

CUERPOS DIGITALES, TERRITORIOS EN DISPUTA

Análisis feminista de las violencias digitales contra las defensoras de derechos humanos en Mesoamérica

IM-DEFENSORAS

AGRADECIMIENTOS

Tienes en tus manos el resultado de un esfuerzo y compromiso colectivo que nace de la necesidad que tenemos las defensoras mesoamericanas por comprender la situación que enfrentamos en el ámbito digital y desmitificar la inocuidad de las tecnologías digitales en nuestra labor y trayectoria de vida.

Este informe es parte de un proceso más amplio de trabajo riguroso que venimos impulsando en la IM-Defensoras por la justicia, los cuidados y la protección integral en las distintas dimensiones de nuestra vida, donde lo digital es parte de los territorios que habitamos.

Fue gracias a la generosidad, disposición y confianza de decenas de defensoras mesoamericanas que han sido víctimas de violencias digitales que hoy podemos compartir este análisis feminista a nivel regional y a quienes honramos por su valentía y compromiso. Este informe no hubiera sido posible sin el compromiso y disposición de las redes de defensoras quienes validaron los hallazgos que aquí compartimos. También queremos agradecer al equipo de investigadoras feministas que lideraron este proceso, a las aliadas estratégicas que fueron parte del conseo asesor, así como también a las organizaciones dedicadas a la defensa de los derechos digitales que nos orientaron con su experiencia en la construcción de este análisis.

EQUIPO DE INVESTIGACIÓN

Paz Peña Ochoa - Investigadora principal

Nicole Yañez - Honduras

Defensora nicaraguense

Philippa Williams - México

Mariana Moisa - El Salvador

CONSEJO ASESOR

Lulú Barrera

Florencia Goldsman

Jes Ciacci

Joana Varon

Nicole Yañez

Tanya Lockwood

COORDINACIÓN, ELABORACIÓN, EDICIÓN Y REVISIÓN DEL TEXTO

Marusia López Cruz, Mar Cervantes, Ana Clara, Berta Moya, Loreto Bravo Muñoz, Lydia Alpízar Durán

Ilustraciones: Sara Kulli

Diseño editorial: María Fe Alpízar

Equipo editorial: Beatriz Escalante y Ruth Orozco

Cuidado editorial: Equipo de comunicación IM-Defensoras

Traducción al inglés: Analía Penchaszadeh

VALIDACIÓN DEL INFORME

El Salvador: Floria

Red Nacional de Defensoras de Derechos Humanos en Honduras: Yesica Trinidad

Red Nacional de Defensoras de Derechos Humanos en México: Aleida Quintana

Nicaragua: Colibrí y Carmen Flores

MESOAMÉRICA. NOVIEMBRE, 2026

IM-DEFENSORAS

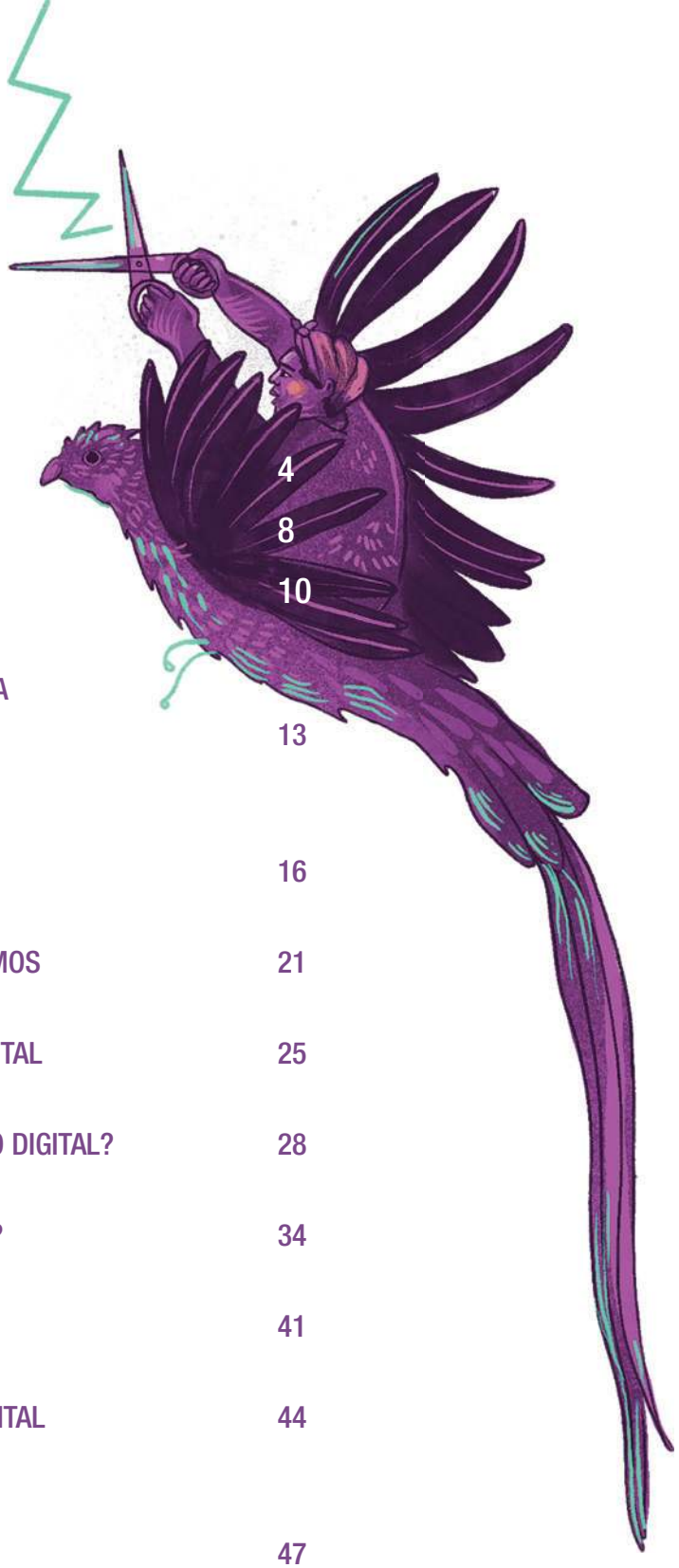


TABLA DE CONTENIDO

RESUMEN EJECUTIVO 4

1. INTRODUCCIÓN 8

2. METODOLOGÍA 10

3. ASPECTOS CLAVES PARA ANALIZAR LA VIOLENCIA DIGITAL EN EL CONTEXTO MESOAMERICANO 13

4. ¿CÓMO NOS RELACIONAMOS LAS DEFENSORAS MESOAMERICANAS CON LAS TECNOLOGÍAS? 16

5. LA VIOLENCIA DIGITAL A LA QUE NOS ENFRENTAMOS 21

6. LA DIMENSIÓN DE GÉNERO DE LA VIOLENCIA DIGITAL 25

7. ¿QUÉ AGRESIONES ENFRENTAMOS EN EL ÁMBITO DIGITAL? 28

4. ¿QUIÉNES NOS AGREDEN EN EL ÁMBITO DIGITAL? 34

9. ¿CÓMO NOS AGREDEN EN EL ÁMBITO DIGITAL? 41

10. LA INQUIETANTE IMPUNIDAD EN LA ESFERA DIGITAL 44

11. ¿A QUÉ RIESGOS NOS EXPONE LA VIOLENCIA EN EL ÁMBITO DIGITAL? 47

12. RECOMENDACIONES 50

RESUMEN EJECUTIVO



Las defensoras mesoamericanas de derechos humanos desarrollamos nuestra labor en contextos cada vez más complejos debido a la hegemonía del patriarcado capitalista, racista y colonial que profundiza las desigualdades y los conflictos sociales y territoriales, precariza nuestras vidas, despoja nuestras comunidades y nos expulsa de nuestros territorios. Como consecuencia, en la actualidad asistimos a una profundización del autoritarismo, al debilitamiento de las ya de por sí frágiles instituciones públicas y al auge de discursos ultraconservadores que ponen en riesgo los avances logrados en materia de derechos humanos. Las agresiones en nuestra contra son la respuesta de los Estados y los poderes fácticos ante nuestra denuncia e impugnación de las políticas de muerte que nos pretenden imponer. A través de éstas, nuestros agresores también buscan reestablecer la jerarquización racial y de género mediante el disciplinamiento, el amedrentamiento y la desligitimización de nuestro trabajo.

Una de las expresiones más visibles y recurrentes de la violencia que enfrentamos las defensoras es la que se lleva a cabo a través de las tecnologías digitales, muchas veces bajo el amparo de marcos legales y políticas públicas que no sólo no nos protegen de ella, sino que incluso la posibilitan y legitiman.

Entre 2020 y 2025 nuestro sistema de registro documentó un total de 9,091 agresiones digitales contra 1337 defensoras y 179 organizaciones en El Salvador, Honduras, México y Nicaragua. Esto representa una de cada cuatro agresiones registradas durante el mismo período.

A través del diagnóstico que nutre este informe, el cual tiene dimensión regional, buscamos entender nuestra situación, en tanto que defensoras, en el ámbito digital; los contextos, patrones y modus operandi de las agresiones que vivimos; así como las estrategias de protección y cuidado digital que aplicamos.

Entre los principales hallazgos hemos identificado que los marcos legales y políticos existentes **en nuestros países son débiles e insuficientes para proteger nuestros derechos en el ámbito digital; o que directamente son manipulados para perjudicarnos.** También se hace patente la **enorme inversión en recursos orientados a desplegar un amplio rango de estrategias digitales en contra nuestra;** desde las que buscan sembrar desinformación hasta las que nos someten a actos de vigilancia ilegal por medio del llamado software espía *(spyware)*.

"El mundo digital allana caminos para ataques más directos"

Otra evidencia a destacar es **la línea de continuidad entre los ataques digitales y los no digitales,** los cuales tienen las mismas causas y perpetradores y se dan en nuestra experiencia vital como un todo, pues ambos tipos de violencia se mezclan y se entrecruzan. En Honduras, El Salvador, México y Nicaragua, **el Estado es uno de los principales perpetradores de violencia digital.** Muchos gobiernos, en connivencia con diversos poderes fácticos, han iniciado procesos de criminalización de la labor de organizaciones de derechos humanos, lo que implica que los recursos públicos —financieros, policiales y, muchas veces, militares— se usen para perseguirnos. **No obstante, los perpetradores de violencia digital provienen de diversos ámbitos, desde empresas o grupos ultraconservadores hasta nuestros círculos cercanos e incluso íntimos.**

“Llega un punto en que no sabemos quién podría ser un agresor: si es un agresor estatal, si es un agresor por un tema de la defensa, o si puede ser un ex demente que todavía sigue clavado”

Asimismo, **hemos constatado una gran coincidencia en la tipología de los ataques digitales que se cometen en la región.** Se trata de patrones de agresión que muestran los grandes riesgos digitales a los que estamos expuestas. Las campañas de desinformación de género son unas de las agresiones que se han hecho más frecuentes en los últimos años. Éstas generan preocupación y desgaste en quienes las viven, sobre todo porque muchas veces están involucrados en ellas altos funcionarios. Entre las otras agresiones digitales más comunes destacan el acoso digital, las amenazas a nuestra integridad física y la de nuestro círculo más cercano, la violencia sexual digital, la vigilancia y, especialmente en contextos autoritarios, nuestra desanonimización.

“En las agresiones recibimos comentarios bien fuertes sobre nuestros cuerpos: comparaciones, burlas... El valor de la mujer reside sobre nuestros cuerpos”

La razón de mayor peso que tienen nuestros agresores para recurrir a la violencia digital es su eficacia, dada la relación costo-beneficio que presenta. Esto se debe a varios factores: una inquietante persistencia de la impunidad, la naturalización de la violencia digital en las sociedades —incluso por parte de nosotras mismas—, falta de protección legal, desconfianza para denunciar —puesto que en no pocas ocasiones la agresión proviene del Estado—, y la convicción de que las corporaciones del sector digital, por acción u omisión, no brindan los estándares mínimos para gestionar y resolver las denuncias.

Los impactos de la violencia digital sobre nosotras, nuestras familias, comunidades y colectividades u organizaciones abarcan un amplio espectro: afectaciones en nuestra salud mental y física, pérdidas materiales y económicas, desplazamiento forzado, pérdida de participación política y detrimento de nuestros derechos humanos. Todas estas afectaciones también se traducen en impactos políticos que buscan debilitar nuestras luchas y movimientos.

“No hemos dimensionado los miedos que provocan estos mensajes. Creemos que lo que te puede afectar es que alguien te agreda, te persiga, o lleguen a tu casa, pero no dimensionamos, ni siquiera sistematizamos, las agresiones que se están dando en las plataformas”

Pese a todo, una evidencia positiva que se desprende de esta situación es la adquisición, por nuestra parte, de una mayor conciencia sobre los cuidados digitales que debemos aplicar. Más aún, muchas de nosotras, en distintos grados, ya estamos en contacto con materiales, cursos o acompañamientos en cuidados digitales. En las reflexiones y prácticas de las defensoras que han participado en este estudio se evidencia como la mayoría ya contamos con un acervo de cuidados digitales y con una visión crítica de las tecnologías.

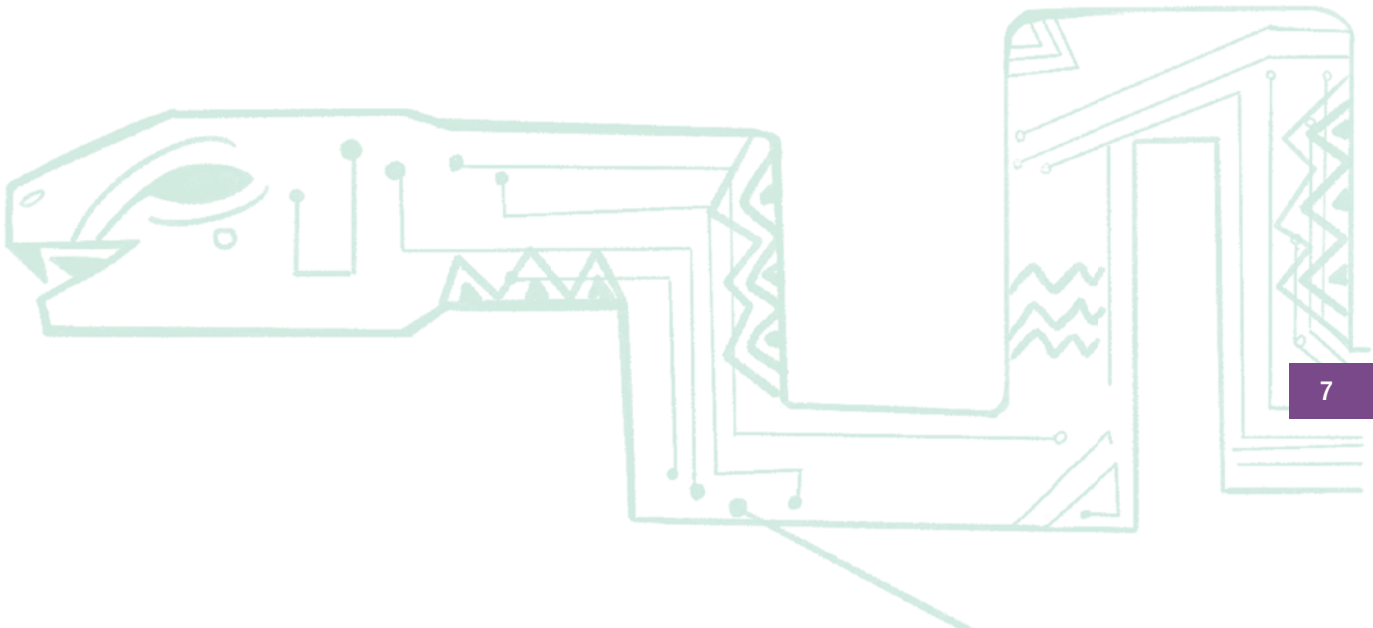
Finalmente, a partir de los hallazgos de este diagnóstico generamos una serie de recomendaciones dirigidas a cuatro actores clave:

1) A los Estados los exhortamos a reconocer la gravedad de la violencia digital que enfrentamos las defensoras de derechos humanos, a crear mecanismos de protección y rendición de cuentas ante estas agresiones y a abstenerse de utilizar tecnologías digitales para la vigilancia, censura o criminalización.

2) A los mecanismos internacionales y organismos de derechos humanos les recomendamos ampliar la definición de violencia digital contra defensoras reconociendo el vínculo de ésta con la violencia en el ámbito físico; así como impulsar el desarrollo de estándares, investigaciones, guías y fondos de emergencia que respondan a las agresiones digitales con perspectiva de género.

3) A las corporaciones de redes sociales les demandamos priorizar los derechos humanos sobre las ganancias, invirtiendo en mecanismos de atención y protección con enfoque de género y cooperación transnacional para identificar las violencias y a sus perpetradores y garantizar reparación del daño y la no repetición.

4) A nuestras organizaciones sociales y de derechos humanos les recomendamos integrar la seguridad digital y el bienestar psicosocial como componentes permanentes de las estrategias de protección, con enfoques contextualizados y perspectiva interseccional. También recomendamos visibilizar los vínculos entre violencia digital y la perpetrada en el ámbito físico, y fortalecer la documentación de las agresiones facilitadas por la tecnología, la capacidad de respuesta personal y colectiva ante los ataques digitales, y la colaboración para responder de manera coordinada y exigir rendición de cuentas a los Estados y empresas tecnológicas.



1 INTRODUCCIÓN



En Mesoamérica, como en el resto del planeta, vivimos un contexto político cada vez más complejo, en el que las tecnologías digitales se han convertido en herramientas para la resistencia y la defensa de derechos humanos, pero también para ejercer la represión y prácticas de vigilancia por parte de Estados y otros actores. Ante ello, esta investigación busca fortalecer nuestra comprensión, en tanto que defensoras de derechos humanos, sobre cómo se despliega la violencia digital en El Salvador, Honduras, México y Nicaragua, así como respecto a las estrategias de protección por las que apostamos desde la IM-Defensoras para hacerle frente: la Protección Integral Feminista (PIF) y, en particular, nuestra estrategia de Protección y Cuidados Digitales.

Esta tarea la abordamos mediante el análisis de los diferentes actores, contextos y marcos políticos —ideológicos, económicos, legales e institucionales— que inciden en los riesgos, así como en el de nuestras posibilidades reales y las de nuestros movimientos, organizaciones, colectivas y comunidades, para acceder a estrategias y medidas de protección y cuidados.

Así, desde un análisis feminista e interseccional que contempla la diversidad de condiciones socioeconómicas y culturales en las que desarrollamos nuestra labor como defensoras, a través de esta investigación buscamos responder a los siguientes objetivos:

- Entender nuestra situación en el ámbito digital.
- Identificar las acciones y estrategias de protección y cuidado digital que aplicamos, así como las lecciones aprendidas.
- Identificar a los perpetradores directos o indirectos de las agresiones que enfrentamos en el ámbito digital.

El informe inicia con un capítulo de alcance regional en el que reflexionamos sobre los aspectos contextuales clave que intervienen en el análisis de nuestra situación en el ámbito digital; sigue con un diagnóstico cuanti-cualitativo de la violencia digital que enfrentamos, incluyendo la dimensión de género, los perpetradores, los ataques más comunes, los riesgos que implican en nuestras vidas y proyectos políticos, así como nuestras necesidades prioritarias de protección y seguridad digital. El capítulo concluye con una serie de recomendaciones que buscan fortalecer nuestras luchas y capacidades de protección, así como el trabajo a nivel regional de la IM-Defensoras y de las redes y articulaciones territoriales que la conforman.

A continuación, siguiendo una estructura similar, aterrizamos el análisis en El Salvador, Honduras, México y Nicaragua. En estos apartados, profundizamos en los contextos políticos particulares de cada uno de estos países, en los marcos legales y políticas públicas digitales existentes en los mismos, en el análisis de la relación de las defensoras con la tecnología y en las diferentes expresiones y *modus operandi* de las violencias facilitadas por la tecnología.

2 METODOLOGÍA



En la elaboración de este informe han participado cuatro investigadoras locales —una en cada uno de los países analizados: El Salvador, Honduras, México y Nicaragua—, quienes han desarrollado su trabajo a partir de la revisión de diversas fuentes bibliográficas y el análisis de las entrevistas en profundidad realizadas a cuatro defensoras de cada país entre marzo y julio de 2024.

Las dieciséis defensoras entrevistadas fueron seleccionadas con base en dos criterios:

1) Haber sido víctimas de violencia facilitada por medio de las tecnologías —con constancia de sus casos en nuestro registro de agresiones.

2) Que en conjunto reflejaran una diversidad de derechos defendidos y de procedencia territorial (Tabla 1).

Es importante mencionar que, debido a que nos enfrentamos a contextos políticos cada vez más represivos, a lo largo del informe garantizamos el anonimato de todas ellas como medida para preservar su seguridad y protección.

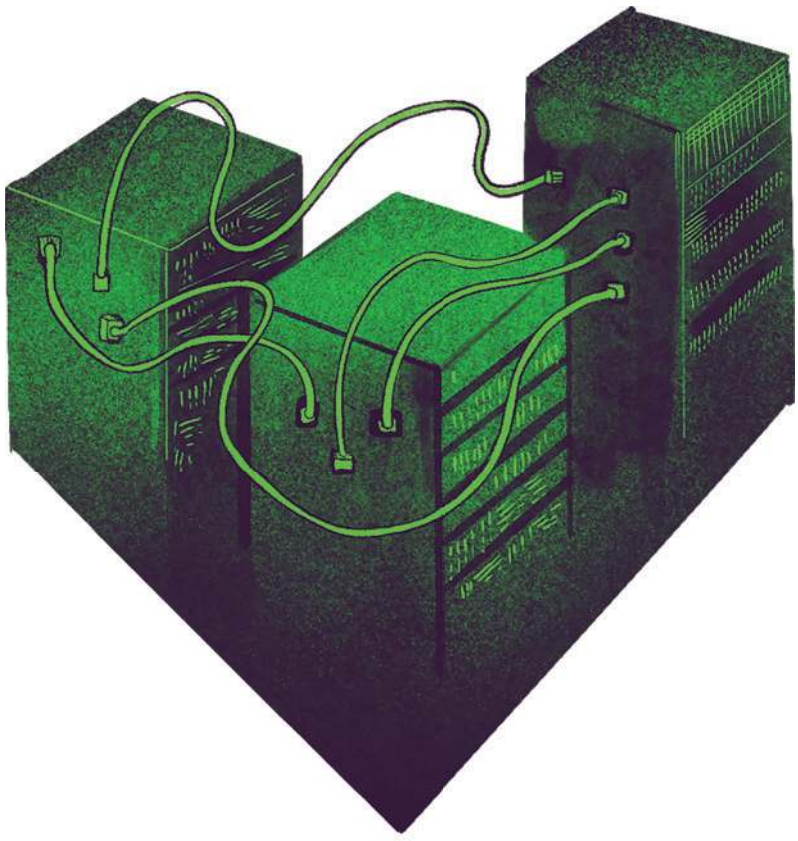
TABLA 1. PERFIL DE LAS DEFENSORAS ENTREVISTADAS

EL SALVADOR	HONDURAS	MÉXICO	NICARAGUA
Defensoras que trabajan en San Salvador, el occidente y el oriente del país. Defensoras acompañantes de familiares de víctimas de feminicidio. Defensoras por los derechos de las personas LGBTTIQ+, principalmente, por los de las mujeres trans. Defensoras por la libertad de expresión y la seguridad de periodistas que se encuentran en el exilio. Defensoras de los derechos sexuales y reproductivos de las mujeres. Defensoras que defienden el derecho a la tierra, el territorio y los bienes naturales.	Defensoras que trabajan por los derechos colectivos y los de las minorías. Defensoras que defienden sus territorios y los derechos políticos, económicos, sociales y culturales de los pueblos indígenas y indígenas, garífunas y afroamericanos. Defensoras que promueven la justicia, la equidad de género y los derechos sexuales y reproductivos de la mujer. Defensoras que defienden la libertad de expresión.	Defensoras de Oaxaca, Puebla, Estado de México y Ciudad de México. Defensoras cuya labor se centra en el derecho al trabajo, a la tierra y los bienes naturales. Defensoras que trabajan por la libertad de expresión. Defensoras feministas que luchan por los derechos de las mujeres a la autonomía, a la decisión sobre sus cuerpos, la libertad de reunión y de pensamiento.	Defensoras originarias del pacífico sur, centro, norte y Costa Caribe del país. Defensoras en el exilio. Defensoras de los derechos de las mujeres a una vida libre de violencias para las mujeres. Defensoras de la libertad de expresión y participación. Defensoras de la tierra, el territorio y los bienes naturales.

El informe también se nutre de las entrevistas en profundidad realizadas a ocho especialistas en seguridad digital y violencia de género facilitada y/o perpetrada a través de medios tecnológicos, quienes aportaron una mirada regional sobre las problemáticas vividas por las defensoras. La información cualitativa la complementamos con dos fuentes cuantitativas: los datos de violencia por medios digitales extraídos de nuestro **Registro mesoamericano de agresiones a defensoras de derechos humanos** y una encuesta en línea aplicada a defensoras de la región que han enfrentado violencia de género facilitada y/o perpetrada a través de medios tecnológicos.

La encuesta en línea se alojó en una plataforma segura. Las defensoras que la respondieron fueron seleccionadas por las redes y aliadas de la IM-Defensoras en los países objeto de estudio y contactadas por las investigadoras locales. Debido a las dificultades que planteaba la infraestructura digital y al tiempo que requería cumplimentar la encuesta se optó, además de por dar autonomía a las compañeras para responder individualmente, por brindar apoyo telefónico para contestar y hacer jornadas de acompañamiento presencial por parte de las investigadoras locales. Esto permitió garantizar que las defensoras dispusieran del acompañamiento psicoemocional y en protección y seguridad digital en los casos en los que fue necesario.

De esta forma, obtuvimos un total de 105 respuestas provenientes de los cuatro países: 25 de El Salvador, 27 de Honduras, 29 de México y 24 de Nicaragua. La mayoría de las defensoras encuestadas (83%) residen en los países analizados, mientras que 17% viven en países distintos al suyo de origen; entre éstas últimas, 11 se autoidentificaron como exiliadas.



ASPECTOS CLAVES PARA ANALIZAR LA VIOLENCIA DIGITAL EN EL CONTEXTO MESOAMERICANO

3



Tecnología y sociedad son inseparables, se interrelacionan y se co-constituyen una a la otra, por lo que no podemos analizar la tecnología como algo separado de las dinámicas sociales con las que interactúa. Así, para analizar nuestra situación como defensoras en el ámbito digital, resulta fundamental comprender factores de los contextos político, social y tecnológico que influyen en nuestras vidas. En esta investigación hemos identificado al menos dos aspectos contextuales clave a considerar: los políticos, que influyen en la situación de los derechos humanos en los diferentes países; y los que se refieren a las actuales lógicas de la economía política de las empresas tecnológicas dominantes. La combinación de ambos aspectos nos permite historizar nuestra situación en el ámbito digital y comprender los retos que tenemos por delante. En cada país y territorio, las tecnologías se insertan en un contexto de uso histórico particular, que se alimenta de fenómenos globales, como el auge de la ultraderecha y la agenda reaccionaria (ver figura 1).

FIGURA 1. FACTORES DEL CONTEXTO DE LA VIOLENCIA DIGITAL



En toda la región nos enfrentamos a dinámicas políticas, sociales y económicas generadas por la hegemonía del patriarcado capitalista, racista y colonial que profundiza las desigualdades y los conflictos sociales y territoriales, precarizando nuestras vidas, despojando a nuestras comunidades y expulsándonos de nuestros territorios. Ante este fenómeno, la respuesta política en la región mesoamericana —con diferentes matices en cada país— ha sido el auge de líderes con tintes autoritarios y retórica conservadora que interpretan el desencanto social imponiendo su narrativa y creando enemigos internos y externos para justificar sus políticas. Estos líderes siguen siendo voceros de los poderes fácticos que dominan la región: el empresariado extractivista, los líderes ultraconservadores, fundamentalistas religiosos o el crimen organizado. En los países estudiados, observamos cómo a las defensoras de derechos humanos la retórica polarizadora nos señala e identifica como "el enemigo", ya sea por nuestra posición pública como denunciantes de abusos del Estado y de los poderes fácticos o por nuestra agenda feminista y por la justicia social.

En este entramado de polarización discursiva, vemos que el uso estratégico de las tecnologías digitales, la consolidación de marcos legales restrictivos y la profundización de políticas autoritarias y militaristas son centrales para la gobernanza de los Estados y las agendas propias de los poderes fácticos. Además, parece que uno de los objetivos más importantes detrás de este modelo de gobernanza es interrumpir, acallar y deslegitimar nuestra labor.

En el ámbito digital de los distintos países existen, por un lado, marcos legales y políticos que resultan débiles o insuficientes para proteger nuestros derechos como defensoras, que van en contra de nuestra labor o que, directamente, son manipulados y aplicados maliciosamente para perjudicarnos. Por otro lado, se invierten recursos para desplegar un amplio abanico de estrategias digitales contra nosotras, las cuales pueden ir desde el permanente monitoreo de nuestros datos personales y la desinformación, a través de redes sociales, hasta la vigilancia ilegal con la implantación de programas espía, conocidos como *spyware*, que recopilan información de nuestros dispositivos sin nuestro consentimiento.

El papel que juegan las tecnologías en este ambiente hostil no ocurre porque sí, sino que es facilitado por los intereses de las corporaciones tecnológicas que favorecen, por acción y por omisión, la irrupción de violencias contra las defensoras. Las razones son muchas, entre ellas, que sus lógicas de ordenamiento de contenidos premian a los más violentos y ofensivos para poder generar mayores interacciones y, por ende, más datos que puedan ser extraídos y mercantilizados por las plataformas. Esto es aprovechado por los gobiernos de la región para accionar tácticas en el ámbito digital y agredir a cualquier persona percibida como opositora. La violencia, además, es un motor para el lucro económico de las plataformas, porque les da réditos y porque todavía les parece demasiado caro crear mecanismos sustentables que moderen los contenidos de un modo eficaz y a escala y que protejan los derechos humanos. En la mayoría de casos, se trata de empresas cuya base se encuentra en el llamado Norte global, lo que reproduce las dinámicas coloniales existentes y provoca que regiones como la nuestra sean terreno abonado para su capitalismo extractivo: las corporaciones tecnológicas extraen los recursos —en este caso, los datos personales de los estratos más empobrecidos de la población, quienes, además, sufren los efectos indeseados de esa operación, como la desinformación, por ejemplo— y se quedan con la riqueza que genera ese desigual intercambio.

Otro aspecto que merece una observación directa es el papel que están teniendo las grandes empresas tecnológicas en la infraestructura digital de los Estados. Como parte fundamental de su economía política y con el objetivo de consolidar su dominio planetario, entre otros servicios, las empresas proveen a los Estados de información digital *(big data)* que permite analizar el comportamiento de las personas para formular predicciones o alimentar la inteligencia artificial, e invierten en la infraestructura digital —satélites de conexión, cables submarinos, centros de datos, etcétera—. Sin embargo, como en el tecno-capitalismo los mercados están tan concentrados verticalmente, encontramos que los mismos dueños de plataformas como las redes sociales también dominan la infraestructura que posibilita los servicios de internet. Un ejemplo de estos vínculos entre Estados y empresas tecnológicas es la cercana relación de negocios que tiene la empresa Alphabet, a la que pertenece Google, con el gobierno de El Salvador.

Cualquier análisis, tanto presente como futuro, sobre la situación de las violencias que vivimos las defensoras en la región debe hacerse con base en estas dos importantes variables: el contexto político y la economía política de las empresas digitales; pues no hay política nacional ni territorial que no tenga una correlación con los intereses y la economía política de las corporaciones tecnológicas. Ambas se influyen y configuran el contexto social, económico y político en el que nos movemos las defensoras.

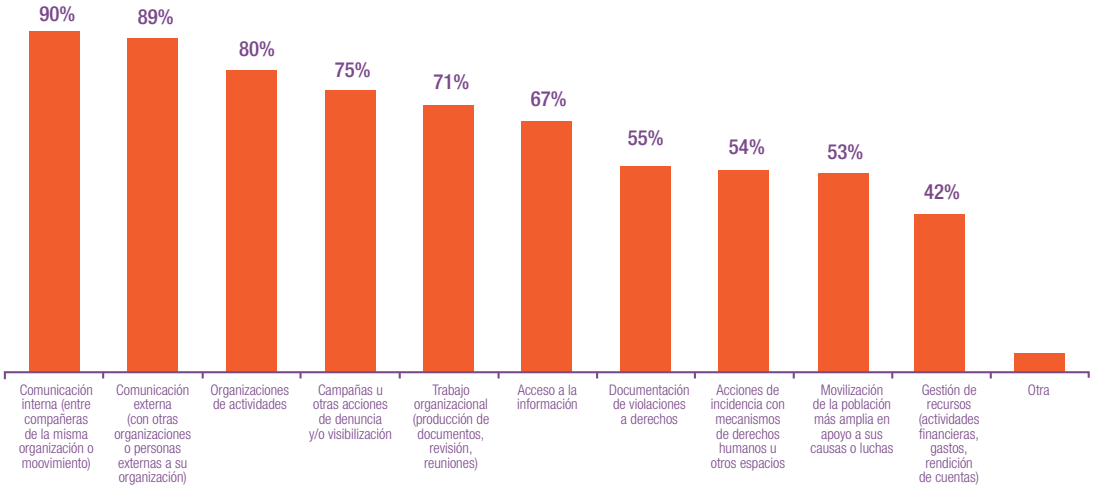
4 ¿CÓMO NOS RELACIONAMOS LAS DEFENSORAS MESOAMERICANAS CON LAS TECNOLOGÍAS?



De acuerdo con la encuesta en línea respondida por 105 defensoras de El Salvador, Honduras, México y Nicaragua, las defensoras mesoamericanas accedemos con mucha frecuencia a internet, ya sea a través de computadoras conectadas por banda ancha o fibra óptica, o por plan de conexión móvil a nuestros teléfonos inteligentes.

La gran mayoría de las encuestadas (79%) hacen uso continuo de aparatos conectados a internet y 77% emplea las tecnologías a diario para realizar acciones relacionadas con su activismo. Con relación a estas acciones, destaca el uso la comunicación interna (entre compañeras de la misma organización o movimiento), la comunicación externa (con otras organizaciones o personas fuera de su organización) y la organización de actividades (ver gráfico 1).

GRÁFICO 1. ¿CÓMO USA LAS TECNOLOGÍAS DIGITALES EN SU TRABAJO COMO DEFENSORA? (N: 105)



Con base en las entrevistas y las encuestas realizadas, es posible determinar cuatro factores que influyen en nuestra relación, acceso y apropiación de las tecnologías digitales:

1. La intersección entre nuestras diferentes identidades y condiciones socioeconómicas, culturales, étnicas, territoriales y sexo-genéricas.

2. Los pulsos políticos concretos de nuestros países y territorios.

3. Nuestros saberes sobre seguridad digital.

4. Las violencias digitales que hemos vivido como defensoras.

¿CÓMO LAS VARIABLES INTERSECCIONALES CONDICIONAN NUESTRA RELACIÓN CON LAS TECNOLOGÍAS?

La relación que tenemos las defensoras con las tecnologías está influenciada por nuestras condiciones sociales, económicas, étnicas, generacionales, territoriales y sexo-genéricas, entre otras, lo que se conoce como

interseccionalidades, pues éstas influyen en cómo accedemos y nos apropiamos de la tecnología y también en nuestro conocimiento y acceso a los cuidados digitales.

Las mujeres nos encontramos en situación de mayor vulnerabilidad ante las agresiones digitales porque la brecha digital, entendida como la falta de acceso significativo a las tecnologías por parte de las mujeres, es una injusticia estructural grave y persistente en la región. Además, nuestro género impacta no sólo en el acceso y la apropiación de la tecnología —pues aún se percibe lo tecnológico como un ámbito masculino—, sino también en los ataques digitales que recibimos y, por lo tanto, en nuestra forma de vincularnos con el espacio digital.

Si bien nuestras interseccionalidades abrazan muchos contextos, hay aspectos comunes en Mesoamérica, como la ubicación geográfica —rural o urbana— y la situación socioeconómica, que son determinantes para el acceso a la conexión, a los servicios de contenido más demandantes de ancho de banda y a los dispositivos de última generación. Asimismo, identificamos que la accesibilidad a canales de ayuda en cuestiones digitales suele concentrarse en entornos urbanos. Aquí se cruza otra intersección relevante: ser parte de un grupo indígena, lo que puede generar una barrera idiomática y cultural que dificulte apropiarse de la tecnología y de conceptos de seguridad digital cargados de una perspectiva colonial y patriarcal.

Otro aspecto a destacar son las diferencias generacionales. De los testimonios se desprende que las mujeres jóvenes son más eruditas en el ámbito digital que las mayores, y se reconoce que éstas hacen un esfuerzo adicional, no siempre exitoso, para conocer los usos de las tecnologías y adaptarse a ellos. Las generaciones más jóvenes tienden a reconocer más facilidades en la apropiación de las tecnologías.

LOS PULSOS POLÍTICOS DE NUESTROS PAÍSES

De los testimonios recabados se desprende que otra problemática respecto a la apropiación de las tecnologías digitales surge de las diversas realidades políticas de nuestros países o de los pulsos políticos que se dan a cada momento, pues éstos nos obligan a recurrir a nuevos servicios y a planificar nuevas estrategias de comunicación y cuidados.

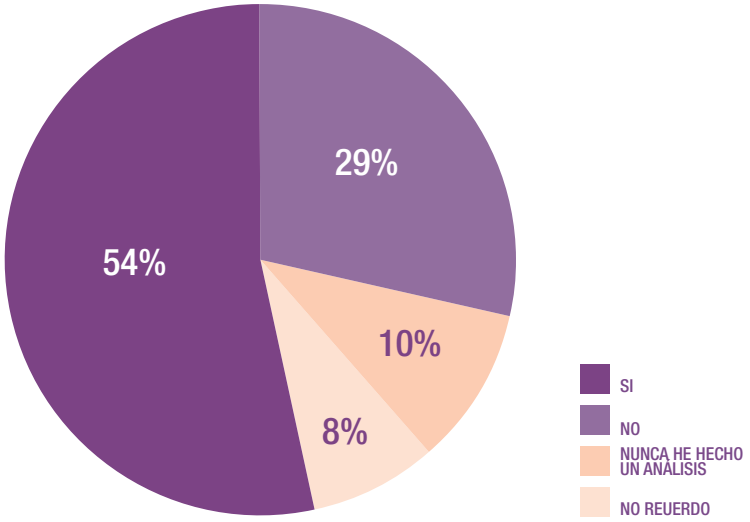
Un hecho fundamental reconocido en los países del estudio lo constituyen los efectos de la migración masiva al ámbito digital a la que nos vimos orilladas a raíz de la sindemia por covid-19 y las políticas de confinamiento, obligado o no, implementadas en su marco. No obstante, los países presentan situaciones políticas concretas que influyen de maneras diversas en la relación de las defensoras con las tecnologías: en Nicaragua, por ejemplo, los testimonios identifican la prohibición absoluta de la protesta como la razón fundamental para la migración del activismo al ámbito digital; mientras que en El Salvador la relevancia que han adquirido las redes sociales en la estrategia comunicativa y propagandística del gobierno es la que ha llevado a las defensoras a adoptar un planteamiento de usos más estratégicos del internet.

NUESTROS SABERES SOBRE CUIDADOS DIGITALES

Muchas de nosotras, en distinto grado, tenemos acceso a materiales, cursos o acompañamiento en cuidados digitales. Nuestras reflexiones y prácticas demuestran que entre **la mayoría de nosotras ya existe un acervo en cuidados digitales y una visión crítica de las tecnologías, lo que es una base fundamental para cualquier trabajo de mitigación y enfrentamiento de estas violencias en nuestros propios territorios.**

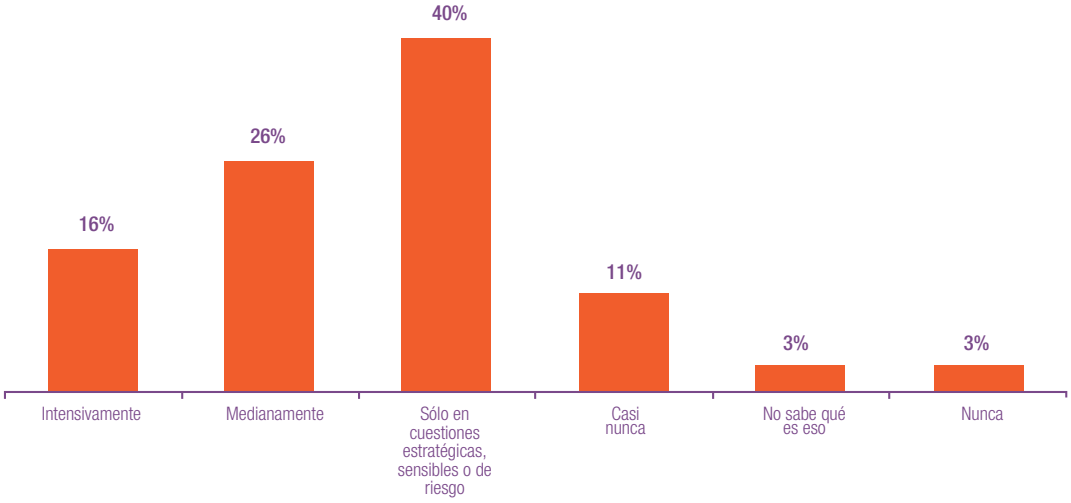
En la región, la seguridad digital no es una materia totalmente desconocida: más de la mitad de las encuestadas reconocen que sus análisis de riesgo contemplan las actividades digitales que realizan (véase gráfico 2).

GRÁFICO 2. ¿HA HECHO UN ANALISIS DE RIESGO DE SU ACTIVIDAD QUE INCLUYA LOS RIESGOS DIGTIALES? (N: 105)



Además, es interesante constatar cómo la mayoría afirma recurrir a prácticas de seguridad digital y cómo el porcentaje de las que no lo hacen es menor (ver gráfico 3).

GRÁFICO 3. ¿APLICA PRÁCTICAS DE SEGURIDAD DIGITAL EN SI ACTIVISMO? (N: 105)



LA VIOLENCIA DIGITAL

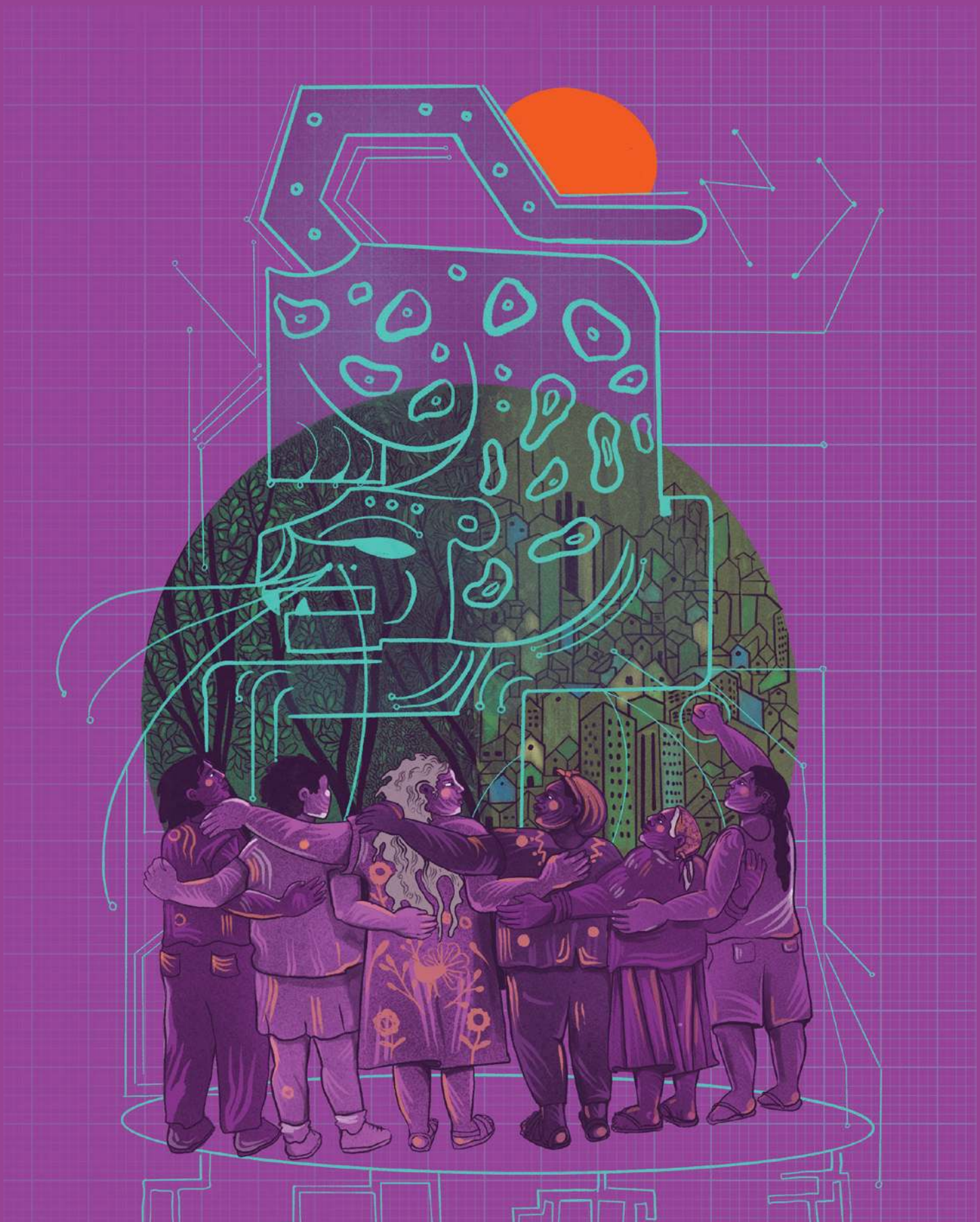
Sin duda, el factor que más influye en nuestra relación con las tecnologías es, precisamente, la violencia digital que vivimos. Pues si bien la mayoría de nosotras comprendemos los potenciales personales, profesionales y políticos del internet, también tenemos una conciencia más clara de que se trata de una herramienta que se usa para generar violencia. Muchos de los testimonios hablan de un punto de inflexión, de una suerte de "fin de la inocencia", tras el cual debido a la violencia se han visto empujadas a poner en práctica modalidades distintas de uso, como dejar de compartir datos personales en redes sociales, restringir la utilización de plataformas y la interacción con usuarios, compartimentar los contenidos de forma estratégica según las plataformas, buscar apoyo profesional en seguridad digital, etcétera.

Hoy, los usos que hacemos de las tecnologías son parte de un proceso de transición que ha demandado un esfuerzo personal y organizacional, así como un proceso de transformación personal y colectiva: las tecnologías digitales han cambiado nuestro trabajo y también nuestras trayectorias de vida. Y más allá de nuestro éxito y nuestro autorreconocimiento como personas con experiencia en el ámbito digital, esta investigación es una muestra de que en Mesoamérica hay un acervo de prácticas de cuidados digitales que vale la pena analizar y que puede ayudar mucho a la comunidad.



LA VIOLENCIA DIGITAL A LA QUE NOS ENFRENTAMOS

5



“El mundo digital allana caminos para ataques más directos”

Las defensoras mesoamericanas enfrentamos contextos cada vez más complejos, donde el incremento de las agresiones digitales y la disputa por el territorio digital son una constante.

Entre 2020 y 2025, nuestro registro de agresiones ha documentado un total de 9,091 agresiones digitales contra 1337 defensoras y 179 organizaciones en El Salvador, Honduras, México y Nicaragua. Esto supone que una de cada cuatro agresiones registradas durante este período se perpetró en el ámbito digital.

De acuerdo con estos datos, las defensoras más agredidas a través de medios digitales son quienes defienden el derecho a la información y libertad de expresión (23%), el derecho a la participación política y a participar en espacios de toma de decisión (22%), el derecho a las mujeres a una vida libre de violencia (17.2%), el derecho a la verdad, justicia y reparación (9.9%) y quienes trabajan por el derecho a la tierra, territorio y bienes naturales (9%). (ver gráfico 4)

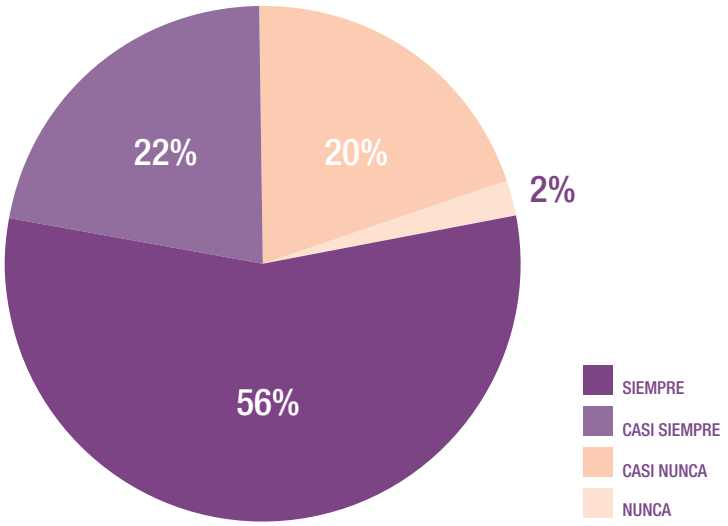
GRÁFICO 4. AGRESIONES DIGITALES A DEFENSORAS MESOAMERICANAS POR AÑO 2020-2025



A partir de la encuesta realizada en el marco de esta investigación, advertimos que la mayoría de las defensoras (88%) perciben que las agresiones a través de plataformas digitales han empeorado en nuestros países en los últimos dos años.

Del total de defensoras encuestadas, la mayoría (78%) afirman haberse sentido vulnerables ante ataques digitales siempre o casi siempre que hacen uso de las tecnologías en calidad de activistas (véase gráfico 5).

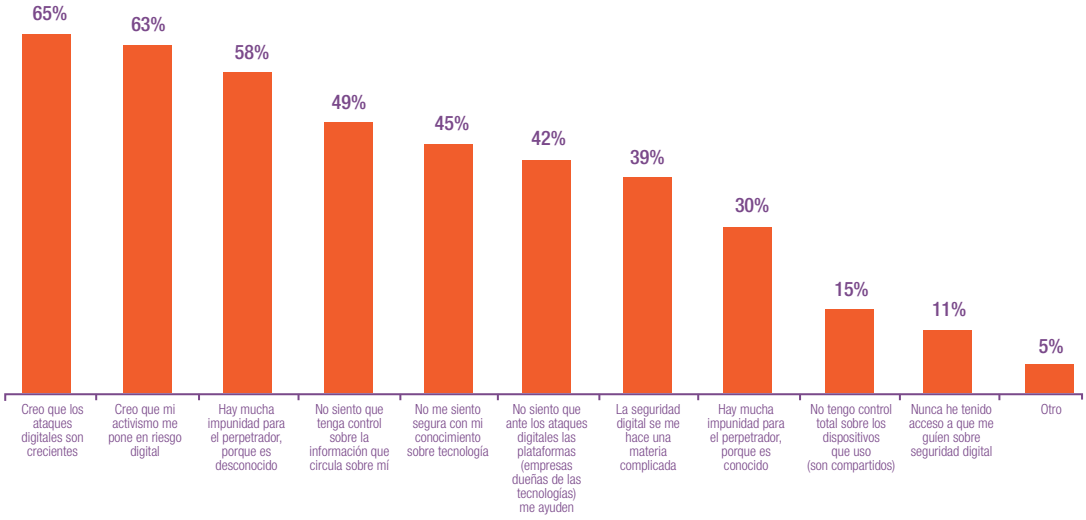
GRÁFICO 5. ¿SE HA SENTIDO ALGUNA VEZ VULNERABLE A ATAQUES EN SU USO DE TECNOLOGÍAS CUANDO SE TRATA DE SU TRABAJO COMO DEFENSORA? (N: 105)



Las razones son variadas: predomina la idea de que los ataques digitales están aumentando (65%) y la percepción de que nuestro activismo y el de nuestras organizaciones nos ponen en particular riesgo (63%); además, existe una sensación de impunidad respecto a los perpetradores de estos ataques debido a su anonimato (58%).

Las razones imperantes a la hora de explicar esta sensación de vulnerabilidad están fuera de nuestro alcance y del de nuestras organizaciones, es decir, remiten al ámbito de lo público. Sin embargo, entre los motivos de esta vulnerabilidad que se hallan en nuestro radio de acción destacan: el (des)conocimiento sobre las tecnologías, que está en quinto lugar (45%); la percepción de la seguridad digital como una materia complicada, en séptimo (39%); y, por último, la falta de acceso a guías sobre seguridad digital (11%) (ver gráfico 6.)

GRÁFICO 6. ¿POR QUE RAZONES SE HA SENTIDO VULNERABLE A LA VIOLENCIA POR MEDIOS DIGITALES? (N: 105)



Lo anterior puede indicar que, por una parte, nos identificamos como vulnerables ante los ataques digitales debido al contexto político exterior; y, por la otra, debido a que nuestro conocimiento en materia de seguridad digital es de nivel mediano, a lo que se une que ese conocimiento tiene un alcance limitado en el contexto político actual.



LA DIMENSIÓN DE GÉNERO DE LA VIOLENCIA DIGITAL

6



“En las agresiones recibimos comentarios bien fuertes sobre nuestros cuerpos: comparaciones, burlas... El valor de la mujer reside sobre nuestros cuerpos”

Podemos afirmar que el objetivo principal de los ataques digitales que vivimos es acallar nuestra voz crítica, lo que tiene una dimensión de género ineludible que responde a una estrategia patriarcal de silenciamiento.

Así, a través de nuestro registro identificamos discriminación por razones de género en 63% de las 9,091 agresiones por medios digitales documentadas entre 2020 y 2025.

La violencia digital es la respuesta a la denuncia y la expresión pública de insatisfacción y rechazo que las defensoras hacemos frente al capitalismo extractivista, colonial y patriarcal dominante en la región. Por ello, las agresiones buscan restablecer la jerarquización de géneros a través del disciplinamiento, el amedrentamiento y la deslegitimación de nuestro trabajo, ética y liderazgo. Bajo estas premisas, la dimensión de género se hace patente en los cuatro aspectos de la violencia digital que analizamos a continuación.

¿POR QUÉ NOS ATACAN?

La principal causa detrás de las agresiones digitales que vivimos las defensoras es la agenda antifeminista y misógina sostenida por los Estados y los poderes fácticos. Se trata de atacar, con especial ensañamiento, todos los valores del feminismo y, en especial, los derechos de las mujeres y de las personas LGBTTTIQ+, como símbolo de un movimiento popular que busca la justicia social y que, al parecer, representa una amenaza central para el *statu quo* y el conservadurismo político transversal. Así, lo que se busca es ridiculizar nuestra agenda como defensoras y minar la credibilidad de las mujeres como lideresas y la de nuestras organizaciones como agentes sociales. Otras veces, se busca dividir o generar conflicto dentro del movimiento de mujeres por medio de campañas de desinformación.

¿A QUIÉNES ATACAN?

Las mayoría de las veces, los objetivos de los ataques son las mujeres que se organizan y articulan en colectivas y movimientos sociales, aunque esto no significa que éstas sean las únicas víctimas. Con todo, existe cierta sevicia y ensañamiento contra las mujeres y personas LGBTTTIQ+ que lideran organizaciones, aún más si son afrodescendientes, garífunas o indígenas. Los mecanismos aleccionadores del patriarcado se potencian para frenar los liderazgos de quienes son señaladas como “malas mujeres”, “malas madres”, “malas esposas”, “malas indias”, “malas negras”, entre otras descalificaciones afines, y buscan trasladar su mensaje a la sociedad entera: “las mujeres, en especial las racializadas y representantes de movimientos populares, no tienen permitido un espacio en la vida pública”.

¿CÓMO NOS ATACAN?

Los insultos que recibimos como defensoras aluden a nuestras identidades de género y de etnia para atacarnos: abunda la sexualización de los cuerpos, el menosprecio de las facultades cognitivas y el desprecio a todo lo que se oponga al mandato heterosexual y al supremacismo blanco. También son comunes los chantajes sexuales, desde la publicación de fotos e imágenes íntimas hasta la violación. Las amenazas de muerte y violación no sólo

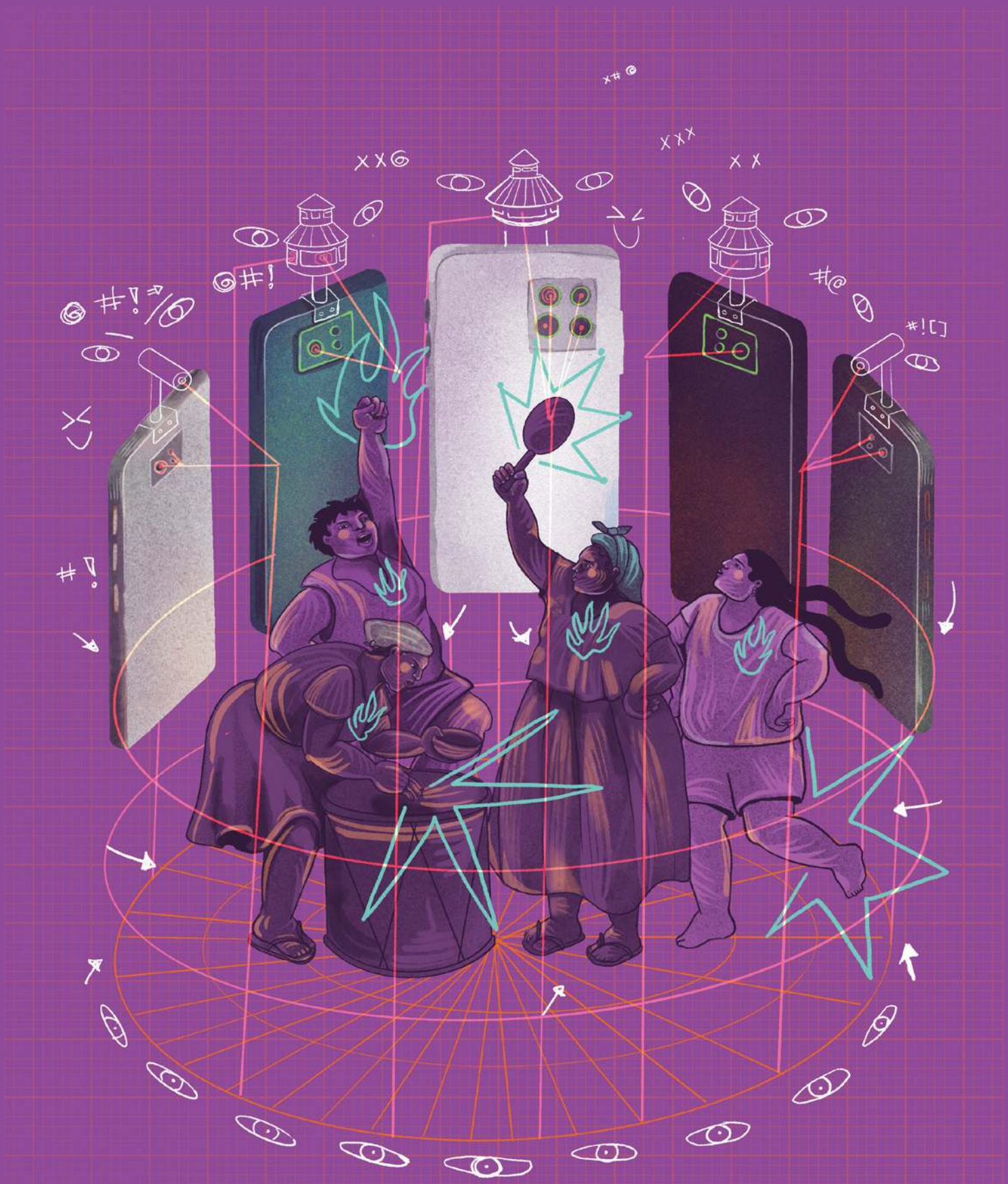
son contra nosotras, sino contra nuestras familiares mujeres. Asimismo, son comunes las campañas coordinadas para deslegitimar al movimiento feminista. Todas estas acciones de estigmatización están muy marcadas por los prejuicios respecto al rol que se espera que asumamos las mujeres en la sociedad.

¿QUIÉNES NOS ATACAN?

Más allá del hecho que los perpetradores sean mayoritariamente hombres, también destaca la relación de poder desigual que algunos de ellos ejercen respecto a nosotras. Esta desigualdad se hace muy explícita cuando se trata de funcionarios del Estado o de actores vinculados a los poderes fácticos, pues difícilmente tenemos acceso a los recursos económicos y políticos que ellos ostentan. Este ejercicio de poder es una forma de intimidación que nos amedrenta y nos genera un miedo muy particular ante los agresores. Cuando éstos usan las tecnologías digitales —desde plataformas de redes sociales hasta herramientas de vigilancia— la diferencia de poder aumenta, tanto en la práctica como en nuestra percepción, pues tenemos certezas legítimas sobre el impacto violencia que apelan a los mandatos patriarcales sobre lo que significa ser una "buena mujer", como en el caso de las exparejas, quienes suelen usar material íntimo y datos personales para amenazarnos y desacreditarnos.



7 ¿QUÉ AGRESIONES ENFRENTAMOS EN EL ÁMBITO DIGITAL?



EL DESAFÍO DE CATEGORIZAR LAS AGRESIONES

Un elemento muy presente en los testimonios recabados para esta investigación es la dificultad para identificar y distinguir las categorizaciones técnicas de las agresiones en el ámbito digital, las cuales han sido tipificadas por personas especialistas en cuidados digitales. Esto queda claro, por ejemplo, cuando se habla de hackeo o craqueo —que es el acto de romper de forma ilícita un sistema de seguridad digital—, y que algunas de nosotras confundimos con phishing, es decir, la técnica de engañar a una persona para realizar una acción que permita robarle información, u otro tipo de agresiones.

Otro reto identificado es la distinción entre los ataques en línea *(online)* y los que se dan fuera de ésta *(offline)*; las encuestan hacen patente cómo para algunas defensoras ambos son lo mismo y se viven como parte de un ciclo de violencia que se produce en varios ámbitos. Los testimonios saltan de un ámbito a otro y tan pronto como hablan de un ataque digital lo relacionan con una agresión fuera de internet.

De acuerdo con nuestro registro de agresiones, casi la mitad de las defensoras (47%) que fueron víctimas de una agresión digital en 2025 también enfrentaron agresiones fuera del entorno digital durante ese mismo año.

Este hallazgo evidencia que la violencia digital no ocurre de manera aislada, sino que suele formar parte de un continuo de agresiones dirigido a obstaculizar y castigar la labor de defensa de derechos humanos. Documentamos, por ejemplo, casos de defensoras que tras ser blanco de de campañas de desprestigio en redes sociales fueron sometidas a procesos judiciales o amenazas que las obligaron a exiliarse. Esto permite comprobar que los ataques digitales y no digitales ocurren como un todo, pues se mezclan y cruzan constantemente en la experiencia vital de las defensoras.

Lo intrincado del ataque personal y organizacional es que en las lideresas y rostros más visibles de nuestras organizaciones se concentran la mayoría de ataques y violencias. Sin embargo, también las defensoras con menos perfil público, pero que están en una organización relevante o reconocida por enfrentarse a las violaciones de derechos humanos, reciben agresiones en línea. Así, para nuestros agresores, las defensoras pasamos a encarnar el conjunto de la organización: se nos ataca para atacar a ésta; y se agrede a ésta para dañarnos como defensoras. Todo ello tiene el objetivo de minar cualquier discurso crítico y perpetuar los conflictos sociales.

Lo anterior da cuenta de la inutilidad de separar lo digital de lo no digital y a la defensora de la organización, pues los ataques afectan la experiencia de vida y trabajo en su complejidad y completitud. Pero también representa un desafío para las redes de apoyo y registro: las tipologías técnicas parecen tener una utilidad limitada con las mismas víctimas.

En este escenario, **hemos optado por agrupar las tipologías técnicas en categorías más grandes, basadas en los objetivos de los ataques.** Este enfoque nos permite distinguir cómo los ataques afectan nuestra experiencia vital en el activismo y la defensa de derechos humanos, lo que puede ser una forma más cercana y estratégica de comprenderlos.

LOS ATAQUES MÁS COMUNES EN LA REGIÓN

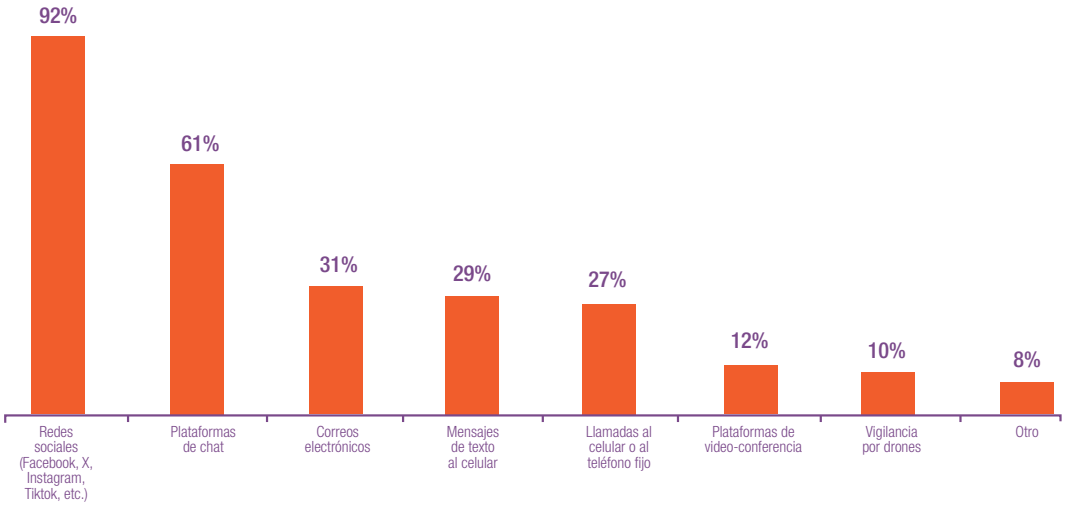
A partir de los resultados de la encuesta en línea, se identificaron dos agresiones que las defensoras percibieron como más comunes para su activismo y sus organizaciones, ambas con más de 50% (ver gráfico 7): la vigilancia y el rastreo digital (en el celular, computadora o redes), así como el ciberacoso u hostigamiento digital, es decir, la difamación en línea con información falsa —personal y organizacional—, los mensajes de acoso por cualquier medio digital, las amenazas y el uso de información privada contra ellas o personas cercanas.

GRÁFICO 7. ¿CUALES AGRESIONES DIGITALES CREES QUE SON LAS COMUNES EN TU ACTIVISMO? (N: 105)



De acuerdo con la encuesta, 92% cree que las redes sociales son una de las plataformas en las que ocurren más agresiones. Este dato coincide con que 89% de las agresiones por medios digitales documentadas en nuestro registro durante el periodo 2020-2025 se concentra en las redes sociales. Asimismo, 61% de los testimonios identifica las plataformas de chat como una de las más utilizadas para perpetrar la violencia digital (ver gráfico 8).

GRÁFICO 8. ¿POR CUÁLES PLATAFORMAS O MEDIOS OCURREN LAS AGRESIONES DE FORMA MÁS RECURRENTE? (N: 105)



Los resultados de este diagnóstico muestran que hay una gran coincidencia entre los ataques nombrados por las especialistas y los recogidos en nuestros testimonios. Se trata de ciertos patrones que evidencian los grandes riesgos digitales a los que estamos expuestas las defensoras mesoamericanas. Con base en los testimonios recogidos, identificamos un conjunto de ataques más frecuentes en la región que pueden presentarse por separado, en combinación o en conjunto. Todos están presentes en los cuatro países analizados en este diagnóstico, sin embargo, son mencionados con mayor o menor impacto en ciertos territorios y contextos (ver tabla 2).

1. **Desinformación de género.** La desinformación es la difusión masiva de información falsa —y con consciencia de su falsedad— con el propósito de engañar a las audiencias y causar daño. A diferencia de otras formas de desinformación, ésta no sólo se basa en información falsa, sino también en propagar narrativas misóginas preexistentes para lograr sus objetivos sociales y políticos, entre ellos mantener el statu quo de género o polarizar a la sociedad. Con relación a ello, la relatora sobre libertad de expresión de las Naciones Unidas, Irene Khan (2023), afirma que:

   "…es de género porque está dirigida a las mujeres y a las personas disconformes con su género, por la naturaleza de género de los ataques y sus consecuencias en cuestiones de género y, lo que es muy importante, porque refuerza los prejuicios, los sesgos y los obstáculos estructurales y sistémicos que se interponen en el camino de la igualdad de género y la justicia de género… ataca no sólo a las personas sino también a sus luchas colectivas tratando de deslegitimar el feminismo y los derechos de género"

   Así, **la desinformación de género busca hacer daño a partir de reafirmar los estereotipos de género, exacerbar los sesgos y prejuicios existentes, incluir de forma explícita o implícita amenazas de violencia de género,** o utilizar tácticas superpuestas de intimidación, vergüenza y descrédito del liderazgo, moral o ética de las mujeres.

   Según las especialistas entrevistadas, son el tipo de agresiones que se han hecho más frecuentes en los últimos años y que generan más preocupación y desgaste debido la escala de su alcance, la viralidad de su

expansión en redes sociales, el anonimato del que se nutren o la facilidad para generar pruebas de forma convincente a partir del uso de la inteligencia artificial, entre otros potenciales de internet y la tecnología para amplificar la violencia.

De acuerdo con lo anterior, la desinformación de género combina tres características definitorias de la desinformación en línea: la falsedad, la intención maliciosa y la coordinación. Y, según lo recogido en esta investigación, esas tres características concurren en las campañas de desinformación de género dirigidas contra nosotras. Hay, pues, una estrategia de coordinación con intenciones maliciosas para presentar información falsa que denueste y nos desacredite tanto a nosotras como a nuestras organizaciones. Esto se hace, comúnmente, por medio de la publicación de información abiertamente falsa —por ejemplo, fotos trucadas o declaraciones con información manipulada o incorrecta— o mediante la difusión de información sacada de contexto —por ejemplo, producción de videos con información parcial que cimenta acusaciones falsas—. Ambas modalidades tienen un discurso bastante distinguible: se basan en la misoginia, la violencia de género y la agenda antifeminista; además, polarizan a la opinión pública con el binarismo básico de los "buenos" contra los "malos", con todas sus posibles variaciones.

Para obtener la información base para construir los ataques, existe una coordinación encargada de recabar la información, producirla y viralizarla. Hay indicios de que para recabar esta información base los perpetradores llevan a cabo un monitoreo constante y complejo sobre nuestras vidas. Los materiales producidos para desinformar reflejan una previa indagación de aspectos personales que, incluso, van mucho más allá de lo que compartimos en redes sociales. Así, tal y como las especialistas entrevistadas apuntan, se da, por ejemplo, un uso malicioso de la información íntima con fines de descrédito. Asimismo, se constata una variedad importante en los medios, soportes y formatos para difundir esta desinformación: desde publicaciones o posteos de opinión, fotografías y videos, hasta redes sociales y webs falsas.

2. **El acoso digital.** Se trata de un amplio espectro de conductas repetitivas y no deseadas, dirigidas contra nosotras con el propósito de causarnos temor, angustia, intimidación o perturbación emocional. Las más comunes son los insultos misóginos continuados, la denuncia masiva desde cuentas de redes sociales para desactivar nuestros perfiles, bloquearlos e incluso provocar que los perdamos; el uso de la fuerza bruta para obtener acceso a las cuentas de diversos servicios que proporcionamos —lo que inunda nuestros correos electrónicos de seguridad, crea confusión, miedo y frustración—; y la creación de etiquetas que agrupan publicaciones sobre un mismo tema, conocidos como *hashtags,* para fomentar el acoso masivo.
3. **Amenazas a nuestra integridad y a la de nuestro entorno.** Son ataques que, generalmente, vienen de cuentas anónimas y apuntan directamente a nuestra integridad física y psicológica. Pueden consistir en amenazas directas a nuestra vida o en advertencias de violación sexual, incluso hacia nuestras familias y círculos cercanos, que nos generan vulnerabilidad y miedo. Este tipo de ataques suelen marcar un punto de inflexión, pues al recibirlos es cuando muchas de nosotras empezamos a tomarnos en serio la violencia por medios digitales.
4. **Violencia sexual digital.** Al respecto, destacan, principalmente, las amenazas de violencia sexual y la difusión no consentida de imágenes íntimas por parte de exparejas, con el fin de perjudicarnos personal y profesionalmente.
5. **Vigilancia electrónica ilegal.** Hemos logrado recabar antecedentes de implantación de *spyware* por parte de los gobiernos en dispositivos de algunas defensoras, así como sospechas de escuchas telefónicas. Otras compañeras intuyen que sus exparejas tienen acceso a sus dispositivos, pero no han podido comprobar si se trata de algún tipo de programa malicioso o de otra forma de acceso menos técnica. Aquí podría agregarse el acceso que tienen las fuerzas policiales a nuestros celulares y otros dispositivos electrónicos cuando hemos sido detenidas o allanadas. En el caso de Nicaragua, tienen acceso a los dispositivos de las familias de las

defensoras, lo que se hace sin cumplir las garantías legales mínimas. En México pudo identificarse claramente que existe un binomio entre el uso del espionaje electrónico y el físico. Con todo, se trata de ataques que nos dejan especialmente vulnerables por el acceso que terceras partes tienen a nuestra información personal e íntima, a la de nuestras familias y a la relacionada con nuestro activismo.

Es importante comprender que no siempre puede distinguirse la vigilancia por medios electrónicos. Pero hay pruebas del empleo de diversas tecnologías para ello, desde spyware hasta herramientas de vigilancia que actúan como antenas de telefonía móvil y capturan identificadores de dispositivos cercanos, conocidos como IMSI-Catchers, que siempre deben ser considerados como un factor de riesgo para nosotras.

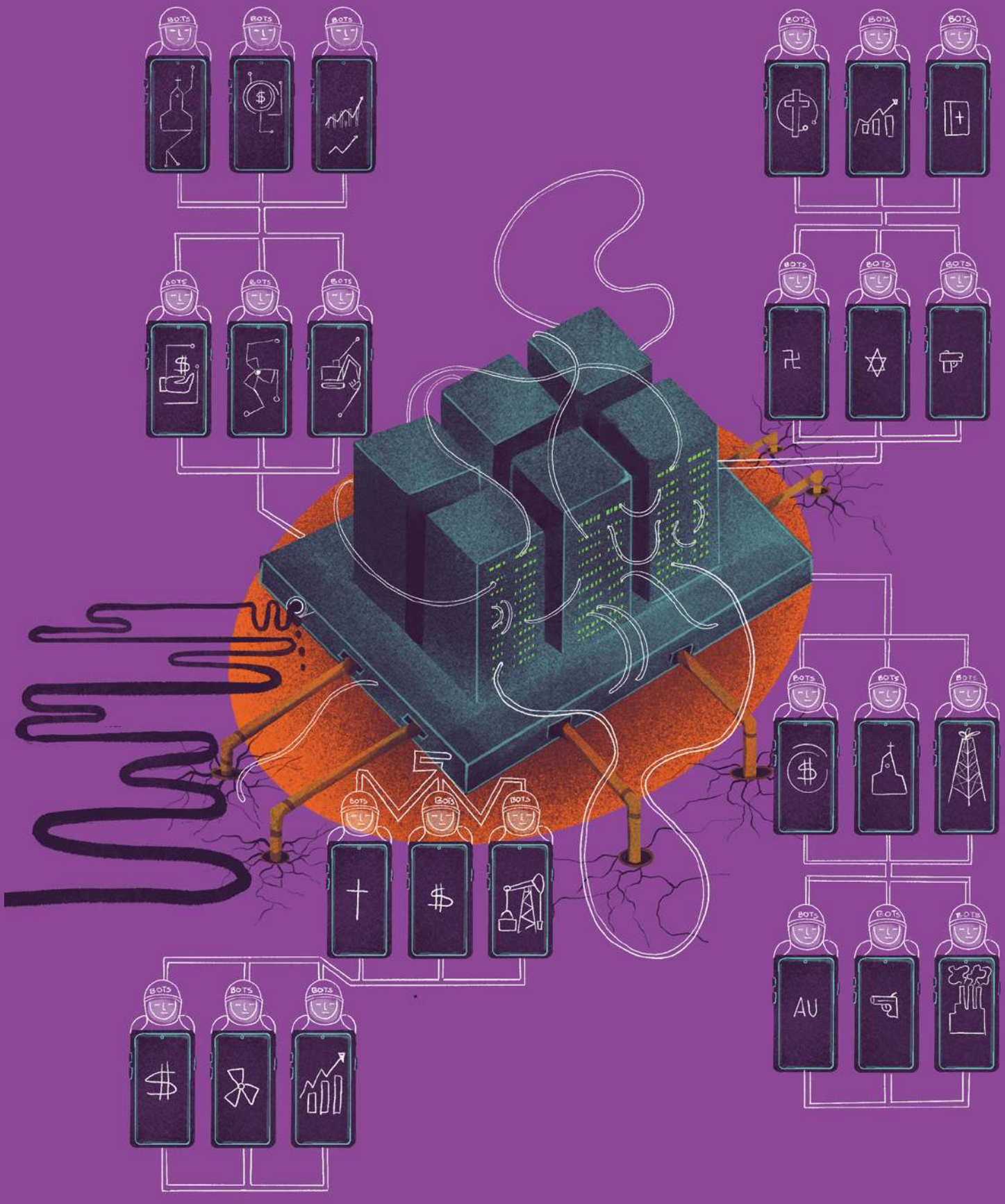
6. **Desanonimización.** Ésta usualmente se lleva a cabo a través de técnicas como el *doxxing* o acto de revelar y publicar intencionalmente información personal a través de internet, generando riesgos para la víctima; así como la publicación de mensajes engañosos que, al crear proximidad, buscan exponer el activismo. Es particularmente relevante en Nicaragua tras el giro totalitario que se ha dado en este país a partir de 2018, donde el peligro real de sufrir las duras consecuencias de exponer la propia identidad ha significado que las tácticas de nuestros adversarios se dirijan a buscar la desanonimización. En Nicaragua, parte importante de este tipo de ataque proviene de exparejas o integrantes de los mismos movimientos sociales, y se originan con la intención de inmovilizar y detener el activismo y el trabajo de las defensoras de derechos humanos.

TABLA 2. TIPO DE AGRESIONES QUE SE IDENTIFICAN COMO MÁS FRECUENTES EN MESOAMÉRICA



La intensidad de los colores refleja la frecuencia en la que se identifican estas agresiones en la experiencia de las defensoras de cada país.

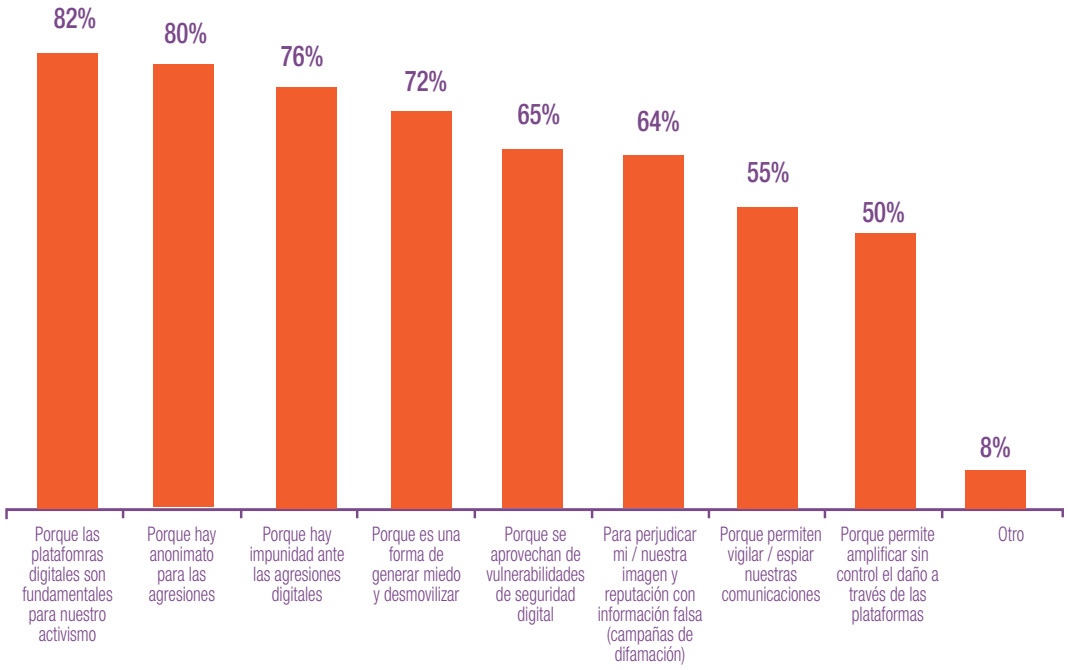
8 ¿QUIÉNES NOS AGREDEN EN EL ÁMBITO DIGITAL?


BOTS
BOTS
BOTS

“Llega un punto en que no sabemos quién podría ser un agresor: si es un agresor estatal, si es un agresor por un tema de la defensa, o si puede ser un ex demente que todavía sigue clavado”

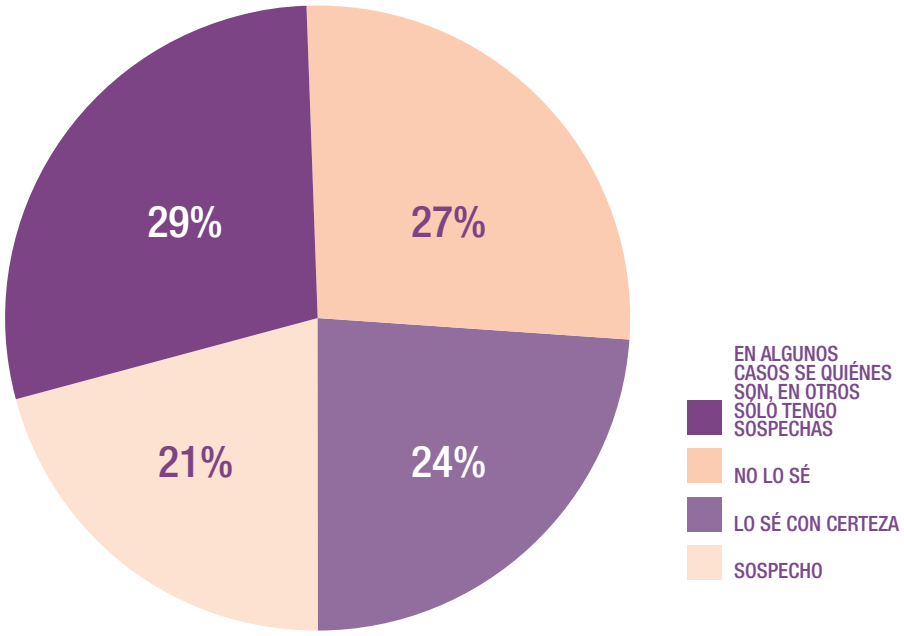
La gran mayoría de las defensoras encuestadas (94%) piensan que las agresiones digitales que recibimos están directamente vinculadas a nuestra labor de defensa de derechos humanos. Esto significa que los perpetradores usan de forma planificada las plataformas digitales para agredirnos debido al papel clave que en la actualidad éstas desempeñan en el activismo, a la facilidad para perpetrar ataques anónimos a través de ellas y a la impunidad que suele imperar con relación a estas agresiones. A ello se une que este tipo de agresiones son muy rentables y eficientes, ya que a un bajísimo coste logran un impacto enorme sobre nosotras y la opinión pública (ver gráfico 9).

GRÁFICO 9. ¿POR QUÉ CREE QUE LOS PERPETRADORES AGREDEN A TRAVÉS DE LAS PLATAFORMAS DIGITALES? (N: 105)



Según nuestro registro de agresiones, entre 2020 y 2025 se documentaron como "desconocidos" 61% de los perpetradores directos de las agresiones por medios digitales. A pesar de que el anonimato en el territorio digital es una condición que dificulta el rastreo de los agresores, éstos no necesariamente constituyen una masa anónima difícil de distinguir. De acuerdo a los testimonios que nutren esta investigación, 21% de las defensoras entrevistadas no saben ni sospechan quiénes están detrás de estos ataques. Sin embargo, a partir de análisis de riesgos, la mayoría (79%) sospecha o ha identificado a los principales presuntos responsables de algunas o de todas las agresiones que han recibido en las plataformas digitales. (ver gráfico 10).

GRÁFICO 10. ¿SOSPECHA O SABE CON CERTEZA QUIÉNES ESTÁN DETRÁS DE LOS ATAQUES DIGITALES? (N: 105)



Al momento de señalar quiénes son los responsables de las agresiones —ya sea porque se sospecha o se sabe con certeza— una abrumadora mayoría de las defensoras encuestadas (70%) cree que se trata de autoridades públicas de alto rango: autoridades federales o nacionales, estatales, provinciales, municipales y comunitarias. En segundo lugar están los partidos políticos —simpatizantes o integrantes de éstos— con 52%; y en tercero, con 49%, fuerzas policiales de diferente nivel —federales, nacionales, centrales, estatales, provinciales, municipales, comunitarias—.

GRÁFICO 11. ¿QUIÉN O QUIÉNES ESTÁN DETRÁS DE LAS AGRESIONES DIGITALES? (N: 105)

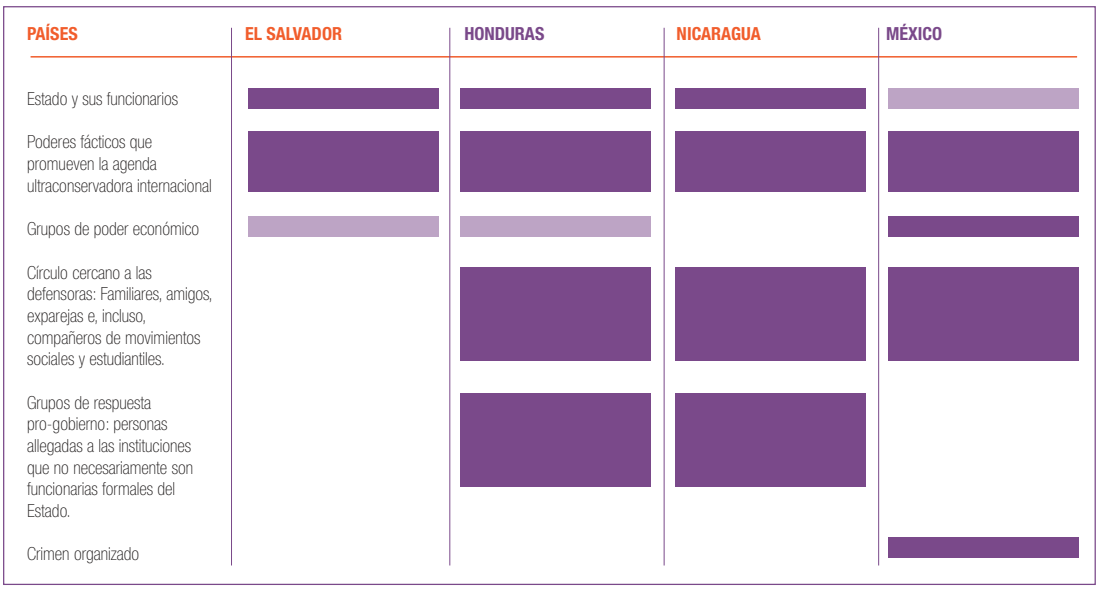


Tras las agresiones digitales que vivimos están los mismos intereses y propósitos que tras las agresiones en el ámbito físico: buscan castigarnos, ejemplificar las consecuencias de enfrentarnos a grupos de poder y desmovilizar nuestras luchas por la defensa de derechos humanos. Por lo tanto, nuestros principales agresores digitales son los mismos que hemos identificado en las agresiones no digitales: el Estado, grupos de poder económico, político y otros poderes fácticos y ultraconservadores, así como personas del entorno cercano como parejas e integrantes de nuestra familia, comunidad u organización. Los testimonios también identifican que en ocasiones los perpetradores directos son personas usuarias de redes sociales que de manera independiente, sin pertenecer a un colectivo o tener una estrategia definida, actúan como caja de resonancia de estrategias de agresión más complejas orquestadas por grupos de poder.



En la tabla 3 puede apreciarse el amplio rango de perpetradores identificados, empezando por los Estados, continuando por los poderes fácticos y llegando hasta nuestro círculo cercano e íntimo (figura 2). Muchos de estos perpetradores se repiten en los distintos países y generan alianzas entre ellos.

TABLA 3. TIPO DE PERPETRADORES DE VIOLENCIA DIGITAL EN MESOAMÉRICA



EL ESTADO Y SUS FUNCIONARIOS

Identificamos a los Estados de los cuatro países a los que ceñimos nuestro estudio como los principales perpetradores de violencia facilitada y/o ejercida a través de la tecnología. Esto se debe a que la mayoría de ellos han implementado políticas de criminalización de la labor de defensa de derechos humanos en sintonía con sus agendas de control político y sus alianzas con una diversidad de poderes fácticos: empresas nacionales y trasnacionales, crimen organizado y grupos ultraconservadores que promueven una agenda antifeminista y antiderechos. Por ello, cuando hablamos del Estado como perpetrador, en realidad, se trata de una amplio espectro de actores que utilizan los recursos e infraestructura públicas para atacarnos de forma física y digital. Esto significa que los recursos financieros, policiales y, muchas veces, militares estén disponibles para perseguirnos, facilitando el uso de técnicas digitales coordinadas para el ataque, que van desde las campañas de desinformación hasta el uso de programas espía.

En países como Nicaragua y El Salvador, el acoso comienza en el poder ejecutivo, con funcionarios de alto rango involucrados en los hostigamientos y discursos de odio que se manifiestan en la esfera digital. Esto genera un efecto en cascada que provoca que otros funcionarios, grupos de choque —voluntarios o pagados— y personas usuarias de redes sociales simpatizantes del gobierno se involucren en campañas de acoso y desinformación.

PODERES FÁCTICOS

Entendemos por poderes fácticos a aquellos actores y grupos que ya sea de manera directa y/o a través de la cooptación de los Estados y sus instituciones ejercen un poder real en los territorios: grupos ultraconservadores o fundamentalistas; poderes económicos y financieros; crimen organizado, caciques y terratenientes locales, grupos paramilitares, entre otros.

Estos perpetradores tienen una característica en común: ostentan poder. No se trata de simples agresores, sino de actores que pueden ejercer una violencia extrema contra nosotras, nuestras organizaciones y familiares, pues gozan de una preocupante capa de impunidad. Asimismo, en la región se constata que estos actores suelen converger y aliarse entre sí, tienen un radio de acción transnacional e incluso comparten fuentes de información y financiamiento entre ellos, lo que se hace evidente a través de las similitudes de sus narrativas y estrategias de uso de las tecnologías para atacarnos.

Grupos que promueven la agenda ultraconservadora internacional.

En los últimos años, en la región y en el mundo ha emergido una fuerte agenda ultraconservadora impulsada por amplias alianzas trasnacionales entre partidos políticos de ultraderecha, sectores fundamentalistas religiosos y grupos de poder económico con intereses extractivistas. Sus narrativas abiertamente racistas, xenófobas y misóginas generan consecuencias tangibles tanto en el ámbito físico como en el digital. En la esfera digital, condicionan la opinión pública mediante el control de las redes sociales y la manipulación de sus algoritmos. En el plano político y jurídico, a través de la cooptación de los Estados y sus instituciones, impulsando políticas públicas, marcos jurídicos y fiscales que erosionan los derechos humanos y promueven el despojo territorial.

De manera directa o indirecta, estos grupos construyen los discursos que se reproducen en las campañas digitales de desprestigio y desinformación en contra nuestra. Perfiles de usuarios virtuales se escudan en la bandera de "Dios, Patria, Libertad y Familia" para defender el orden patriarcal de género y el sistema económico que se beneficia de él. Así, durante los últimos años hemos notado un incremento en la cantidad y la gravedad de las agresiones en contra de nosotras y nuestras organizaciones, en las que se estigmatiza nuestra apuesta por la soberanía de nuestros cuerpos-territorios calificándola como "ideología de género", se ridiculiza el activismo de las mujeres y disidencias sexo-genéricas y se exige que perdamos derechos políticos mandándonos "a la casa a lavar los platos".

Poder económico.

Identificamos que algunas agresiones contra defensoras son perpetradas, directa o indirectamente, por un conjunto de actores vinculados al poder económico: empresas extractivistas, agroindustriales, mineras, tecnológicas, impulsoras de megaproyectos urbanísticos y turísticos, terratenientes locales en disputas territoriales, oligarquías locales, entre otros. Estos grupos empresariales locales, nacionales y trasnacionales impulsan modelos de "desarrollo" basados en dinámicas de acumulación por desposesión y despojo que confrontan las luchas de quienes defienden la tierra y el territorio. A tal fin, impulsan estrategias articuladas de hostigamiento y agresión física y digital con la intención de estigmatizar las demandas y criminalizar los liderazgos.

Todos ellos, si bien pueden actuar de forma independiente, tienden a operar en articulación con funcionarios del Estado, el poder judicial o con otros poderes fácticos como los medios de comunicación hegemónicos o plataformas digitales. Estas últimas, a través de la manipulación algorítmica, amplifican discursos racistas funcionales a sus intereses económicos mediante los cuales construyen una imagen de las defensoras del territorio como revoltosas, usurpadoras y enemigas del progreso y el desarrollo económico.

Crimen organizado.

Algunas defensoras mesoamericanas identifican al crimen organizado como uno de los perpetradores que emplean la violencia física y digital como herramienta de control territorial y silenciamiento. En el ámbito digital, sus agresiones suelen operar como antesala o prolongación de la violencia física. Se expresan, por

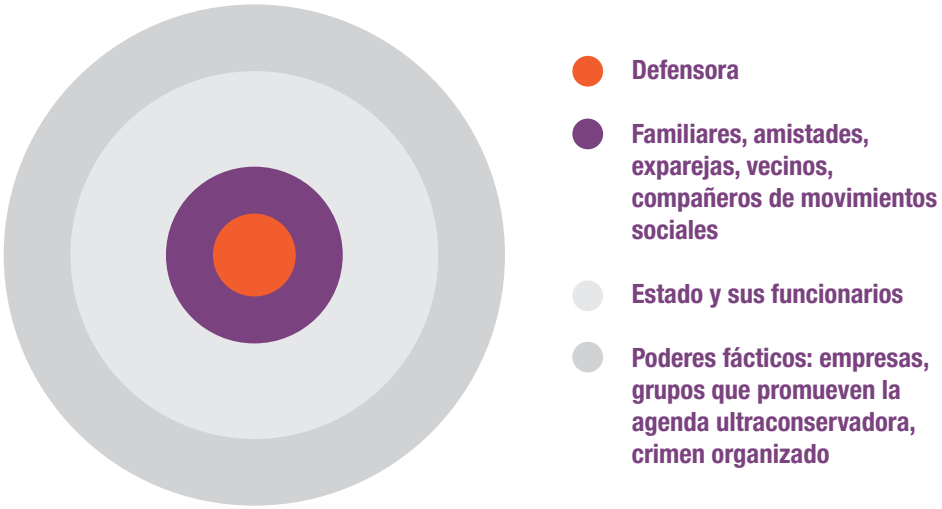
ejemplo, en amenazas directas por medio de mensajes a celulares o redes sociales dirigidas a defensoras del territorio, buscadoras o periodistas que denuncian sus crímenes o los complejos entramados políticos y económicos en los que se insertan.

La capacidad de daño e impunidad de estos grupos trasciende las fronteras nacionales y se sostiene sobre dos pilares: el despliegue de mecanismos militarizados operados por profesionales de la violencia; y la complicidad, tolerancia o colusión de funcionarios e instituciones locales, estatales o nacionales. Estos vínculos con el poder público se expresan, en algunos países de la región, en el financiamiento o promoción de candidatos políticos para operar sus intereses en el marco de una aparente legitimidad institucional.

ACTORES DE NUESTRO ENTORNO CERCANO

Es ocasiones, los perpetradores de la violencia digital pertenecen a nuestros círculos cercanos: familiares, exparejas, colegas, compañeros de organización o movimiento social, incluso personas del vecindario. Como se aprecia en los testimonios, estos círculos comparten con los grupos ultraconservadores el antifeminismo y posturas patriarcales que tratan de desmovilizarnos políticamente reforzando roles tradicionales de género que nos quieren mantener en silencio y fuera de la esfera pública. Tener a los agresores en nuestras casas, comunidades y organizaciones genera un entorno de hipervigilancia que es desgastante para nuestra salud mental y física.

FIGURA 2. PERPETRADORES DE VIOLENCIA DIGITAL CONTRA DEFENSORAS



¿CÓMO NOS AGREDEN EN EL ÁMBITO DIGITAL? 9



La formas de operar de los distintos perpetradores de violencia digital en la región mesoamericana presentan bastantes similitudes y pueden desglosarse en tres momentos, los cuales, al combinarse, logran mayores grados de eficiencia.

Preparación del contexto para la criminalización. Las agresiones que recibimos ocurren en un ambiente hostil para nuestro trabajo. Los Estados y poderes fácticos cuentan con recursos, medios de comunicación e impunidad para realizar señalamientos y campañas que estigmatizan nuestra labor. El acoso explícito que sufrimos en los países en donde se llevó a cabo esta investigación hace que el alcance de la agresión sea infinitamente mayor, debido a que las autoridades de distintos niveles nos han señalado como enemigas o criminales. La estigmatización hacia lo que hacemos —ya sea a través de declaraciones públicas o de acciones gubernamentales y estatales— es parte de una estrategia de preparación del contexto para justificar procesos de criminalización. En muchos países, además, esa criminalización se ejerce, de manera especial, contra la prensa crítica, e impide la verificación de los hechos y el control del poder estatal.

Uso de tecnologías de vigilancia. Un componente fundamental de los ataques digitales es el monitoreo constante de nuestras actividades digitales. Muchos testimonios señalan la posibilidad de que se pague a personas para realizarlo. Esto denota que las agresiones digitales parten de una base para después concretarse: el perfilamiento digital de la defensora, su círculo y su organización. De hecho, a partir de sufrir estos ataques es cuando empezamos a comprender cabalmente la necesidad de ser muy estratégicas al hacer uso de internet, pues debido a los intereses extractivos de las plataformas respecto a nuestros datos personales, es casi imposible no dejar huella de éstos, lo que nos mantiene continuamente en el punto de mira de nuestros agresores. Esto reafirma lo dicho por las especialistas entrevistadas: los ataques basados en la recolección de datos personales permiten que éstos sean dirigidos a nuestra esfera íntima, por lo que asuntos como la orientación sexual o las actividades de nuestras familias son usados en las agresiones. Ahora bien, existen diversos mecanismos legales e ilegales que pueden estar alimentando este monitoreo. Por un lado, el uso malicioso de técnicas legales como la inteligencia de fuentes abiertas (OSINT, por sus siglas en inglés), una metodología de recolección, análisis y toma de decisiones sobre datos de fuentes disponibles de forma pública —como las redes sociales— para ser utilizados en un contexto de inteligencia. Por otro, en la región identificamos el uso de diferentes software para la vigilancia ilegal como Pegasus, FinFisher, RCS-Remote Control System, entre otros. Paralelamente, algunos gobiernos han creado marcos legales para que las empresas de telecomunicaciones, sin consentimiento claro de las personas usuarias, faciliten los datos personales que conservan.

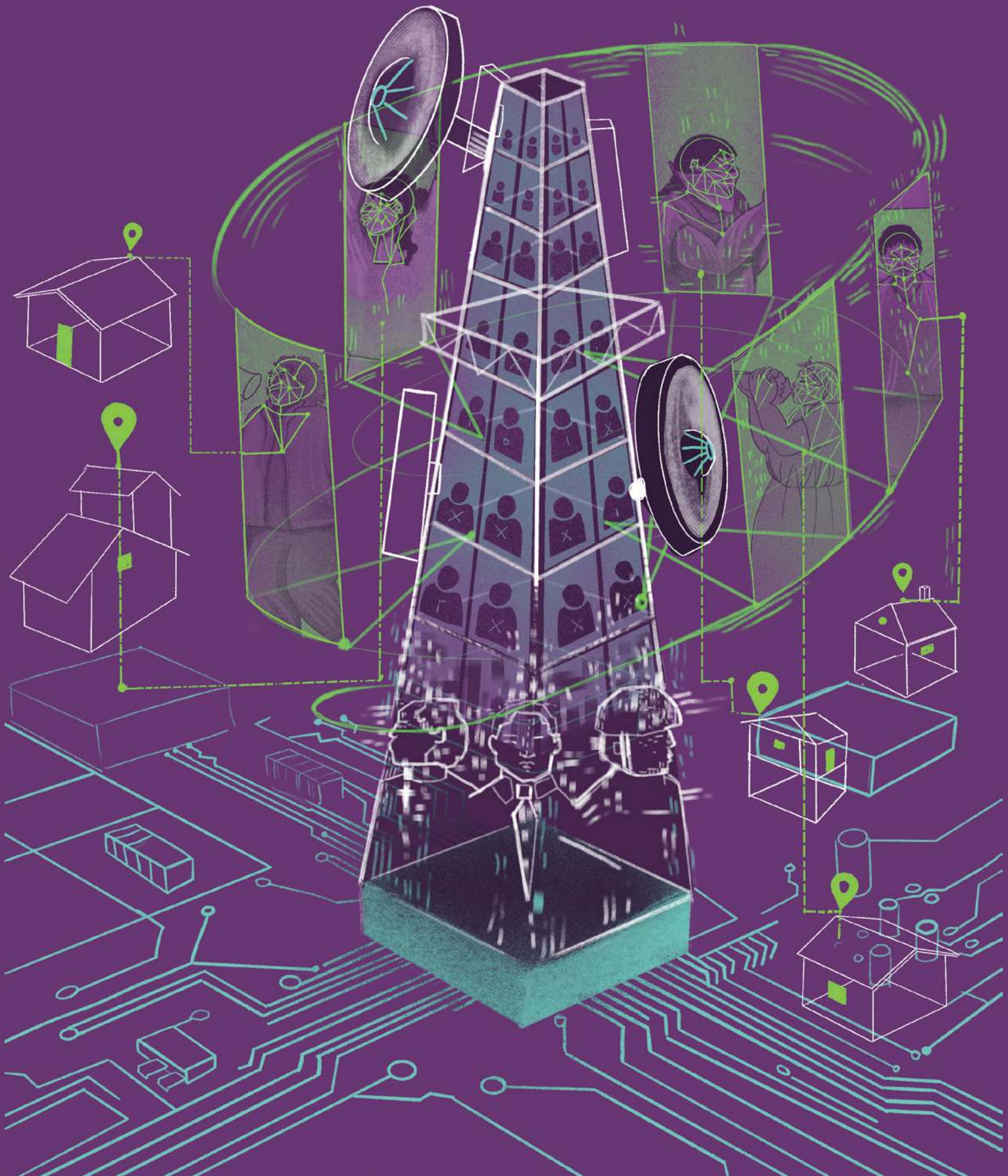
Estrategias de viralización. Otra forma de operar de los perpetradores es aplicar estrategias de viralización de los ataques, pues no hay daño cabal si no se logra un ataque que asegure el alcance masivo del contenido malicioso. Para la viralización, destacan las estrategias organizadas de cuentas con identidades falsas, el conjunto de cuentas digitales que son creadas para desinformar o manipular, llamados netcenters, y sus programas informáticos que automatizan tareas de forma repetitiva y que son usados para atacar perfiles en internet, denominados bots. Asimismo, en muchos países, se repite el patrón de uso del posteo o del reposteo del ataque por parte de personas populares en redes, lo que significa una reacción en cascada, tanto planeada —con personas pagadas con identidad desconocida, que publican mensajes provocadores y agresivos, llamadas trolls— como con el alcance orgánico de seguidores. En el caso del Estado, son los altos funcionarios —incluso los presidentes— los que emplean esa estrategia de viralización. En relación con lo anterior, conviene destacar que los medios de comunicación hegemónicos juegan el papel de caja

de resonancia de las agresiones digitales, pues indudablemente son parte de la estrategia de viralización de los perpetradores. Algunos testimonios señalan que las agresiones digitales aumentan notablemente cuando algún perpetrador usa un medio de comunicación para señalarlas.

Los tiempos estratégicos de los ataques. Las agresiones digitales responden a ciertos tiempos definidos por los perpetradores. Por ejemplo, como una escalada: se agrede primero a las lideresas de las organizaciones para luego ir a por el resto. Otros testimonios apuntan a que las agresiones digitales aumentan cuando la organización atraviesa un momento importante, como el veredicto de un juicio o el lanzamiento de un informe.



10 LA INQUIETANTE IMPUNIDAD EN LA ESFERA DIGITAL



Es ineludible preguntarse por qué las agresiones digitales contra nosotras son cada vez más habituales. Tanto los testimonios de las defensoras entrevistadas como los de las especialistas participantes en esta investigación dan cuenta de que la razón principal es que estas agresiones son muy eficientes en cuanto a costo y resultado, pues requieren poca inversión para el alto retorno que suponen. Parte importante de su eficiencia radica en la inquietante prevalencia de la impunidad en varios ámbitos.

IMPUNIDAD SOCIAL

Es el tipo de impunidad que nos toca más de cerca y tiene que ver con la naturalización social de los ataques. Se nutre de la equivocada idea de que lo digital no es real o es menos importante que lo físico, también del hecho de vivir los ataques de forma individual sin poder compartirlos con el colectivo, así como de la falta de recursos para poder hacerles frente. Ello contribuye a que no se denuncien a los Estados ni a las plataformas y a que tampoco haya un mecanismo de justicia social para prevenirlos, desactivarlos y garantizar su no repetición. De esta forma, como en un círculo vicioso, este silencio sólo genera más silencio sobre la violencia digital.

IMPUNIDAD EN LA ACCIÓN DE LOS ESTADOS

Con base en los testimonios recavados, una tendencia resuena claramente: **sólo una de cada cuatro defensoras encuestadas (25%) ha denunciado alguna agresión digital ante instancias del Estado.** Probablemente, esto se relaciona con el hecho de que 95% de las defensoras considera que el marco político legal de su país no garantiza su protección digital.

Desde el análisis cualitativo, esta impunidad se debe, por un lado, a que los marcos legales respecto a las plataformas de internet aún están en desarrollo y a que, cuando los hay, no siempre se pueden emplear para garantizar nuestros derechos humanos o, incluso, en no pocas ocasiones se usan en contra nuestra. Por otro lado, hay una desconfianza general de las defensoras a la hora de denunciar. Primero, por los altos niveles de impunidad que prevalecen en las instancias del sistema de justicia en casi todos los delitos; y, segundo, porque muchas veces los agresores son funcionarios y no existen garantías suficientes de que vaya a prosperar la denuncia. A ello se une que muchos funcionarios no han sido capacitados para comprender lo digital y, menos aún, la violencia de género en línea, así que ponen diversas trabas para la denuncia. También existen factores estratégicos para no interponer denuncia ante los sistemas de justicia de los Estados, pues en algunos casos hacerlo puede complicar la delicada situación personal de las defensoras, sus familias y organizaciones.

Finalmente, en los pocos casos en los que las defensoras denunciaron, no pasó nada. En esta línea, se hace una crítica transversal a los mecanismos de protección, en los que las medidas casi siempre están diseñadas para enfrentar situaciones de riesgo y amenazas en el ámbito físico, y no tanto en el digital, por lo que tienden a no ser nada eficaces respecto a la violencia que se da en este ámbito.

IMPUNIDAD CON LAS PLATAFORMAS

Respecto a las empresas tecnológicas, la encuesta mostró que 35% de las defensoras denunció el ataque a la empresa proveedora del servicio en el que ocurrió. Sin embargo, la mayoría de quienes interpusieron denuncia afirmaron que, si bien recibieron respuesta, ésta fue insatisfactoria (51%); o que, a pesar de la denuncia, no tuvieron respuesta (35%).

Esto evidencia una crítica transversal muy preocupante respecto a la ineficiencia creciente de los canales de ayuda de las plataformas. Por nuestra parte, damos cuenta de lo casi inexistentes que son éstos, de la poca posibilidad de usarlos, de los largos periodos de espera de respuesta —que puede incluir meses de cuentas desactivadas a causa de las denuncias maliciosas de los agresores— y de la incapacidad de apelación. Muchos testimonios reconocen también que, con los años, pareciera que los estándares de ayuda y protección de derechos humanos

de las plataformas han decaído. A tal punto llega la impunidad que no pocas defensoras ya nos abstenemos de denunciar, lo que genera que los reportes de denuncias publicados por algunas plataformas no reflejen lo que de verdad está ocurriendo.

Lo mismo opinan las especialistas entrevistadas, lo que resulta muy interesante porque trabajan directamente con los canales de ayuda de algunas plataformas. Según su visión, parece existir un diseño especial en las plataformas para destinar recursos mínimos al combate y prevención de las agresiones digitales, lo que no deja de sorprender, debido a la escala y al uso masivo de estas compañías en el mundo. Más aún, se indica que los canales están siempre dominados por respuestas y análisis automatizados a través de bots, lo que hace que resulte casi imposible que una persona usuaria común logre llegar a tener una respuesta humana. Peor todavía, muchos de los problemas más complejos, como los discursos de violencia de género, se autorregulan con la detección automática de palabras peligrosas que no siempre son culturalmente relevantes y son muy fáciles de burlar.

Algunas especialistas consideran que no sólo se trata de inacción, sino de un diseño particular para evadir responsabilidades, pues estas compañías se limitan a mantener sus relaciones públicas y no buscan responder a estándares de derechos humanos. Incluso plantean sus propias ideologías al momento de diseñar los algoritmos y la moderación de sus contenidos y no contestan a los requerimientos de ayuda de las organizaciones especializadas.



¿A QUÉ RIESGOS NOS EXPONE LA VIOLENCIA EN EL ÁMBITO DIGITAL? 11



“Los ataques virtuales son a mi persona, a mi humanidad”.

Esta frase sintetiza cómo la violencia digital trasciende el espacio virtual y puede materializarse en múltiples dimensiones de la vida: personal, social, comunitaria y político-organizativa. Aunque la defensora que la enunció ya había escuchado la idea de que lo virtual también es real, fue a través de recibir violencia digital que esta idea adquirió un significado concreto. Su intensificación puede afectar nuestra manera de comunicarnos, informarnos y ejercer el activismo, generando procesos de desmovilización y silenciamiento que debilitan nuestra labor de defensa de los derechos humanos.

RIESGOS PARA NUESTRO BIENESTAR PERSONAL Y EL DE NUESTRO ENTORNO FAMILIAR

Afectaciones emocionales: la violencia de los mensajes misóginos, campañas de desinformación y amenazas —que suelen incluir a integrantes de nuestras familias— que se difunden a través del territorio digital persiguen impactar a nivel psicoemocional generando consecuencias como estrés, insomnio, miedo, depresión, ansiedad o un estado de alerta o hipervigilancia.

Afectaciones físicas: las afectaciones emocionales pueden manifestarse también en el cuerpo a través de dolores y enfermedades.

Afectaciones materiales: las agresiones digitales también pueden implicar altos costos económicos, desde la pérdida de nuestros empleos ante campañas de desprestigio, hasta los impactos materiales que implica un desplazamiento forzado tras amenazas de muerte o la difusión de datos sensibles sobre nuestras ubicación.

Afectaciones a nuestras relaciones personales y profesionales: estar expuestas al acoso constante puede generar una pérdida de confianza o miedo a relacionarse con nosotras de parte algunas personas de nuestro entorno cercano.

Afectaciones a nuestros derechos políticos: nuestra primera reacción ante la violencia y acoso digital es limitar nuestra exposición a redes sociales, bloquear perfiles sospechosos y usarlas de manera más cautelosa. Si bien esto puede ser una buena estrategia para prevenir y mitigar las violencias, también puede poner barreras a nuestro acceso a derechos que pueden ser facilitados por internet, como el acceso a la información, la libertad de expresión y el derecho de reunión y organización. Así, las agresiones digitales limitan el uso del territorio digital como espacio de opinión, acceso al conocimiento y redes políticas o profesionales.

RIESGOS PARA NUESTROS MOVIMIENTOS

Afectación en la credibilidad de nuestras demandas: la desinformación de género y otras formas de violencia facilitada por la tecnología pueden tener consecuencias en la opinión pública y en la credibilidad de nuestros liderazgos, luchas y movimientos

Afectaciones en las relaciones dentro de los movimientos sociales: las agresiones constantes en el territorio digital pueden afectar nuestras relaciones políticas al fomentar la desconfianza y amenazar con afectar a quienes se relacionen con nosotras.

Afectaciones al alcance de nuestras ideas: la constancia de las agresiones nos lleva a

modificar nuestras estrategias de interacción virtual, limitando el alcance de nuestro activismo y el de nuestras organizaciones. Esto puede generar consecuencias en las discusiones políticas a nivel nacional y regional, ya que disminuye la libre circulación de diversidad de ideas y desaparece la crítica desde una mirada contrahegemónica.

Cambios en nuestras medidas de cuidado y protección digital: enfrentar violencias digitales puede generar un reconocimiento de la necesidad de contar con estrategias más cuidadosas acerca de nuestra presencia en ellas y nuestra seguridad digital. Así, identificamos que hemos adquirido una mayor conciencia del cuidado en el uso de las tecnologías digitales. A nivel organizativo, esta conciencia de las necesidades de cuidados digitales ha llevado a muchas organizaciones a especializarse o a articularse con redes de especialistas para implementar análisis de riesgo y medidas en pro de la seguridad digital. Como muestra, 64% de las defensoras encuestadas señaló haber recibido algún tipo de apoyo de organizaciones o colectivas afines en casos de violencia facilitada por las tecnologías.

GRÁFICO 12. ¿CUALES SON LOS EFECTOS QUE HAN TENIDO ESTAS AGRESIONES DIGITALES SOBRE SU PERSONA? (N: 105)

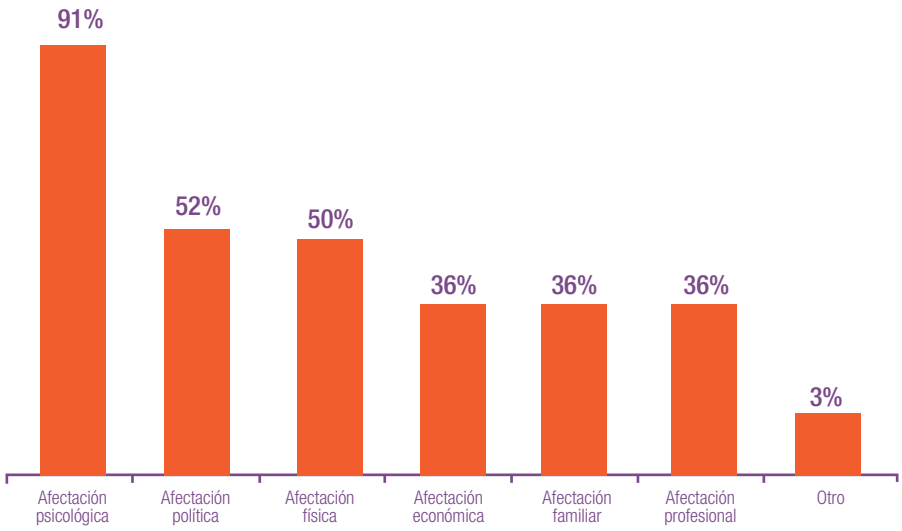
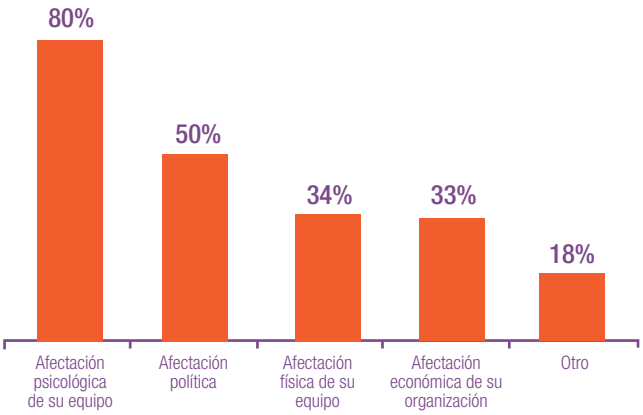


GRÁFICO 13. ¿CUALES SON LOS EFECTOS DE ESTAS AGRESIONES DIGITALES EN SU ORGANIZACIÓN, GRUPO O COLECTIVA? (N:105)



12 RECOMENDACIONES



Este diagnóstico pone de relieve cómo la violencia digital contra mujeres y disidencias sexo-genéricas que defienden derechos es utilizada para silenciar voces críticas, así como para preservar y perpetuar las estructuras de poder patriarcales, racistas y clasistas.

Tomando en cuenta la complejidad del entorno digital actual, con el fin de transformar la situación de violencia descrita y garantizar la protección integral feminista de las defensoras formulamos las siguientes recomendaciones:

A LOS ESTADOS

- Reconocer la gravedad de la violencia digital contra defensoras y tomar acciones urgentes enfocadas en desnaturalizarla y en visibilizar su imbricación con la violencia en el ámbito físico.
- Crear registros nacionales estandarizados de agresiones digitales contra defensoras, esenciales para generar medidas que permitan prevenir, investigar y garantizar la no repetición de estos hechos.
- Fortalecer y capacitar los mecanismos de protección nacionales para la atención integral de la violencia digital con enfoque diferenciado para la protección de mujeres defensoras de derechos humanos y disidencias sexo-génericas.
- Garantizar respuestas urgentes ante las violencias digitales a través de medidas específicas como el retiro de contenidos, el apoyo psicosocial y material, la reposición de equipos y conectividad.
- Crear mecanismos y fiscalías especializadas con enfoque diferenciado que consideren y protejan la situación de particular vulnerabilidad de las mujeres defensoras y disidencias sexo-génericas en el ámbito digital.
- Garantizar procesos de investigación eficaces y coordinados con tiempos de respuesta ágiles, investigación del uso de software espía y acción interinstitucional frente a redes organizadas de odio y desinformación.
- Garantizar marcos normativos que protejan derechos digitales y que establezcan la responsabilidad de las plataformas de redes sociales de cara a propiciar un espacio digital libre de violencia.
- Abstenerse de usar o de permitir el uso de cualquier plataforma o herramienta digital para la censura, vigilancia o criminalización de la labor de defensa de derechos humanos.

A LOS MECANISMOS INTERNACIONALES Y ORGANISMOS DE DERECHOS HUMANOS

- Reconocer y nombrar la violencia digital contra defensoras como una amenaza especialmente grave.
- Ampliar la definición de la violencia digital contra defensoras, relacionándola con la violencia offline, visibilizando sus componentes e impactos diferenciados de género y ampliando los tipos de violencia digital incluyendo agresiones basados en nuestra experiencia como el zoombombing o el odio viral.
- Impulsar la coordinación entre los distintos mecanismos internacionales para dar respuestas prontas que respalden y contrarresten los impactos de las agresiones digitales, incluyendo el establecimiento de mandatos específicos y la emisión de medidas de protección, publicar guías prácticas así como

diagnósticos basados en experiencias reales con el fin de conocer la situación, profundizar y ampliar los estándares, analizar los impactos del uso de la Inteligencia Artificial en la violencia digital contra defensoras, impulsar fondos flexibles de emergencia, infraestructura de protección digital y estándares comunes de registro.

A LAS CORPORACIONES DE REDES SOCIALES

- Priorizar los derechos humanos y la ética antes que las ganancias; ello implica invertir recursos en mecanismos de ayuda y atención pronta frente a agresiones digitales, eliminar contenidos violentos contra mujeres defensoras y personas de las disidencias sexo-genéricas, restaurar oportunamente cuentas y contenidos de defensa de derechos humanos, contar con canales verificados, incorporar una revisión humana con peritaje local así como frenar la amplificación algorítmica del odio.
- Fortalecer los mecanismos de ayuda a través de la inversión de recursos que garanticen revisión humana, confiable, con enfoque de derechos humanos y de género para la atención y respuesta integral a las violencias digitales contra defensoras y disidencias sexo-genéricas.
- A través de publicaciones y campañas, asumir una postura clara de respaldo a la labor de las defensoras y disidencias sexo-genéricas que utilizan las redes sociales para realizar su legítima labor de defensa de derechos humanos.
- Generar medios de cooperación transnacional y facilitar información que permita ubicar a los agresores para prevenir nuevos ataques, garantizar la reparación del daño y la no repetición.

A LAS ORGANIZACIONES SOCIALES Y DE DERECHOS HUMANOS

- Incorporar la seguridad digital y el bienestar psicosocial como componentes permanentes de las estrategias de protección a partir de metodologías contextualizadas que consideren la diversidad de realidades en los territorios: edad, género, educación, acceso a internet y a equipos digitales, etc.

- Desarrollar protocolos de respuesta ante ataques digitales, que permitan identificar, documentar, evaluar y atender de manera oportuna incidentes de violencia facilitada por la tecnología, incluyendo criterios para determinar cuándo activar mecanismos de protección.

- Fortalecer las capacidades de documentación y preservación de evidencias digitales, de manera que los ataques puedan ser sistematizados y utilizados para acciones de denuncia, incidencia y, cuando corresponda, investigación y judicialización.

- Documentar de manera sistemática los vínculos entre la violencia digital y las agresiones en el ámbito físico, con el fin de visibilizar cómo ambas formas de violencia se refuerzan y forman parte de estrategias más amplias de persecución y silenciamiento.

- Generar sistemas colectivos de alerta y monitoreo, especialmente para identificar campañas coordinadas de acoso, estigmatización, desinformación y otras formas de violencia digital dirigidas contra nosotras y nuestras organizaciones.

- Establecer mecanismos de apoyo y respuesta colectiva que eviten que las personas afectadas enfrenten los ataques de manera aislada y que permitan distribuir las tareas de contención, documentación, comunicación y denuncia.

- Promover estrategias de comunicación y respuesta frente a campañas de desinformación y estigmatización, evitando que la respuesta amplifique los ataques y priorizando acciones que protejan a las personas afectadas.

- Fortalecer la colaboración entre organizaciones, periodistas, personas expertas en tecnología y actores de protección, para mejorar la capacidad de identificar patrones e impactos de la violencia digital, y responder de manera coordinada.

- Impulsar acciones de incidencia para exigir transparencia y rendición de cuentas a los Estados y a las empresas tecnológicas y de telecomunicaciones respecto del uso de tecnologías de vigilancia, la protección de datos personales y las medidas adoptadas frente a la violencia digital.




IM-DEFENSORAS