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.

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

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.

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

¿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

- X Considera si necesitas una cuenta pública o privada.
- X 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

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

Registrar sin sobreexponerse

- X Documentar ataques y publicaciones dañinas de manera ordenada.
- X Evitar el monitoreo compulsivo que profundiza el desgaste emocional.
- X 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.

HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

MOVER coop

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.

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

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 nosotres, 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

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

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?

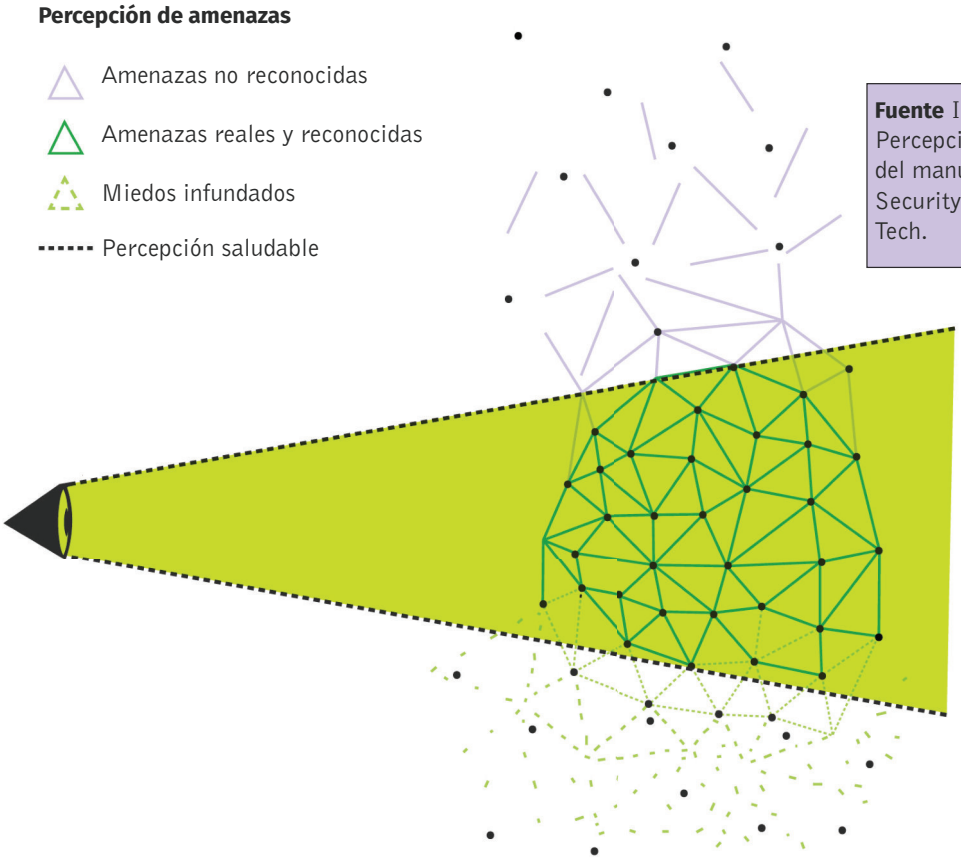
Cuando no hacemos este ejercicio, todo parece peligroso y terminamos paralizades o cuidándonos de cualquier cosa sin criterio. El modelo de amenazas sirve justamente para **dejar de reaccionar a ciegas**.

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.

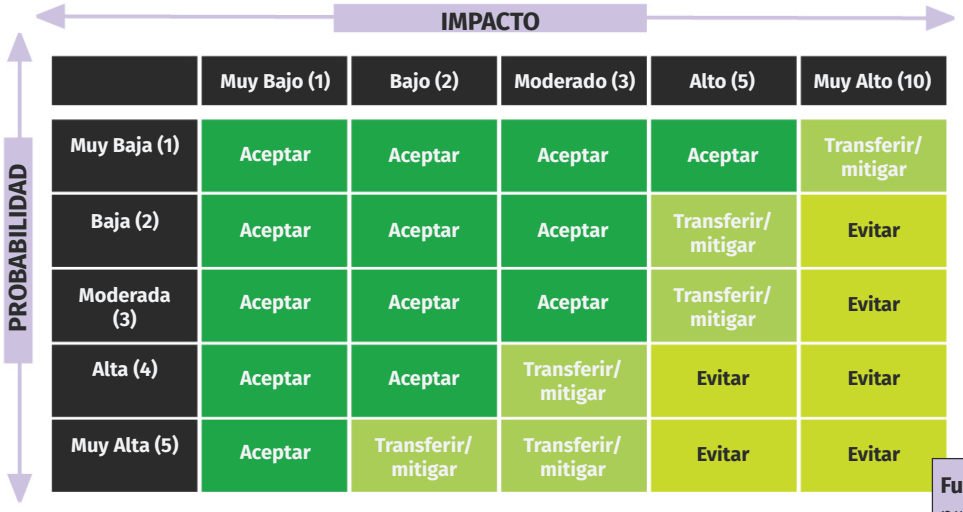
LAS DOS PREGUNTAS CLAVE

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 nosotros, nuestra organización o nuestro entorno?

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



	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.

HEINRICH BÖLL STIFTUNG
BUENOS AIRES
Argentina | Uruguay | Paraguay

MOVER coop