MANUAL DE PREVENCIÓN DEL DOXING

MOVER coop

HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

MANUAL DE PREVENCIÓN DEL DOXING

Elaborado por
Magui Fernández Valdez y Celine Redon

Asesoría tecnológica
Sol Verniers

Diseñado por
Flora Dunand

Versión accesible
https://movercooperativa.com/wp-content/uploads/2026/02/Manual-de-prevencion-del-doxing-Mover-Cooperativa-y-Fundacion-Boll-versionacccesible.pdf

MOVER COOPERATIVA

Mover es una cooperativa de trabajo dedicada a la investigación, el análisis y el desarrollo de asesorías desde una perspectiva interseccional y de derechos humanos. Desde un enfoque crítico y comunitario, impulsa proyectos orientados a la incidencia, la formación y el acompañamiento de organizaciones, activismos e instituciones.

Contacto
info@movercooperativa.com

Web
www.movercooperativa.com

FUNDACIÓN HEINRICH BÖLL
Oficina Buenos Aires

La Fundación Heinrich Böll es la fundación política alemana cercana al partido Alianza 90/Los Verdes. Tiene su sede central en Berlín y actualmente está presente en más de 34 países. En América Latina la fundación se siente especialmente comprometida, junto con muchas organizaciones socias y amigas, con la política climática, la promoción de la democracia y la justicia de género, así como con la consolidación institucional y profundización de los derechos humanos. Consideramos clave fortalecer a la sociedad civil en el diálogo permanente entre ciudadanía e institucionalidad política como práctica democratizadora, siguiendo ese lineamiento es que apoyamos proyectos de diversas organizaciones civiles, promovemos debates y producimos publicaciones gratuitas.

Contacto
info@ar.boell.org

Web
www.ar.boell.org

Mover coop

HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

MANUAL DE PREVENCIÓN DEL DOXING

ÍNDICE

Clickeá sobre cada capítulo
para redirigir al mismo

HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

Capítulo 1

MARCO POLÍTICO

El doxing -la publicación de información personal sin consentimiento- no es un hecho aislado ni una práctica marginal del ecosistema digital. Puede leerse como una tecnología de violencia* que aporta a la **producción de normalidad**, en tanto esa normalidad se sostiene históricamente sobre dispositivos de exclusión y disciplinamiento como la violencia machista, la heterosexualidad obligatoria, el racismo, el clasismo y el neoliberalismo, entre otros. El doxing no irrumpe desde afuera del orden social: **lo refuerza**, operando como un mecanismo de corrección y disciplinamiento.

Esta práctica se inscribe en un contexto específico: el de la **infocracia**. En el régimen infocrático, la información no funciona como base de la deliberación democrática, sino como un flujo constante que gobierna los afectos y las conductas. Todas las personas somos, de manera simultánea, productoras y consumidoras de información (prosumidor), sometidas a una exigencia permanente de actualización, novedad y sorpresa. Este consumo ininterrumpido fragmenta la percepción, acelera los tiempos de atención y produce subjetividades atravesadas por una inquietud cognitiva constante.

El efecto político de este proceso es profundo dado que asistimos a una **crisis cognitiva que afecta a la democracia**. La sobreabundancia de información no fortalece el pensamiento crítico, sino que lo debilita, desplazando la reflexión por la reacción. La información ya no se organiza en torno a la verdad, sino en torno a su capacidad de **afectar**, de movilizar emociones y producir efectos inmediatos. En este contexto, lo verdadero importa menos que lo viral y las convicciones ceden frente a los impactos afectivos.

Este régimen se despliega principalmente en el marco de las **plataformas digitales**, que no operan de forma jerárquica ni centralizada, sino de manera rizomática. Los ataques no necesariamente tienen un único origen ni un centro identificable: se expanden, se replican, se amplifican. Un ataque coordinado en redes —por ejemplo, en X— no requiere una estructura formal ni una autoría clara. La violencia se vuelve difusa, distribuida, difícil de contener.

TECNOLOGÍA DE VIOLENCIA

En este texto, el término *tecnología* no se utiliza en un sentido técnico ni vinculado exclusivamente a las tecnologías de la información y la comunicación. Se emplea en un sentido político, en diálogo con tradiciones del pensamiento postestructuralista donde tecnología refiere a conjuntos de prácticas, saberes, procedimientos y racionalidades que organizan el ejercicio del poder y producen efectos sobre los cuerpos, las conductas y las subjetividades. En este marco, hablar de tecnología de violencia permite señalar que el doxing no es solo una técnica aislada o un acto individual, sino una forma organizada y socialmente disponible de ejercer violencia que contribuye a procesos de normalización, corrección y disciplinamiento.

PROSUMIDOR

Término acuñado por Alvin Toffler (1980) que refiere a la persona que, en los entornos contemporáneos -especialmente digitales- consume y produce bienes, servicios o información al mismo tiempo, desdibujando la separación tradicional entre producción y consumo.

Lo retomamos en la página 7

La jerarquización de los afectos por sobre la verdad permite comprender por qué prácticas como el doxing resultan tan eficaces. No buscan convencer ni argumentar: buscan **afectar**, producir miedo, vergüenza, exposición, desgaste. La circulación de fake news, deepfakes, la utilización de la IA o la apelación directa a emociones intensas -como en el uso estratégico de redes por parte de figuras como Donald Trump- muestra cómo la política se desplaza del plano de las ideas al de los impactos emocionales. En ese clima, el doxing se vuelve una herramienta privilegiada para silenciar, disciplinar y expulsar del espacio público digital.

Frente a este escenario, no alcanza con respuestas técnicas ni individuales. Se vuelve necesario construir **respuestas políticas** que articulen **cuidados digitales** y el **derecho a defenderse**, entendiendo que ambos conceptos están atravesados por tensiones propias del régimen infocrático.

Pensar los cuidados digitales exige partir de una premisa fundamental: **el cuidado no es un gesto privado ni una responsabilidad individual**. Históricamente, los feminismos y los movimientos LGBTI+ han mostrado que el cuidado es un trabajo socialmente organizado, atravesado por relaciones de poder, y que su privatización produce desigualdades y violencias. Pensar desde esta perspectiva en el ámbito digital implica cuestionar la idea de que cada persona debe "arreglárselas sola" frente a la violencia en redes.

Desde una **perspectiva de la socioafectividad**, el afecto se entiende como un organizador central de los cuidados que brindamos y recibimos, más allá de las lógicas de obligación familiarista. Los cuidados, en estos términos, no se agotan en el vínculo privado: tienen una **proyección social y política**. Esta mirada permite reconocer redes de sostén afectivo -amistades, compañeres, colectivas, organizaciones- que hacen posible la vida.

Sin embargo, esta perspectiva introduce una tensión central: en el régimen de la infocracia, aquello que permite pensar una politicidad de los afectos es, al mismo tiempo, lo que los vuelve una materia prima clave del gobierno de la información. Los afectos no solo circulan como experiencias subjetivas o vínculos sociales, sino que son capturados, amplificados y administrados por las plataformas, orientando la atención, moldeando percepciones y produciendo adhesión o rechazo. De este modo, lo afectivo deja de ser solo un terreno de resistencia o de sentido compartido y pasa a funcionar también como un insumo estratégico para la gestión del poder. Las plataformas privilegian la producción de afectación por sobre la construcción de sentido. Por eso, los cuidados digitales tienen que poder reflexionar sobre una **repolitización del afecto**, sacándolo de su captura mercantil y poniéndolo al servicio del sostén de la vida y de la acción colectiva.

En este marco, resulta central adoptar una **perspectiva comunitaria de los cuidados**. Esto implica romper con la idea de que el daño y su resolución se producen en el ámbito privado. En el espacio digital, esta lógica puede pensarse a partir de una analogía: la cuenta personal, el perfil, funciona como una "casa propia". Cuando ocurre un ataque, se espera que la persona lo resuelva puertas adentro, como si fuera un asunto doméstico. Pensar desde una perspectiva comunitaria de los cuidados rompe con esa expectativa y habilita respuestas colectivas.

Asimismo, la **desindividualización de los cuidados digitales** profundiza esta crítica. Desindividualizar implica romper con la culpa, el aislamiento y la fantasía del individuo autónomo digital. La violencia digital no se ejerce sobre sujetos aislados, sino sobre personas situadas en tramas sociales. Sin embargo, esta propuesta también tensiona con una característica central de la infocracia: la dificultad para construir comunidades políticas duraderas. Las comunidades de followers no son comunidades de cuidado, sino **mercancías a disputar**, organizadas por lógicas algorítmicas y de mercado. Desindividualizar el cuidado digital supone, entonces, un gesto contrahegemónico: producir comunidad allí donde el régimen sólo habilita agregados de atención.

Este entramado se completa al incorporar la perspectiva del **derecho a defenderse**. La autodefensa no es un derecho universal ni se ejerce en condiciones de igualdad. No toda defensa es leída como legítima y, en muchos casos, defenderse es una necesidad antes que una elección. La posibilidad de defenderse está **socialmente distribuida**: algunas personas deben demostrar que existe una violencia, que hay un daño real, que "no exageran", para recién entonces habilitar su defensa.

Ante el doxing, defenderse puede implicar reducir la exposición, apoyarse en otres, proteger identidades, cambiar hábitos, retirarse temporalmente. **Defenderse no exige necesariamente confrontar ni castigar, ni escalar la violencia**. Es, ante todo, una forma de **preservación** y, fundamentalmente, es un derecho que no se garantiza de manera individual: **debe construirse colectivamente**.

La pregunta —¿quién tiene la legitimidad y las herramientas para defenderse?— resulta clave para pensar el doxing. Muchas violencias digitales no son reconocidas como tales, especialmente cuando afectan a militantes, personas LGBTINB+, mujeres, personas racializadas, gordes, y podría seguir la lista. Desde esta perspectiva, la defensa deja de pensarse como un acto excepcional y se entiende como una **práctica cotidiana para sostener la propia existencia**.

¿QUÉ ES PROSUMIDOR?

El concepto de **prosumidor** fue introducido por **Alvin Toffler** (1980) para describir la emergencia de un sujeto que rompe la separación clásica entre productores y consumidores, al participar activamente en la creación, modificación y circulación de bienes, servicios e información. Para Toffler, este desplazamiento anticipa transformaciones profundas en los modos de producción, en el consumo y en la organización social, al diluir los límites entre quien produce y quien consume.

En los entornos digitales contemporáneos, les prosumidores al mismo tiempo que consumen información, también la producen. Sin embargo, esta condición no es neutra ni homogénea, sino que puede abrir a **escenarios divergentes**, atravesados por relaciones desiguales de poder.

Por un lado, existen formas de prosumo en las que la producción cotidiana de contenidos, interacciones y datos -muchas veces sin plena conciencia de su alcance- se traduce en la **cesión masiva de información personal y comportamental**. Estos datos, una vez agregados, procesados e interpretados a gran escala, fortalecen los algoritmos del mercado digital y contribuyen a la acumulación de valor por parte de las grandes empresas tecnológicas. En este escenario, el prosumo refuerza lógicas extractivas, donde les usuaries producen gratuitamente los insumos que luego consumen, bajo formas cada vez más personalizadas, opacas y concentradas.

Un ejemplo central de esta dinámica es el desarrollo contemporáneo de los sistemas de **inteligencia artificial**, cuyo funcionamiento se apoya en el procesamiento de enormes volúmenes de información previamente disponible en la red. Los modelos de IA aprenden, en gran medida, a partir de datos, textos, imágenes y códigos que fueron producidos y publicados por comunidades de usuaries en contextos muy diversos. De este modo, la capacidad actual de la IA para generar contenidos, resolver problemas o escribir código se asienta sobre un acervo colectivo preexistente, que es reutilizado y resignificado en nuevos marcos de valorización económica.

Este proceso se vuelve particularmente visible en relación con el **software libre**: la apertura histórica del código fuente permitió la circulación del conocimiento técnico y la construcción de saberes compartidos, que hoy son parte del entrenamiento de sistemas automatizados. Aquello que surgió bajo lógicas colaborativas y de acceso abierto fue posteriormente apropiado por actores privados, tensionando la relación entre bienes comunes digitales y captura corporativa.

Por otro lado, el prosumo puede asumir una **dimensión política y estratégica**, vinculada a la disputa por el control de la información, los datos y las narrativas. Desde esta perspectiva, les prosumidores son entendides como **actores actives en entornos digitales distribuidos**, capaces no solo de producir información, datos y narrativas, sino también de analizarlos, disputarlos y resignificarlos colectivamente. Aquí, el prosumo se orienta al fortalecimiento de redes comunitarias, la amplificación de expresiones culturales, la circulación de saberes situados y la construcción de contranarrativas frente a discursos hegemónicos.

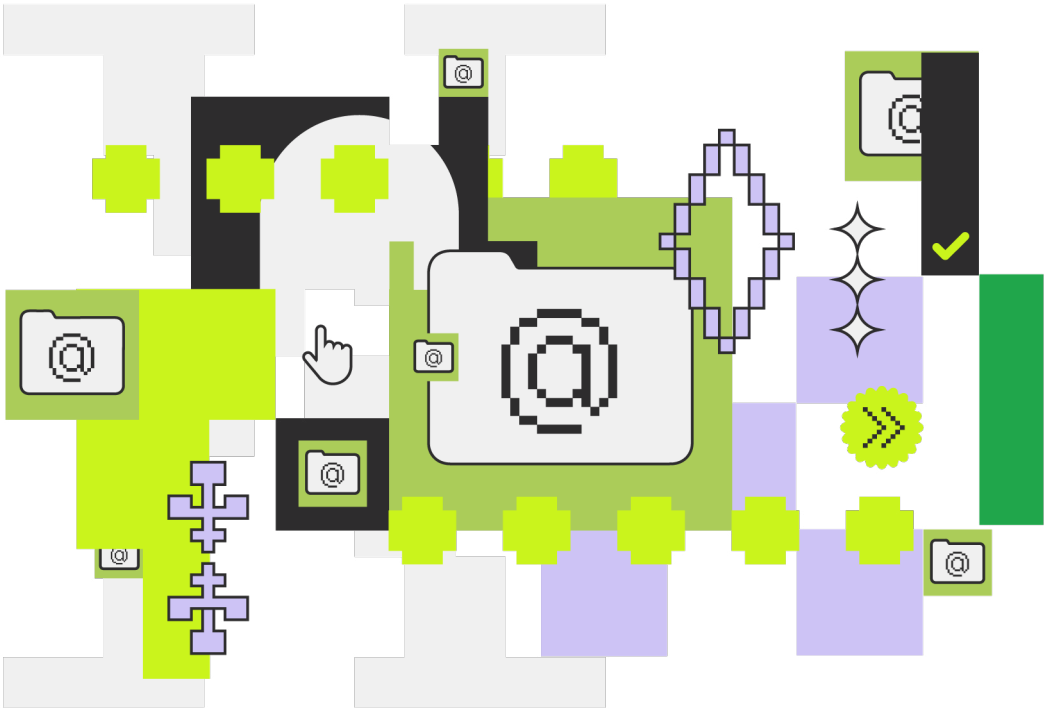
En este sentido, el prosumo deja de ser únicamente una práctica técnica o cultural para constituirse como una **forma de incidencia política**, estrechamente ligada a la defensa de derechos, a la democratización de la información y a la disputa por el sentido común en el espacio público digital.

Todo este marco se piensa desde una **perspectiva antipunitivista**. La razón punitiva organiza la respuesta al daño a partir del castigo, el control, la vigilancia y la moralización de las personas, fijando posiciones rígidas de víctima y victimario que dificultan un análisis político de las condiciones que producen la violencia. En el caso del doxing, esta lógica se expresa en respuestas como denunciar automáticamente, exigir el cierre de cuentas ajenas, pedir más controles y más vigilancia.

Estas respuestas, lejos de desmantelar las condiciones de violencia, pueden producir efectos contraproducentes: ampliación del poder de las plataformas, naturalización de la vigilancia como forma de protección y legitimación de lógicas de control que históricamente han vulnerado a los mismos colectivos que más sufren la violencia digital. El ensañamiento con los victimarios no repara el daño ni reconstruye las tramas rotas.

El punitivismo no repara el daño psicosocial del doxing, no revierte el aislamiento que produce, reproduce desigualdades y expone a las personas a nuevas vulnerabilidades. En cambio, una mirada no punitivista habilita otras respuestas: **defenderse sin castigar, protegerse sin escalar la violencia, delegar, retirarse o bloquear sin culpa, buscar redes de apoyo**.

Desde esta perspectiva, los cuidados digitales se proponen no como una promesa de seguridad total, sino como una **política de rearticulación** en un contexto infocrático: prácticas colectivas que buscan reducir el daño, preservar la vida y ampliar la capacidad de defenderse sin reproducir las lógicas de control que hacen posible la violencia.



Capítulo 2

¿QUÉ ES EL DOXING Y CÓMO OPERA?

¿Qué es el doxing? Aproximaciones a algunas definiciones

El **doxing** es una práctica que consiste en la **publicación, difusión o exposición de información personal sin el consentimiento de la persona afectada**, con el objetivo de **acosar, intimidar, censurar, extorsionar o generar daños económicos, reputacionales o simbólicos.** En situaciones extremas, estas acciones pueden derivar en **violencia física directa.**

La información expuesta puede incluir

Cada tipo de dato habilita distintos niveles de agresión y riesgos, que pueden incluir hostigamiento digital, robo de identidad, violencia en línea o incluso en la vida cotidiana.

El **doxing** es una forma de **violencia digital** que busca generar miedo, daño emocional, pérdida de privacidad, autocensura y, en algunos casos, riesgos reales para la integridad física y económica de la persona afectada.

En este material adoptamos una **perspectiva de seguridad holística**, entendida como un enfoque que integra de manera inseparable las dimensiones físicas, digitales y psicosociales. Esta mirada no se limita a situaciones excepcionales ni a episodios de violencia puntual, sino que propone una forma de **habitar los entornos digitales** que pueda sostenerse en la vida cotidiana.

Desde esta perspectiva, la seguridad no se reduce al uso correcto de herramientas técnicas ni a la prevención de ataques específicos. Implica también considerar los impactos emocionales, vinculares, laborales y políticos que el uso de tecnologías —y las violencias mediadas por ellas— producen en las personas y los colectivos. Por eso, no analizamos el doxing como un fenómeno meramente tecnológico, sino como una **práctica de violencia** que atraviesa la vida cotidiana, los vínculos sociales, el trabajo, la militancia y la participación pública.

Adoptar una mirada de seguridad holística permite **salir de respuestas fragmentadas** y fortalecer prácticas de cuidado que no se activan solo ante un ataque, sino que se incorporan de manera sostenida en la forma en que nos organizamos, nos comunicamos y participamos en el espacio público digital.

¿Cómo se obtiene la información para hacer doxing?

El doxing puede realizarse a partir de múltiples vías de obtención de información que combinan técnicas tecnológicas y sociales. En la mayoría de los casos, la información que se usa para doxear **no se "hackea"**, sino que se **reconstruye** a partir de muchos datos sueltos. Pequeñas pistas que, juntas, permiten identificar, ubicar o exponer a una persona.

Las formas más comunes son:

Recolección de datos a través de redes sociales

Gran parte de los datos se obtienen de lo que las personas **publicamos sin darnos cuenta**:

- Fotos donde se ve una calle, una casa, un cartel o una patente.
- Historias que muestran rutinas (horarios, lugares, recorridos).
- Perfiles con nombre real, trabajo, ciudad, vínculos familiares.
- Comentarios viejos, publicaciones cruzadas entre plataformas.

Nada de eso parece peligroso por separado, pero **todo junto arma un mapa**.

Filtraciones de datos

A veces la información proviene de:

- Filtraciones de empresas o del Estado.
- Bases de datos vendidas o compartidas ilegalmente.
- Servicios que no protegieron bien la información.

Phishing

Mediante mensajes falsos que buscan engañar para robar accesos, datos o instalar malware. Es un tipo de engaño digital que busca que la persona:

- Ingrese su contraseña en un sitio falso.
- Descargue un archivo malicioso.
- Autorice accesos sin saberlo.

Con una sola cuenta o dispositivo vulnerado, se podría acceder a muchas más y realizar diferentes acciones que compliquen a la persona que está siendo atacada.

Sniffing

Analiza el tráfico de red para captar datos sensibles.
Puede ocurrir cuando:

- Se usan **redes Wi-Fi públicas o abiertas** (bares, aeropuertos, plazas).
- La red no está bien protegida.
- Alguien con conocimientos técnicos está "escuchando" lo que pasa por esa red.

A través del sniffing se pueden obtener:

- Contraseñas.
- Datos de inicio de sesión.
- Mensajes.
- Información sobre los sitios que se visitan.

La persona atacada **no hace nada raro ni incorrecto**: simplemente está conectada a una red insegura.

Búsqueda de información abierta

La búsqueda de información abierta consiste en **recolectar y analizar datos que ya están disponibles públicamente en internet**, sin acceder a información privada ni vulnerar sistemas. Es una práctica habitual en investigaciones periodísticas, académicas y de derechos humanos, pero también es utilizada en contextos de hostigamiento y doxing.

Es la recopilación de datos que ya están disponibles públicamente en internet. Puede incluir:

- **Registros públicos y bases de datos oficiales**.
- **Archivos y contenidos antiguos** (publicaciones, capturas, notas, perfiles ya inactivos).
- **Información técnica básica** asociada a dominios web (WHOIS, fechas de registro, proveedores).
- **Datos publicados en redes sociales** (biografías, fotos, interacciones, ubicaciones).
- **Cruce de información entre plataformas**, a partir de nombres, usuarios, correos, imágenes u otros rastros compartidos.

Ingeniería social

Consiste en **hacerse pasar por alguien confiable** para obtener información:

- Mensajes que parecen de una empresa, un banco o una red social.
- Pedidos "inocentes" de datos por mail, WhatsApp o redes.
- Formularios falsos o links que roban contraseñas.

No explotan fallas técnicas, explotan la **confianza e información** o conocimientos previos que tengan de la persona.

Ataques digitales

En algunos casos, la información utilizada para hacer doxing se obtiene a través de accesos no autorizados a cuentas o dispositivos. Esto puede ocurrir mediante:

- **Malware:** programas maliciosos que se instalan sin que la persona lo note, muchas veces al descargar archivos o hacer clic en enlaces.
- **Exploits:** aprovechamiento de fallas de seguridad en sistemas, aplicaciones o dispositivos que no están actualizados.
- **Descifrado o robo de contraseñas:** uso de contraseñas débiles, repetidas o filtradas previamente en otras plataformas.

Estas técnicas pueden utilizarse de manera aislada o combinada, aumentando la eficacia del ataque.

¿Cómo opera y se despliega el doxing?

El doxing **no ocurre de un día para otro**. Suele desplegarse como un proceso:

- Se juntan datos dispersos.
- Se los cruza y ordena.
- Se publican de forma estratégica.
- Se amplifica a través de redes, grupos o medios.

> Las plataformas digitales permiten que un ataque **escale rápido**, incluso cuando empezó con una sola persona o cuenta.

Una vez difundida la información, las **agresiones asociadas al doxing** pueden adoptar diferentes niveles de intensidad, que no siempre se presentan de forma lineal o inmediata.

- Amenazas y hostigamiento en entornos digitales
- Acoso sistemático y campañas de odio coordinadas con uso de bots o cuentas creadas específicamente para hostigar.
- Realización de compras falsas a nombre de las personas a través de plataformas de comercio o mensajería que permiten ubicar las direcciones de las personas (Por ejemplo, Pedidos Ya, Facebook Market, entre otras)
- Extorsión mediante la amenaza de difusión de información
- Robo de identidad y suplantación
- Swatting: es una forma de violencia que consiste en **hacer denuncias falsas y graves ante fuerzas de seguridad** (por ejemplo, avisar de un secuestro, una bomba o una situación armada inexistente) **con el objetivo de que la policía o fuerzas especiales se movilicen hacia el domicilio de una persona**.

La IA como amplificadora del doxing

En el contexto actual, resulta clave **incorporar la inteligencia artificial en los análisis vinculados al doxing**, ya que amplifica y complejiza las amenazas existentes. La IA no crea el doxing, pero **modifica su escala, velocidad y capacidad de daño**, reduciendo las barreras de entrada para quienes atacan y aumentando la dificultad de detección y defensa.

Entre los principales riesgos emergentes se destacan:

- Deepfakes (contenidos falsos), que permiten crear mediante IA imágenes y videos falsos utilizando rostros de personas reales**.
- Audiofakes (audios falsos), mediante la imitación de voces.
- Optimización de ataques de phishing y malware, a partir del análisis automatizado de sistemas y comportamientos.

En enero de 2026, **Grok**, el sistema de inteligencia artificial desarrollado por **xAI** e integrado a la plataforma **X (ex Twitter)**, facilitó la **difusión masiva de deepfakes íntimos generados sin consentimiento**, incluyendo imágenes sexualizadas de **personas adultas y niñes y adolescentes**. Investigaciones periodísticas y denuncias públicas señalaron que la herramienta permitía editar imágenes de personas reales mediante funciones integradas, con **controles insuficientes y fácilmente eludibles**, lo que derivó en bloqueos, investigaciones regulatorias y debates legislativos en distintos países. La funcionalidad que facilita el despliegue de estas acciones sigue disponible para algunes usuaries.

¿Quiénes son los actores del doxing?

El doxing **no es una práctica aislada ni individual, sino que forma parte de estrategias organizadas de hostigamiento digital**, que se despliega de manera coordinada.

Distintos actores cumplen roles específicos dentro de estas dinámicas, desde quienes impulsan el ataque hasta quienes lo amplifican o lo ejecutan. Entre esos actores se pueden identificar:

Milicias digitales de ultraderecha: grupos organizados que operan en redes sociales con objetivos políticos claros. Funcionan de manera coordinada, se organizan alrededor de liderazgos ideológicos, influencers o figuras públicas. Estas milicias no buscan solo debatir ideas, sino neutralizar adversarios, generar miedo y expulsar voces críticas del espacio público.

Influencers políticos y nodos de amplificación: señalan públicamente a personas (por ejemplo: periodistas, militantes, activistas), difunden información personal o habilitan que otrxs lo hagan. Funcionan como disparadores de campañas de doxing, aun que no siempre publiquen ellxs mismxs directamente los datos. Estos actores cumplen un rol clave porque legitiman el ataque y multiplican su alcance.

Trolls, cuentas anónimas y bots : Cuentas anónimas o pseudónimas, muchas veces creadas específicamente para hostigar, redes de trolls que actúan en masa. En algunos casos se utiliza la automatización (bots) para amplificar ataques, amenazas o datos personales. El anonimato, combinado con la falta de procesos de las plataformas para responder a estos ataques y minimizarlos, permite escalar la violencia con bajo costo personal y alta impunidad.

Simpatizantes y participantes espontáneos: seguidores que replican ataques "por militancia", usuarios que participan del hostigamiento como forma de pertenencia identitaria. Ahi, aplica una lógica de linchamiento digital, donde el ataque se vuelve colectivo. Esto diluye responsabilidades, vuelve difícil identificar un único agresor, complejiza identificar orígenes de los ataques y habilita la idea de "viralización orgánica" como excusa para que no vuelva visible la existencia de una metodología establecida.

Vínculos previos: el doxing también puede ser impulsado por **personas individuales**, especialmente cuando existen **vínculos previos o relaciones de cercanía**. Incluye situaciones como ex parejas o vínculos sexoafectivos; conflictos personales, laborales o militantes; disputas dentro de organizaciones o comunidades; personas conocidas que acceden a información sensible.
En estos casos, el doxing suele combinar **información obtenida por cercanía** con lógicas de exposición pública. Aunque el ataque pueda comenzar de manera individual, **rápidamente puede escalar** cuando otros actores (trolls, seguidores, cuentas anónimas) se suman y amplifican la violencia.

¿A quién puede afectar el doxing? Una mirada desde la interseccionalidad

El doxing no impacta a todas las personas de la misma manera. Si bien cualquiera puede ser víctima, **sus efectos se intensifican cuando se combinan distintas desigualdades estructurales**. Desde una **perspectiva interseccional**, entendemos que múltiples factores como géneros, clase social, origen étnico, edad, discapacidad, orientación sexual, diversidad corporal, identidad de género, religión o nacionalidad, entre otras, no actúan por separado, sino que se **entraman** y producen formas específicas de exposición y daño.

Por eso, el doxing afecta de manera particularmente grave a **activistas, mujeres, personas LGBTIQNB+, periodistas y defensorxs de derechos humanos**: no solo porque están más expuestxs en el espacio público y digital, sino porque sus cuerpos, voces y trayectorias ya son objeto de vigilancia, cuestionamiento y violencia previa. En estos casos, la difusión de datos personales no busca únicamente incomodar, sino **disciplinar**, reforzar jerarquías y marcar límites sobre quién puede hablar, existir o disputar sentido en el espacio público.

Desde esta mirada, el doxing no es un hecho aislado ni individual, sino una **práctica política** que se inscribe en relaciones de poder desiguales. Funciona como un mecanismo de control social que aprovecha las plataformas digitales para amplificar violencias ya existentes, produciendo miedo, autocensura y desgaste, no solo en la persona atacada, sino también en los colectivos y redes que la rodean.

Pensar el doxing desde la interseccionalidad implica entonces **correrse de una lectura neutral del riesgo** y reconocer que la exposición digital tiene consecuencias distintas según las posiciones que se habitan. Esto es clave para diseñar estrategias de prevención, cuidado y respuesta que no sean genéricas, sino **situadas, colectivas y conscientes de las desigualdades que atraviesan la vida digital**.

¿Qué efectos produce el doxing?

Los efectos del doxing son múltiples y acumulativos. Entre los impactos más frecuentes se identifican:

Impactos psicosociales

El doxing produce efectos profundos en las personas atacadas como miedo permanente, sensación de vigilancia, estrés, ansiedad, agotamiento emocional, autocensura, retraimiento del espacio público (físico y digital), ruptura de vínculos personales y militantes, entre otras. El objetivo no es solo dañar, sino quebrar subjetivamente a la persona.

Impactos en la vida pública y política

El doxing funciona como una tecnología de silenciamiento dado que expulsa voces críticas del debate público, especialmente en personas con exposición pública o militancia política y social (por autocensura o silenciamiento). Esto reduce la participación política e instala un clima de intimidación generalizado en base a la lógica "si hablás, te puede pasar". Esto pone en peligro la calidad democrática.

Impactos económicos y reputacionales

Pérdida de trabajos, contratos o fuentes de ingreso, desvío de recursos económicos para defensa legal, seguridad, mudanzas o reparación de dispositivos. Afectación de organizaciones, medios y colectivos (renuncias, rotación, parálisis). Daños reputacionales, que afectan la trayectoria laboral, profesional o comunitaria. El doxing actúa así como una forma de castigo económico indirecto.

Impacto estructural de normalización de la violencia

Se legitiman como "humor", "batalla cultural" o "libertad de expresión", lo que son ataques de disciplinamiento. Este proceso produce un **corrimiento del marco de lo decible y lo legítimo**, habilitando formas de crueldad como modos aceptados de intervención política y reorganizando las condiciones en las que se disputa el espacio público.

Capítulo 3

EL PARADIGMA DE REDUCCIÓN DE RIESGOS Y DAÑOS: UNA CLAVE PARA PENSAR LA PREVENCIÓN DEL DOXING

El paradigma de **reducción de riesgos y daños** surge históricamente en el campo de la salud pública, especialmente en el abordaje de los consumos problemáticos de sustancias, como una respuesta crítica a los enfoques punitivos, moralizantes y prohibicionistas. Frente a políticas que buscan erradicar conductas consideradas indeseables mediante el castigo, la criminalización o la sanción moral, la reducción de daños parte de un principio distinto: **las prácticas existen**, forman parte de la vida social, y lo urgente no es negarlas sino **reducir los daños que producen sobre las personas y las comunidades**.

Este paradigma luego **se expande** a otros campos: salud mental, VIH, trabajo sexual, políticas urbanas, violencia, y hoy también al mundo digital.

Este enfoque no se centra en disciplinar sujetos ni en producir "buenas conductas", sino en el **cuidado**, el reconociendo la autonomía, las trayectorias situadas y las condiciones materiales en las que las personas toman decisiones. En lugar de preguntar "¿por qué hacés esto?", la reducción de daños se pregunta: **¿qué riesgos existen?, ¿qué impactos genera?, ¿qué herramientas tenemos para disminuir el daño hoy, en este contexto concreto?**

Este enfoque **abandona la fantasía de control total** que caracteriza a los enfoques punitivos y paternalistas.

Con el tiempo, la reducción de daños dejó de ser un enfoque exclusivo del campo sanitario y comenzó a **dialogar con perspectivas feministas, comunitarias y de derechos humanos**, ampliándose a otros escenarios donde el castigo demuestra ser ineficaz y productor de nuevas violencias.

En ese desplazamiento, el paradigma se vuelve especialmente fértil para pensar las **violencias digitales**. Así como en salud pública se asumió que el consumo existe y que el desafío es reducir sus daños, en el mundo digital se reconoce que la exposición, la circulación de datos y el conflicto forman parte del entorno, y que el objetivo no es erradicarlos sino **mitigar su impacto, fortalecer las capacidades de respuesta y evitar que el daño se profundice**.

El doxing —la publicación de información personal sin consentimiento— no es un hecho aislado ni una anomalía. Se inscribe en un ecosistema digital atravesado por la exposición constante y la circulación acelerada de datos.

No se trata de negar los límites —el doxing es violencia—, sino de **construir respuestas que no profundicen el daño**.

Desde la reducción de riesgos y daños, el foco se desplaza dado que **no se trata de erradicar el conflicto digital**, sino de **reducir su impacto, su alcance y sus consecuencias** sobre la vida de las personas y los colectivos.

Esto implica reconocer algo central: **habitar lo digital es inevitable**, especialmente para activismos, militancias, organizaciones comunitarias. La pregunta no es cómo desaparecer de las redes, sino **cómo habitarlas con más herramientas, menos exposición innecesaria y mayor red de cuidados**.

¿Qué significa reducción de daños en el mundo digital?

Aplicar este paradigma a la prevención del doxing supone un cambio profundo de mirada:

- No se parte de la idea de "conducta correcta" en redes.
- No se responsabiliza a la persona atacada por su exposición.
- No se exige neutralidad, silencio ni autocensura como forma de protección.

Enfoques punitivos / moralizante	Enfoque de reducción de daños
Buscar culpables y responsables individuales	**Analizar condiciones, contextos y relaciones de poder**
Responder cuando el daño ya ocurrió	**Intervenir antes, durante y después del ataque**
Exigir pruebas, coherencia y "buena víctima"	**Priorizar el bienestar y la agencia de la persona afectada**
Apostar a la denuncia como única salida	**Combinar estrategias técnicas, psicosociales y colectivas**
Promover el silencio o la retirada como protección	**Reconocer múltiples formas de habitar lo digital**
Delegar la respuesta en el Estado o plataformas	**Fortalecer redes comunitarias y de apoyo y exigir al Estado y las plataformas**

En este marco, la reducción de daños **no elimina el riesgo**, pero **reduce su impacto**, amplía las opciones de respuesta y evita que la violencia se multiplique por aislamiento, culpa o sobreexposición.

Buenas prácticas para la prevención del doxing

La prevención del doxing no se basa en eliminar todo riesgo —algo imposible en entornos digitales— sino en **reducir la exposición innecesaria, anticipar escenarios y fortalecer la capacidad de respuesta individual y colectiva**. Estas prácticas no son recetas universales: se combinan y ajustan según contextos, niveles de visibilidad y decisiones personales y políticas.

Cuando alguien hace doxing, no siempre usa técnicas complicadas: muchas veces junta pedacitos de información pública y los cruza hasta armar un perfil completo.

Alfabetización digital integral

- Comprender cómo funcionan las plataformas, qué datos recolectan y cómo circula la información.
- Reconocer que la violencia digital no es un problema técnico aislado, sino político, afectivo y relacional.

Reconocimiento del propio cuerpo digital

- Identificar qué información personal está disponible, dónde circula y en qué contextos.
- Asumir que la identidad digital es una combinación de datos, vínculos y performances.
- Reducir el rastro digital cuando sea posible: **la información que no existe no puede ser utilizada**. Esto puede implicar borrar lo que ya no hace falta, ocultar datos sensibles, cerrar cuentas viejas.
- Realizar ejercicios de revisión de tu información pública (OSINT) para saber cuál es accesible públicamente.

Incluye, por ejemplo:

- Lo que aparece cuando alguien busca tu nombre o apodo en Google.
- Tus redes sociales abiertas o viejas cuentas que quedaron activas.
- Fotos, comentarios, etiquetas, likes, amistades visibles.
- Datos que compartiste alguna vez sin pensar que quedaban públicos (lugares, trabajos, vínculos, rutinas).
- Información que subieron otres sobre vos (fotos, notas, menciones).

¿QUÉ ES OSINT?

OSINT es una sigla en inglés que significa inteligencia de fuentes abiertas. Dicho en simple: es **toda la información sobre una persona que cualquiera puede encontrar en internet sin hackear nada**.

Reducir exposición innecesaria

- Limitar la publicación de datos sensibles (direcciones, rutinas, vínculos familiares).
- Revisar configuraciones de privacidad y permisos en plataformas y aplicaciones.
- Revocar accesos innecesarios o antiguos que amplían la superficie de ataque.

Compartimentar identidades y roles

- Separar, cuando sea posible, espacios personales, laborales, militantes o públicos.
- Evaluar el uso de identidades colectivas, seudónimas o compartidas según el contexto.

Separación de identidades públicas y privadas

Identidad seudónima:
Implica la utilización de un alias. Permite construir presencia y reputación sin usar el nombre real. Brinda protección relativa, pero puede volverse rastreable si se cruza con otros datos

Identidad anónima:
No tiene vínculo con la identidad real. Ofrece alta protección, pero requiere cuidados constantes y no permite construir visibilidad pública sostenida.

Identidad colectiva:
Es una identidad compartida por varias personas. Reduce el riesgo individual y es especialmente útil para acciones políticas o comunicacionales sin atribución personal.

Identidad altamente visible:
En algunos contextos, ser visible también puede ser una defensa, ya que dificulta ataques silenciosos y habilita respuestas solidarias rápidas.

Fortalecer la seguridad básica

- X Usar contraseñas robustas y únicas.
- X Activar factores adicionales de verificación. Configurar **2FA/MFA** en todas las cuentas posibles.
- X Revisar accesos a cuentas y dispositivos de forma periódica.
- X Revisar sesiones abiertas y dispositivos vinculados.

¿Qué es 2FA / MFA y por qué es importante?

2FA (segundo factor de autenticación) **y MFA** (autenticación multifactor) son formas de agregar una capa extra de seguridad a tus cuentas digitales.

Normalmente, para entrar a una cuenta usás solo una contraseña. Con 2FA o MFA, además de la contraseña, se pide **una segunda verificación**.

Por ejemplo:

- un código que llega al celular o al mail,
- una app que genera números temporales,
- una huella digital o reconocimiento facial,
- o una llave de seguridad.

Esto significa que **aunque alguien consiga tu contraseña**, no puede entrar fácilmente a tu cuenta sin ese segundo paso.

¿Por qué sirve para prevenir el doxing?

Muchos ataques de doxing empiezan con:

- cuentas hackeadas,
- accesos no autorizados,
- robo de información desde redes sociales o correos.

Activar 2FA/MFA **reduce mucho ese riesgo**, porque dificulta que alguien tome control de tus cuentas y acceda a datos personales, mensajes privados o contactos.

¿Dónde podés activar el segundo factor?

Estas son algunas de las plataformas más usadas donde **conviene activar sí o sí** el segundo factor de verificación. En casi todos los casos se encuentra en

CONFIGURACIÓN » **SEGURIDAD**

INSTAGRAM
Configuración » Centro de cuentas » Contraseña y seguridad » Autenticación en dos pasos

TIKTOK
Mi perfil » Configuración » Configuración y seguridad » Seguridad y permisos » Verificación en dos pasos

WHATSAPP
Configuración » Cuenta » Verificación en dos pasos

TELEGRAM
Ajustes » Privacidad y seguridad » Verificación en dos pasos

GMAIL (y cuentas Google en general)
Administrar tu cuenta de Google » Seguridad y acceso » Verificación en dos pasos

FACEBOOK
Mi perfil » Configuración y privacidad » Configuración » Contraseña y seguridad » Contraseña y seguridad (nuevamente) » Autenticación en dos pasos

X
Configuración y soporte » Configuración y privacidad » Seguridad y acceso a la cuenta » Seguridad » Autenticación de dos fases

MICROSOFT (Outlook, Hotmail, OneDrive)
Cuenta Microsoft » Seguridad » Verificación en dos pasos

APPLE (Apple ID, iCloud)
Apple ID » Seguridad » Autenticación de dos factores

Configurar la privacidad en redes sociales

- Considera si necesitas una cuenta pública o privada.
- Ajustar quién puede ver, comentar, etiquetar, repostear o enviar mensajes.

En algunas oportunidades puede ser útil **limitar la indexación de perfiles y contenidos** cuando sea posible. Esto refiere a información tuya que los buscadores (como Google) tienen disponible. Muchas veces esta información es tomada de las redes sociales. Cuando los perfiles se encuentran indexados es más fácil juntar información personal, se pueden cruzar datos entre plataformas y esto aumenta la exposición.

Limitar la indexación de perfiles y contenidos permite que los buscadores no puedan encontrar la información de tus redes sociales sin tener cuenta en la red social o sin ser tu contacto/amigx.

Construir un mapeo de apoyos

- Identificar personas y espacios de confianza para apoyo emocional, técnico y organizativo.
- Acordar de antemano cómo actuar ante un ataque (a quién avisar, qué delegar).
- No hay que esperar a un posible ataque para contar con esta información y saber cómo actuar.

Registrar sin sobreexponerse

- Documentar ataques y publicaciones dañinas de manera ordenada.
- Evitar el monitoreo compulsivo que profundiza el desgaste emocional.
- Evaluar la delegación de esta tarea en alguien de confianza como una práctica de autocuidado.

Para más información sobre este tema, se puede consultar el **Capítulo 4**.

Validar decisiones parciales

- **Ajustar progresivamente la exposición**
  Aumentar la privacidad de las cuentas, limitar temporalmente comentarios e interacciones públicas o habilitarlas solo para personas conocidas.
- **Delegar la gestión de cuentas** a personas de confianza cuando la exposición directa resulte desgastante o riesgosa.
- **Bloquear o silenciar cuentas agresoras**, teniendo en cuenta que esta decisión puede priorizar el cuidado inmediato aun cuando no detenga el ataque.
- **Pausar la actividad o cerrar cuentas**, entendiendo que estas medidas pueden ser necesarias en ciertos momentos, pero que no siempre resuelven situaciones de violencia sostenida o escalada.

Recordá que a veces mayor visibilidad representa una estrategia de cuidado y da más seguridad.

No hay una única respuesta correcta: cada decisión es situada.

Proteger la conexión

- Usar VPN para proteger la dirección IP, especialmente en contextos sensibles.
- Evitar redes públicas sin protección.

¿Qué es una VPN y para qué sirve?

Una **VPN** (Red Privada Virtual) es una herramienta que **oculta tu dirección IP**, es decir, el dato que identifica desde dónde te estás conectando a internet.

Cuando navegás sin VPN:

- las páginas y servicios pueden ver tu IP,
- la IP puede dar pistas sobre tu ubicación,
- y puede usarse para rastrear tu actividad o cruzarla con otros datos.

Cuando usás una VPN:

- X tu conexión pasa por otro lugar,
- X tu IP real queda oculta,
- X y aparece como si estuvieras navegando desde otra ubicación.

¿Por qué es importante para prevenir el doxing?

En situaciones de acoso o ataques digitales:

- X la IP puede usarse para ubicar geográficamente a una persona,
- X vincular cuentas entre sí,
- X o sumar información para un doxing más grave.

Usar VPN **no te hace invisible**, pero:

- X dificulta el rastreo,
- X reduce la exposición,
- X y agrega una capa más de protección, sobre todo en momentos sensibles.

Algunas VPN que podés usar...

- ✦ VPN de RiseUp.net
- ✦ ProtonVPN
- ✦ Mullvad

¿Cuándo conviene usar VPN?

- X Cuando estás atravesando un conflicto o ataque digital.
- X Si usás redes públicas (bares, trabajo, universidades, aeropuertos, espacios con redes abiertas, entre otros).
- X Si manejás cuentas sensibles, militantes o colectivas.
- X Si necesitás reducir al mínimo la información que dejás al navegar.

Ampliar la mirada: estrategias para conocer nuestra existencia digital

La prevención del doxing no empieza cuando configuramos una cuenta o cambiamos una contraseña, sino mucho antes: cuando entendemos cómo existimos en el mundo digital y qué condiciones hacen posible una exposición o un daño. Aquí proponemos un cambio de enfoque: pasar de reaccionar ante los ataques a **anticiparnos con criterio**, identificando qué vale la pena cuidar, frente a quiénes y con qué nivel de esfuerzo. Para esto proponemos trabajar desde una mirada que combine el desarrollo de un **modelo de amenazas** y una **matriz de riesgos**. Esto no busca generar miedo ni control total, sino ofrecer herramientas para tomar decisiones informadas, reducir daños y fortalecer una cultura de cuidados digitales situada y realista.

Modelo de amenazas

Antes de hablar de contraseñas, configuraciones o herramientas, hay algo más básico: **entender cómo existimos en internet**. Qué dejamos ver, qué circula sobre nosotros, que debemos preservar en el ambiente digital y, mediante un modelado de amenazas posibles, entender qué cosas podrían usarse para exponernos, dañarnos o intimidarnos.

Muchas veces recién tomamos dimensión de estos temas cuando algo ya explotó: una filtración, una amenaza, una campaña de hostigamiento o incluso, la pérdida de una contraseña. Otras veces, la seguridad digital se siente tan técnica o lejana que preferimos no mirarla. Ninguna de esas dos situaciones ayuda a prevenir el doxing.

Por eso, una de las estrategias más importantes de cuidado es **ordenar la cabeza antes de actuar**.

Pensar amenazas ..... no es vivir con miedo

Trabajar con un modelo de amenazas no significa imaginar catástrofes ni pensar que todo el tiempo alguien nos está atacando. Significa algo mucho más simple: **hacernos preguntas concretas sobre qué podría pasar y qué nos afectaría de verdad**.

Algunas pistas para empezar:

- ¿Qué cuentas y datos míos no me gustaría que se hagan públicos?
- ¿Qué situaciones me generarían más daño si ocurrieran?
- ¿Hay antecedentes, propios o cercanos, que valga la pena tener en cuenta?

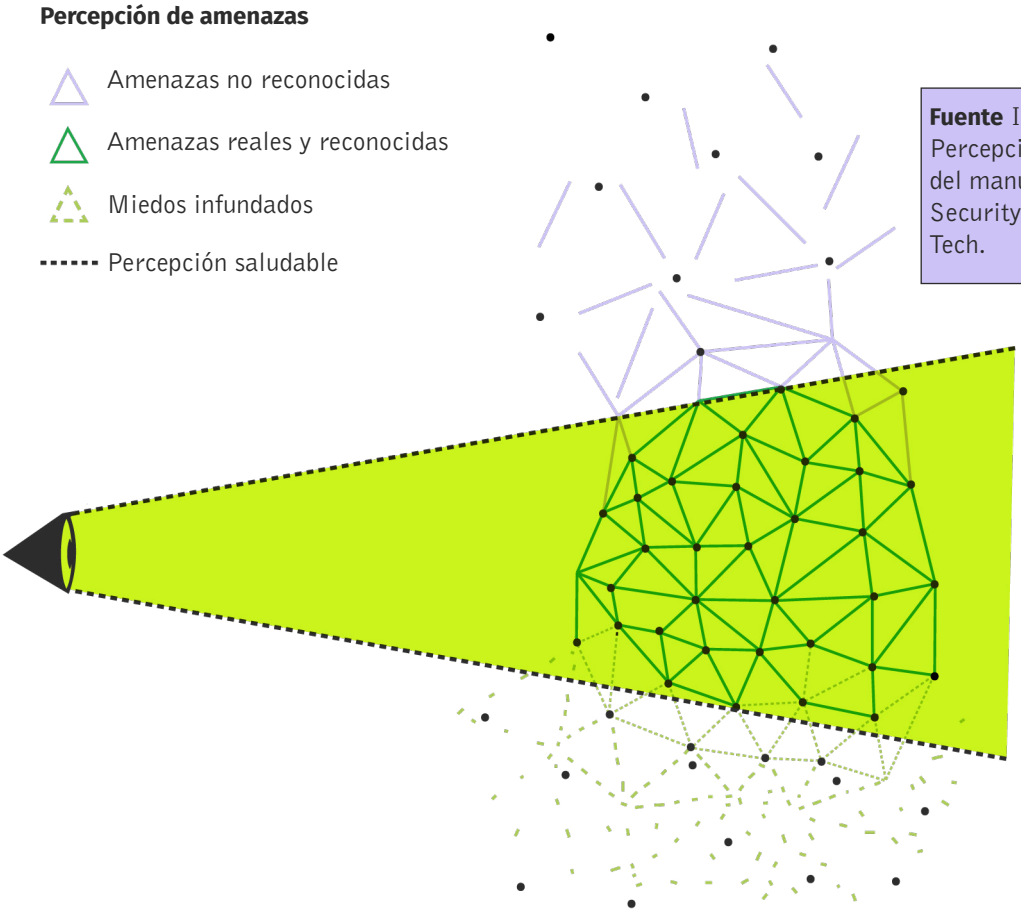
Cuando no hacemos este ejercicio, todo parece peligroso y terminamos paralizades o cuidándonos de cualquier cosa sin criterio. El modelo de amenazas sirve justamente para **dejar de reaccionar a ciegas**.

El modelo de amenazas es una forma sistemática de **identificar qué cosas pueden ponernos en riesgo y dónde están nuestras vulnerabilidades**, con un objetivo muy concreto: reducir el daño posible sobre aquello que queremos proteger.

El gráfico que se presenta a continuación en este apartado ayuda a entender algo clave: no todo lo que tememos es una amenaza real, y **no todas las amenazas reales están en nuestro radar**.

En el campo de visión aparecen distintos tipos de riesgos:

- **Miedos infundados**
  cosas que nos preocupan mucho, pero que en la práctica tienen baja probabilidad o bajo impacto.
- **Amenazas no reconocidas**
  riesgos que existen, pero que no estamos viendo o no sabemos identificar.
- **Amenazas reales y reconocidas**
  aquellas que efectivamente podrían ocurrir y que sí afectarían nuestra vida personal u organizacional.



Fuente Imagen de la Percepción de riesgos del manual «Holistic Security» de Tactical Tech.

El desafío del modelo de amenazas es **achicar ese campo**, dejando afuera lo que no es central y enfocándonos en las amenazas reales que vale la pena atender. No para eliminar todo riesgo (eso no existe), sino para construir una **percepción más justa y saludable** de nuestra situación digital.

Matriz de riesgos

En el mundo digital hay muchísimos riesgos posibles, pero **no todos tienen la misma importancia para todes**. El nivel de riesgo depende de quiénes somos, qué hacemos, en qué contextos participamos y cuánta exposición tenemos en internet.

Algunos riesgos son poco probables. Otros son más frecuentes. Algunos, aunque no ocurran seguido, pueden tener un impacto enorme si suceden. El desafío no es la existencia de riesgos, sino la dificultad para distinguir cuáles merecen nuestra atención y cuáles no.

Para eso usamos una herramienta clave: **la matriz de riesgos**.

Cuidarnos también es no sobrecargarnos ni intentar prevenir todo al mismo tiempo.

¿PARA QUÉ SIRVE UNA MATRIZ DE RIESGOS?

La matriz de riesgos nos ayuda a **priorizar**. Es una forma visual y práctica de decidir:

- qué riesgos necesitan una respuesta urgente,
- cuáles pueden quedar en observación,
- y cuáles no justifican que gastemos tiempo, energía o recursos.

LAS DOS PREGUNTAS CLAVE

La matriz cruza dos variables simples, pero muy potentes:

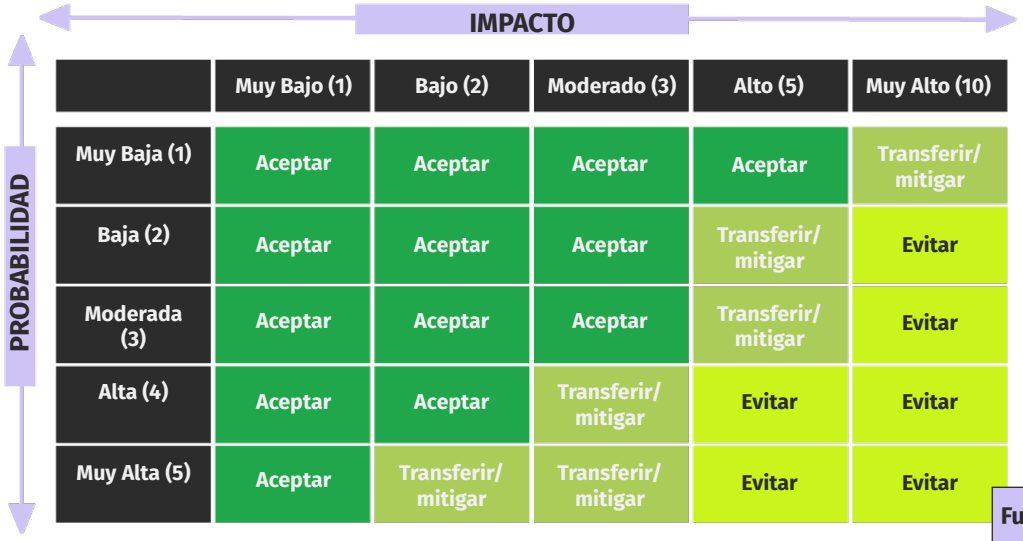
PROBABILIDAD

¿Qué tan posible es que esto pase en nuestro caso concreto?

IMPACTO

Si pasa, ¿qué tan grave sería para nosotres, nuestra organización o nuestro entorno?

Cuando cruzamos estas dos preguntas, aparece algo fundamental: **las prioridades**.



PROBABILIDAD	Muy Bajo (1)	Bajo (2)	Moderado (3)	Alto (5)	Muy Alto (10)
Muy Baja (1)	Aceptar	Aceptar	Aceptar	Aceptar	Transferir/ mitigar
Baja (2)	Aceptar	Aceptar	Aceptar	Transferir/ mitigar	Evitar
Moderada (3)	Aceptar	Aceptar	Aceptar	Transferir/ mitigar	Evitar
Alta (4)	Aceptar	Aceptar	Transferir/ mitigar	Evitar	Evitar
Muy Alta (5)	Aceptar	Transferir/ mitigar	Transferir/ mitigar	Evitar	Evitar

Fuente Enredando proyectos. La gestión de riesgos en los proyectos. Disponible en: https://enredandoproyectos.com/la-gestion-de-los-riesgos-en-los-proyectos/

En la imagen vemos una matriz donde:

- el eje vertical representa la probabilidad (de muy baja a muy alta),
- el eje horizontal representa el impacto (de muy bajo a muy alto).

Cada cruce nos da una orientación sobre qué hacer con ese riesgo:

- **Aceptar**
  Riesgos de bajo impacto y baja probabilidad. Existen, pero no ameritan acciones específicas por ahora.

- **Mitigar / Transferir**
  Riesgos intermedios. Conviene pensar medidas para reducir el daño posible o repartir la carga (por ejemplo, cambiar prácticas, sumar apoyos, usar herramientas).

- **Evitar**
  Riesgos de alta probabilidad y alto impacto. Acá es clave tomar decisiones claras para prevenir o directamente no exponerse.

No se trata de eliminar todo riesgo -eso no existe- sino de **elegir conscientemente dónde ponemos el foco**.

Armar nuestro propio mapa

El modelo de amenazas no es una receta universal. Siempre es **situado**. Puede pensarse para una persona, para una organización, para un grupo, para una campaña puntual o para un proceso específico.

Para darle forma, podemos trabajar con estas preguntas:

- **¿Qué queremos cuidar?**
  (cuentas, dispositivos, información sensible, contactos, ubicaciones, identidad digital, reputación)

- **¿De quiénes nos cuidamos?**
  (personas conocidas, desconocides, grupos organizados, troles, medios, empresas, instituciones)

- **¿Qué capacidad tienen para dañarnos?**
  (acceso a información, tiempo, dinero, herramientas técnicas, redes)

- **¿Qué tan probable es que intenten algo?**
  (según el contexto, la visibilidad, los temas que tocamos, el momento)

- **¿Hasta dónde estamos dispuestes a cuidarnos?**
  ¿Qué costo tiene para nosotres prevenir?
  ¿Qué consecuencias tendría no hacerlo?

Responder estas preguntas nos permite pasar de una sensación vaga de amenaza a un **mapa más claro y manejable**.

A modo de cierre

Estas prácticas **no buscan controlar a las personas, sino ampliar su margen de agencia**. La prevención del doxing no es una responsabilidad individual aislada: requiere **acuerdos colectivos, redes de cuidado y una lectura política del entorno digital**.

Una prevención efectiva del doxing no puede recaer únicamente en la persona expuesta. Desde la reducción de daños, **el cuidado es siempre colectivo**.

Esto implica:

- Construir acuerdos internos en organizaciones y colectivos sobre exposición, vocerías y protocolos de respuesta.
- Evitar la lógica del "arreglate solx" frente a ataques digitales.
- Reconocer que el impacto del doxing no es solo individual: afecta vínculos, equipos, proyectos y comunidades.

Checklist de cuidado digital

SEGURIDAD DE CUENTAS

- [ ] Cambié mis contraseñas por otras **largas y únicas**.
- [ ] Activé **segundo factor (2FA/ MFA)** en mis cuentas principales.
- [ ] Revisé qué dispositivos tienen sesiones abiertas.
- [ ] Saqué accesos a apps o servicios que ya no uso.

Se sugiere que tengan **al menos entre 14 y 16 caracteres**, combinando palabras, frases, números o símbolos. Como criterio mínimo de cuidado, se recomienda priorizar contraseñas **únicas y robustas** al menos para:

el correo electrónico personal,
correos de trabajo, militancia
u organización,
redes sociales,
y servicios bancarios o financieros.

Se recomienda evitar el uso del gestor de contraseñas de Google para el almacenamiento de contraseñas sensibles, priorizando herramientas especializadas en gestión segura de credenciales.

PLATAFORMAS CLAVE CON 2FA ACTIVADO

- [ ] Instagram
- [ ] WhatsApp
- [ ] Telegram
- [ ] TikTok
- [ ] Gmail / cuenta Google
- [ ] Facebook
- [ ] X
- [ ] LinkedIn
- [ ] Microsoft (Outlook / Hotmail)

Apple (Apple ID / iCloud)

EXPOSICIÓN Y RASTRO DIGITAL

- [ ] Me busqué en internet y vi qué información aparece sobre mí.
- [ ] Revisé fotos, posteos viejos y datos sensibles visibles.
- [ ] Borré u oculté lo que ya no necesito que esté público.
- [ ] Revisé si mis perfiles aparecen en Google (indexación).
- [ ] Revisé la información de tercerxs que he compartido.

HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

MOVER coop

CUERPO DIGITAL E IDENTIDADES

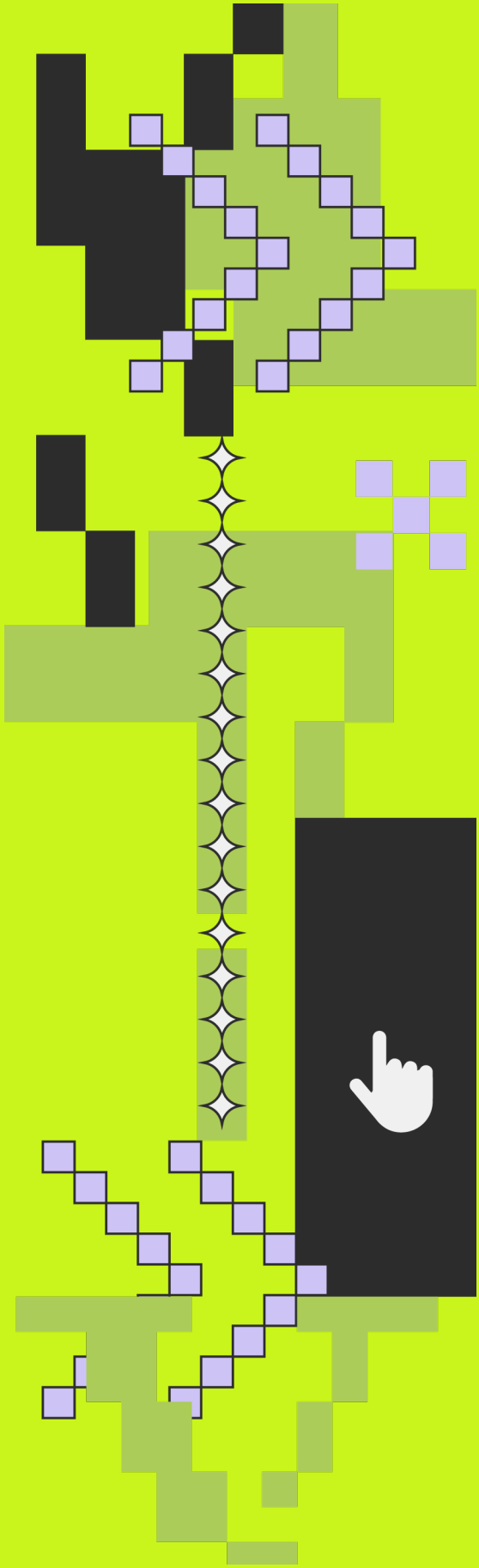
- [ ] Pensé cómo aparezco en redes (qué muestro, qué digo, qué datos dejo).
- [ ] Separé, cuando pude, lo personal de lo laboral / militante.
- [ ] Definí si uso identidad real, seudónima, anónima o colectiva según el contexto.
- [ ] Recordé que **ser visible también puede ser una estrategia**, no solo un riesgo.

CONEXIÓN Y DISPOSITIVOS

- [ ] Tengo mi dispositivo actualizado.
- [ ] Definí si mis actividades y visibilidad en internet requieren un modelo de seguridad más complejo.
- [ ] Uso **VPN** en momentos sensibles o redes públicas.
- [ ] Evito conectarme sin cuidado desde WiFi abiertas.
- [ ] Evito descargar aplicaciones de orígenes desconocidos.
- [ ] Chequeé el uso de la localización en mis dispositivos.

RED DE APOYOS

- [ ] Tengo identificadas personas de confianza para apoyo emocional.
- [ ] Sé a quién recurrir para ayuda técnica.
- [ ] Tengo contactos para orientación legal o institucional.



HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay
MOVER coop

Capítulo 4

¿QUÉ HACER SI OCURRE UN ATAQUE?

Registro, cuidado y toma de decisiones colectivas

Frente a un ataque de doxing es frecuente experimentar confusión, desorientación o urgencia por "hacer algo ya". Sin embargo, **no todas las situaciones son iguales ni requieren las mismas respuestas**. La violencia digital busca desorganizar, aislar y acelerar respuestas individuales, generando confusión, desgaste y sensación de indefensión.

Frente a eso, registrar la información no es un acto técnico ni burocrático sino que se constituye en una herramienta política de cuidado y defensa. La información permite frenar la lógica de la urgencia, ampliar el margen de análisis y recuperar capacidad de decisión, evitando respuestas impulsivas que muchas veces profundizan la exposición o el daño.

El registro permite transformar una experiencia vivida como caótica en un escenario legible, que puede ser compartido, analizado y abordado de manera colectiva. Registrar es una forma de **recuperar agencia**, de salir del lugar de exposición pasiva y volver a tomar decisiones sobre qué hacer, con quién y cómo. También es una forma de construir memoria, detectar patrones, sostener procesos de denuncia y evitar que la violencia quede reducida a un hecho individual.

Este apartado propone una secuencia posible para acompañar situaciones de ataque: orientaciones iniciales para los primeros momentos, una mirada sobre el autocuidado entendido como práctica colectiva, y herramientas para organizar la información de manera cuidada.

Antes de cualquier cosa: primeros pasos frente a un ataque

Cuando ocurre un ataque, antes de definir acciones concretas, algunas orientaciones básicas pueden ayudar a no perder información clave:

- **El ataque no es tu culpa**
  El doxing es una práctica de violencia, no una consecuencia de decisiones individuales.
- **No borrar contenido de inmediato**
  Mensajes, publicaciones o perfiles pueden funcionar como prueba.
- **No es necesario hacer todo ya ni hacerlo sola/e**
  Registrar y pensar puede llevar tiempo.
- **Identificá una persona o grupo de apoyo**
  (amigue, compañere, colectivo, organización) para no atravesar la situación en aislamiento.

Buena práctica: archivar el contenido

Antes de borrar o denunciar una publicación, es recomendable **archivar el enlace** para conservar una copia del contenido tal como estaba publicado, incluso si luego se elimina o modifica.

Una herramienta sencilla para esto es **https://archive.is/**, que permite generar un enlace con una versión archivada de la página.

Una mirada desde el autocuidado: del abordaje individual al acompañamiento colectivo

El doxing no es una experiencia individual, aunque impacte en una persona concreta. En la mayoría de los casos, forma parte de **dinámicas más amplias**, organizadas o amplificadas en red. Por eso, el autocuidado no puede pensarse sólo como una respuesta individual, sino como una **práctica colectiva y situada**.

Algunas estrategias posibles durante el acompañamiento:

Primeros Auxilios Psicológicos (PAP)
es un enfoque de cuidado desarrollado en el campo de la salud pública y la respuesta a crisis, orientado a brindar contención y apoyo psicosocial inmediato frente a situaciones de violencia o impacto repentino. No se trata de una intervención terapéutica, sino de un acompañamiento humano y situado que puede ser ofrecido tanto por profesionales como por personas del grupo o la comunidad (compañeres de trabajo o militancia, referentes comunitaries, integrantes de organizaciones, entre otres) con el objetivo de reducir el malestar inicial, recuperar sensación de seguridad, fortalecer redes de apoyo y devolver capacidad de decisión a la persona afectada.

Evaluar impactos y riesgos en grupo
conversar con un círculo de confianza (amistades, compañeres, colectivos u organizaciones) para leer el escenario y coordinar respuestas.

Delegar tareas y cuentas
en caso de evaluarlo necesario, transferir temporalmente la gestión de redes sociales a personas de confianza. Estar expueste al ataque en tiempo real puede ser profundamente desgastante sobre todo si se extiende el ataque.

Suspender o pausar el uso de redes
eliminar aplicaciones del celular, silenciar notificaciones o cerrar sesiones durante el ataque.

Bloquear o silenciar agresores
teniendo en cuenta que esto puede afectar el registro para denuncias futuras. Una buena práctica es anotar o guardar los nombres de usuario antes de bloquear (y dejar registro, screenshot, enlace/link del posteo y foto).

Coordinar denuncias colectivas
en plataformas o ante autoridades, cuando sea pertinente.

Activar redes de apoyo organizacional
articular con otras organizaciones, colectivos y espacios aliados para acompañar la situación, coordinar acciones públicas en simultáneo y construir respaldo colectivo. Esto incluye evaluar de manera situada si una intervención pública —comunicados, posteos, pronunciamientos— contribuye a generar protección y apoyo, o si podría incrementar la exposición y los riesgos para la persona o el colectivo afectado.

Securizar cuentas y dispositivos
revisar contraseñas, activar segundo factor, cerrar sesiones abiertas, revisar dispositivos conectados. Para esto se puede retomar el "Checklist de cuidado digital" compartido en el capítulo anterior.

Protocolos de emergencia
definir una persona de referencia para comunicar y centralizar información hacia la red de afectos, y prever fondos o apoyos ante posibles necesidades urgentes.

El autocuidado no implica desaparecer, sino **redistribuir cargas, sostenerse en red y proteger la continuidad de la vida cotidiana y política**.

Ordenar el escenario: amenazas y riesgos

Cuando ocurre un ataque de doxing, **registrar lo sucedido puede ser una herramienta de cuidado**. No como un trámite ni como una exigencia externa, sino como una forma de ordenar el escenario, evaluar riesgos y tomar decisiones informadas en un momento de alta exposición y vulnerabilidad.

El registro permite reconstruir qué está pasando sin quedar atrapades en el impacto inmediato. No existe una única forma correcta de hacerlo: puede ser una planilla simple, un cuaderno, un documento digital o cualquier soporte que resulte posible en ese momento. Lo importante es que el registro ayude a **identificar qué información circula, dónde, desde cuándo y con qué efectos**, sin exigir a la persona afectada una exposición permanente al daño.

Desde un enfoque de prevención y cuidados digitales, proponemos pensar el registro **no como una obligación técnica**, sino como una herramienta situada, que debe adaptarse a los tiempos, límites y necesidades de cada persona o colectivo. Registrar también implica decidir **qué no registrar**, cuándo frenar y cuándo pedir ayuda, para evitar la sobrecarga emocional o la revictimización.

Desde Mover promovemos una mirada que permita **ordenar la información sin revivir la violencia**, evitar la sobreexposición y acompañar la toma de decisiones. Para eso retomamos dos herramientas ya trabajadas en el capítulo anterior -el **Modelo de Amenazas** y la **Matriz de Riesgo**-, pero ahora **aplicadas a un escenario en el que el ataque ya ocurrió**. No funcionan acá como checklists técnicos, sino como **herramientas políticas de lectura y acción**.

Usar las herramientas cuando el ataque ya está en curso

Cuando el ataque ya sucedió, estas herramientas permiten **pasar del caos a un escenario más legible**, sin imponer urgencias externas ni respuestas únicas.

Usadas en conjunto, ayudan a:

- transformar una experiencia fragmentada en un escenario comprensible,
- distinguir hechos de interpretaciones,
- identificar patrones y posibles escaladas,
- evaluar riesgos reales,
- y decidir colectivamente cómo actuar.

Ante un ataque de doxing...

El Modelo de Amenazas: ordenar lo ocurrido

En este contexto, el Modelo de Amenazas sirve para **reconstruir la situación** sin exigir un relato exhaustivo ni revictimizante. Busca comprender **qué está pasando y qué está en juego**.

Algunas preguntas que pueden orientar el registro son:

- ¿Qué información fue difundida?
- ¿Dónde fue difundida?
- ¿Quién difundió la información?
- ¿Con qué intención?
- ¿Qué efectos tiene o podría tener en la vida personal, laboral o pública?

Responder estas preguntas permite salir del impacto inmediato y empezar a **leer el ataque como un proceso**, no como un hecho aislado.

La Matriz de Riesgo: priorizar respuestas

A partir de la información registrada, la Matriz de Riesgo permite **ordenar las decisiones**. Cruza dos dimensiones:

- **Probabilidad:** qué tan posible es que el ataque continúe o escale.
- **Impacto:** qué tan grave sería ese escenario para la persona o el colectivo.

Este cruce no indica qué hacer, pero sí **ayuda a priorizar**, evitando tanto la inacción como la sobrerreacción. La matriz permite decidir qué acciones son urgentes, cuáles pueden esperar y cuáles requieren acompañamiento específico.

En el marco de este manual, estas estrategias no tienen como objetivo anticipar el conflicto ni controlar todas las variables, sino **mejorar las condiciones de respuesta cuando el ataque ya está en marcha**.

La información que se sistematiza a partir del registro, el modelo de amenazas y la matriz de riesgos tiene un propósito claro: responder a una pregunta central

¿Qué **acciones** puedo implementar ahora **para protegerme**?

Se trata de herramientas para tomar decisiones informadas, respetando los tiempos, límites y recursos disponibles, y evitando que la carga del proceso recaiga en una sola persona. Registrar, en este sentido, es una forma de cuidado y de defensa colectiva, no una exigencia más en un momento de vulnerabilidad.

Puesta en práctica: organizar la información

Una vez analizado el escenario con el Modelo de Amenazas y priorizadas las respuestas con la Matriz de Riesgo, el registro cumple otra función: **dejar constancia de lo ocurrido y de las decisiones tomadas**, sin volver a analizar todo desde cero.

Este registro no busca explicar el ataque, sino **documentarlo**. Puede servir para seguimiento, para pedir ayuda, para activar apoyos, para una eventual denuncia o simplemente para no cargar todo en la memoria de quien atraviesa la situación.

El registro puede hacerse de manera gradual, en distintos momentos y, siempre que sea posible, con acompañamiento. No es necesario escribir todo ni hacerlo perfecto.

Como orientación práctica, el registro puede incluir:

HECHOS RELEVANTES
Fecha aproximada de inicio del ataque y principales momentos o hitos.

INFORMACIÓN EXPUESTA
Tipo de datos difundidos (personales, laborales, imágenes, contactos, etc.) y nivel de sensibilidad.

ESPACIOS INVOLUCRADOS
Plataformas, redes o canales donde circuló la información.

DINÁMICA DEL ATAQUE
Si hubo repetición, amplificación, coordinación entre cuentas o cambios en la intensidad.

IMPACTOS CONCRETOS
Consecuencias observables (emocionales, laborales, vinculares, organizacionales).

RESPUESTAS ACTIVADAS
Medidas tomadas (bloqueos, denuncias, pausas de actividad, cambios de configuración, pedidos de ayuda).

REDES DE APOYO
Personas, colectivos u organizaciones que acompañaron el proceso.

Este registro no reemplaza al análisis previo: **lo continúa en el tiempo**. Permite revisar decisiones, detectar cambios en el escenario y ajustar las estrategias de cuidado si el ataque persiste o se transforma.

Registrar, en este sentido, no es volver a pensar todo otra vez, sino **sacar peso de la experiencia**, compartir la carga y construir una memoria que permita cuidarse mejor.

A modo de cierre

El doxing no es un episodio aislado ni un problema individual. Un ataque de doxing no se resuelve con una reacción inmediata ni con una respuesta individual aislada.

Este capítulo propuso correrse de la lógica del "hacer algo ya" para habilitar un abordaje que combine **cuidado, lectura del escenario y decisión consciente**. Registrar lo ocurrido, activar apoyos y evaluar riesgos no garantiza que la violencia desaparezca, pero sí permite evitar que marque por completo el curso de la situación. La información organizada amplía las posibilidades de acción y reduce la sensación de estar a merced de lo que otros decidan.

El cuidado, pensado en clave colectiva, aparece aquí como una práctica política concreta: distribuir tareas, delegar exposiciones, sostenerse en red y reconocer límites. No se trata de resistir en soledad ni de responder a todas las provocaciones, sino de **preservar la vida cotidiana, los vínculos y los procesos colectivos** frente a intentos de desgaste.

En el marco de este manual de prevención, estas herramientas no funcionan como instrucciones cerradas ni como mandatos de acción. Son **recursos para leer mejor lo que está pasando**, priorizar lo importante y elegir cómo seguir, con quiénes y en qué tiempos. Frente al doxing, la posibilidad de registrar, cuidar y decidir en conjunto es una forma concreta de disputar los efectos de la violencia y de sostener la agencia incluso en escenarios adversos.

HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

MOVER coop

Mover coop

HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

MANUAL DE PREVENCIÓN DEL DOXING

El doxing no es un problema individual. Es una forma de violencia que se sostiene en desigualdades estructurales y en plataformas que amplifican el daño.

No todas las situaciones
se resuelven igual.
No todas las respuestas
tienen que ser inmediatas.
No todo se puede controlar.

Cerrar una cuenta, pausar,
delegar, bloquear, denunciar
o no denunciar son decisiones
válidas cuando están tomadas
desde la información,
el acompañamiento y el cuidado.

Las prácticas comunitarias de cuidado digital -acompañar, registrar en conjunto, delegar tareas, amplificar apoyos y decidir colectivamente- reducen el daño, rompen el aislamiento y fortalecen la capacidad de respuesta frente a la violencia digital.

Versión accesible
https://movercooperativa.com/wp-content/uploads/2026/02/Manual-de-prevencion-del-doxing-Mover-Cooperativa-y-Fundacion-Boll-versionacccesible.pdf