Curso para
CANDIDATAS ELECTORALES

Violencia digital contra las mujeres en la vida política:

Cómo identificarla y estrategias para combatirla

OEA | CIM

MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN
aecid
Cooperación Española

Violencia digital contra las mujeres en la vida política:

Cómo identificarla y estrategias para combatirla

Dirección General:
Alejandra Mora Mora, Secretaria Ejecutiva de la Comisión Interamericana de Mujeres (CIM) de la Organización de los Estados Americanos (OEA)

Elaboración del documento:
Marta Martinez y **Lucía Martelotte**

*La **Organización de los Estados Americanos** (OEA) reúne a los países del hemisferio occidental para promover la democracia, fortalecer los derechos humanos, fomentar el desarrollo económico, la paz, la seguridad, la cooperación y avanzar en el logro de intereses comunes. Los orígenes de la Organización se remontan a 1890, cuando las naciones de la región formaron la Unión Panamericana con el objetivo de estrechar las relaciones hemisféricas. Esta unión se convirtió en la OEA en 1948, luego que 21 naciones adoptaran su Carta. Desde entonces la Organización se ha expandido para incluir a las naciones del Caribe de habla inglés y Canadá, y hoy todas las naciones independientes de Norte, Sur y Centroamérica y el Caribe conforman sus 35 Estados miembros.*

*La **Comisión Interamericana de Mujeres** (CIM) es el principal foro generador de políticas hemisféricas para la promoción de los derechos de las mujeres y la igualdad de género. Creada en 1928 - en reconocimiento de la importancia de la inclusión social de las mujeres para el fortalecimiento de la democracia y del desarrollo humano en las Américas - la CIM fue el primer órgano intergubernamental establecido para promover los derechos humanos de las mujeres.*

Violencia digital contra las mujeres en política: Cómo identificarla y estrategias para combatirla

Esta publicación cuenta con la colaboración de la Cooperación Española a través de la Agencia Española de Cooperación (AECID). El contenido de la misma es responsabilidad exclusiva de la Comisión Interamericana de Mujeres y no refleja, necesariamente, la postura de la AECID.

OAS Cataloging-in-Publication Data
Inter-American Commission of Women.
Violencia digital contra las mujeres en política: Cómo identificarla y estrategias para combatirla / [Comisión Interamericana de Mujeres].
p.; 21x29,7 cm. (OAS. Official Records; OEA/Ser.L/II.6.44)

ISBN 978-0-8270-7687-7

1. Women's rights. 2. Women--Violence against--America. 3. Computer crimes--America. 4. Computer security--America. I. Title. II. Series.

OEA/Ser.L/II.6.44

Comisión Interamericana de Mujeres (CIM)
cim@oas.org
http://www.oas.org/cim
/ComisionInteramericanaDeMujeres
@CIMOEA

Diseño y diagramación: Patricio Bascuñán

1. Identificar la violencia digital contra las mujeres en la vida política

1.1 Definición del problema

La "Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer" (1994) o "Convención Belén do Pará, en su artículo 3, establece el derecho de todas las mujeres a vivir una vida libre de violencia, tanto en el ámbito público como el privado. Esta definición tiene alcance al ámbito digital y, en general, a todos los ámbitos donde las mujeres desarrollen sus relaciones interpersonales.

La Ley Modelo Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra las Mujeres en la Vida Política (2017), elaborada en el marco de la Convención de Belém do Pará, define a la violencia contra las mujeres en política (VCMP) como: "Cualquier acción, conducta u omisión, realizada de forma directa o a través de terceros que, basada en su género, cause daño o sufrimiento a una o a varias mujeres, y que tenga por objeto o por resultado menoscabar o anular el reconocimiento, goce o ejercicio de sus derechos políticos. La violencia contra las mujeres en la vida política puede incluir, entre otras, violencia física, sexual, psicológica, moral, económica o simbólica" (artículo 3).

Naciones Unidas define la violencia digital contra las mujeres como "*Cualquier acción o conducta en contra de la mujer, basada en su género, que le cause muerte, daño o sufrimiento físico, sexual o psicológico, económico o simbólico, en cualquier ámbito de su vida, la cual es cometida, instigada o agravada, en parte o en su totalidad, con la asistencia de las tecnologías de la información y comunicación*." (Párrafo 22).

"....todo acto de violencia por razón de género contra la mujer cometido, con la asistencia, en parte o en su totalidad, del uso de las TIC, o agravado por este, como los teléfonos móviles y los teléfonos inteligentes, Internet, plataformas de medios sociales o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada."(Párrafo 23)[1].

1 El Informe del Mecanismo de Seguimiento de la Convención de Belém do Pará (MESECVI) en 2018, retoma la definición de violencia digital/violencia en línea contra las mujeres del Informe de la Relatoría Especial de Naciones Unidas sobre "la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos" (2018).

Por lo tanto, la violencia digital contra las mujeres en la vida política puede entenderse como:

> Cualquier acción, conducta u omisión, realizada de forma directa o a través de terceros que, basada en su género, cause daño o sufrimiento a una o a varias mujeres, la cual es cometida, instigada o agravada, en parte o en su totalidad, con la asistencia de las tecnologías de la información y comunicación y que tiene, por objeto o por resultado, menoscabar o anular el reconocimiento, goce o ejercicio de sus derechos políticos

1) **Está basada en el género** (es decir que se dirige a las mujeres por el hecho de ser mujeres, tiene efectos desproporcionados o impactos diferenciados sobre las mujeres, y adquiere formas específicas)

2) **Causa daño o sufrimiento**

3)Es cometida, instigada o agravada, en parte o en su totalidad, con la **asistencia de las tecnologías de la información y comunicación**

4)Tiene como objetivo o resultado **impedir total o parcialmente a las mujeres el ejercicio de sus derechos políticos**

Además, la VDCMP tiene las siguientes características:

- **Forma parte de un contexto de discriminación de género y violencia sistémica contra las mujeres que se da en todos los ámbitos de su vida.** No debemos caer en el error de considerar que la violencia digital es un fenómeno separado de la violencia en el mundo "real", pues forma parte de la violencia que las mujeres ya vivían fuera de internet. Estamos hablando del mismo viejo sistema de dominación y violencia de género del que hablamos siempre, que ahora usa una nueva plataforma para replicarse.

- **Continuum de la violencia online/offline (en línea y fuera de línea).** El ciberespacio y la vida cotidiana fuera de línea están cada vez más imbricados. Una manifestación de violencia puede comenzar o ser instigada online y trasladarse a la vida fuera de línea de las mujeres, poniendo en juego su integridad física, su salud y bienestar, incluso su vida.

- **Inmediatez:** tienen impacto en tiempo real independientemente de la dimensión espacial/geográfica.

- **Replicabilidad:** puede escalar y amplificar el alcance por la rapidez de la replicación (viralización) de los mensajes y contenidos.

- **Anonimato:** las personas o grupos de personas que la realizan pueden 'ocultarse' tras pseudónimos, cuentas impersonales o colectivas, lo que dificulta su identificación.

- **Permanencia:** los contenidos (mensajes, audios, imágenes, videos) quedan en línea y/o pueden ser archivados para ser republicados posteriormente.

- **Transfronterizos:** los hechos pueden ser cometidos, instigados y/o agravados por personas o grupos de personas por fuera de la jurisdicción del Estado en el que reside o se encuentra la víctima.

Test para identificar las TICs que han utilizado para ejercer VDCMP, marque con una X las opciones que correspondan a su experiencia:

La violencia digital puede ser cometida, instigada o agravada en[2]:		**A través de dispositivos tecnológicos tales como:**	
Redes sociales (Instagram, Twitter, Facebook, Reddit, YouTube, Tik Tok, Snapschat y Tumblr y otras)		Teléfonos móviles e inteligentes, tabletas, computadoras,	
Comunicaciones de telefonía móvil		Sistemas de posicionamiento global (GPS)	
Sitios de microblogs y otros sitios (medios de comunicación)		Dispositivos de audio, cámaras, o asistentes virtuales	
Aplicaciones de mensajería (WhatsApp, Snapchat, Messenger, Weibo y Line)			
Otras aplicaciones (de cita, etc.)			

2 Todas estas son organizaciones o empresas del sector privado, intermediarias de internet de diversos tamaños (gigantes de la tecnología o start ups)radicadas en diversas partes del mundo.

1.2 Principales manifestaciones de la violencia digital contra las mujeres en la vida política

- Incluye un espectro muy variado de prácticas violentas y comportamientos dañinos u ofensivos facilitados por las TIC, que pueden constituir ofensas, faltas e incluso delitos.
- En función de esto ameritan **diversas respuestas: administrativa, civil o penal** según lo establecido en las normativas nacionales, regionales e internacionales que regulan sobre la materia.
- **El listado de tipos y manifestaciones de violencia digital contra las mujeres en la vida política no es exhaustivo ni cerrado:** las tecnologías, internet, la inteligencia artificial avanzan y se transforman permanentemente, pueden surgir nuevos tipos y manifestaciones de violencia digital contra las mujeres políticas.
- Estas formas de violencia en muchos casos son interdependientes y se habilitan o se potencian entre sí, **suelen darse de manera combinada, y se encadenan** en un espectro que va escalando y aumentando los niveles la violencia.
- En el **continuum "online/offline"** la violencia puede comenzar o ser instigada en un ámbito y rápidamente trasladarse al otro (y viceversa), también escalando los niveles de violencia.

Violentómetro:

¿Cómo escala y se encadena la violencia digital contra las mujeres en la política?

Fuente: gráfico elaborado en base al Violentómetro Digital del Frente Nacional para la Sororidad de México de Defensoras Digitales, y del Informe "Violencia de género en línea hacia mujeres con voz pública. Impacto en la libertad de expresión" de ONU Mujeres. Argentina (2022), en la sección "Cómo escala la violencia en línea", página 27, y adaptado a las categorías y conceptos utilizados en el presente documento (fuentes ya mencionadas).

1.3 Efectos sobre las mujeres de la violencia digital contra las mujeres en la vida política

Los sitios de internet, las plataformas y, en especial, las redes sociales son **un espacio con especial relevancia en la dinámica política y en el debate público,** se han convertido en plataformas importantes para la participación política, para expresar ideas y potenciar la voz.

Las consecuencias de la violencia de género online muchas veces son relativizadas debido a la idea de que lo online "no es real". Para las mujeres que la enfrentan, conlleva diversas violaciones de sus derechos: el derecho a una vida libre de violencia, el derecho a ejercer todas las funciones públicas, el derecho a la libertad de expresión, el derecho a la intimidad, entre otros. Además, causa en las víctimas daños y sufrimientos psicológicos, físicos, sexuales y/o económicos, y tiene efectos familiares, sociales y colectivos. Se trata de discursos y acciones que tienen como objetivo silenciar las voces de las mujeres, controlar su participación en línea y la construcción de sus perfiles, limitar su presencia en línea; ello restringe el ejercicio de los derechos políticos.

En el ámbito político suele estar naturalizada como "parte de las reglas de juego" o como "un costo necesario" para participar, hacer oír su voz o defender determinadas agendas de igualdad. Este es un problema que afecta gravemente a la calidad de la democracia, pues restringe el pluralismo de voces y miradas en el debate público que se produce en el mundo digital, así como la igualdad sustantiva.

La violencia digital contra las mujeres en la política afecta a todas las mujeres en su condición de tales; pero no afecta a todas en igual manera y/o intensidad. Como sucede con la violencia política fuera de internet, la violencia digital por razones de género interactúa con otros determinantes sociales estructurales e identitarios que, al ser mecanismos de exclusión pone en mayor riesgo de ser víctimas a ciertos grupos de mujeres; entre ellos: la raza, la etnia, nacionalidad, estrato socioeconómico, orientación sexual, identidad de género, entre otros. Estos grupos de mujeres pueden ser objeto de algunas formas específicas de violencia digital, con consecuencias agravadas y/o persistentes. Esta violencia puede afectar en mayor medida a mujeres activistas (por los derechos humanos y por la agenda feminista) en especial jóvenes, mujeres políticas, mujeres rurales, de pueblos originarios, afrodescendientes, migrantes, con discapacidad y/o pertenecientes al colectivo LGBTIQ+, entre otras.

Test para identificar los efectos de la VDCMP, marque con una X las opciones que correspondan en su experiencia:

Dimensiones	Efectos	
Restricciones a la movilidad fuera de línea, y a la seguridad	• Cambiar de dirección física debido a amenazas recibidas en los espacios virtuales/en línea • Solicitar acompañamiento para el traslado/circulación a personas de mi entorno de confianza • Solicitar formalmente al Estado protección de las fuerzas de seguridad, de manera temporal o permanentemente • Contratar seguridad privada, de manera temporal o permanentemente • Evitar hacer públicas las agendas, modificar circuitos cotidianos, traslados y/o medios de transportes públicos rutinarios para garantizar mi seguridad	
Psicológicos y padecimiento emocional	• Sufrir padecimientos subjetivos, psicológicos y emocionales tales como: depresión, ansiedad, estrés, miedo, ataques de pánico, angustia, pérdida de confianza en sí misma, trastornos del sueño, irritabilidad, frustración • Sufrir impactos en la vida sexual a raíz de situaciones de ciberviolencia de diversa gravedad y reiteración (ciberacoso, violación a la privacidad, desprestigio, amenazas a la vida, a la integridad física y/o sexual) • Tener sentimientos de indefensión y vulnerabilidad frente a la falta de mecanismos de denuncia, abordaje y acompañamiento en situaciones de violencia política digital, y/o por la falta de respuesta de las autoridades (revictimización) • Tener pensamientos suicidas	
Físicos	• Sentir dolores en distintas partes del cuerpo, tensiones y contracturas • Ataques de índole físico y/o sexual luego de recibir amenazas online	
Aislamiento social	• Distanciamiento/retiro de los vínculos del entorno familiar en la vida pública, de forma permanente o temporal • Distanciamiento/retiro de los vínculos del entorno laboral en la vida pública, de forma permanente o temporal • Distanciamiento/retiro de los vínculos del entorno social/comunitario en la vida pública, de forma permanente o temporal	

Afectación de los derechos políticos	• Abandonar los espacios virtuales, temporal o permanentemente • Limitar mi participación en redes sociales, plataformas, sitios de internet por temor a recibir nuevas amenazas o represalias • Sentirme condicionada/limitada en la construcción de perfiles políticos en línea • Pérdida de su lugar en la lista (candidatura) • Pérdida de su cargo público o político y de sus ingresos • Pérdida o reducción del financiamiento del partido -u otras organizaciones- para su candidatura	
Daños económicos para las víctimas y sus familias	• Incurrir en gastos onerosos en el acceso a la justicia (pagar honorarios legales, servicios de protección en línea o fuera de línea) • Gastos de consulta para la salud mental (terapias grupales y/o individuales) y/ o problemas de salud sexual.	

Fuente: elaboración propia a partir de la tipología, categorías y definiciones establecida en el "Informe sobre ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención Belém Do Pará" de la CIM/MESECVI/OEA (2022), complementado con el Informe "La violencia en línea contra las mujeres en México. Informe para la Relatora sobre Violencia contra las Mujeres Ms. Dubravka Šimonović"; de la organización Luchadoras (2017).

1.4 ¿Quiénes pueden ejercer, instigar o reproducir violencia digital contra las mujeres en la vida política?

Test para identificar quien/quienes ejercen VDCMP, marque con una X las opciones que correspondan:

Actores	Responsabilidad primaria	Responsabilidad secundaria
En el entorno cercano (personas conocidas en la vida real)		
Persona o grupo de personas dentro del partido político propio		
Persona o grupo de personas dentro de otro partido político		
Persona o grupo de personas afiliada/s al sindicato propio		
Persona o grupo de personas de otro sindicato		
Colega/s dentro de los medios de comunicación		
Familiar/es		
Persona o grupo de personas de la comunidad/barrio		
Agentes del Estado		
Poder Ejecutivo		
Poder Legislativo		
Poder Judicial		
Otros:		
Medios de comunicación hegemónicos		
Televisión		
Radio		
Prensa gráfica		
Instituciones (entidades jurídicas), personas representantes de		
Partidos políticos		
Sindicatos		
Organizaciones no gubernamentales		
Usuarios/as de internet		
Persona/s dentro de un grupo o comunidad en las redes sociales, blog, sitios de internet, comunicaciones		
Influencers, personas formadoras de opinión en las redes y sitios de internet		
Personas, grupos de personas, comunidades desconocidas		
Bots, trolls		

** PERSONA/GRUPO DE PERSONAS QUE PERPETUAN LA VIOLENCIAN EN PRIMERA INSTANCIA: comete/n el acto inicial de violencia o abuso digital o que crea, manipula o publica por primera vez información dañina, datos personales o imágenes íntimas sin el consentimiento de la víctima.** PERSONA/GRUPO DE PERSONAS PERPETRADORAS SECUNDARIAS: participan en la continuación y propagación de un acto de violencia en línea al reenviar, descargar, volver a publicar o compartir información dañina, datos personales o imágenes íntimas obtenidas sin el consentimiento de la víctima.*
Fuente: *Elaboración propia a partir del informe "Violencia contra las mujeres en política: hoja de ruta para prevenirla, monitorearla, sancionarla y erradicarla", de ONU Mujeres, el Programa de las Naciones Unidas para el Desarrollo (PNUD) y el Instituto Internacional para la Democracia y la Asistencia Electoral (IDEA), año 2020; complementado con el "Informe sobre ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención Belém Do Pará" de la CIM/MESECVI/OEA (2022), el Informe* "Violencia política a través de las tecnologías contra las mujeres en México. Elecciones 2018" de Luchadoras (2018), y el Informe "*Conocer para resistir. Violencia de género en línea en Perú*", de la asociación civil Hiperderecho (2018).

1.5 Sobre la responsabilidad de las empresas intermediarias de internet[3]

- Son **el escenario (deslocalizado) donde se produce la violencia digital** contra las mujeres: se encuentran radicadas en diversos países del mundo, regidas por diversos marcos normativos.

- Deben **cumplir los principios de Derechos Humanos establecidos en Convenciones y Tratados internacionales** y son responsables de prevenir y mitigar la violencia digital contra las mujeres en la vida política.

- Existen crecientes demandas por **regular y legislar acerca del rol y las responsabilidades de las empresas intermediarias de internet.**

- Deben **elaborar políticas y crear mecanismos y/o características de sus productos y servicios –incorporando la perspectiva de género desde una mirada interseccional-, y que permitan proteger de manera específica a las usuarias en situación de mayor vulnerabilidad o en riesgo**, brindando trato diferenciado y respuesta rápida frente a situaciones de violencia digital.

- **Deben especificar en sus políticas o normas comunitarias cómo abordan esta problemática,** que afecta desproporcionadamente a las mujeres y, en especial, a mujeres con perfil público. Asimismo, también deben facilitar que las medidas y mecanismos que pongan en marcha sean públicos y accesibles.

3 Tomado del "Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias" de la ONU (2016), del "Informe sobre ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención Belém Do Pará" de la CIM/MESECVI/OEA (2022), del Informe "La violencia en línea contra las mujeres en México. Informe para la Relatora sobre Violencia contra las Mujeres Ms. Dubravka Šimonović"; de la organización Luchadoras (2017).

2. Estrategias para combatir la violencia digital contra las mujeres en la vida política

A continuación, se presentan estrategias y medidas para combatir la violencia digital contra las mujeres en la vida política. En general, se trata de medidas y estrategias que buscan generar cambios en las "reglas de juego", tanto en el ámbito digital como en el real.

2.1 Denunciar la violencia ante órganos judiciales

- Un grupo de 16 mujeres con actividad pública, entre las cuales se encuentran algunas políticas, presentó una denuncia penal por acoso y violencia en línea. En un comunicado de divulgación pública, explican que la denuncia se realizó por "*presunta comisión de delitos de incitación al odio, desprecio o violencia hacia determinadas personas; comisión de actos de odio, desprecio o violencia hacia determinadas personas; injurias, en reiteración real con el delito de difamación, ambas agravadas. Incurre también en distintas formas de violencia de género: por identidad de género, simbólica, política y mediática*". La denuncia fue radicada en la Fiscalía General del país.

- Un diputado realizó, en su cuenta Twitter, manifestaciones difamatorias en contra una mujer política. La víctima realizó una denuncia por injurias, calumnias y violencia de género. El Tribunal consideró que el actor es responsable de un delito contra el honor, en la modalidad de injuria y calumnia, aunque no encontró pruebas para acreditar la violencia de género. La Sentencia (abril 2021) estableció un pago de 500 días de multa a razón de B/20.00 por día, a un total de B/10,000.00 pagaderos al Tesoro Nacional, en un periodo del año (equivalente aproximadamente a USD$10,000). Además, se impuso una sanción accesoria de inhabilitación para ejercer funciones públicas por 12 meses, que empezará a regir una vez terminada la pena económica.

- Cuando se destituyó a las y los magistradas/os de la Sala Constitucional, una activista de derechos humanos, abogada de relevancia nacional y candidata a diputada, hizo públicas sus opiniones y recibió ataques de ciberacoso en redes sociales de personas afines al gobierno y de altas autoridades del país, que pusieron en riesgo la vida e integridad de la activista. Las publicaciones incluían contenido sexualizado y estigmatizante y manifestaban la manera en la cual los agresores la atacarían físicamente. Los ataques en redes sociales (Twitter y YouTube) se prolongaron por más de un año. El acoso a la activista incluyó visitas a su domicilio de personas portando carnés de gobierno, que buscaban información personal y de quienes viven en su domicilio. Además, un exdiputado inició una campaña con "hashtags" en su contra que se convirtieron en "trending topics" en Twitter; es decir, tuvieron una difusión masiva.

La activista interpuso una acción judicial que impidió que el exdiputado se postulara como candidato en las siguientes elecciones. La activista solicitó medidas cautelares. Aunque ella cuenta con medidas de protección en contra de las publicaciones del exdiputado; carece de medidas de seguridad personal. La Resolución de la CIDH (76/2021), solicitó al Estado que:

a. Adopte las medidas necesarias para proteger los derechos a la vida e integridad personal de la activista, a la luz de la perspectiva de género para que pueda desempeñarse como defensora de DDHH sin ser objeto de amenazas, intimidación, hostigamientos o actos de violencia.

b. Determine las medidas a adoptarse con la beneficiaria y sus representantes.

c. Informe sobre las acciones adoptadas a fin de investigar los hechos, en un periodo de 15 días, a actualizarse periódicamente.

Denunciar ante otros organismos del Estado

- En **Perú,** el Ministerio de Mujeres y Poblaciones Vulnerables cuenta con una línea telefónica (Línea 100) y un chat (Chat 100) para realizar denuncias de violencia digital o acoso. En los Centros de Emergencia de la Mujer (CEM) cuentan con recursos para abordar y acompañar estas situaciones. En la plataforma de internet "No al Acoso", brinda un test para detectar situaciones de acoso en línea y un botón de alerta, así como un formulario en línea para realizar la denuncia.

2.2 Promover legislación para prevenir, sancionar y erradicar la violencia digital contra las mujeres en la vida política

- En **Brasil, la Ley N° 13.718 (año 2018)** tipifica los crímenes de importunidad sexual y de divulgación de imágenes de violación. **La Ley N° 13.642 "Ley Lola" (año 2018**) atribuye a la Policía Federal la responsabilidad de la investigación de delitos digitales contra las mujeres, incluyendo la difusión digital de contenidos que propagan el odio o aversión en su contra. **La Ley N° 12.965 "Marco Civil de Internet" (año 2014),** establece las responsabilidades de las plataformas de internet por el contenido de terceros. Las empresas proveedoras de internet tienen la obligación de eliminar el contenido íntimo en un tiempo razonable tras la mera notificación de la víctima o su representante legal y sin que medie una orden judicial de remoción. **La Ley N° 12.737 "Ley Carolina Dieckmann" (año 2012)** tipifica como delito la invasión de un dispositivo electrónico para obtener, manipular o destruir datos o información personal sin autorización. **La Ley General de Protección de Datos N° 13.709 (año 2018),** establece

principios, derechos y deberes para el tratamiento de datos personales. Dado que regula la protección de los datos sensibles de las personas (entre ellos, datos relativos a la orientación sexual) y brinda una protección amplia a la privacidad, libertad de expresión y a la inviolabilidad de la intimad, el honor y la imagen, resulta de gran importancia para la protección frente a la violencia digital en contra de las mujeres.

- En **México La Ley Olimpia (año 2020)** (un conjunto de reformas legislativas) reconoce de manera específica la violencia digital (o ciberviolencia) contra las mujeres y niñas, y sanciona los delitos que violen la intimidad sexual de las personas a través de medios digitales. En la Ley General de Acceso de las mujeres a una vida libre de violencia incorpora los conceptos de "violencia mediática" y de "violencia digital", que se entiende como: "*...aquellas acciones en las que se expongan, difundan o reproduzcan imágenes, audios o videos de contenido sexual íntimo de una persona sin su consentimiento, a través de medios tecnológicos y que por su naturaleza atentan contra la integridad, la dignidad y la vida privada de las mujeres causando daño psicológico, económico o sexual tanto en el ámbito privado como en el público, además de daño moral, tanto a ellas como a sus familias.*" También incorpora sanciones por violación a la intimidad sexual a través del Código Penal Federal. Establece la competencia de los juzgados y ministerios públicos de ordenar de manera inmediata la interrupción, bloqueo, destrucción, o eliminación de imágenes, audios, o vídeos, solicitándolo por escrito a redes sociales, medios de comunicación, páginas de Internet y plataformas digitales. Además, se regula el rol de los intermediarios de internet. Enlace con información adicional.

2.3 Otras políticas públicas dirigidas a la atención, acompañamiento y promoción del acceso a la justicia de mujeres en situación de violencia digital contra las mujeres en la vida política

- En **México**, el Instituto de las Mujeres de Ciudad de México presentó en 2016 el "Plan de acciones públicas a emprender de manera integral" a los fines de visibilizar y prevenir la violencia y acoso sexual en las redes sociales. Cuenta con una estrategia para prevenir la violencia sexual en el espacio digital contra niñas y mujeres adolescentes, jóvenes y adultas, dirigido a garantizar el derecho de las mujeres a una vida libre de violencia en el espacio digital, que se encuentra integrada al programa de apoyo a las instancias de Mujeres en las Entidades Federativas. Asimismo, en su portal oficial publicó información para la visibilización y prevención de la violencia cibernética contra las mujeres y niñas, incluyendo varios instructivos para denunciar, buscar asesoría y fortalecer la seguridad digital, además de impulsar actividades de capacitación y sensibilización en la materia.

- En **Perú**, el Ministerio de la Mujer y Poblaciones Vulnerables, a través del Programa Nacional contra la Violencia Familiar y Sexual, ha emitido los "Lineamientos para la Atención en los Centros de Emergencia de la Mujer a Mujeres Políticas Afectadas por Hechos de Acoso Político" (Resolución de la Dirección Ejecutiva 51-2018-MIMP/PNCVFS-DE), que son de carácter obligatorio para todos los Centros de Emergencia Mujer a nivel nacional. Estos lineamientos fueron propuestos en primera instancia, en 2016, por el Centro de la Mujer Peruana Flora Tristán, la Asociación de Comunicadores Sociales Calandria y el Movimiento Manuela Ramos, organizaciones que desarrollan la campaña "Somos la Mitad, Queremos Paridad sin Acoso". Luego han sido impulsados en la Mesa de Trabajo para Promover y Garantizar la Participación Política de las Mujeres, instancia de coordinación público-privada presidida por el Ministerio de la Mujer y Poblaciones Vulnerables.

2.4 Realizar campañas de concientización y sensibilización sobre violencia digital contra las mujeres en la vida política

Promovidas por organismos del Estado

- En **Bolivia,** el Observatorio de Paridad Democrática dependiente del Órgano Electoral Plurinacional de Bolivia, puesto en marcha en conjunto con ONU Mujeres, llevó adelante, en 2020, una campaña contra el ciberacoso dirigida específicamente a mujeres en la vida política. El Observatorio brinda información sobre la violencia política digital, y diferentes canales de denuncia frente a los Tribunales Electorales Departamentales y el Tribunal Electoral Supremo. Enlace con información adicional.

- En **Perú,** el Ministerio de la Mujer y Poblaciones Vulnerables lleva adelante una campaña titulada "Nos Protegemos del Acoso Virtual". El sitio de internet brinda información sobre este problema y ofrece un botón de alarma para registrar casos de violencia digital contra las mujeres en la vida política. Paralelamente, el Estado peruano estableció una mesa de trabajo en la que participa el Ministerio de la Mujer y Poblaciones Vulnerables, que tiene por objeto prevenir el acoso virtual contra las mujeres a través de la propuesta de iniciativas legales y otras medidas en la materia.

Promovidas por organizaciones de la sociedad civil, y/u organizaciones de mujeres

- En **Argentina**, la organización "Equipo Latinoamericano de Justicia y Género" (ELA) llevó adelante la campaña "#MiLugareselqueElijo" con el mensaje "No Naturalicemos la Violencia Política en Redes".

- En **Chile**, la Articulación Territorial Feminista Elena Caffarena realiza una campaña virtual titulada "#DaleUnfollow" para eliminar la violencia política de género en la Convención Constitucional, a partir de los datos del Estudio "Ser política en twitter:

Violencia política de género en redes sociales a candidatas constituyentes", y del Informe Final del "Proyecto Mujeres y Política en Twitter: análisis de mensajes violentos a mujeres Constituyentes 2021".

- En **México**, la organización "Luchadoras" lleva adelante una campaña contra la violencia digital hacia las mujeres en la vida política titulada "La Clika, libres en línea". En su sitio proveen información sobre esta violencia, una "guía de autodefensa" y un espacio para organizarse, tejer redes y ayudar a otras mujeres en situación de violencia digital.

- En **Perú**, durante el año 2020 (pandemia COVID-19), las organizaciones Hiperderechos y Plan Internacional en conjunto con el Ministerio de la Mujer y Poblaciones Vulnerables, llevaron adelante una campaña titulada "Conectadas y seguras", que tiene como objetivo concientizar a la población sobre el impacto del acoso en internet en la vida de niñas y adolescentes y difundir consejos de seguridad digital.

2.5 Acciones en el ámbito de los organismos internacionales e interamericanos

En el sistema de Naciones Unidas

- En 2020, una legisladora del partido político opositor al partido de gobierno realizó una denuncia por la intensificación de amenazas de muerte recibidas luego del asesinato de su colega en la Cámara de Concejales, siendo interceptadas en el año 2020 al menos cinco llamadas telefónicas que tramaban la muerte de la legisladora. A raíz de esta situación, redactó una carta denuncia dirigida a tres Relatoras[4] de la ONU: la Relatora Especial sobre ejecuciones extrajudiciales, sumarias o arbitrarias; la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia y la Relatora Especial sobre la situación de los defensores de derechos humanos. En la misiva destaca la falta de protección por parte del Estado, en un contexto en el que las amenazas a una legisladora son amenazas a la democracia misma. Ello demostró ser un recurso importante de articulación política para exigir el fin de la violencia y la creación de un ecosistema jurídico-político que proteja a las políticas en riesgo, así como para fomentar el debate a nivel internacional y nacional sobre la temática de la violencia digital e interseccional contra mujeres en la política. Enlace con información adicional.

4 Las Relatorías Especiales y Grupos de Trabajo forman parte de lo que se conoce como "Procedimientos Especiales del Consejo de Derechos Humanos". Procedimientos Especiales es el mayor organismo de especialistas independientes del sistema de Derechos Humanos de la ONU, son mecanismos independientes de investigación y monitoreo del Consejo que abordan situaciones específicas de países o cuestiones temáticas en todas partes del mundo. Las y los especialistas de los procedimientos especiales trabajan de forma voluntaria, no son parte del personal estable de la ONU ni reciben un salario por su trabajo. Son independientes de cualquier gobierno u organización, y sirven a título personal.

- En 2017, la organización feminista Luchadoras envió el informe "La violencia en línea contra las mujeres en México" a la Relatora sobre la violencia contra las mujeres de la Organización de las Naciones Unidas. El informe elabora un panorama general sobre la situación de violencia relacionada con las tecnologías contra las mujeres en el país.

En el Sistema Interamericano

- Mujeres que han ocupado cargos políticos en la región han acudido a la OEA, a la CIM y al MESECVI, para denunciar la persecución política en su contra. Por su lado, el Comité de Expertas (CEVI) del MESECVI ha emitido diversos comunicados expresando preocupación por casos de violencia contra mujeres en la vida política por razones de género ocurridos en la región[5].

- En la Comisión Interamericana de Derechos Humanos (CIDH) existen diversas Relatorías especiales; en los últimos años las Relatorías sobre los Derechos de las Mujeres y la Relatoría Especial para la Libertad de Expresión han abordado la temática de violencia en línea contra mujeres, adolescentes y niñas en general, y en particular, contra mujeres periodistas y salas de redacción. Su contenido quedó plasmado en los últimos informes. Esta última Relatoría elaboró el informe "Estándares para una Internet libre, abierta e incluyente" (2017).

2.6 Reportar o denunciar casos de violencia digital contra las mujeres en la vida política en diversas plataformas, sitios o redes sociales (según sus políticas internas y procedimientos)[6]

- **Meta (grupo Facebook, Instagram, Whatsapp y Messenger)** creó en su sitio oficial un "Centro de seguridad de la Mujer", donde brinda consejos y herramientas para aumentar la seguridad de las mujeres en la plataforma. En este Centro, existe una sección específica "Mujeres en posiciones de liderazgo y figuras públicas", dirigida a mujeres candidatas en campaña electoral, pero también para quienes ejercen cargos públicos y para defensoras de los derechos humanos.

- **Facebook** cuenta con la Guía "#SheLeads. Consejos sobre herramientas de seguridad de Facebook para mujeres líderes. Cuando las Mujeres lideran, todos progresan".

- **Instagram** ha elaborado con el apoyo de ONU Mujeres Argentina, una Guía de seguridad para mujeres en la política, en la cual se establece que los diálogos en

5 Pueden consultarse en https://www.oas.org/en/mesecvi/news.asp

6 *Ú*nicamente se ha incluido iniciativas de sitios o redes sociales dirigidas específicamente a mujeres en la vida política, o con perfiles públicos.

torno a figuras públicas también deben cumplir las normas establecidas; caso contrario, se eliminará el contenido. Menciona específicamente el acoso y el lenguaje que incita al odio.

2.7 Mecanismos para el registro y monitoreo de los casos de violencia digital contra las mujeres en la vida política

Registros o mecanismos de monitoreo del Estado

- En **Uruguay**, el Instituto Nacional de la Mujer, con el apoyo de PNUD, puso en marcha el Monitor de Violencia Digital de Género, que proporciona información sobre la violencia digital contra las mujeres en tiempo real. Transmite datos desde Twitter, aplicando herramientas de clasificación de inteligencia artificial y presenta información a través de visualizaciones interactivas e informativas. El Monitor (i) proporciona evidencia accesible con respecto al nivel de agresiones e insultos que reciben figuras públicas como mujeres políticas, periodistas, comunicadoras, activistas y artistas en Twitter y (ii) comprende el análisis de la cantidad de agresiones recibidas, los tipos de agresiones más frecuentes y los agravios más utilizados. La base de datos para el desarrollo del monitor fue construida teniendo en cuenta una muestra de mujeres activas en redes sociales con liderazgo en opinión y visibilidad pública con más de 3.000 seguidores. El análisis se realiza de forma anónima, sin identificar los casos particulares. De esta forma, la identidad de las mujeres que son parte de la muestra no es visible en ningún momento. Para construir el monitor se accede sólo a datos públicos que son almacenados de manera segura. Los tweets comenzaron a ser recolectados y almacenados desde el 1 de marzo de 2022. Se releva la prevalencia en tres momentos: vida del tracker (del 1.03.22 a la fecha), último 7 días, últimas 24hs.

- **Perú** cuenta con mecanismos oficiales y permanentes para cuantificar y dimensionar los casos de violencia en línea a partir de los registros de denuncias que se realizan desde la plataforma "Nos protegemos del acoso virtual", dependiente del Ministerio de la Mujer y Poblaciones Vulnerables. La plataforma incluye una prueba de acoso virtual que ayuda a identificar si se es víctima de violencia digital.

Iniciativas de la sociedad civil para documentar y monitorear la violencia digital contra las mujeres en la vida política

- En **Argentina**, la Fundación de Nuevos Derechos (FUNDECO) cuenta con un Observatorio de violencia contra las mujeres y disidencias en política "Julieta Lanteri" que tiene como objetivo producir, registrar y sistematizar toda información relevante sobre la violencia contra las mujeres y disidencias en política. En 2020, elaboró un In-

forme sobre violencia política hacia mujeres y disidencias en redes en conjunto con otras organizaciones de la sociedad civil (el Observatorio Electoral de Conferencia Permanente de Partidos Políticos de América Latina y El Caribe –COPPPAL-; y el Equipo Latinoamericano de Justicia y Género). Por otro lado, la organización Equipo Latinoamericano de Justicia y Género (ELA) creó una plataforma "Mujeres en el Poder" a los fines de recabar y producir información sobre la violencia política contra las mujeres, lesbianas, trans y travestis, monitoreo sobre procesos electorales, e información acera de las barreras discriminatorias para la participación política. La plataforma brinda información específica sobre violencia política y publicó el informe "Violencia contra las mujeres y disidencias en política a través de redes sociales Una aproximación a partir del análisis de la campaña electoral en Twitter, Facebook e Instagram durante 2019" (2020), junto con otras organizaciones de la sociedad civil antes mencionadas.

- En **Costa Rica**, el Centro de Investigación en Estudios de la Mujer (CIEM) de la Universidad de Costa Rica cuenta con un Observatorio de participación política de las mujeres. Crearon una plataforma "Nosotras en la Política" donde se publican los datos de las investigaciones que llevan adelante.

- En **Ecuador**, la Fundación "Haciendo Ecuador" cuenta con un Observatorio Nacional de la Participación Política de la Mujer, que realiza el "Monitoreo de redes en contra de las mujeres del Ecuador", cuyo objetivo es analizar la violencia digital que enfrentan las mujeres políticas en el país. El Observatorio publica informes periódicos.

- En **Panamá**, el Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC) es una organización sin fines de lucro que promueve el uso y la regulación de las Tecnologías de la Información y Comunicación (TIC's) y la defensa de los Derechos Humanos en el entorno digital. El Instituto contribuye también a la elaboración de propuestas de ley relacionadas con las nuevas tecnologías y desarrolla capacidades para la participación activa de mujeres y colectivos LGTBI+ en el ecosistema digital. También operan a nivel subregional y en ese marco realizaron el Informe "Monitoreo de Violencia de Género en Línea a Candidatas de Elección Popular 2019 en Guatemala".

2.8 Asesoramiento y acompañamiento en situaciones de violencia digital contra las mujeres en la vida política

- En **Brasil**, la red de organizaciones sociales conformada por el Instituto Gênero e Número, Coding Rights, Rede Feminista de Juristas, Ciudadanía Inteligente, Internet LabBeta, Rede Umunna crearon una plataforma para recibir denuncias anónimas de violencia y discurso de odio durante los procesos electorales en Brasil, a los fines de redireccionarlas al Ministerio Público Federal. Por otro lado, la "Rede Feminista de

Juristas" brindan asistencia y acompañamiento frente a situaciones de violencia. La organización Safernet tiene foco en la defensa de los Derechos Humanos en internet en el país y brinda respuesta a los graves problemas relacionados con el uso indebido de internet y violaciones a los Derechos Humanos. En su página web cuenta con un espacio para realizar denuncias, y brinda acompañamiento a situaciones de violencia online (Helpline).

- En **Bolivia**, la asociación Internet Bolivia. Org tiene como objetivo fortalecer el acceso a una internet segura, libre y potenciadora de la democracia. Provee una Guía anti-acoso digital para mujeres y una serie de estudios de libre acceso en su sitio oficial, elaborados con otras organizaciones de la sociedad civil. Además, brinda asesoramiento en diversos ejes y cursos. Por otro lado, la organización SOS Digital brinda acompañamiento frente a situaciones de violencia en línea, desde diversas plataformas.

- En **Chile**, la organización Acoso Online brinda información para realizar denuncias y procesos judiciales, provee un chat para mantener conversaciones con las personas que moderan la plataforma, un botón de emergencia (frente a situaciones de violencia digital) y provee consejos de autodefensa en caso de ser víctima de violencia digital.

- En **Ecuador**, el Observatorio Nacional de la Participación Política de la Mujer de la Fundación "Haciendo Ecuador" brinda asesoramiento jurídico sobre la materia. En su página web aloja un formulario para la realización de denuncias de violencia política (que pueden ser también en el ámbito digital).

- En **México**, la organización Luchadoras brinda información acerca de violencia de género en línea, realiza investigaciones sobre este problema. Se definen como una plataforma para el encuentro y organización de mujeres que luchan por una "internet feminista". Por otra parte, la organización Defensoras Digitales brinda información sobre violencia digital contra las mujeres, y realiza estudios y sensibilización sobre la temática. Cuenta con un formulario para realizar denuncias por violencia digital. Forma parte del Frente Nacional para la Sororidad.

- En **Paraguay**, la asociación TEDIC publicó la "Guía de violencia de género digital"; además brinda asesoramiento especializado y acompañamiento a mujeres víctimas de violencia digital durante los procesos de litigio estratégico.

- En **Perú**, la asociación civil Hiperderecho provee información sobre la violencia de género en línea y una guía para la realización de denuncia para las mujeres víctimas. Cuentan con un test para la detección de la violencia en línea. Además, brindan acompañamiento durante la denuncia y/o proceso judicial.

- **A nivel regional**, la plataforma de internet Vita Activa brinda una mesa de ayuda frente a situaciones de violencia digital, para el abordaje y acompañamiento de mujeres y personas LGBTIQ+ que son víctimas de este tipo de violencias por razones de género.

2.9 Hashtivismo, estrategias individuales o grupales de denuncia y combate a la violencia digital contra las mujeres en la vida política

- Mujeres políticas y activistas han creado o se han unido a diversas campañas en redes sociales denunciando actos de violencia en su contra, o en contra de sus colegas. Algunos de los hashtags que han usado para amplificar el impacto y llamar la atención de la comunidad internacional son: #NoEsElCosto #MeTooPolitics #LevonsLOmerta (termina el silencio) #ParidadSinAcoso #NoEsHoraDeCallar #NeverthelessShePersisted (sin embargo, ella persistió), #ParidadDemocrática #NotTheCost (No es el costo, campaña global).

- Una diputada, la más joven de la legislatura (asumió el cargo con 20 años), recibió un ataque coordinado de violencia en las redes sociales, luego de solicitar justicia por un feminicidio y pedir sanción para el agresor. En la red social Twitter recibió una serie de mensajes violentos. Frente a ello, la diputada movilizó el apoyo de su grupo político, a través de un comunicado que salió en las redes denunciando la violencia política bajo el hashtag #EsViolenciaPolítica.

- Una candidata a diputada nacional fue objeto de una campaña de desprestigio y difamación a través de la viralización de un video falso en perfiles falsos de Facebook y Twitter, en el que supuestamente mantiene relaciones sexuales en una oficina. La campaña comenzó una semana antes del cierre de las candidaturas. El partido político al que pertenece salió a repudiar el hecho y a negar su veracidad.

- Una diputada nacional, afrodescendiente, recibió amenazas de muerte de usuarios en la red social Twitter, como parte de un ataque coordinado, con mensajes muy violentos. Los mensajes presentaban contenido racista, xenófobo y sexista, además de amenazarla de muerte. La diputada recurrió a tres Relatoras del sistema de Naciones Unidas para denunciar las amenazas y la desprotección por parte del Estado.

3. Tests para identificar, prevenir y mitigar la violencia digital contra las mujeres en la vida política

3.1 Test para identificar la violencia digital contra las mujeres en la vida política

Descripción
Ofensas y expresiones discriminatorias
Son manifestaciones de violencia simbólica contra las mujeres a partir de un discurso basado en ideas preconcebidas de género; incluyen comentarios abusivos, insultos y expresiones/ discurso de odio.
Ciberhostigamiento o ciberacoso
Ciberhostigamiento: "...comisión reiterada por parte de una misma persona, de actos abusivos y perturbadores a través del uso de las TIC, con el objetivo de hostigar, intimidar, acechar, molestar, controlar, atacar, humillar, amenazar, asustar, ofender o abusar verbalmente a una víctima". Conlleva referencias a estereotipos de género negativos y dañinos, lenguaje obsceno y es de naturaleza sexual. **Ciberacoso**: "...toda forma de conducta verbal o no verbal indeseada de naturaleza sexual que tiene por objetivo o consecuencia atentar contra la dignidad de la persona y en particular crear un entorno intimidatorio, hostil, degradante, humillante u ofensivo". Estos actos conforman en conjunto un patrón digital de abuso que merma la sensación de seguridad de la víctima y le provoca miedo, angustia o alarma. **Suelen encadenarse con otros tipos y manifestaciones de violencia digital.** **El ciberacoso coordinado**: un ataque grupal, masivo y anónimo (incluso a veces transfronterizo) contra una mujer con el objetivo de humillarla o causarle angustia mediante campañas o estrategias coordinadas por una persona o grupos cerrados, trolls o bots. El acoso dirigido/coordinado afecta particularmente a mujeres periodistas, defensoras de derechos humanos, mujeres políticas o con una participación activa en el debate digital, y funciona como un dispositivo de descalificación, censura y disciplinamiento en el ciberespacio, buscando mermar sus canales de expresión y su presencia en los espacios digitales. Por su dimensión y escalabilidad, estos ataques pueden llegar a constituirse en verdaderas **"ciberturbas" (cybermobs)** en las que se da una despersonalización de la violencia, al provenir en su mayoría de personas totalmente desconocidas para las víctimas o conocidas únicamente en grupos/comunidades en línea.

Manifestaciones / conductas	Momento / Rol
☐ **Comentarios que menosprecian los saberes, conocimientos y/o capacidades para hacer política por el hecho de ser mujeres**; o hacen alusión a la falta de capacidades de las mujeres para hacer política. ☐ **Comentarios respecto del cuerpo y la sexualidad**, vinculados a la apariencia física, estereotipos corporales, calificaciones y valoraciones de su figura, ejercicio de la sexualidad, sobre su identidad u orientación sexual o de género o alguna valoración en función de su supuesto comportamiento sexual. ☐ **Comentarios sobre roles y mandatos de géneros:** hacen alusiones al deber de cumplimiento o supuesto incumplimiento de los mandatos o roles de género ☐ **Discursos de odio:** uso de un lenguaje que insulta, amenaza o ataca a una persona a causa de su identidad y otras características, como su orientación sexual o discapacidad.	☐ Campaña electoral ☐ Ejercicio de cargo público ☐ Ejercicio de un cargo político ☐ Como afiliada a un partido político ☐ ONG o Defensora de derechos humanos
☐ **Comentarios repetitivos en línea** de naturaleza obscena, sexual, difamatoria o amenazante; comentarios abusivos, sexistas y misóginos; violencia verbal u ofensiva asociada a la condición de género o a la apariencia física; expresiones o comentarios discriminatorios. ☐ **Seguimiento obsesivo de publicaciones en redes sociales de la víctima y/o establecer o intentar constantemente entablar comunicación con ella sin su consentimiento**, envío constante de solicitudes de amistad en redes sociales, o unirse a todos los grupos online de los que la víctima forma parte (stalkear). ☐ **Contactar a través de las TIC a la familia, amistades o colegas** de una mujer con el objeto de acceder a ella. ☐ **Monitoreo, persecución, búsqueda de cercanía física o vigilancia constante** de la ubicación, actividades o comunicaciones de la víctima para que esta lo note. ☐ **Formulación de proposiciones sexuales indeseadas** de manera reiterada, o envío de fotos con contenido sexual sin autorización. ☐ **Publicación constante de información falsa u ofensiva** en redes sociales, blogs o sitios web, o distribución de fotos íntimas o videos en plataformas de internet o a través del teléfono móvil. ☐ Incitación en línea a cometer violencia física y sexual en contra de una víctima.	☐ Campaña electoral ☐ Ejercicio de cargo público ☐ Ejercicio de un cargo político ☐ Como afiliada a un partido político ☐ ONG o Defensora de derechos humanos

Descripción
Violación a la privacidad
Uso, control, manipulación, difusión o publicación no autorizada de información privada y datos personales Obtenidos a través del acceso no autorizado, no consentido y/o ataque a un sistema informático o a una cuenta en línea. Consiste en el acceso y publicación no autorizada de información personal que revela la identidad de la víctima o su ubicación física, con el objetivo de dañar su reputación, incitar a cometer violencia en su contra, humillarla, amenazarla o intimidarla o crear daños en su entorno personal, profesional o público, y que genera en muchos casos un contexto de angustia y pánico al propiciar en la víctima miedo sobre su seguridad y la de su familia.
Ataques a la reputación de una mujer (desprestigio) y/o desinformación
Monitoreo, control y vigilancia en línea Consiste en el rastreo constante de las actividades en línea y fuera de línea de una víctima, así como de su ubicación, desplazamientos e información a través del uso de las TIC.
Suplantación y robo de identidad en línea Consiste en la utilización de la imagen, información o datos de una persona o la creación de una identidad falsa con la imagen o datos de una persona, sin mediar su consentimiento y a través del uso de las TIC, con el fin de amenazarla, intimidarla o dañar su reputación.

Manifestaciones / conductas	Momento / Rol
☐ **Acceso no autorizado a cuentas en línea o dispositivos** a fin de obtener información o datos personales mediante robo de contraseñas, phishing o pharming, hackeo, instalación de software espía, keyloggers o control remoto de webcams o micrófonos. ☐ **Uso, manipulación y modificación no consentida de información** (datos personales, fotos y videos) ☐ **Revelación de la identidad o preferencia sexual de una persona (outing)**, incluyendo exposición de mujeres o integrantes de la comunidad LGTBIQ+ ☐ **Bloqueo y/o de acceso a cuentas en línea o cuentas de correo electrónico** y de la información personal de una víctima (doxxeo). ☐ **Publicación sin consentimiento de la ubicación de la víctima** o de la geolocalización automática por plataformas de redes sociales o aplicaciones	☐ Campaña electoral ☐ Ejercicio de cargo público ☐ Ejercicio de un cargo político ☐ Como afiliada a un partido político ☐ ONG o Defensora de derechos humanos
☐ **Utilización de software espía en dispositivos electrónicos**, sin el consentimiento de la usuaria, que permiten el control remoto de cámaras o micrófonos en teléfonos móviles ☐ **Monitoreo clandestino de llamadas y mensajes**, para el monitoreo de las actividades de la víctima ☐ **Uso de geolocalizadores para rastrear la ubicación de una mujer** sin su consentimiento. ☐ **Ciberespionaje de Estado** en contra de mujeres con un perfil público, políticas, defensoras de derechos humanos, activistas feministas, y periodistas.	☐ Campaña electoral ☐ Ejercicio de cargo público ☐ Ejercicio de un cargo político ☐ Como afiliada a un partido político ☐ ONG o Defensora de derechos humanos
☐ Creación de perfiles o cuentas falsas en redes sociales que utilizan la información o imagen de una persona u organización. ☐ Robo o usurpación de cuentas de correo electrónico o números de teléfono, para eliminar, enviar o manipular mensajes de correo electrónico o cuentas en línea sin el consentimiento de la víctima. periodistas.	☐ Campaña electoral ☐ Ejercicio de cargo público ☐ Ejercicio de un cargo político ☐ Como afiliada a un partido político ☐ ONG o Defensora de derechos humanos

Descripción
Ataques a la reputación de una mujer (desprestigio) y/o desinformación (continuación)
Implica la creación, manipulación y publicación de información personal falsa, manipulada o fuera de contexto (desinformación) con la intención de descalificar o dañar la reputación/prestigio de una persona o que puede implicar un daño a su trayectoria, credibilidad, o imagen pública
Creación, difusión, publicación, manipulación de fotografías, videos o audios de naturaleza sexual o íntima sin consentimiento: Consiste en la difusión no consensuada de imágenes íntimas obtenidas con o sin el consentimiento de la persona, con el propósito de avergonzar, estigmatizar o perjudicar a la víctima Esta forma de violencia digital conlleva la participación de diversas personas con diferentes grados de responsabilidad e involucramiento: persona o grupos de personas que producen y publican el material sin consentimiento, y las personas que eventualmente comparten o republican ese material.

Manifestaciones / conductas	Momento / Rol
☐ **Creación de perfiles falsos en redes sociales** o cuentas en línea con la intención de afectar la reputación de la víctima. ☐ **Difusión de información falsa** en línea o publicaciones, manipulación de los discursos o posicionamientos políticos de las mujeres respecto a una temática con la intención de dañar la reputación de la víctima, incluidos actos de calumnia, manipulación o difamación sexual. ☐ **Diseminación de información privada o sensible**, incluida exposición pública de la identidad o preferencia sexual de una persona (outing), o información relativa a una causa judicial que involucre a la víctima. ☐ **Creación y publicación no consensuada de imágenes sexuales** editadas o videos deep fake, a partir de fotografías obtenidas en cuentas privadas, registradas en espacios públicos (creepshots), o manipulación y/o creación de fotografías o videos falsos (fotomontajes o deep fakes) con contenido sexual. ☐ **Publicación de imágenes o videos sin autorización en sitios pornográficos**, en páginas web de anuncios indicando que la víctima ofrece servicios sexuales, o en sitios de venganza sexual en los que se publican los datos personales de las víctimas (doxeo), o en grupos cerrados de Facebook o Whatsapp. ☐ **Creación de memes con contenido sexual, misógeno y/o discriminatorio** en foros de discusión, redes sociales o páginas de internet. ☐ **Campañas de desprestigio o desinformación**	☐ Campaña electoral ☐ Ejercicio de cargo público ☐ Ejercicio de un cargo político ☐ Como afiliada a un partido político ☐ ONG o Defensora de derechos humanos

Descripción
Ataques digitales a grupos, organizaciones, comunidades o colectivas de mujeres (censura)
Implican acciones intencionales para censurar y/o causar daño a organizaciones o grupos de mujeres, para afectar el desarrollo de sus funciones, atacar sus canales de expresión, intimidarlas para retirar publicaciones o silenciarlas y disminuir o anular su presencia en los espacios y conversaciones digitales. Estos ataques pueden realizarse de manera masiva y ser coordinados por una persona o grupos cerrados, trolls o bots, y realizare en contra de una publicación, perfil de redes sociales o el sitio web de una organización.
Amenazas directas de daño o violencia y extorsión
Implica el envío o publicación de **comunicaciones o contenidos digitales que le anticipan a una persona la intención de cometer un daño físico o violencia sexual hacia su persona,** o en contra de sus familiares, amistades o bienes.

Manifestaciones / conductas	Momento / Rol
☐ **Hackeo** de sitios web, cuentas de redes sociales o cuentas de correo electrónico. ☐ **Actos para dar de baja el perfil de redes sociales** mediante el uso de normas comunitarias reportando de forma masiva contenido que se considera sensible (publicaciones, páginas o perfiles de la organización). ☐ **Suplantación de identidad y/o canales de expresión** (copiar identidad gráfica de la organización o alteración de sus imágenes o logos oficiales) o cuentas de redes sociales ☐ **Monitoreo y vigilancia de las actividades** de las personas integrantes de una organización. ☐ **Amenazas directas de violencia** en contra de integrantes de una organización o comunidad, o ciberacoso de contenido sexual. ☐ **Difusión de información privada y anónima** (por ejemplo, direcciones de refugios). ☐ **Ataques de denegación de servicio** ☐ **Restricciones de uso de dominio o robo de dominio.** ☐ **Difusión de noticias o información falsas**	☐ Campaña electoral ☐ Ejercicio de cargo público ☐ Ejercicio de un cargo político ☐ Como afiliada a un partido político ☐ ONG o Defensora de derechos humanos
☐ **Envío o publicación de mensajes de correo electrónico o redes sociales, imágenes o videos anunciando un peligro inminente o violencia sexual.** ☐ **Extorsión digital,** que involucra el uso de las TIC para ejercer presión sobre una persona a fin de forzarla a actuar de cierto modo (renunciar a un cargo, tomar alguna decisión, destinar/desviar recursos determinados, etc.) ☐ **Sextorsión:** amenazar con difundir fotografías intimas de la víctima para extorsionarla a fin de obtener más fotografías o videos de actos sexuales explícitos o mantener relaciones sexuales con la víctima.	☐ Campaña electoral ☐ Ejercicio de cargo público ☐ Ejercicio de un cargo político ☐ Como afiliada a un partido político ☐ ONG o Defensora de derechos humanos

Descripción
Actos de violencia física o sexual; femicicios
Esta forma de violencia digital conlleva el uso de las TIC para ubicar y acceder a una víctima a fin de agredirla física o sexualmente, en el continuum "online/offline".

Fuente: elaborado en base a la tipología, categorías y definiciones establecida en el "Informe sobre ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención Belém Do Pará" de la CIM/MESECVI/OEA, y adaptado al ámbito/vida política. También se incorporaron tipos, categorías y definiciones propuestas en los informes: "Violencia contra las mujeres y disidencias en política a través de redes sociales Una aproximación a partir del análisis de la campaña electoral en Twitter, Facebook e Instagram durante 2019" del Equipo Latinoamericano de Justicia y Género (ELA), "Violencia de género en línea hacia mujeres con voz pública. Impacto en la libertad de expresión" de ONU Mujeres en Argentina; y en la "Guía Práctica contra la Violencia Política de Género Digital" de la Fundación Friedrich Ebert Stiftung (FES).

Manifestaciones / conductas	Momento / Rol
☐ **Agresiones físicas como consecuencia de actos de doxeo.** ☐ **Ataques sexuales organizados o planificados mediante el uso de las TIC.**	☐ Campaña electoral ☐ Ejercicio de cargo público ☐ Ejercicio de un cargo político ☐ Como afiliada a un partido político ☐ ONG o Defensora de derechos humanos

3.2 Test para identificar medidas de prevención de la violencia digital contra las mujeres en la vida política

Medida de prevención	Detalle/recomendación	X
Chequear la existencia de cuentas falsas entre tus seguidores/as, entre tus "amigos/as" de las redes sociales	A partir de los siguientes criterios: fecha de creación (si es reciente, pero tiene un gran caudal de seguidores/as o amigos/as puede ser falsa); ¿Tiene foto? Si tiene, ¿es genérica o específica?; ¿Tienes amigos/as o seguidores/as en común con la cuenta en cuestión?; ¿Presenta información sospechosa, o abiertamente discriminatoria o violenta contra las mujeres?, entre otros.	
Utilizar las opciones "dejar de seguir", "bloquear" o "eliminar"[7]. Bloquear el odio	A las cuentas falsas o maliciosas y aquellas que proponen contenidos violentos (fascistas, neonazis o antifeministas, etc.) y/o formas de interacción violentas (haters).	
Utilizar las opciones "ignorar y silenciar"	A aquellas cuentas que presentan conductas "mansplainers", o que demandan atención y explicaciones para discutir contigo con la finalidad de inferiorizarte o ridiculizarte (no es un debate real y democrático); también con trolls. evitar contestar comentarios o entablar discusiones con estos perfiles/cuentas.	
Realizar listados de "amigos/as cercanos/as" en las redes sociales	Incluyendo en ellas sólo personas que sean conocidas y confiables en la vida real que puedan ver las publicaciones de la vida cotidiana, o más íntimas.	
Evaluar cuidadosamente cada posteo (mensaje, foto, video, texto o documento) a compartir en diversos, sitios de internet y redes sociales	Especialmente aquellos que pueden generar reacciones, brindar información/datos personales y/o ser utilizados maliciosamente fuera de contexto. Esto resta autenticidad y espontaneidad a nuestros perfiles públicos, pero es una medida preventiva para resguardar nuestra seguridad física y bienestar mental.	
Evitar publicaciones sobre datos personales	Sobre el entorno familiar, laboral y amistoso, cuestiones de salud, hábitos, dirección de residencia y/o de trabajo, rutinas y circuitos, historias personales, lugares preferidos. Si bien permiten humanizar los perfiles públicos y generar cercanía, proporcionan datos sensibles que pueden ser utilizados por personas o grupos maliciosos para desinformar o desprestigiarnos. Evitar publicar fotos de tu domicilio o del entorno de residencia que con un simple análisis del entorno puedan detectar tu ubicación.	
Evitar publicar fotos (o historias) de su ubicación en tiempo real	Mejor hacerlo luego, para evitar ser ubicada.	
Evitar utilizar las mismas contraseñas en diferentes sitios de internet o redes sociales	Se recomienda contar con un administrador de contraseñas, que crea automáticamente contraseñas con criterios de seguridad máxima y según las normas de cada uno de los sitios y plataformas. De esta manera, sólo se precisa saber y recordar una sola clave de acceso.	
Activar el factor de doble autenticación (2FA, en inglés) en todas tus cuentas de sitios y plataformas de internet	Permite añadir una segunda capa de seguridad para acceder a nuestras cuentas de Internet: además de solicitar una contraseña para el acceso a cualquier sitio o plataforma de internet, se requieren confirmaciones y datos adicionales que son enviados a la persona físicamente (en formato de llamada telefónica, mensaje de texto, código generado en alguna aplicación o una llave de seguridad física).	
Utilizar aplicaciones o plataformas con comunicaciones encriptadas/protegidas de extremo a extremo[8]	Los mensajes se encuentran traducidos o cifrados en códigos (números y letras) que sólo pueden ser cifrados desde los dispositivos receptores (móviles o computadoras). Las aplicaciones, plataformas o sitios no encriptados pueden ser hackeados por personas o grupos maliciosos y Estados que vigilan.	

Utilizar una red virtual privada (VPN, en inglés) o redes de internet privado[9] y evitar el uso de VPN públicas:	Las redes privadas de internet impiden que personas o grupos maliciosos, el Estado o empleadores/as puedan ver tu actividad en internet, al dirigir el tráfico de internet a direcciones en otras localidades y encriptar la información.	
Contratar un servicio antidoxing (antidoxeo)	Servicio para la 'limpieza' de datos sensibles, imágenes, videos, mensajes, textos, documentos existentes en línea sobre nosotras, que podrían ser utilizados sin nuestro consentimiento por personas o grupos maliciosos para desinformar o para desprestigiarnos, o para venderlos a quienes estén dispuestos a pagar por ellos[10]. Esta tarea también puede ser realizada en forma manual, aunque lleva mucho tiempo.	
Conocer y mantenerse actualizada acerca de las políticas de seguridad y privacidad de cada una de las plataformas y redes sociales en las que tiene presencia	Para reportar cualquier acción o manifestación de violencia y abuso contra mi persona o contra otras mujeres con perfiles públicos.[11]	
Verificar tus cuentas en redes sociales	A los fines de brindar mayor integridad a tu perfil y contribuye a combatir el fraude y los plagios. Da más credibilidad y genera más interés sobre tu cuenta.	
Poner clave de acceso a tus dispositivos	(Celular y computadora) ya que contienen y brindan acceso a una gran cantidad de información privada/datos personales (direcciones, datos bancarios, tus actividades o las de personas de tu entorno). Un dispositivo sin una contraseña le deja la puerta abierta a terceros a que accedan a toda esta información. La mejor opción es una clave alfanumérica de al menos 6 dígitos. Desactivar las opciones de reconocimiento facial y huellas dactilares (son más inseguras).	
Separar las cuentas personales de las profesionales, y compartimentar las cuentas de redes sociales y de mensajerías.	Cuando se tiene una actividad política se debe pensar estratégicamente en la construcción de la identidad digital y las comunicaciones que se quieren tener. Se pueden tener perfiles diferentes en distintos dispositivos. Se recomienda separar la identidad digital en una de carácter más personal (donde compartes información solo con tu círculo más cercano y quizás uses un pseudónimo, o donde envíes correos de índole personal) y otra, pública, donde compartes con el resto de las personas.	
Configurar la privacidad en las plataformas que usas, en especial, redes sociales y mensajería	Revisar y modificar las configuraciones de privacidad de tu cuenta, de acuerdo con tu estrategia (participación en las redes con tu identidad digital); existe una diversidad de 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 o solicitudes de amistad, entre otras. No dejar la configuración de privacidad por defecto que tienen las redes sociales.	
Respaldar los datos de tus dispositivos de manera periódica	Para evitar la pérdida de información en caso robo o daño. Se puede realizar en un servicio de almacenamiento en línea o, preferentemente, de forma física en un disco duro externo. Otra alternativa es a través de carpetas cifradas: existen varios programas[12] que te permiten añadir una contraseña a archivos y carpetas en tu computadora, de modo que solamente las personas con la clave puede tener acceso a ellos.	

Prevenir el phishing	Tiene como finalidad engañarte para que reveles contraseñas o para que se instale algún malware (programa malicioso) en tu dispositivo; suelen realizarse a través de mensaje (por correo electrónico, SMS, chat, etcétera) para que hagas clic en un enlace, o abras algún documento, o instales algún software en tu dispositivo, o ingreses tu nombre de usuario y contraseña en un sitio web, plataforma que luce real. 5 consejos para prevenirlo: sólo ingresa contraseñas en sitios web reales; verifica las direcciones de los correos de los remitentes; activa la verificación en dos pasos; abre los documentos sospechosos en Google Drive; mantén actualizado los softwares (los Programas y aplicaciones) en todos tus dispositivos.	
Construir comunidad en línea con otras mujeres colegas, o que compartan semejante trayectoria, mismos intereses y causas	Que puedan brindarte apoyo público y soporte emocional ante una eventual situación de ciberviolencia. Participa activamente en estos grupos tanto en la virtualidad como en la vida real, y brinda apoyo a otras mujeres que atraviesen este tipo de situaciones.	
Tener especial cuidado con las personas que conocemos en línea	Se recomienda partir de la presunción que cualquier persona que conocemos en este medio puede infiltrarse en nuestra vida personal, familiar, laboral o negocios con fines maliciosos.	

Fuente: Elaborada con base al trabajo de Nina Jankowics "*How to be a woman online. Surviving abuse and harrasment and how to fight back"* (2022); y la *"Guía práctica contra la violencia política de género digital" de la* Fundación Friedrich Ebert Stiftung (FES).

7 Según bibliografía mencionada, existen servicios para bloquear/eliminar cuentas falsas o maliciosas de las redes sociales tales como BlockParty;que, por el momento, funciona solo para Twitter.

8 Según bibliografía mencionada, los servicios de mensajería encriptados son: WhatsApp, Telegram (los usuarios/as deben activar la encriptación) ySignal (que además no realiza back up del historial de las conversaciones y permite desaparecer el contenido de las conversaciones individuales); los servicios no encriptados: Facebook Messenger o mensajes de textos. Servicios de mail encriptados: ProtonMail (cobra una tarifa, pero brinda una capa más de seguridad que aquellos proveedores más conocidos); Gmail (especialmente si se usa un administrador de contraseñas, el autenticador multi-factor; además, Google tiene un Programa Avanzado de Protección)

9 Redes privadas de Internet (VPN) nombradas en la bibliografía citada: Express VPN; Surfshark; NordVPN; Proton VPN; IPVanish.

10 Sitios como DeleteMe (arancelado); este sitio provee también guías gratuitas para la realización particular de esta tarea (borrar información y datos valiosos en línea).

11 Facebook, Instagram, Tik Tok, Google: tienen políticas especiales de protección de mujeres con perfiles públicos en cada una de sus plataformas. Facebook: herramientas de seguridad para mujeres, y para mujeres que son figuras públicas; Instagram: Guía de seguridad para mujeres en la política Tik Toc: Normas de la comunidad, secciones "intimidación y acoso" y "comportamiento de odio"; Twitter: Alfabetización y seguridad digital.

12 Se menciona n los siguientes programas en la bibliografía citada: Truecrypt, Sophos Free Encryption o Axcrypt.

3.3 Test para identificar medidas de mitigación de la violencia digital contra las mujeres en la vida política

Medida de mitigación	Detalle/recomendación	
Chequear la existencia de cuentas falsas entre tus seguidores/as, entre tus "amigos/as" de las redes sociales	Se pueden tener en cuenta los siguientes criterios: fecha de creación (si es reciente pero tiene un gran caudal de seguidores/as o amigos/as puede ser falsa); ¿Tiene foto? Si tiene, ¿es genérica o específica?; ¿Tienes amigos/as o seguidores/as en común con la cuenta en cuestión?; ¿Presenta información sospechosa, o abiertamente discriminatoria o violenta hacia mujeres? No son exhaustivos.	
Utilizar las opciones "dejar de seguir", "bloquear" o "eliminar"[13]	A las cuentas falsas o maliciosas, las cuentas falsas o maliciosas, y aquellas que proponen contenidos violentos (fascistas, neonazis o antifeministas, etc.) y/o formas de interacción violentas (haters).	
Utilizar las opciones "ignorar y silenciar"	A aquellas cuentas que presentan conductas "mansplainers", o que demandan atención y explicaciones para discutir contigo con la finalidad de minimizarte o ridiculizarte (no es un debate real y democrático); también con Trolls. evitar contestar comentarios o entablar discusiones con estos perfiles/cuentas.	
Buscar apoyo público institucional por parte de organizaciones de la sociedad civil durante ataques coordinados	En sindicatos, grupos académicos, organizaciones sociales y de mujeres; incluso empleadores/as.	
Intentar entrar en contacto con algún representante –persona humana- de la plataforma o red social	Donde ocurre la situación de violencia, acoso o ataque, a los fines de reportar/denunciar la violación a los términos y condiciones de uso de esta.	
Documentar minuciosamente y guardar todas las acciones y manifestaciones de violencia, acoso y ataques recibidos	En diversas plataformas, sitios o redes sociales, a los fines de realizar una denuncia y recurrir a un proceso judicial. Tratar de juntar el máximo de información posible; guardar en el dispositivo, en la nube y en servicios online.[14]	
Realizar una consulta jurídica, iniciar un proceso judicial	A los fines de poner fin a la violencia digital, sancionar a la/s personas/s agresoras y lograr una reparación.	
Realizar consultas por salud mental y/o tratamiento terapéutico	Durante o luego de los ataques, acosos u hostigamientos, a los fines de lograr bienestar.	

Fuente: Elaborada con base al trabajo de Nina Jankowics *"How to be a woman online. Surviving abuse and harrasment and how to fight back"* (2022); y la *"Guía práctica contra la violencia política de género digital" de la* Fundación Friedrich Ebert Stiftung (FES). [13][14]

13 Según bibliografía mencionada, existen servicios para bloquear/eliminar cuentas falsas o maliciosas de las redes sociales tales como BlockParty; que, por el momento, funciona solo para Twitter.

14 Para documentar casos de violencia digital en diversas redes sociales - acosos, hostigamientos, ataques-: Wayback Machine's Internet Archive;
Hunchly; PageVault (proveen servicios arancelados). El Proyecto #Seguridad Digital cuenta con un Manual para registrar y documentar incidentes

Glosario de términos

- **Hackeo:** acceso no autorizado a las cuentas y dispositivos de una persona. Suplantación de identidad: hackeo o creación de falsos perfiles personales, para difundir noticias falsas, información personal, ataques a otras personas, etc. Monitoreo, control y vigilancia en línea: rastreo constante de las actividades online y offline de una persona.
- **Blackouts**: o apagón de internet. Una interrupción de la internet causada por un ataque a un sitio web, a un proveedor de servicio de internet (ISP) o al sistema de nombres de dominios de internet (DNS). También puede ser una interrupción debido a una configuración incorrecta de la infraestructura del servidor web.
- **Keyloggers:** o registrador de teclas. Es un software malicioso que se coloca entre el teclado y el sistema operativo para interceptar y registrar información de cada tecla pulsada en el dispositivo sin que la persona usuaria lo sepa.
- **Bluejacking:** es una técnica consistente en enviar mensajes no solicitados entre dispositivos Bluetooth, como, por ejemplo, teléfonos móviles o computadoras portátiles.
- **Phishing:** o ataque de pesca de información. Es una estafa cometida a través de una comunicación electrónica engañosa y aparentemente oficial (correo electrónico, mensaje de texto o telefónicamente) mediante la cual el estafador o phisher suplanta la personalidad de una persona o empresa de confianza para que la persona receptora facilite información confidencial (contraseñas, datos bancarios, etc.).
- **Pharming:** ciberataque con el que se intenta redirigir el tráfico web al sitio del atacante, explotando vulnerabilidades de software en los sistemas de nombre de dominio o en los equipos de los propios usuarios.
- **Outing:** revelación en línea de la identidad o preferencia sexual de una persona, sin autorización ni consentimiento.
- **Malware** o programa malicioso. El término nace de la unión de las palabras en inglés malicious software y hace referencia a un tipo de software que tiene como objetivo infiltrarse y/o dañar un sistema de información sin el consentimiento de la persona usuaria.
- **Spyware:** software malicioso que se instala en los dispositivos de una persona para registrar todo lo que hace, incluidos los mensajes de texto, los correos electrónicos, las fotografías o hasta todas las teclas pulsadas. Con ciertos tipos de software malicioso, los agresores pueden encender de forma remota la cámara o el micrófono del teléfono móvil, rastrear la ubicación de la víctima, monitorear el uso de aplicaciones o interceptar llamadas.
- **Doxing** (o doxeo): consiste en la extracción y la publicación no autorizada de información personal —como el nombre completo, la dirección, números de teléfono,

correos electrónicos, el nombre del cónyuge, familiares e hijos, detalles financieros o laborales— como una forma de intimidación o con la intención de localizar a la persona en "el mundo real" para acosarla. También puede tener como objetivo publicar la información personal en sitios pornográficos junto con el anuncio de que la víctima está ofreciendo servicios sexuales.

- **Creepshot**. Se refiere a una foto tomada por un hombre a una mujer o niña en público sin su consentimiento. Las fotos suelen centrarse en los glúteos, las piernas o el escote de la víctima.
- **Cyberflashing:** envío de fotografías obscenas a una mujer sin su consentimiento con el objetivo de molestarla, intimidarla o incomodarla.
- **Deepfake** o video ultra falso. Técnica de inteligencia artificial que permite editar videos falsos de personas que aparentemente son reales mediante el uso de algoritmos de aprendizaje y videos o imágenes ya existentes.
- **Trolls**: usuarios no identificados que dirigen mensajes violentos y ofensivos, con frecuencia organizados en "ejércitos", "granjas" o netcenters, para actuar de forma simultánea creando una verdadera turba virtual en coordinación con usuarios regulares de las redes, anónimos o no.
- **Troleo de género**: es la publicación de mensajes, imágenes o videos, así como la creación de hashtags, con el propósito de molestar a mujeres o incitar a la violencia contra ellas.
- **Bots**: cuentas creadas para generar mensajes de forma automática y repetitiva, y diseminarlos rápida y masivamente.
- **Sextorsión:** consiste en amenazar a una persona con difundir imágenes o videos íntimos con la finalidad de obtener más material sobre actos sexuales explícitos, mantener relaciones sexuales, sacar dinero u obligar a realizar algo a la víctima en contra de su voluntad. Esta forma de violencia afecta desproporcionadamente a mujeres.
- **Geolocalización.** Es la capacidad para obtener la ubicación geográfica real de un objeto, como un radar, un teléfono móvil o un ordenador conectado a internet.

Bibliografía

Aboulez, N.; Harrison, J.; Posetti, J. & Waisbord, S. *"Online violence Against Women Journalists: A Global Snapshot of Incidence and Impacts*". United Nations Educational, Scientific and Cultural Organization (UNESCO), International Center for Journalists (ICFJ). Publicación electrónica: https://unesdoc.unesco.org/ark:/48223/pf0000375136

Albaine, Laura. "*Violencia contra las mujeres en política: hoja de ruta para prevenirla, monitorearla, sancionarla y erradicarla"*, con el apoyo de ONU Mujeres, el Programa de las Naciones Unidas para el Desarrollo (PNUD) y el Instituto Internacional para la Democracia y la Asistencia Electoral (IDEA), en el marco de "Atenea, por una democracia 50-50". Año 2020. Publicación electrónica: https://ateneaesparidad.com/wp-content/uploads/2021/03/IDEA-Atenea-Final.pdf

Albornoz, D. y Flores, M. "*Conocer para resistir. Violencia de género en línea en Perú"* Hiperderecho. Perú. Año 2018. Link: https://hiperderecho.org/tecnoresistencias/wp-content/uploads/2019/01/violencia_genero_linea_peru_2018.pdf

Alcaraz, F.; Beck, I.; Rodríguez, P. *"Violencia de género en línea hacia mujeres con voz pública. Impacto en la libertad de expresión*". Estudio realizado en el marco de un acuerdo de trabajo conjunto entre la Alianza Regional por la Libre Expresión e Información y ONU Mujeres para las Américas y el Caribe. Año 2022. Publicación electrónica: https://lac.unwomen.org/sites/default/files/2023-03/Informe_ViolenciaEnLinea-16Mar23.pdf

Asamblea General de las Naciones Unidas. *"Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias*". Consejo de Derechos Humanos, 32º período de sesiones, tema 3 de la agenda "Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo". Abril de 2016. Publicación electrónica: https://www.ohchr.org/es/special-procedures/sr-violence-against-women

Comisión Interamericana de Mujeres / Mecanismo de Seguimiento de la Convención de Belém do Pará de la Organización de Estados Americanos. "*La violencia de género en línea contra las mujeres y niñas: guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta*"; [Preparado por la Secretaría General de la Organización de los Estados Americanos], v; cm. (OAS. Documentos oficiales; OEA/Ser.D/XXV.25). Publicación electrónica: https://www.oas.org/es/sms/cicte/docs/Guia-conceptos-basicos-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf

Comisión Interamericana de Mujeres / Mecanismo de Seguimiento de la Convención de Belém do Pará de la Organización de Estados Americanos y ONU Mujeres. *"Informe Ciberviolencia y Ciberacoso contra las mujeres y niñas en el marco de la Convención Belém Do Pará";* herramientas para la Implementación de la Convención de Belém do Pará. Una alianza entre la Organización de los Estados Americanos y ONU Mujeres en el marco de la Iniciativa Spotlight en América Latina. Año 2022. Publicación electrónica: http://www.oas.org/es/mesecvi/docs/MESECVI-Ciberviolencia-ES.pdf

Defensoría del Público de Servicios de Comunicación Audiovisual de la Nación, Argentina; Fondo de Población de las Naciones Unidas (UNFPA). *"El abordaje mediático de la violencia de género digital. Claves para una comunicación responsable*". Argentina. Año 2023. Publicación electrónica: https://defensadelpublico.gob.ar/wp-content/uploads/2023/03/violencia-en-entornos-digitales-v3.pdf

Equipo Latinoamericano de Justicia y Género (ELA). "*Violencia contra las mujeres y disidencias en política a través de redes sociales Una aproximación a partir del análisis de la campaña electoral en Twitter, Facebook e Instagram durante 2019*". Buenos Aires, mayo 2020. Publicación electrónica: https://www.ela.org.ar/c/app187/53/87/43/4234

Instagram, ONU Mujeres, Instituto Nacional Electoral (INE). *"Guía de seguridad de Instagram para mujeres en la política*". Publicación electrónica: https://about.fb.com/ltam/wp-content/uploads/sites/14/2021/04/Gui%CC%81a-de-seguridad-de-Instagram-para-mujeres-en-poli%CC%81tica.pdf

Jankowicz, Nina. "How to be a woman online. Surviving abuse and harrasment, and how to fight back". 1st Edition, Bloomsbury Academic & Publisher. April, 2022.

Luchadoras. *"La violencia en línea contra las mujeres en México. Informe para la Relatora sobre Violencia contra las Mujeres Ms. Dubravka* Šimonović"; con el apoyo de Henrich Böll Stiftung México y El Caribe y Asociación para el Progreso de las Comunicaciones (APC). Noviembre 2017. Publicación electrónica: https://luchadoras.mx/wp-content/uploads/2017/12/Informe_ViolenciaEnLineaMexico_InternetEsNuestra.pdf

Luchadoras. "Violencia política a través de las tecnologías contra las mujeres en México. Elecciones 2018"; con el apoyo del Instituto Nacional Demócrata (NDI). Septiembre de 2018. Publicación electrónica: https://archive.org/details/ViolenciaPoliticaATravesDeLasTecnologiasContraLasMujeresEnMexico

Mecanismo de Seguimiento de la Convención de Belém do Pará (MESECVI) de la Organización de Estados Americanos. "*Declaración sobre la Violencia y el Acoso Políticos contra las Mujeres",* durante la Sexta Conferencia de los Estados Parte de la Convención. Lima, Perú. Año 2015. Publicación electrónica: https://www.oas.org/es/mesecvi/docs/declaracion-esp.pdf

ONU Mujeres. "*Guía sobre la violencia política de género contra las mujeres en medios de comunicación y redes sociales"*, con el apoyo del Departamento de Asuntos Políticos y de Consolidación de la Paz de las Naciones Unidas (UNDPPA), y en alianza con el Programa de las Naciones Unidas para el Desarrollo (PNUD) en el marco del Proyecto 'Apoyo al Ciclo Electoral en Ecuador 2020-2022'. Publicación electrónica:https://www.undp.org/es/ecuador/publications/gu%C3%ADa-sobre-violencia-pol%C3%ADtica-de-g%C3%A9nero-contra-las-mujeres-en-medios-de-comunicaci%C3%B3n-y-redes-sociales

ONU Mujeres. *"Cuantificación y análisis de la violencia contra las mujeres políticas en redes sociales"*. Uruguay. Año 2022. Publicación electrónica: https://lac.unwomen.org/es/digital-library/publications/2022/03/cuantificacion-y-analisis-de-la-violencia-contra-las-mujeres-politicas-en-redes-sociales-uruguay#view

Peña, Paz. *"Guía práctica contra la violencia política de género digital".* Fundación Friedrich Ebert Stiftung (FES), en el marco del Proyecto Regional FESminismos. Mayo 2022. Publicación electrónica: https://library.fes.de/pdf-files/bueros/chile/19251-20220914.pdf

Souza, L. y Varón, J. Policy Paper América Latina y El Caribe *"Violencia política de género en Internet"*; consorcio de organizaciones de la sociedad civil "Al Sur". Año 2021. Publicación electrónica: https://www.alsur.lat/sites/default/files/2021-07/Violencia%20Pol%C3%ADtica%20de%20G%C3%A9nero%20en%20Internet%20ES.pdf

Legislación:

México:

a) "Ley Olimpia" (año 2020) ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf http://bibliodigitalibd.senado.gob.mx/handle/123456789/5043

Brasil:

b) Ley N° 13.718 (año 2018) http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm

c) Ley N° 13.642 "Ley Lola" (año 2018) http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13642.htm

d) Ley N° 12.965 "Marco Civil de Internet" (año 2014) https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

e) Ley N° 12.737 "Ley Carolina Dieckmann" (año 2012) https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

f) Ley General de Protección de Datos N° 13.709 (año 2018) https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Jurisprudencia:

Comisión Interamericana de Derechos Humanos (CIDH), Resolución N° 76/2021, Medida cautelar No. 475-21 sobre "Bertha María Deleón Gutiérrez respecto de El Salvador", 19 de septiembre de 2021. https://www.oas.org/es/cidh/decisiones/mc/2021/res_76-21_mc_475-21_sv_es.pdf

Tribunal de Juicio del Primer Circuito Judicial de Panamá. Sentencia N°78/TJ-J sobre delitos contra el Honor, en la modalidad de Calumnia e Injuria.de 30 de abril de 2021. https://www.organojudicial.gob.pa/noticias/tribunal-de-juicio-sanciona-a-un-ciudadano-por-delito-de-calumnia-e-injuria

Cámara Nacional Electoral, República Argentina. Causa: "Unión Cívica Radical y otros/ impugnación de acto de órgano o autoridad partidaria - integrantes del tribunal de Conducta U.C.R solicita se deje sin efecto decisión del comité Provincia U.C.R.". Año 2021. https://www.electoral.gob.ar/nuevo/paginas/jurisprudencia/resultado_periodo.php

Políticas públicas:

Instituto de las Mujeres de la Ciudad de México. "Plan de acciones públicas a emprender de manera integral" (año 2016). Enlace: https://semujeres.cdmx.gob.mx/violencia-digital

Ministerio de la Mujer y Poblaciones Vulnerables del Gobierno de Perú. "*Lineamientos para la Atención en los Centros de Emergencia de la Mujer a Mujeres Políticas Afectadas por Hechos de Acoso Político*" (Resolución de la Dirección Ejecutiva 51-2018-MIMP/ PNCVFS-DE). https://observaigualdad.jne.gob.pe/documentos/acoso_politico/herramientas/Lineamientos%20para%20la%20atenci%C3%B3n%20en%20los%20CEN-MIMP%20a%20mujeres%20pol%C3%ADticas.pdf

¿TE HA SIDO ÚTIL ESTE MATERIAL?

Cuéntanoslo en **spcim@oas.org**

OEA | CIM

Comisión Interamericana de Mujeres

www.oas.org/es/cim

spcim@oas.org

ComisionInteramericanaDeMujeres

@CIMOEA

@cim.oea

MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN

aecid

Cooperación Española