) y 5 (muy alta).	Cuál sería el impacto sobre la persona u organización si la amenaza se hiciera realidad (siendo 1, severidad baja, y 5, severidad alta)
En Twitter: • Es mi principal medio de comunicación política; casi no uso mi web, mucha info importante está ahí. • Mando mensajes directos que son privados. • Tengo una lista privada de personas voluntarias que trabajan en mi campaña y no quisiera perderla	En Twitter: • Trolls comunes que me quieren desprestigiar; de baja sofisticación pues solo responden a todo lo que digo. • Miembros de otras campañas políticas, pagados; podrían ser de alta sofisticación, sospecho que están organizados.	Acosarme online con discurso antifeminista. Esto ya lo vivo.	5	2
		Iniciar campañas de desinformación con bots; esto porque a compañeras ya le ha comenzado a pasar y les bajan las publicaciones.	2	4
		Apoderarse de mis contraseñas y tomar control de mi cuenta y mi información: me llegan correos diciéndome que alguien está intentando acceder a mi cuenta.	4	5

Este modelo dará pie a una serie de priorizaciones que terminarán con un plan de mitigación. Si tanto el riesgo como el impacto de la amenaza es alto, las medidas de seguridad digital deben tomarse de forma preferente e inmediata. De ahí, cada persona y organización debe ordenar sus prioridades de acuerdo, de nuevo, a su tiempo, recursos e interés.

Con este mapeo inicial y priorización de amenazas, se puede hacer un plan de prevención y mitigación para mejorar la seguridad digital. Las estrategias de seguridad digital en que nos concentramos en este documento son dos:

- **Estrategias de prevención de riesgos.** Es decir que, una vez identificados los riesgos reales que las personas se enfrentan a Internet por sus actividades políticas, se despliegan acciones que eviten las peores consecuencias de esos ataques. Este enfoque se concentra en las amenazas.
- **Estrategias de mitigación.** Estas están referidas a las acciones que se pueden emprender cuando ha ocurrido o está ocurriendo un ataque en Internet, es decir, este enfoque se centra en los incidentes. Para prevenir nuevos incidentes, necesitamos detectar las amenazas y, por ende, hacer una estrategia de prevención de riesgos.

Las acciones para la prevención y la mitigación pueden ser costosas (significan, por ejemplo, la compra de un servicio o producto) o pueden tomar tiempo, porque implican la capacitación de las personas. Es importante que lo tengas en cuenta, porque eso le puede permitir a tu comunidad u organización hacer un plan de corto, mediano y largo plazo, basado en las fortalezas y capacidades que ya se tienen.

Recuerda que todas nosotras ya llevamos adelante diversas formas de seguridad digital, nadie empieza de la nada: desde esas prácticas que ya conocemos se pueden construir hábitos que fortalezcan nuestra seguridad y bienestar individual y colectivo.

Conductas y herramientas de seguridad digital

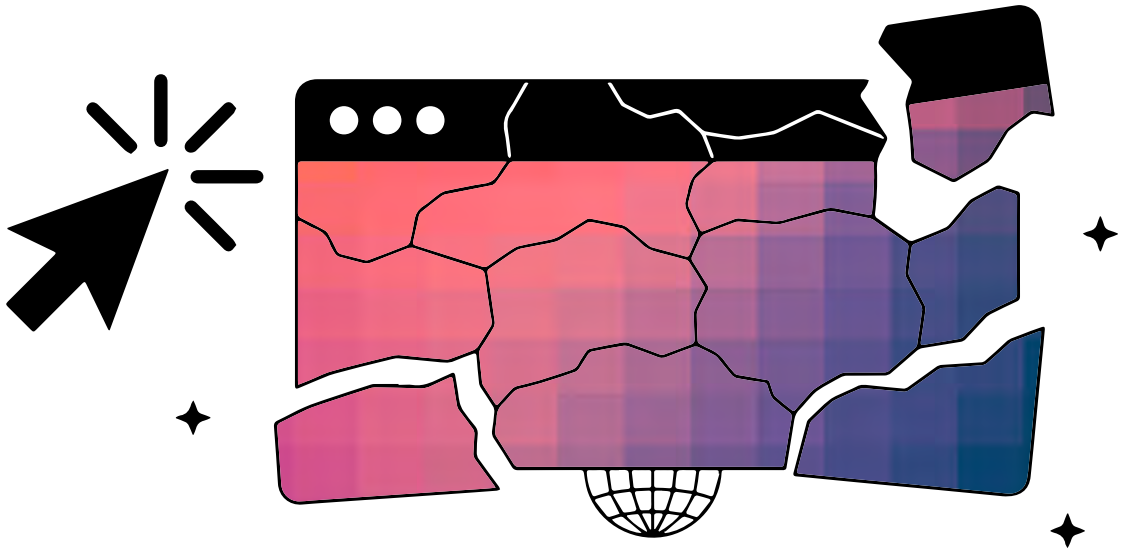
Si bien cada una de las acciones que se pueden emprender y herramientas que se pueden adoptar van a depender del modelo de riesgo, esta sección se concentra en conductas mínimas y herramientas que son bastante comunes, basadas en el cuadro de la tipología de ataques frecuentes que revisamos anteriormente.

Esto no implica, en ningún caso, que son las únicas acciones que deben tomarse: la conversación colectiva y la transferencia de experiencias y buenas prácticas, a todo nivel, ayudan a tener mejores estrategias de prevención.

Para conocer específicamente las diversas acciones de seguridad digital que pueden responder a tus necesidades, consulta la SEGUNDA PARTE de esta guía.

TIPOLOGÍA DE ATAQUE	ALGUNAS ACCIONES QUE SE PUEDEN TOMAR EN EL CONTEXTO DE LAS ESTRATEGIAS DE PREVENCIÓN EN SEGURIDAD DIGITAL
Desinformación	• Verificar tus cuentas en redes sociales • Documentación de ataques y definición de patrones • Denuncia a plataformas • Verifica la información que se comparte • Piensa estratégicamente antes de discutir con bots • Borra publicaciones antiguas masivamente de tus redes sociales • Borra o desactiva las cuentas que ya no usas • Compartimenta cuentas de redes sociales y de mensajería
Violaciones de la intimidad	• Verificar tus cuentas en redes sociales • Contraseñas seguras • Prevenir phishing • Utilizar administradores de contraseñas • Denuncia a plataformas • Autentificación de dos pasos • Gestiona tu identidad digital • Usa comunicaciones cifradas • Compartimenta cuentas de redes sociales y de mensajería • Configura la privacidad en las plataformas que usas, en especial, redes sociales y mensajería • Pon clave de acceso a tus dispositivos
Ofensas	• Bloqueo de agresores en Internet • Configura la privacidad en las plataformas que usas, en especial, redes sociales y mensajería • Denuncia a plataformas • Gestiona tu identidad digital • Compartimenta cuentas de redes sociales y de mensajería

Amenazas	• Bloqueo de agresores en Internet • Configura la privacidad en las plataformas que usas, en especial, redes sociales y mensajería • Denuncia a plataformas • Gestiona tu identidad digital • Compartimenta cuentas de redes sociales y de mensajería
Censura	• Sé estratégica con tus publicaciones • Documentación de ataques y definición de patrones • Denuncia a plataformas • Realizar respaldos de la información • Compartimenta cuentas de redes sociales y de mensajería
Invasiones	• Prevenir phishing • Prevenir zoombombing • Verificación dos pasos • Contraseñas seguras • Realizar respaldos de la información • Autentificación de dos pasos • Usa comunicaciones cifradas • Compartimenta cuentas de redes sociales y de mensajería • Actualiza tu software



La importancia de documentar los ataques

¿Cuánto sabes de la organización que hay detrás en los ataques que personalmente recibes en el mundo digital? ¿Conoces si hay más colegas que están pasando por lo mismo? ¿Hay patrones similares? ¿Han hecho algún análisis que les permita comprender el problema?

Documentar los ataques es importante porque nos permite analizar y buscar patrones, entender lo que nos pasa como sujetas en la política, pero también, si se hace como ejercicio colectivo, comprender el panorama que afrontamos en conjunto. Asimismo, podría ser también una forma de documentar pruebas que podrían ayudarle en procesos judiciales.[29]

El proyecto #SeguridadDigital da recomendaciones concretas de cómo comenzar esta bitácora de incidentes, incluido una propuesta de planilla que puedes modificar de acuerdo con tu situación.[30] Asimismo, el proyecto Acoso.Online hizo una guía para documentar ataques de violencia de género online que incluye medidas de seguridad digital, que vale la pena consultar sobre todo si la información en esa documentación es delicada.[31] Derechos Digitales[32] también tiene más documentación en esa línea.

Bienestar psicosocial

El enfoque psicosocial pone énfasis en los impactos que generan las violencias de género en el ámbito digital en los distintos niveles de la vida: individual, familiar, colectiva y social. La posibilidad de recuperación, entonces, depende de los recursos con los que una persona cuente a su alrededor, como apoyo psicológico, colectivo, sostén emocional y el desarrollo de herramientas para la protección digital.

En esa línea, muchas activistas feministas en el contexto Latinoamericano han desarrollado mecanismos de afrontamiento a la violencia en línea como espacios de acompañamiento feminista que busca relevar la práctica política de cuidado entre mujeres.[33]

Así, de acuerdo con organizaciones como Hiperderecho de Perú,[34] hay al menos cuatro pasos para incluir el bienestar psicosocial de las víctimas:
Construir redes de apoyo para asegurar el cuidado y la respuesta organizada.
Buscar acompañamiento psicológico si la persona se siente agobiada, cansada o angustiada.
Realizar prácticas de autocuidado y descanso estratégicos de los medios digitales.
Buscar una fuente de motivación para emprender cambios en la seguridad digital, desde construir plataformas distintas a las que hoy imperan desde paradigmas patriarcales y racistas, a negarse a que Internet se constituya en un espacio solo de violencia.

---

29 Esto va a depender de los estándares de prueba digital de cada país.

30 #SeguridadDigital (2028). ¿Por qué y cómo registrar y documentar incidentes? https://segudigital.org/por-que-y-como-registrar-y-documentar-incidentes/

31 Ver https://acoso.online/wp-content/uploads/2020/09/documentacion-difusion-de-imagenes.pdf

32 Ver https://twitter.com/derechosdigital/status/1443667020529213452?s=20

33 Taller de Comunicación Mujer (2020) DIAGNÓSTICO DE VIOLENCIA DE GÉNERO DIGITAL EN ECUADOR. https://www.navegandolibres.org/images/navegando/Diagnostico_navegando_libres_f.pdf

34 Salas, D., Albornoz, D., Huaranga, E. (2020) Kit de cibercuidado para activistas. Seguridad digital para cuidar nuestro activismo y reapropiarnos de Internet. Hiperderecho. https://hiperderecho.org/wp-content/uploads/2020/11/Kit-de-cibercuidado-para-activistas-.pdf

DENUNCIA A LAS PLATAFORMAS

Como se ha visto en este informe, las plataformas digitales juegan un papel particular en los casos de violencia política de género: son los intermediarios. En esta sección, más allá de la responsabilidad legal que tienen o no, nos concentramos en las herramientas que muchas de ellas brindan para morigerar este tipo de ataques.

Debido a que mucho de los problemas de las plataformas con la violencia de género tiene que ver con problemas estructurales que comienzan desde su diseño, su modelo de negocio y hasta los equipos que las desarrollan, estas herramientas son insuficientes y están lejos de ser ajustadas a la realidad de países que no están en el Norte Global. Con todo, es importante conocer que puede haber herramientas que pueden ayudar.

Los contenidos que más se penalizan en redes sociales

En las plataformas hay canales de denuncia de contenidos e interacciones que violan sus Términos y Condiciones (también conocidas como sus Políticas de Comunidad). Para saber si se pueden denunciar ciertas conductas de las personas usuarias, es importante leer las reglas y, de seguro, allí habrá explicaciones de cómo denunciar.

En el contexto de esta guía, es importante destacar el "Centro de seguridad de la mujer"[35] que plataformas que son parte del mismo conglomerado -Facebook, Instagram, WhatsApp y Messenger- han habilitado con información de políticas, herramientas y otros recursos para mujeres que puedan verse acosadas en ellas. Asimismo, Facebook, ONU Mujeres y el Instituto Nacional Electoral (INE) de México, lanzaron dos guías con consejos para que las mujeres en política, incluyendo candidatas, tengan mayores opciones para prevenir y reportar actos de violencia política en razón de género en redes sociales, y se conecten con sus comunidades en Facebook[36] e Instagram.[37]

Ahora bien, en general, en las plataformas más populares, hay una cierta transversalidad en que se penalizan comportamientos:[38]

Suplantación de identidad	Facebook
	Instagram
	Twitter
Información falsa	Instagram
Incitación al odio	Twitter

35 Ver Centro de seguridad de la mujer https://es-la.facebook.com/safety/womenssafety/tools

36 Ver Consejos sobre herramientas de seguridad de Facebook para mujeres líderes. #SheLeads CUANDO LAS MUJERES LIDERAN, TODOS PROGRESAN https://www2.unwomen.org/-/media/field%20office%20mexico/documentos/noticias/2021/04/sheleads_guide_online_es_la_foreword.pdf?la=es&vs=2947

37 Ver GUÍA DE SEGURIDAD DE INSTAGRAM PARA MUJERES EN LA POLÍTICA https://www2.unwomen.org/-/media/field%20office%20mexico/documentos/noticias/2021/04/mx-safety-security-guide-for-women-in-politics.pdf?la=es&vs=2843

38 Este cuadro es solo una muestra. Las reglas de las plataformas cambian constantemente y esto puede variar, incluso entre países, por lo que siempre se debe consultarlas.

Infracción al derecho de autor	Instagram
	Facebook
	Twitter
Difamación	Facebook
Desnudos	Instagram
	Facebook
Phishing	Instagram
	Facebook
	Twitter
Otras infracciones a tu privacidad (doxing, etc)	Facebook
	Twitter
Acoso u otras amenazas	Instagram
	Facebook
Difusión no consentida de imágenes íntimas	Instagram
	Facebook
	Twitter

Hay otras conductas que dependen de cada plataforma, sobre todo, en asuntos más peligudos como los discursos de odio y las noticias falsas y campañas de desinformación. Con todo, de parte de algunas plataformas, ha habido cierto compromiso público para brindar mejores herramientas de seguridad en caso de violencia de género.[39]

Precauciones importantes

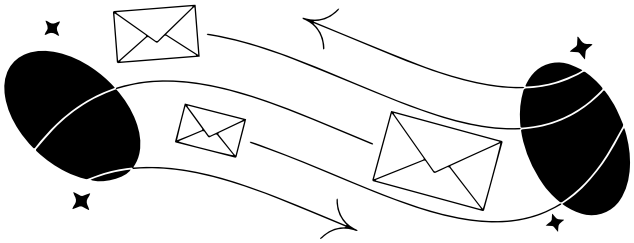
Es importante repetirlo para no crear falsas ilusiones: las soluciones no son perfectas. Sobre todo, cuando nos enfrentamos a ataques más sofisticados.
Puede ser que las herramientas sean confusas de usar y no den información básica sobre cuánto demorarán en responder.
Ten cuidado con solicitar el borrado de material a las plataformas, porque si persigues una acción judicial luego, no tendrás acceso a esa prueba. Lo mejor siempre es guardar un respaldo.

DENUNCIA LEGAL

A continuación, se da cuenta de algunas iniciativas legales sobre violencia política en América Latina que son especialmente dedicadas al ámbito digital o hacen particular mención a los espacios electrónicos. Esto no obsta que otros proyectos y leyes sobre violencia política de género no se apliquen al ámbito digital. Con todo, un análisis más detallado de su efectividad y alcance debe hacerse en estudios futuros.

Asimismo, los ataques por sí mismos pueden ser constitutivos de otros delitos locales, como la suplantación de identidad o el hackeo, entre otros tantos, por lo que es importante asesorarse con un especialista que analice cada caso.

39 Hern, A. (2021) Social network giants pledge to tackle abuse of women online. The Guardian. https://www.theguardian.com/society/2021/jul/01/social-networks-facebook-google-twitter-tiktok-pledge-to-tackle-abuse-of-women-online



PAÍS	TIPO	ESPECIFICACIÓN
COLOMBIA	Proyecto de ley: "Por medio de la cual se establecen medidas para Prevenir y Erradicar la Violencia contra las Mujeres en la Vida Política y se dictan otras disposiciones".	"Así mismo, adoptará medidas adecuadas para promover el uso responsable y respetuoso de la comunicación, a través de las nuevas tecnologías de información y comunicación, en relación a los derechos de las mujeres y su participación política, en los periodos legales de campaña electoral."
PERÚ	Ley N° 31155 que previene y sanciona el acoso contra las mujeres en la vida política	Artículo 3. Definición de acoso contra las mujeres en la vida política Es cualquier conducta que se ejerce contra una o varias mujeres por su condición de tal, realizada por persona natural o jurídica, en forma individual o grupal, de manera directa, a través de terceros, o haciendo uso de cualquier medio de comunicación o redes sociales y que tenga por objeto menoscabar, discriminar, anular, impedir, limitar, obstaculizar o restringir el reconocimiento, goce o ejercicio de sus derechos políticos. Artículo 4. Manifestaciones de acoso político contra las mujeres e) Divulgar imágenes o mensajes a través de medios de comunicación o redes sociales que transmitan y/o reproduzcan relaciones de desigualdad y discriminación contra las mujeres con el objetivo de menoscabar su imagen pública y/o limitar sus derechos políticos.

PANAMÁ	Ley 184 De violencia política. De 25 de noviembre de 2020.	Artículo 9. El instituto Nacional de la Mujer, a través del Comité Nacional contra la Violencia en la Mujer, dentro del marco de sus funciones, con la asesoría de la Asociación de Parlamentarias y Exparlamentarias de la República de Panamá, el Foro Nacional de Mujeres de Partidos Políticos y asociaciones u organizaciones vinculadas con la violencia política contra la mujer, en coordinación con las entidades competentes, adoptará las siguientes medidas: 6. Promover que los medios de comunicación y las redes sociales no violenten los derechos y la imagen de las mujeres que participan en la vida pública y su privacidad, así como el combate a los contenidos que refuerzan, justifican o toleran la violencia política contra las mujeres.
MÉXICO	DECRETO por el que se reforman y adicionan diversas disposiciones de la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, de la Ley General de Instituciones y Procedimientos Electorales, de la Ley General del Sistema de Medios de Impugnación en Materia Electoral, de la Ley General de Partidos Políticos, de la Ley General en Materia de Delitos Electorales, de la Ley Orgánica de la Fiscalía General de la República, de la Ley Orgánica del Poder Judicial de la Federación y de la Ley General de Responsabilidades Administrativas.	X. Divulgar imágenes, mensajes o información privada de una mujer candidata o en funciones, por cualquier medio físico o virtual, con el propósito de desacreditarla, difamarla, denigrarla y poner en entredicho su capacidad o habilidades para la política, con base en estereotipos de género;

Es importante recordar que, al igual que otras formas de violencia de género, además de procurar marcos normativos, hay que estar pendiente de cómo es la respuesta del sistema judicial ante esas nuevas leyes. En este sentido, y debido a que leyes de violencia de género digital aún son incipientes en el continente, aún es temprana la evidencia de sus resultados. No obstante, un estudio hecho por Luchadoras en México es inquietante: a pesar de que desde el 2012 se han introducido reformas legales en todo el país para penalizar la difusión no consentida de imágenes íntimas (una forma de violencia de género digital muy común), a mayo del 2020 solo se habían iniciado 24 causas penales en los Poderes Judiciales de siete Estados del país. Es más, solo se había emitido una sentencia condenatoria en el Estado de Chihuahua por el delito de sexting (Artículo 180 bis), y tres sentencias en Tamaulipas por el delito de "Pornografía de menores e incapaces" (Artículo 194 bis).[40]

Otras acciones

De acuerdo con la organización ecuatoriana, Taller de Comunicación Mujer, es necesario "abrir espacios de diálogo al interior de las organizaciones y entre organizaciones para hablar de temas de protección y seguridad digital. El objetivo es nombrar, reconocer, analizar, socializar estas violencias para desarrollar estrategias y tomar medidas de afrontamiento que permitan empoderarse con las tecnologías".[41]

En este sentido, más allá de las respuestas que las plataformas tengan y lo que las legislaciones propongan, a continuación, se revisan algunas iniciativas que, desde otros mecanismos de incidencia, buscan denunciar, contener y revertir la violencia política de género digital.

Campañas públicas

Estas acciones de comunicación organizadas son instancias muy interesantes para llegar a públicos más grandes y crear conciencia sobre la violencia política de género online. Por ejemplo, en Chile, y a propósito de la evidencia sobre el fenómeno en el contexto de la Convención Constituyente, en el 2020 se lanzó la campaña #DaleUnfollow a la violencia política digital de género.[42] En tanto, en México, Luchadoras se unió con Instagram para realizar una campaña en esa plataforma en torno a concientizar sobre el fenómeno.[43]

A nivel global, en el 2016, el Instituto Nacional Demócrata para Asuntos Internacionales (NDI) lanzó la campaña #NotTheCost, un llamado mundial a la acción para concienciar sobre el fin de la violencia contra las mujeres en la política. El título de la campaña refleja el hecho de que a muchas mujeres se les dice que el acoso, las amenazas, el maltrato psicológico (en persona y en línea) y las agresiones físicas y sexuales son "el coste de hacer política". La campaña tuvo una versión en México el 2017.[44]

---

40 Aguirre, I., Barrera, L., Zamora, A. & Rangel, Y. (2020) Justicia en trámite. El limbo de las investigaciones sobre violencia digital en México. Luchadoras. https://luchadoras.mx/wp-content/uploads/2020/11/Luchadoras_JusticiaEnTramite.pdf

41 Taller de Comunicación Mujer (2020) DIAGNÓSTICO DE VIOLENCIA DE GÉNERO DIGITAL EN ECUADOR. Página 83. https://www.navegandolibres.org/images/navegando/Diagnostico_navegando_libres_f.pdf

42 Observatorio Género y Equidad (2021). "#DaleUnfollow": La Articulación Territorial Feminista Elena Caffarena realiza campaña virtual para derribar la violencia política de género en la Convención http://oge.cl/daleunfollow-la-articulacion-territorial-feminista-elena-caffarena-realiza-campana-virtual-para-derribar-la-violencia-politica-de-genero-en-la-convencion/

43 Ver https://www.instagram.com/p/CPGcgfALkCz/?hl=en

44 Ver https://www.ndi.org/mexico-office-launch-notthecost-noelcosto-campaign

Observatorios independientes

La creación y coordinación de espacios independientes que sigan de cerca el fenómeno pueden no solo ayudar a documentar evidencia, sino que apoyar a las personas que están bajo ataque, además de llevar a cabo diversas acciones de incidencia política respecto a la violencia política de género en línea.

Por ejemplo, en Brasil, diversas organizaciones de la sociedad civil que trabajan temas como ciudadanía y democracia, derechos digitales, feminismo interseccional, entre otros, crearon la plataforma TretAqui.org, la cual recoge las denuncias de las y los candidatos que atacan y son atacados con discursos de odio y desinformación en Internet. Así, el 2018 enviaron estas denuncias a la Organización de Estados Americanos (OEA), organismo internacional que estaba siguiendo de cerca aquellas elecciones.

Estos observatorios, además, pueden alojar acciones de apoyo y solidaridad ante ataques, como también derivar a espacios de apoyo en seguridad digital feminista.

Coaliciones en los partidos políticos

Es importante trabajar en códigos de conducta al interior de los partidos que incluyan la violencia política de género digital; pero, como afirma el consorcio de organizaciones de derechos digitales de América Latina, Al Sur, en su informe sobre el fenómeno, es importante "mantener un enfoque suprapartidario: la movilización debe involucrar a distintos partidos políticos, ya que las coaliciones son fundamentales para la efectividad y sostenibilidad de las medidas".[45]
No obstante, es una labor complicada debido a las trabas históricas en los partidos políticos patriarcales. En este sentido, quizás es importante, primero, trabajar en conjunto con coaliciones suprapartidistas con militantes feministas que, en conjunto, puedan presionar a sus propios partidos.

Crear códigos de conducta digital en espacios políticos más allá de los partidos

La violencia política de género digital es mucho más amplia que la política partidista. Por eso, es importante que se sancione este tipo de agresiones en los diversos códigos de conducta y ética en instancias políticas formales locales, regionales, nacionales e internacionales. Un ejemplo reciente de esto es el "Código de Ética" de la Convención Constituyente en Chile que también se enfoca en la violencia política de género digital.[46]

De todas formas, es importante trabajar en modelos de código de conducta o de ética digital que permitan ser adaptados localmente.

Esta segunda parte de la guía está abocada a especificar las diversas acciones de seguridad digital que puedes seguir ante los ataques más comunes en el contexto de la violencia política

45 Souza, L. & Varón, J. (2020) Violencia política de género en Internet. Policy paper América LAtina y el Caribe. Al Sur. Página 20. https://www.alsur.lat/sites/default/files/2021-07/Violencia%20Pol%C3%ADtica%20de%20G%C3%A9nero%20en%20Internet%20ES.pdf

46 Ver https://www.chileconvencion.cl/wp-content/uploads/2021/09/Propuesta-reglamentaria-Comisio%CC%81n-de-E%CC%-81tica.pdf

SEGUNDA PARTE:

ACCIONES BÁSICAS DE SEGURIDAD DIGITAL

de género.

Es importante reiterar que no son las únicas, pero son las básicas que debes tener siempre presentes en el contexto de este tipo de violencia.

ACCIONES BÁSICAS DE SEGURIDAD DIGITAL

Contraseñas seguras

Las contraseñas son un tema fundamental y sumamente importante para evitar ataques. Muchos de los ataques ocurren porque tenemos contraseñas universales como "12345", combinaciones adivinables (fecha de cumpleaños) o, aunque sea una contraseña muy compleja, la repetimos para varios servicios, por lo que si se filtra esa información en un solo servicio te deja vulnerable en otras plataformas.

Si el servicio te lo permite, usa los siguientes principios para crear tus contraseñas:

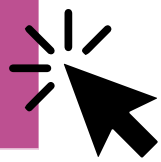
- **Larga -** Cuanto más larga es la contraseña, más difícil de descifrar.
- **Compleja -** Si es posible, siempre incluye en tu contraseña letras mayúsculas, minúsculas, números y símbolos, como signos de puntuación.
- **Impersonal -** Evita que se relacionan a ti de manera personal, de manera que no pueda ser fácilmente adivinada.
- **Secreta -** NADIE debe saberla. Si usas una contraseña y otra gente accede a ese servicio (por ejemplo, un tercero que maneja tus redes sociales) NO repitas esa contraseña en otro servicio.
- **Única -** Nunca las repitas.

Empleamos muchas contraseñas y es difícil recordarlas, sobre todo cuando las queremos complejizar. Dos consejos:

Siempre que sea impersonal, selecciona un concepto base, que sea fácil recordar para ti (por ejemplo, la parte de una canción que nadie sabe que te gusta) y crea tus propias reglas con ella (haz combinaciones o agrega elementos nuevos) de acuerdo con los diferentes servicios que usas.

Usa gestores de contraseñas, que te ayudan a guardar tus contraseñas de todas tus webs en un solo sitio y, además, crear contraseñas complejas y recordarlas. Consulta más adelante en esta guía sobre cómo funcionan estas herramientas.

Ocurren muchos hackeos masivos todos los días y nuestros correos electrónicos, números de teléfono y contraseñas pueden haber sido filtrados. Revisa si aquello ocurrió en haveibeenpwned.com y toma medidas si es necesario.



Activa la verificación (o autentificación) de dos pasos

La autentificación de dos pasos nos permite añadir una segunda capa de seguridad para acceder a nuestras cuentas de Internet. Muchos servicios, desde las aplicaciones de chat, correo electrónico y hasta las redes sociales, ofrecen una autenticación de dos factores.[47]

47 Por ejemplo:
- Twitter https://help.twitter.com/es/managing-your-account/two-factor-authentication
- Facebook https://es-la.facebook.com/help/148233965247823

Cuando se activa, se envía un código por SMS o correo electrónico, que sirve como paso adicional de seguridad en el proceso de inicio de sesión.

Es un factor muy importante, porque, aunque alguien consiga tu contraseña, necesitará un segundo paso, por lo que no podrá acceder a su cuenta y, por tanto, no podrá robarte información, suplantarte, etc. Ahora bien, los hackers saben que esto es una posibilidad, por lo que van a tratar de engañarte incluso para que les brindes esa información (consulta en esta guía la sección sobre phishing).

¡Habilita la autenticación de dos factores, especialmente en las redes sociales de la campaña!

Asegúrese de que el número de teléfono que recibe estos mensajes de autenticación sea de una persona que tenga prácticas de cuidados digitales y, al habilitar esta función, tampoco olvides buscar cómo emitir un código de respaldo y guardarlo en un lugar secreto y seguro. Así, si pierdes el teléfono, también podrás acceder a tu cuenta con ese código.

Usa administradores de contraseñas

Son aplicaciones que nos permiten guardar y generar claves aleatorias y seguras. El programa es capaz de elegir contraseñas como "mCyXRQ3p$Kdkp\CRJxjl0v" (es decir, que un ser humano no tenga probabilidades de adivinar) y las recuerda por ti, en cada servicio. Lo único que debes hacer es aprenderte una contraseña maestra para acceder a la aplicación y nada más.

No es obligatorio tener este tipo de servicios y va a depender de sus necesidades. Se recomienda conocer la herramienta y ver si te acomoda. Con todo, como muchos especialistas advierten que, si un adversario poderoso como un gobierno tiene a una persona en la mira, quizás un administrador de contraseñas no sea el método más seguro.[48] Para saber más sobre estas herramientas y cómo funcionan, consulta la guía de Infoactivismo.[49]

Pon clave de acceso a tus dispositivos

Tu celular y computadora contienen acceso a una gran cantidad de información privada, incluyendo direcciones, datos bancarios, así como rastros sobre tus actividades o las de otras personas cercanas a ti. Perder un dispositivo sin una contraseña le deja la puerta abierta a terceros a que accedan a toda esta información personal.

Por estas razones, es importante proteger el acceso a tu dispositivo con una contraseña. La mejor opción es un PIN alfanumérico de (al menos) seis dígitos, pero no uses números que sean fácilmente vinculables contigo (como el número de tu matrícula de un automóvil), ya que, si alguien tiene información sobre ti, es

- Gmail https://www.google.com/landing/2step/?hl=es_419

48 https://ssd.eff.org/es/module/creando-contrase%C3%B1as-seguras

49 https://infoactivismo.org/que-es-un-gestor-de-contrasenas-y-para-que-sirve/

posible que descifre tu clave. De preferencia, desactiva el desbloqueo mediante reconocimiento facial o con huellas dactilares porque es muy inseguro.

¡Respalda!

Para evitar la pérdida de información en caso de daño a un dispositivo o robo, es esencial hacer un respaldo de forma periódica en un servicio de almacenamiento en línea o, preferentemente, de forma física en un disco duro externo que guardes en un lugar seguro. Lo mejor es calendarizar esta práctica, así tu información no estará desactualizada.
Otra forma de proteger tu información es con el uso de carpetas cifradas. Existen varios programas como Truecrypt, Sophos Free Encryption o Axcrypt que te permiten añadir una contraseña a archivos y carpetas en tu computadora, de modo que solamente las personas con la clave puede descifrarlos.

Prevenir phishing

Estas técnicas buscan engañarte para que reveles contraseñas o para que se instale algún malware[50] en su dispositivo. Un ataque de phishing suele venir en forma de mensaje (por correo electrónico, SMS, chat, etcétera) que parece legítimo y que está destinado a convencerte para que:

- hagas clic en un enlace;
- abras documentos;
- instales algún software en tu dispositivo;
- o ingreses tu nombre de usuario y contraseña en un sitio web que luce real.

El phishing es usado tanto por delincuentes comunes, como por agentes maliciosos y Estados. Es una técnica común y transversal, que ocurre en todas las plataformas (emails, chats, SMS, etc.) por lo que debemos ser muy cuidadosas, sobre todo porque en nuestras campañas políticas debemos estar más alertas con la información que manejamos en nuestros dispositivos.

50 Malware es un término general para referirse a cualquier tipo de "malicious software" (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento. Son ataques comunes sobre periodistas, defensores de derechos humanos y personeros políticos https://www.dw.com/es/nso-group-se%C3%B1alado-de-espiar-a-50000-tel%C3%A9fonos-con-pegasus/a-58311353

Para prevenirlo, recuerda cinco consejos:[51]

SOLO INGRESA CONTRASEÑAS EN SITIOS WEB REALES	VERIFICA LAS DIRECCIONES DE CORREO DE LOS REMITENTES	ACTIVA LA VERIFICACIÓN DOS PASOS	ABRA DOCUMENTOS SOSPECHOSOS EN GOOGLE DRIVE	MANTÉN ACTUALIZADO SU SOFTWARE
En general, los servicios NUNCA te van a pedir que verifiques tu cuenta, ni en caso de una emergencia. El uso de este tipo de mensajes maliciosos es común porque te obliga a actuar rápido y a no pensar mucho. Si la emergencia parece real, chequea con las fuentes, directamente. Solo ingresa contraseñas en sitios web reales que tengan el candado de cifrado en la URL. Ojo que tratarán de engañarte y pueden hasta usar la imagen del sitio web original.	¿Las direcciones coinciden con la que yo conozco? A veces solo nos fijamos en el nombre y no en el correo para abrirlo. Tómate un segundo para verificar, ojo que buscarán engañarte con el mínimo detalle, por ejemplo, cambiar una i con una ele. Si tienes dudas, no hagas clic ni bajes ningún archivo.	La autentificación de dos pasos nos permite añadir una segunda capa de seguridad para acceder a nuestras cuentas de Internet. Es decir, si logran obtener tu contraseña, el segundo paso de la verificación podría impedir sus propósitos.	Si recibimos documentación sospechosa, deberíamos verificarla antes de abrirla. En estos casos, no haga clic en el archivo para descargarlo. En su lugar, ábrelo en Google Drive u otro lector de documentos en línea. Esto convertirá el documento en una imagen o en HTML, lo que casi con seguridad le impedirá instalar software malicioso en su dispositivo. Una vez verificada la legitimidad del archivo, lo puedes bajar.	Los ataques de phishing que utilizan malware, a menudo se basan en vulnerabilidades en el software. Una vez que un error se conoce, un fabricante de software lanzará una actualización para solucionarlo y te avisará. No lo dejes para mañana. ¡Mantén el software actualizado de todos tus dispositivos!

51 Para más consejos para evitar el phishing, consulta https://ssd.eff.org/es/module/c%C3%B3mo-evitar-los-ataques-de-phishing--o-suplantaci%C3%B3n-de-identidad

Actualiza tu software

Actualizar tus dispositivos es básico para tu seguridad digital, ya que las compañías desarrolladoras constantemente descubren vulnerabilidades en sus programas, así como nuevas amenazas de seguridad, como malware. Muchas personas aprovechan estos fallos para realizar ataques informáticos.

En respuesta, los desarrolladores lanzan actualizaciones y parches para remediar las vulnerabilidades, por lo que es necesario que mantengas al día tu sistema operativo y los softwares que utilizas. Aunque no representan una garantía infalible, las actualizaciones sí reducen considerablemente el riesgo de ser víctima de un ataque.

¿Están intervenidos mis dispositivos?

Es casi imposible saberlo sin la intervención de especialistas, por lo que NO creas en test que corren por Internet, pues muchos de ellos pueden además ser ataques maliciosos. Por eso, es importante activar las medidas de precaución, en el entendido que parte importante de los malware de actores particulares o estatales peligrosos se aprovechan de vulnerabilidades en los softwares, como también de ataques de phishing. Si tienes dudas fundadas, mejor contactar y consultar a CiviCERT (Computer Incident Response Center for Civil Society).

Usa comunicaciones cifradas

El cifrado es el proceso matemático de hacer que un mensaje sea ilegible, excepto para la persona que posee la clave para descifrarlo en forma legible. Es decir, aun cuando un tercero puede interceptarlo, si está cifrado, lo verá en clave matemática y no podrá comprenderlo. El cifrado en las comunicaciones puede darse en diversos niveles en nuestros distintos canales de comunicación, y que supondrán más o menos esfuerzos de adopción dependiendo del canal.

Hay diversas formas de adoptar el cifrado en nuestras comunicaciones, como usar VPN cuando utilizamos una WiFi pública,[52] usar https en nuestra web y en las que visitamos,[53] o aprender a cifrar nuestros correos,[54] entre otras acciones.

52 Ver https://www.adslzone.net/reportajes/internet/mejores-vpn-gratis/

53 Ver https://es.wikipedia.org/wiki/HTTPS_Everywhere

54 Ver https://ayudaleyprotecciondatos.es/2021/07/10/cifrar-correo-electronico/

Pero debido a la masividad de su uso, es importante optar por servicio de mensajería cifradas que puede ser clave para, al menos, las comunicaciones políticas que tengas. Los niveles de seguridad de las plataformas siempre van variando de acuerdo a distintos factores, por lo que es importante estar siempre informada. De todas formas, te presentamos información básica de los servicios de chats que pueden orientarte en tus decisiones de comunicación.





Signal	WhatsApp	Telegram	Wire	Facebook Messenger
Es una solución gratuita de mensajería, llamadas de voz y chat grupal todo en uno que utiliza su propio cifrado de extremo a extremo. El protocolo de cifrado de Signal es tan fuerte que WhatsApp y Facebook Messenger también lo usan. Pero a diferencia de Facebook, la empresa matriz de Signal es una fundación sin fines de lucro.	Utiliza el protocolo de cifrado de extremo a extremo de Signal en todos los mensajes desde 2016, y ha agregado continuamente ajustes a las funciones de seguridad y privacidad de la aplicación, como invitaciones y controles de grupo ajustados para que la persona usuaria esté siempre consciente de quién está leyendo tus chats grupales. WhatsApp ahora es propiedad de Facebook, algunos datos de comportamiento de las y los usuarios de WhatsApp ahora se comparten con Facebook, pero los mensajes permanecen completamente aislados.	A diferencia de otras aplicaciones de mensajería cifrada, el cifrado de extremo a extremo no está habilitado de forma predeterminada en Telegram. Para obtenerlo, se debe optar por un modo de chat secreto.	Cuenta con cifrado de extremo a extremo para mensajes instantáneos, llamadas de voz y video. Utiliza su propio protocolo de cifrado basado en el protocolo Signal, y su código es de código abierto y está sujeto a auditorías de seguridad externas. Las versiones móvil y web de la aplicación son gratuitas, con un nivel premium disponible para empresas.	Las versiones móviles de la aplicación incluyen opciones de comunicación cifrada de extremo a extremo en forma de conversaciones secretas (Secret Conversations). Basado en el mismo sistema de encriptación utilizado en Signal, Secret Conversations requiere que los usuarios opten por la función. Sigue siendo vulnerable a que lo capturen de pantalla, y las limitaciones de suscripción y de un solo dispositivo pueden ser un problema. Además, es de Facebook.

Para cualquier canal de comunicación que uses, recuerda deshabilitar la previsualización de los mensajes en la pantalla de inicio de tu dispositivo móvil. Un extraño puede ver fácilmente información importante.

ACCIONES DE SEGURIDAD DIGITAL EN REDES SOCIALES

Las redes sociales son, reconocidamente, uno de los espacios donde más se recibe violencia política de género en Internet. Por eso, además de la capa básica de seguridad digital que vimos en la sección anterior, es importante agregar otras herramientas y comportamientos específicos.

Gestiona tu identidad digital

Parte importante de nuestra vida personal, social y política ocurre en plataformas digitales que son provistas por empresas privadas, por lo que son parte de una estrategia para conseguir utilidades. Como hemos visto en el primer apartado de esta guía, parte importante de estas plataformas tienen como base el modelo de negocio de ofrecer servicios gratuitos a cambio de recolectar los datos personales de las personas, por lo que muchas de sus lógicas buscan persuadir a las personas a que compartan todo tipo de pensamientos y relaciones. Esto incluye que las configuraciones de privacidad de datos que vienen por defecto en las redes sociales son siempre mínimas.

En ese contexto, ocurren nuestras vidas personales, sociales y políticas. Aquello significa que es importante que tengamos claro la extensión del uso de nuestra identidad digital y la gestionemos de acuerdo con nuestros objetivos y, también, nuestro modelo de riesgo.

Gestionar nuestra identidad digital es tener el mayor control posible sobre qué datos personales de mí (y de lo que me rodea) quiero que esté publicado en Internet. Esto es particularmente importante para mujeres en política, pues muchos ataques hoy son recibidos en base a datos personales que los agresores manejan.

Para hacerlo, te recomendamos algunas acciones que pueden resultarte útiles:

Verifica tus cuentas de redes sociales

Este es un servicio que ofrecen las redes sociales para poder autentificar las cuentas y verificar que, quien dice que es la persona dueña de la cuenta, lo es. Cada plataforma brinda un sello público de cuenta verificada, que ayuda al público tener información concreta de la

fuente y, para la persona dueña de la cuenta, evitar el robo de identidad o la confusión con cuentas parecidas, como parodias.

Con todo, algunas advertencias:

- Las cuentas verificadas pueden presentar un riesgo de seguridad para sus propietarios, ya que llaman la atención de los piratas informáticos que pueden intentar tomar el control de una cuenta verificada para comercializar el perfil según el sello y el número de seguidores.
- En general, no es posible transferir una cuenta verificada a otra. Las cuentas verificadas no pueden cambiar el nombre de la cuenta o transferir esa verificación a una cuenta diferente. Dado que el propósito del sello de verificación es que las personas sepan que la cuenta ha sido revisada.
- No es un ejercicio automático y muchas veces la verificación es denegada, sin muchas explicaciones del porqué por parte de las plataformas.

Actualmente, servicios populares de redes sociales que ofrecen verificar las cuentas, son, entre otras: Twitter, Instagram, Facebook y YouTube.

En su campaña ¡verifique las cuentas oficiales de sus redes sociales! Así, podrá tener un canal oficial de comunicación con las personas y podrá aminorar el riesgo de suplantación de identidad.

Compartimenta cuentas de redes sociales y de mensajería

Tu identidad digital no tiene por qué ser una sola. ¡Puedes tener varios perfiles, distintos dispositivos! Por eso es importante que pienses estratégicamente tus comunicaciones, sobre todo cuando tienes una actividad política. ¿Qué tipo de interacciones vas a tener? ¿Vas a compartir esa foto de tu familia? ¿Puede esa información que estoy publicando brindar más pistas de lo deseado de mi paradero?

Una recomendación común es, si así lo concluyes de tu modelo de riesgo, dividir tu identidad digital en una de carácter más personal (donde compartes información solo con tu círculo más cercano y quizás uses un pseudónimo) y otra, pública, donde compartes con el resto de las personas.

Configura la privacidad en las plataformas que usas, en especial, redes sociales y mensajería

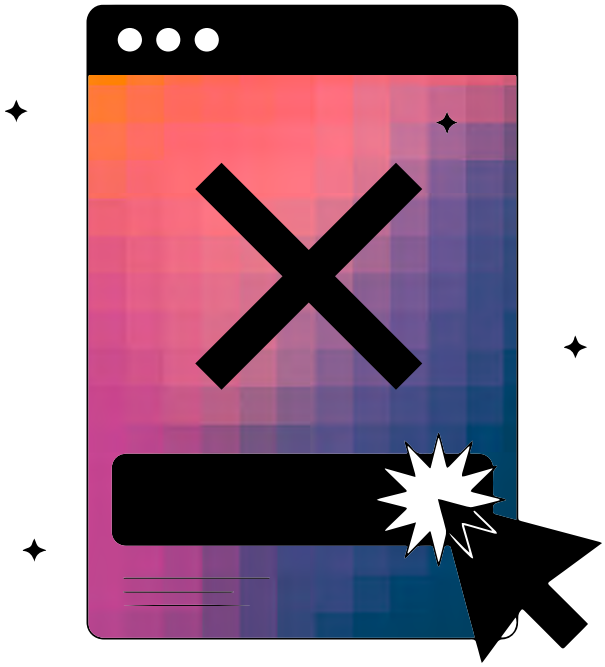
Una vez que tienes definida la forma en que va a desenvolver tu identidad digital, revisa y modifica las configuraciones de privacidad de tu cuenta, de acuerdo con tu estrategia. Recuerda que hay muchas opciones, desde leer solo a la gente que sigues, silenciar interacciones que no quieres tener, desconectar la georreferenciación de tus publicaciones (que muestra las coordenadas del lugar donde estás publicando), limitar a las y los usuarios que pueden enviarte mensajes directos, entre tantas otras que pueden mejorar tu experiencia online.

No dejes la configuración de privacidad que por defecto tienen las redes sociales, porque siempre serán las mínimas posibles. Revísalas constantemente porque, debido a los cambios en Términos y Condiciones, las plataformas pueden cambiarlas. No tengas miedo de experimentar con ellas: no vas a romper Internet si pruebas con las opciones y siempre puedes volver atrás.

Bloquea el odio

Las redes sociales cuentan con mecanismos de seguridad que permiten a las y los usuarios bloquear, silenciar y denunciar los contenidos abusivos, pero se trata de un proceso que lleva mucho tiempo puesto que, sí o sí, requiere leer las publicaciones negativas y decidir cómo responder o no.[55]

Para ahorrar tiempo y energía, y para evitar perder accidentalmente información importante y comentarios acertados, existen herramientas como Block Party para Twitter.[56] Con Block Party puedes filtrar los tuits según una serie de criterios y guardarlos en una carpeta separada. Por ejemplo, puedes apartar los comentarios de las cuentas nuevas o las que no tienen foto de perfil, que tienen más probabilidades de ser cuentas falsas o incluso bots creados para enturbiar los debates o intimidar a los usuarios legítimos. Luego, puedes revisar los tuits más tarde, cuando estés mentalmente preparada, o incluso puedes pedirle a otra persona que los revise por ti.



55 Ver https://help.twitter.com/es/safety-and-security/control-your-twitter-experience

56 Ver https://www.blockpartyapp.com

ACCIONES DE SEGURIDAD EN VIDEOCONFERENCIAS

Debido a las restricciones de movilidad obligatorias por la pandemia de COVID-19, en muchos países se vivió un aumento masivo de reuniones virtuales a través de plataforma electrónicas, como Google Meet, Jitsi o Zoom, entre otras.

En ese contexto, también se popularizó un fenómeno bastante común: las invasiones no deseadas de las reuniones virtuales para capturarlas y proferir mensajes violentos, muchos de ellos misóginos y racistas. Las actividades feministas fueron particularmente afectadas. Por la popularidad de la plataforma Zoom y sus, hasta entonces, pobres medidas de seguridad, a ese fenómeno se le conoció como zoombombing.

Debido a que las conferencias y seminarios públicos de manera online son fundamentales en campañas políticas, es muy importante tener en cuenta acciones de seguridad al organizarlas.

¿Qué plataforma de videollamada elegir?

De acuerdo con la organización latinoamericana Derechos Digitales en su guía especial para elegir una herramienta de videollamada, no hay ninguna plataforma perfecta, por lo que la idoneidad de un software dependerá en gran medida de las necesidades específicas de la videollamada, como: ofrecer seguridad contra la interceptación de llamadas, su costo monetario, su masividad, la posibilidad de grabar, entre otros.

Para determinar qué herramienta puede ser interesante para tus necesidades, te recomendamos consultar el diagrama especial que Derechos Digitales tiene en su guía.[57]

Prevenir el zoombombing

- ***Genera un ID (identificación) de reunión aleatorio:*** evite poner nombres en la reunión porque pueden ser fácilmente adivinables, utilice IDs aleatorios que muchas de las plataformas permiten.

- ***Control sobre personas invitadas:*** No compartir masivamente el link de la reunión. Se recomienda usar la función que permite proteger las juntas virtuales vía contraseña de acceso, así como hacer uso de las salas de espera en las que los participantes pueden estar mientras el anfitrión prepara la reunión técnicamente. Luego, este último puede aprobar la integración de las personas que están en la sala de espera.

- ***Mantén el control de la pantalla:*** El anfitrión debe mantener en todo momento el control de lo que se transmite en pantalla, si un participante quiere compartir contenido, es recomendable que lo envíe previamente al anfitrión para su transmisión en reunión; o que antes de abrir masivamente la reunión, le dé la posibilidad de compartir la pantalla a esa persona.

- Si ocurre un ataque, el anfitrión puede hacer uso de las medidas de seguridad, como eliminar a los intrusos de la reunión, limitar el uso de pantallas compartidas y restringir el chat.[58]

57 Ver https://www.derechosdigitales.org/wp-content/uploads/pub_videollamadas.pdf

58 Particularmente para ver los pasos de seguridad en la plataforma Zoom, ver https://cudi.edu.mx/noticia/recomendaciones-de-seguridad-para-administradores-de-las-cuentas-zoom-del-servicio-vc-cudi

Acciones de seguridad para evitar la desinformación y las noticias falsas

La desinformación es uno de los ataques que, últimamente, más preocupación conlleva respecto a la gobernanza de Internet y los debates respecto a la libertad de expresión; aún más, muchos Estados la consideran como parte de ataques a su ciberseguridad. En el caso de la violencia política de género digital, generalmente, la desinformación toma forma en campañas de desprestigio hacia la lideresa (destinadas a desacreditarla) y la difusión de información falsa (a menudo vinculada a la sexualidad y el matrimonio).

Si bien se trata de un problema complejo, de múltiples capas, que excede los hábitos de seguridad digital y que dependen de acciones de las comunidades, los Estados, pero también de las plataformas, sí hay acciones que nos pueden ayudar a enfrentarla mejor desde la seguridad digital.

Verificar la información que se comparte

No difundas noticias falsas, un perfil político responsable debe ser muy cuidadoso con esto porque puedes recibir reacciones muy fuertes debido a eso. Acá, cinco formas para evitar la desinformación en redes sociales y mensajería:

- Antes de compartir, verifica la fuente: al calor de la inmediatez de las redes sociales o de otros medios de comunicación como los chats, compartimos todo, de inmediato, sin verificar antes. Nuestra acción consciente y la de la comunidad puede terminar con la cadena de desinformación. Si la fuente es desconocida o sospechosa, simplemente no compartas. Hay muchos sitios web que parece ser legítimos pero que no cumplen estándares mínimos de veracidad.

- No te dejes llevar por el clickbait. Este último es un concepto que refiere a los contenidos diseñados intencionadamente para captar la atención de la gente y que hagan clic sobre él. En otras palabras, es una suerte de sensacionalismo que busca captar la atención. Esta técnica es muchas veces usada en las campañas de desinformación. Recuerda, el título o el resumen muchas veces dista de los contenidos. Antes de compartir, lee y verifica.

- Fíjate en la fecha de publicación. Algo tan simple, es crucial. Muchas veces se comparten, maliciosamente, noticias antiguas sin informar la fecha, como forma de agregar polémica a una discusión actual. Hay que tomarse algunos segundos y verificar la fecha, si no la tiene, buscar la noticia y ver si hay otro portal que la haya tomado con seriedad y verificar allí.

- Envía la noticia a chequeadores especializados de noticias falsas en tu país (muchas veces conocidos como fact-checkers).

- Denuncia los perfiles falsos en las redes sociales que lo permitan.

Piensa estratégicamente antes de discutir con un bot

Cada vez es más dificultoso saber si es una cuenta automatizada o semiautomatizada.
Hay, de todas formas, algunos consejos para sopesar si se trata estos perfiles: a) si el perfil tiene una fecha reciente de creación, b) si tiene mensajes repetitivos y/o 3) si la imagen personal que usa no es personalizada o si fue

creada por Inteligencia Artificial con el fin de simular una persona real.[59]

En Twitter, por ejemplo, puedes restringir ver perfiles sin verificación de teléfono o que no tienen avatar, que podrían también buscar ciertos grados de anonimato para atacar.

Ahora bien, como muchos de estos perfiles están hechos para fines maliciosos, debes dejar atrás la idea de que puedes entablar condiciones de diálogo, y **sopesar, estratégicamente, si quieres engancharte en interacciones con ellos.** Esto, porque siempre debes recordar que en las redes sociales la "atención" se premia con visibilidad, por lo que contestar o no contestar se transforma en proyectar cuánta visibilidad le quieres dar al diálogo y a extender el mensaje.

Una estrategia, por ejemplo, puede ser ver cuánta visibilidad tiene el mensaje de odio o desinformación que la fuente original tiene, por ejemplo, a través de cuántas veces se ha compartido el mensaje. Si, efectivamente tiene un alcance importante, quizás puedas planificar una respuesta. Si este es el caso, debes estar preparada para tener, probablemente, una avalancha de respuestas de apoyo y rechazo. Que aquello ocurra, jugando las reglas de los algoritmos de redes sociales, estaría bien porque lleva tu mensaje a más personas. De todas formas, puedes silenciar las respuestas de tu mensaje o permitir que solo te responda la gente que sigues, de tal forma de evitar interacciones peligrosas.

Sé estratégica con tus publicaciones

Las reglas de comunidad, también conocidas como los términos de servicios, son los parámetros que las plataformas tienen para definir qué contenidos son o no aceptables en su plataforma. Son variopintos, pueden variar mucho entre plataformas y muchos de ellos entran en conflicto con la libertad de expresión. Por ejemplo, Instagram no acepta la publicación de pezones femeninos, sí masculinos, lo que ha impactado también sobre la censura de mucho activismo feminista en la plataforma. O en Facebook y Twitter hay pruebas de que se censura el discurso palestino.[60]

Más allá de que las acciones de las plataformas sean legítimas o incluso legales, es importante ser consciente en las publicaciones que se hacen, pues muchas pueden ser maliciosamente denunciadas, por lo que no solo pueden bajar la publicación sino hasta penalizar tu perfil. En ese sentido, es importante sopesar qué mensajes vas a entregar y, si se está dispuesto a correr el riesgo, tomar todas las medidas pertinentes como multiplicar los canales de comunicación de tu campaña (incluido, ojalá, un sitio web propio donde la gente pueda encontrar información sobre su perfil político, y que esos contenidos no dependan de las reglas de las redes sociales).

Las reglas de las plataformas, además, cambian cada cierto tiempo. Para tener un registro de los últimos cambios, puedes consultar el proyecto del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Universidad de Palermo, Letra Chica.[61] Respecto a lo que se considera violencia, Facebook pone a disposición consejos de qué pu-

59 Ver https://www.xataka.com/robotica-e-ia/asi-puedes-superar-test-para-detectar-que-fotos-celebrities-han-sido-creadas-mediante-inteligencia-artificial

60 IFEX (2021) Facebook and Twitter must immediately stop censoring Palestinian content https://ifex.org/facebook-and-twitter-must-immediately-stop-censoring-palestinian-content/

61 Ver https://letrachica.digital/

blicar o no en sus plataformas que vale la pena conocer pues, en general, podrían aplicarse en campañas políticas.[62]

Borra publicaciones antiguas masivamente de tus redes sociales

Si usas redes sociales y tu línea estratégica de publicaciones ha cambiado con el tiempo, quizás te interese borrar publicaciones antiguas. Muchas veces, los ataques de acoso se hacen reflotando publicaciones que hiciste hace muchos años y, otras veces, su publicación años después forman parte de estrategias de desinformación más producidas.

Borrar publicaciones de Twitter manualmente es casi imposible, sobre todo si tienes un perfil durante años. Para hacerlo de forma más cómoda, hay diversas herramientas que te pueden servir, muchas de ellas son de pago.[63] En Facebook, por ejemplo, puedes borrar y también restringir las publicaciones antiguas.[64]

Otra práctica relacionada que puedes adoptar es el hábito de borrar tus publicaciones en las redes sociales cada cierto periodo de tiempo.

Borra o desactiva las cuentas que ya no usas

Las cuentas que ya no usas pueden ser una fuente de tergiversaciones para campañas de desinformación o, también, fuente de información que ya no quieres compartir. Borra aquellas cuentas que ya no usas. Ojo, puede tomar tiempo: redes sociales como Facebook, por ejemplo, se toman algunas semanas antes de borrar completamente la cuenta.

62 Ver https://transparency.fb.com/es-la/policies/community-standards/violence-incitement/?from=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fcredible_violence

63 Ver https://expansion.mx/tecnologia/2021/08/05/como-borrar-tweets-viejos-masivamente

64 Ver https://www.adslzone.net/como-se-hace/facebook/borrar-publicaciones-antiguas-facebook/

MÁS RECURSOS DE AYUDA

A continuación, un listado de más recursos de ayuda que pueden apoyar a las personas políticas y sus equipos en saber más acciones de seguridad

TIPO	NOMBRE	DESCRIPCIÓN
Mesas de ayuda	Vita Activa[1]	Línea de ayuda para víctimas de violencias de género online para América Latina.
	Línea de Ayuda de Seguridad Digital de Access Now[2]	Trabaja con individuos y organizaciones de todo el mundo para mantenerlos seguros en línea. Si está en riesgo, ayudan a mejorar sus prácticas de seguridad digital para mantenerse fuera de peligro. Si ya está bajo ataque, proporcionan asistencia de emergencia de respuesta rápida.
Seguridad digital en protesta	Karisma: Tips de seguridad digital: antes, durante y después de una protesta[3]	Información sobre algunas de las preguntas más recurrentes que hemos recibido de parte de las personas que están ejerciendo su derecho a la protesta en las calles.
	Varias orgs: ¡No me cuidan! Contra la violencia institucional machista. Del 25N al 8M[4]	Este Kit de protesta feminista tiene el objetivo de dar herramientas para prepararnos y protegernos ante la violencia institucional machista en movilizaciones.

1 Ver https://vita-activa.org/

2 Ver https://www.accessnow.org/help/

3 Ver https://web.karisma.org.co/kit-de-seguridad-digital-para-antes-durante-y-despues-de-la-protesta/

4 Ver https://hiperderecho.org/vigilandovigilantes/assets/resources/kit-feminista.pdf

Videoconferencias	Infoactivismo: Cómo lanzar un webinar: herramientas para transmisión en vivo[5]	Opciones de herramientas y un breve paso a paso.
Seguridad digital en general	Conexo: Seguridad digital: conceptos y herramientas básicas[6]	Esta guía ha sido escrita pensando en periodistas, defensores y defensoras de derechos humanos, activistas y personas que, independientemente de su espacio de desarrollo profesional, desean iniciarse en el camino de la seguridad digital y la privacidad.
	FLIP: Manual Antiespías: herramientas para la protección digital de periodistas[7]	Tiene como objetivo mejorar el conocimiento y conciencia sobre la seguridad digital de la información y las comunicaciones.

5 Ver https://infoactivismo.org/como-lanzar-un-webinar-herramientas-para-transmision-en-vivo/

6 Ver https://conexo.org/project/921/

7 Ver https://www.flip.org.co/images/Documentos/manual-antiespias.pdf

AUTORA:

Paz Peña (pazpena.com) es una consultora independiente y activista en materia de tecnologías,
feminismo y justicia social. Es la cocreadora de Acoso.Online, un recurso web que proporciona información y recomendaciones fiables para las víctimas de la difusión no consentida de imágenes íntimas en Internet en 19 países de América Latina, el Caribe y España. Es periodista, licenciada en Comunicación Social (Pontificia Universidad Católica Valparaíso, Chile) y máster en Estudios de Género y Cultura (Universidad de Chile).

FICHA TÉCNICA

Fundación Friedrich Ebert en Chile
Hernando de Aguirre 1320 I Providencia I
Santiago de Chile

Responsable

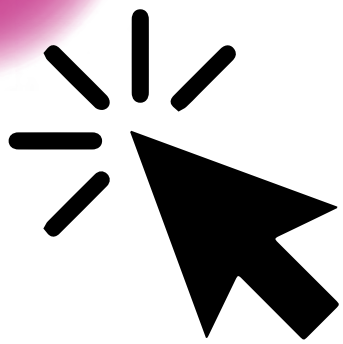
Dr. Cäcilie Schildberg
Directora del Proyecto Regional
FESminismos | Representante de la FES Chile

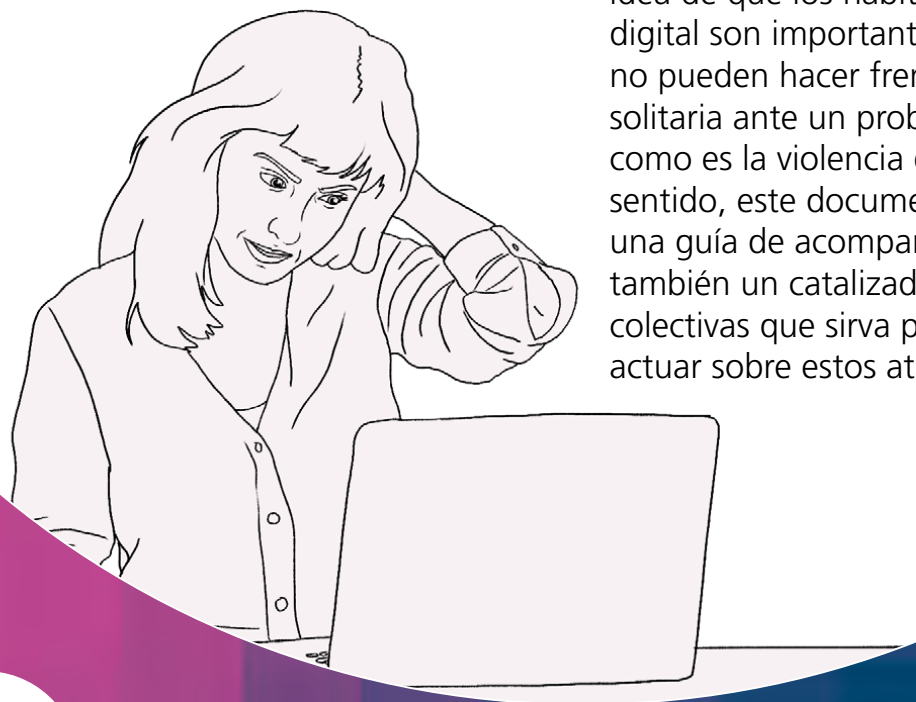
Sarah Herold
Coordinadora del Proyecto Regional
FESminismos
www.fes-minismos.com
@fesminismos

Edición / corrección: Matías Galleguillos Muñoz

Diseño y diagramación: María Elvira Espinosa Marinovich

ISBN 978-956-6138-16-7





La violencia política contra las mujeres comprende todo acto de violencia basada en el género, o la amenaza de esos actos, que se traduce, o puede resultar en daños físicos, sexuales o psicológicos o sufrimiento, y está dirigida contra la mujer en la política por su condición de mujer.

Esta es una guía de recomendaciones en seguridad digital y con enfoque feminista para las personas y organizaciones que enfrentan violencia política de género digital.

Es un trabajo que quiere reforzar la idea de que los hábitos de seguridad digital son importantes, pero que no pueden hacer frente como carta solitaria ante un problema estructural como es la violencia de género. En este sentido, este documento espera ser una guía de acompañamiento, pero también un catalizador de actividades colectivas que sirva para resistir y actuar sobre estos ataques.

FESMINISMOS

#TOMAPARTIDO

FRIEDRICH EBERT STIFTUNG