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**.



HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

MOVER coop

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**.



HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

MOVER coop

## 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**.



HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

MOVER coop

## 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.



HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

MOVER coop

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