Image not found or type unknown

Evaluación de riesgos

Introduce a las participantes a los conceptos subyacientes en la evaluación de riesgos, y como aplicar los marcos de evaluación de riesgos a su seguridad personal y/o institucional. **Recomendamos muchísimo** que elijas una Ruta de Aprendizaje para recorrer, ya que éstas incluyen actividades con diferentes niveles de profundidad que deberían ayudar a las participantes a obtener una mayor comprensión de los temas tratados.

- Introducción, objetivos y actividades de aprendizaje
- Introducción a la evaluación de riesgos [actividad inicial]
- Evaluar prácticas de comunicación [actividad inicial]
- Graficar riesgos [actividad inicial]
- La calle de noche [actividad inicial]
- Re-pensar el riesgo y los cinco niveles del riesgo [actividad de profundización]
- El ciclo de vida de los datos como forma de entender el riesgo [actividad de profundización]
- Organización de protestas y evaluación de riesgos [actividad táctica]
- Elementos básicos en la evaluación de riesgos [material de base]
- Evaluación de riesgos en la organización y movilización social [material de base]

Introducción, objetivos y actividades de aprendizaje

Esta página te guiará en el correcto uso y comprensión del módulo. El seguimiento de los caminos de aprendizaje, con actividades de diferente profundidad, debería permitir a las participantes obtener una mejor comprensión de los temas tratados.


EVALUACIÓN DE RIESGOS

Objetivos de aprendizaje

Al terminar este módulo, serán capaces de:

- Entender los conceptos que subyacen a la evaluación de riesgos.
- Utilizar marcos de evaluación de riesgo para su seguridad personal y/o organizacional.
- Crear una forma propia de evaluar riesgos que sea relevante para sus necesidades.

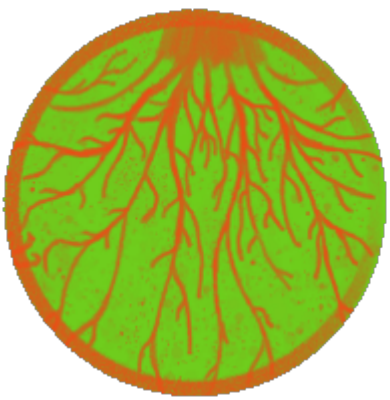
Actividades de aprendizaje

Actividad inicial



- Introducción a la evaluación de riesgos
- Evaluar prácticas de comunicación
- Graficar riesgos
- La calle de noche

Actividad de profundización



- Re-pensar el riesgo y los cinco niveles del riesgo
- Ciclo de vida de datos como forma de entender el riesgo

Actividad estratégica

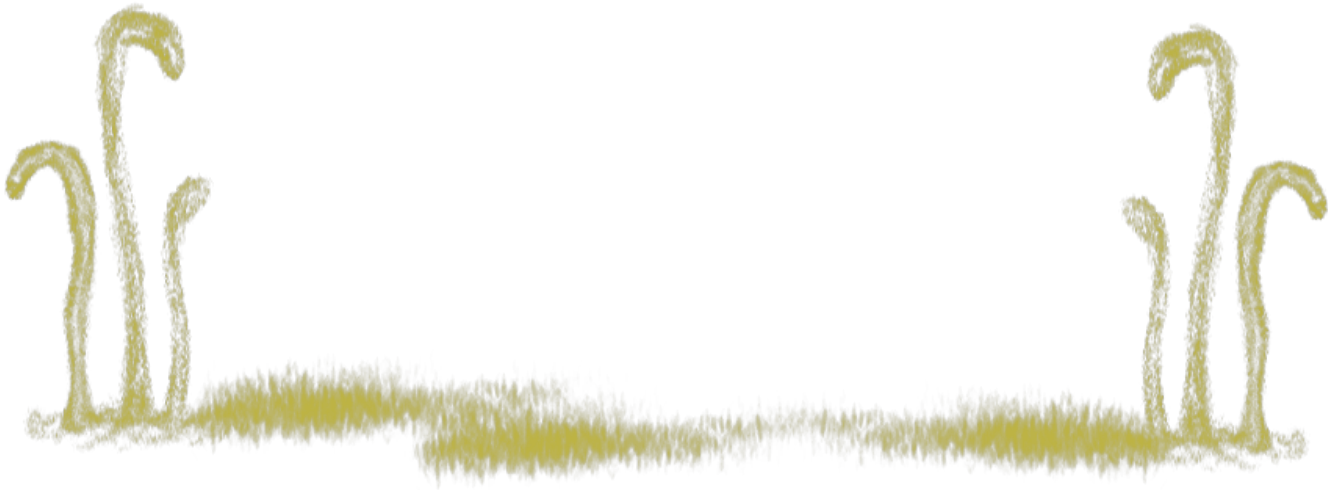


- Organización de protestas y evaluación de riesgos

Materiales de base



- Elementos básicos en la evaluación de riesgos
- Evaluación de riesgos en la organización y movilización social



Introducción a la evaluación de riesgos [actividad inicial]

image-1605892914912.png
Image not found or type unknown

Esta actividad ha sido diseñada para presentar y ejercitar un marco desde el cual realizar la evaluación de riesgos.

Objetivos de aprendizaje

Los objetivos de aprendizaje de esta actividad son:

- Entender los conceptos subyacentes a la evaluación de riesgos.
- Empezar a aplicar un marco de evaluación de riesgos para la seguridad personal y/o organizacional.

¿A quién está dirigida esta actividad?

Esta actividad fue diseñada para participantes con escasa o ninguna experiencia en evaluación de riesgos. También está pensada para realizar un taller con participantes de diferentes organizaciones.

Tiempo requerido

Siendo realistas, se necesita un día (ocho horas, como mínimo) para desarrollar esta actividad de manera adecuada.

Recursos

- Papel de papelógrafo y marcadores
- Proyector
- Laptops

Mecánica

Para esta actividad tendrás que inventar una situación sobre una persona o un grupo a partir de la cual se pueda realizar una evaluación de riesgos.

Según quienes participen de la dinámica, algunas de las opciones son:

- Un grupo de derechos humanos en un país donde se acaba de aprobar una ley que implica la vigilancia de ONGs
- Una mujer trans que está por lanzar un sitio web para apoyar a otras mujeres trans
- Activistas por los derechos de las mujeres que trabajan en algún asunto considerado tabú en sus países
- Un grupo que tiene una casa segura para jóvenes trans
- Un pequeño grupo LGBTIQ que está siendo atacado en línea
- Una mujer queer de un grupo racial minoritario que publica sus opiniones en línea.

Forma sub-grupos. Cada uno puede trabajar en el mismo tipo de organización/grupo o en diferentes tipos de organizaciones.

> **Nota para la facilitación:** en este punto, es importante que la situación resuene con quienes participan, que los casos sean cercanos a sus experiencias.

Una vez formado los grupos, puedes realizar la **Presentación sobre la evaluación básica de riesgos**.

Trabajo en grupo 1: Desarrolla y complementa el contexto y la escena

Antes de completar la **Planilla de evaluación de riesgos**, se tiene que desarrollar la situación elegida.

Para un escenario grupal:

- Crea un perfil para el grupo: su ubicación, tamaño y objetivos/propósitos.
- Describe las actividades o los cambios del contexto que ponen al grupo en riesgo – puede ser una nueva ley, o una actividad que están planeando y que sus detractores querrán interrumpir. También podría ser un cambio interno que presente riesgos – por ejemplo, un conflicto reciente dentro del grupo – o un evento externo que está causando mucho estrés entre las personas integrantes.
- Nombra a las personas que serán hostiles a las acciones del grupo y a las que, por el contrario, serán aliadas.

Para un escenario individual:

- Crea un perfil para este individuo: edad, ubicación, orientación sexual, qué tan activo está en las plataformas de redes sociales.
- Describe una de las siguientes opciones:
    - las opiniones/posturas por las que esta persona está siendo atacada;
    - un sitio web que está creando y que puede ponerla en riesgo;
    - el contexto que genera vulnerabilidad (por ejemplo, la echaron de casa, dejó una relación abusiva con alguien del mismo grupo o red, etc.).
- Nombra a las personas que serán hostiles a sus acciones y las que prestarán su apoyo.

Dale a cada grupo una hora para realizar este ejercicio.

Después, cada grupo presenta su situación rápidamente.

Posteriormente, presenta la Plantilla de evaluación de riesgos (.odt).

Algunas notas sobre la tabla:

- Las amenazas deben ser **específicas** – ¿cuál es el peligro (intención negativa hacia el grupo) y quién lo amenaza?
- Piensa en la **probabilidad** de que una amenaza se cumpla en tres estratos:
  - Vulnerabilidad – ¿cuáles son los procesos, actividades y comportamientos del individuo o grupo que aumentan la probabilidad de que la amenaza se vuelva real?
  - Capacidad de la(s) persona(s) que amenaza(n) – ¿quién(es) está(n) amenazando y qué puede(n) hacer para llevar a cabo su amenaza?
  - Incidentes conocidos – ¿Ya hubo alguna amenaza similar en una situación parecida? Si la respuesta es afirmativa, la probabilidad aumenta.
- Al pensar en el **impacto**, hay que considerar no sólo el impacto individual, sino también el que experimentará la comunidad en general.
- Aunque evaluar el grado (bajo/medio/alto) de probabilidad e impacto siempre es relativo, es importante hacerlo para priorizar sobre qué riesgos elaborar planes de mitigación.
- Riesgo – declaración/afirmación que contiene el peligro y la probabilidad de que se vuelva real.

Trabajo en grupo 2: Evaluación de riesgos

Mediante el uso de la plantilla de evaluación de riesgos, cada grupo analiza los riesgos de su situación. La tarea consiste en identificar diferentes riesgos y analizar cada uno de estos.

> **Nota para la facilitación:** dale a cada grupo una copia en papel de la planilla de evaluación de riesgos para que pueda documentar lo hablado directamente allí.

Este trabajo grupal llevará, como mínimo, dos horas. La(s) persona(s) facilitando realizará(n) consultas con cada grupo a lo largo de toda la actividad.

Al terminar, responde conjuntamente preguntas sobre el proceso, en lugar de simplemente presentar las plantillas por grupo:

- Qué dificultades tuvieron para evaluar riesgos?
- ¿Cuáles fueron los principales peligros que identificaron?
- ¿Cuáles son los desafíos a la hora de analizar el grado de probabilidad de las amenazas?

Insumos y diálogo sobre tácticas de mitigación

Basándote en el texto de presentación sobre tácticas de mitigación (ver la sección Presentación), presenta los puntos principales y organiza un diálogo con las personas participantes.

Trabajo en grupo 3: Planificación de la mitigación

Pídele a cada grupo que identifique un riesgo altamente probable y de alto impacto. A continuación, pídeles que elaboren un plan de mitigación para dicho riesgo.

Preguntas guía

Estrategias de prevención

- ¿Qué acciones y capacidades ya tienes para evitar esta amenaza?
- ¿Qué acciones llevarás a cabo para evitar que la amenaza suceda? ¿Cómo puedes alterar los procesos dentro de la red para impedir que esta amenaza se cumpla?
- ¿Qué capacidades necesitas tener para evitar esta amenaza?

Respuesta frente a incidentes

- ¿Qué harás cuando la amenaza se vuelva realidad? ¿Qué pasos darás?
- ¿Cómo minimizarás la gravedad del impacto de esta amenaza?
- ¿Qué conocimientos/saberes necesitas para dar los pasos necesarios para responder a esta amenaza?

Este trabajo grupal puede durar entre 45 minutos y una hora.

Al terminar, pregunta sobre los procesos y preguntas que tengan acerca de las actividades desarrolladas.

Para sintetizar esta actividad de aprendizaje, reitera algunas lecciones:

- La evaluación de riesgos sirve para elaborar estrategias realistas (de prevención y respuesta).
- Hay que enfocarse en las amenazas y peligros que tengan más probabilidad de suceder y las que tienen mayor impacto.
- La evaluación de riesgos requiere práctica.

Presentación

Hay tres cosas para presentar en esta actividad:

- La presentación sobre evaluación básica de riesgos (presentación .odp)
- La plantilla de evaluación de riesgos
- Insumos sobre tácticas de mitigación (ver el texto a continuación).

Texto para la presentación sobre tácticas de mitigación

Hay cinco maneras generales de mitigar riesgos:

Aceptar el riesgo y elaborar planes de contingencia

La planificación de contingencia se basa en imaginar que el riesgo se cumple, que tiene el peor impacto posible y cuáles serán las medidas necesarias para enfrentar la situación.

Evitar el riesgo

Reduce tus vulnerabilidades. ¿Qué necesitas saber/conocer? ¿Qué cambios de comportamiento habrá que generar para evitar riesgos?

Controlar el riesgo

Reduce la gravedad del impacto. Hay que enfocarse en el impacto, en lugar de la amenaza, para dedicarse a minimizarlo. ¿Qué necesitas saber/conocer para lidiar con el impacto?

Transferir el riesgo

Consigue un recurso externo para que asuma el riesgo y su impacto.

Monitorear el riesgo

Para detectar cambios en la probabilidad de que suceda y en el impacto. Esto se aplica, en general, a riesgos de baja probabilidad.

Hay dos maneras de enfrentar situaciones de riesgo

Estrategias de prevención

- ¿Qué acciones tomaste y qué capacidades tienes para evitar este peligro?
- ¿Qué acciones llevarás a cabo para evitar que este amenaza se concrete? ¿Cómo vas a cambiar los procesos y procedimientos de la red para evitar que el riesgo se cumpla?
- ¿Tienes que elaborar políticas y procedimientos para poder hacer estas cosas?
- ¿Qué capacidades/conocimientos necesitas para evitar que este riesgo se cumpla?

Respuesta frente a incidentes

- ¿Qué harás cuando este riesgo se cumpla? ¿Qué pasos darás?
- ¿Qué harás para minimizar la gravedad del impacto de esta amenaza?
- ¿Qué capacidades/conocimientos necesitas para dar los pasos necesarios para responder a esta amenaza?

Ajustes para un taller grupal

Esta actividad se puede usar en el contexto de un taller donde un grupo realiza una evaluación de riesgos y el papel de quien facilita consiste en guiar al grupo a través de todo el proceso.

Para ello, en lugar de desarrollar la situación, dialoguen sobre las amenazas generales a las que se enfrenta el grupo. Pueden haber cambiado las leyes o ciertos representantes políticos, lo que puede dificultar el trabajo del grupo. También puede haber ocurrido un incidente específico a partir del cual las personas del grupo se sienten en riesgo (por ejemplo, sospechan que están siendo

vigiladas directamente o un grupo aliado suyo descubre que está bajo mira). A continuación, se puede generar una conversación sobre las capacidades con las que cuenta el grupo – recursos, conexiones, apoyos y aliadas, conocimientos. La construcción de un saber compartido sobre los peligros que enfrenta el grupo y las capacidades con las que cuenta es una forma de “aterrizar” la actividad de evaluación de riesgos y es importante hacerlo para el resto del proceso.

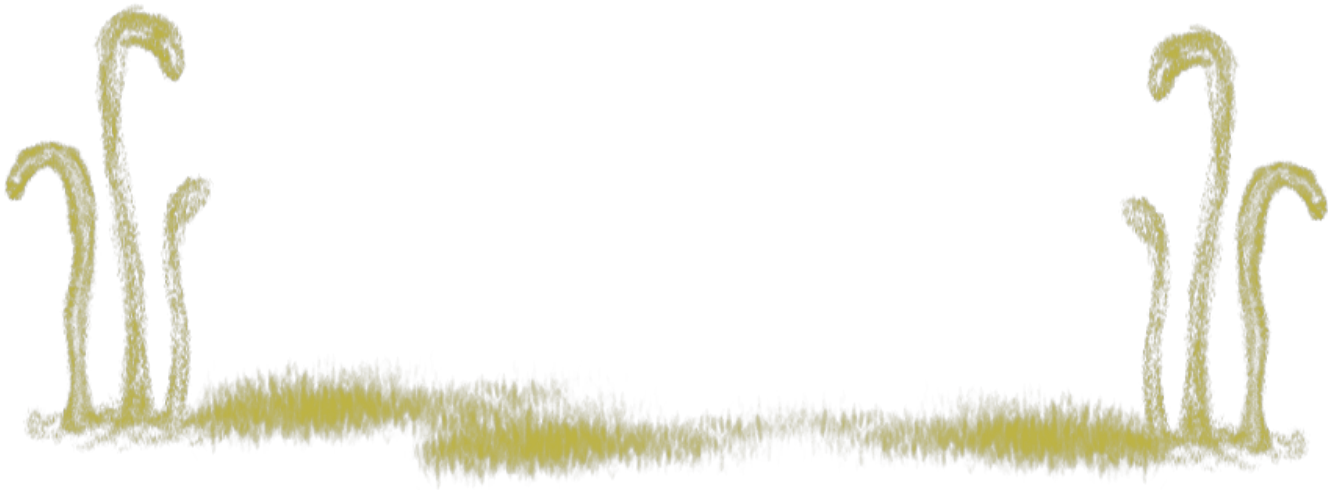
Forma grupos para completar la planilla de evaluación de riesgos.

En este contexto, los planes de mitigación son tan importantes como la planilla de evaluación de riesgos, así que ambas áreas tendrán la misma asignación de tiempo.

En un contexto grupal, esta actividad puede llevar hasta dos días, según el tamaño del grupo y el tipo de acción que realiza.

Más lecturas (opcionales)

- Elementos básicos en la evaluación de riesgos [Material de base]
- Evaluación de riesgos en la organización y movilización social [Material de base]



Evaluar prácticas de comunicación [actividad inicial]



Esta actividad está diseñada para ayudar a examinar nuestras prácticas de comunicación (los temas sobre los cuales nos comunicamos, con quiénes lo hacemos, a través de qué canales) y evaluar qué riesgos implican.

Se trata de una herramienta de diagnóstico que puede utilizarse para priorizar temas de aprendizaje y/o para evaluar prácticas de comunicación.

Objetivos de aprendizaje

Comprender conceptos relacionados con la evaluación de riesgos.

¿Para quién es esta actividad?

Para participantes de nivel principiante e intermedio.

Tiempo requerido

Introducción a la actividad: 15 minutos

Tiempo individual para evaluar: 15 minutos

Trabajo en grupo: 30 minutos

Plenaria y cierre: 30 minutos

Total: 1 hora y media

Materiales requeridos

Copias digitales o impresas de la planilla en blanco

- Material impreso (PDF): EvaluarPracticasComunicacionPlanilla.pdf
- Versión editable (Documento Libre Office): EvaluarPracticasComunicacionPlanilla.odt

Mecánica

Completa la tabla.

Tema de comunicación	¿Con quién tengo comunicas sobre este tema?	¿Es un tema delicado/sensible? (SÍ/NO)	¿Quién podría facilitar por este tipo de comunicación?	Canal de comunicación

		(¿SÍ/NO?)		
		(¿SÍ/NO?)		
		(¿SÍ/NO?)		
		(¿SÍ/NO?)		

		(¿SÍ/NO?)		

En grupos pequeños, habla sobre las respuestas de cada quien. Después se vuelve a juntar todos los grupos y se comparten reflexiones y observaciones.

Preguntas orientativas para discusión colectiva:

- ¿Cuáles de los temas son sensibles/delicados?
- ¿Quiénes podrían ficharte por esta comunicación sensible?
- ¿Cuál es canal de comunicación que más utilizas? ¿Crees que es seguro y privado?

Esta actividad se puede utilizar para priorizar en qué canales de comunicación trabajar durante el resto del taller o para presentar herramientas alternativas de comunicación más seguras.



Graficar riesgos [actividad inicial]



Esta actividad busca mostrar a las participantes cómo evaluar sus tareas diarias/semanales y analizar cuánto tiempo invierten en cada cosa. Hay dos partes de este ejercicio: 1) crear gráficos circulares de tareas semanales/diarias y compartirlos con el grupo; 2) examinar cuáles son las tareas donde sentimos mayor riesgo. Es importante no sacar el tema de riesgo hasta la segunda parte del ejercicio.

Esta forma muy básica de evaluar riesgos se centra en las tareas que realizamos y las amenazas conocidas que solemos enfrentar. Aconsejamos acompañar esta actividad con un análisis de riesgos más detallado.

Objetivos de aprendizaje

- aplicar marcos de evaluación de riesgos en la seguridad personal y/o organizacional

¿Para quién es esta actividad?

- Para participantes que no han realizado evaluaciones de riesgo.
- Funciona en grupos que hacen tareas parecidas en su día a día.
- Puede ser una actividad inicial para un grupo que después va a hacer un análisis de riesgos a nivel organizacional.

Tiempo requerido

1 hora y media mínimo

Materiales requeridos

- Papeles grandes/rotafolios/pizarrón + marcadores

Mecánica

Primera parte: Dibuja tu gráfico

Dibuja un círculo en tu papel y divídelo según las tareas que realizas (por día o por semana) en tu grupo/organización. El tamaño de cada división refleja el tiempo invertido en la tarea: cuanto más grande la porción, más tiempo dedicado.

Para quienes facilitan: anima a las participantes a ser lo más específicas posibles a la hora de enumerar sus tareas.

Una vez finalizado el ejercicio de dibujo, el grupo comparte sus gráficos y discute sobre:

1. ¿En qué tareas dedico más tiempo?
2. ¿Qué tareas tenemos en común en el grupo?
3. ¿En qué tareas no invierto mucho tiempo, pero me gustaría hacerlo? ¿Por qué?

Segunda parte: Identificar riesgos

Reflexiona sobre los gráficos y responde a las siguientes preguntas:

1. De las tareas que haces para tu grupo/organización, ¿cuáles crees que suponen más riesgo? ¿Qué tipo de riesgo? ¿Por qué?
2. ¿Cómo podemos abordar estos riesgos? Describe estrategias.

Piensa en estas preguntas individualmente y después comparte en grupo.

image-1605452256072.png

Image not found or type unknown

La calle de noche [actividad inicial]

image-1605892914912.png
Image not found or type unknown

Esta actividad nos ayuda a darnos cuenta cómo practicamos la evaluación de riesgos para nuestra vida y supervivencia cotidiana. En esta actividad, se muestra una calle oscura en la noche. “¿Qué harías para sentirte a salvo si tuvieras que caminar a solas por esta calle?”

Descubriremos qué maneras tenemos para evaluar y mitigar riesgos en el momento.

Objetivos de aprendizaje

Al final de la actividad, podrás:

- Empezar a entender que la evaluación de riesgos no es una actividad extraña.
- Compartir experiencias sobre las consideraciones que hacemos a la hora de examinar una situación arriesgada.

¿A quién está dirigida esta actividad?

Esta actividad se puede realizar con personas, independientemente de que tengan experiencia en la evaluación de riesgos o no.

> **Nota para facilitación:** es importante conocer al grupo previamente, ya que esta actividad puede activar traumas del pasado.

Tiempo requerido

45 minutos

Recursos

- Un proyector para poder mostrar la imagen de una calle de noche
- Un pizarrón o papelógrafo para escribir las respuestas
- Marcadores

Mecánica

Presenta el ejercicio mostrando la imagen de una calle de noche. Explica que no hay respuestas correctas, ni equivocadas.

Aquí encontrarás algunos ejemplos, pero también puedes utilizar la imagen que mejor se adapte al contexto del taller.



Photo: Yuma Yanagisawa, Small Station at night, on Flickr.

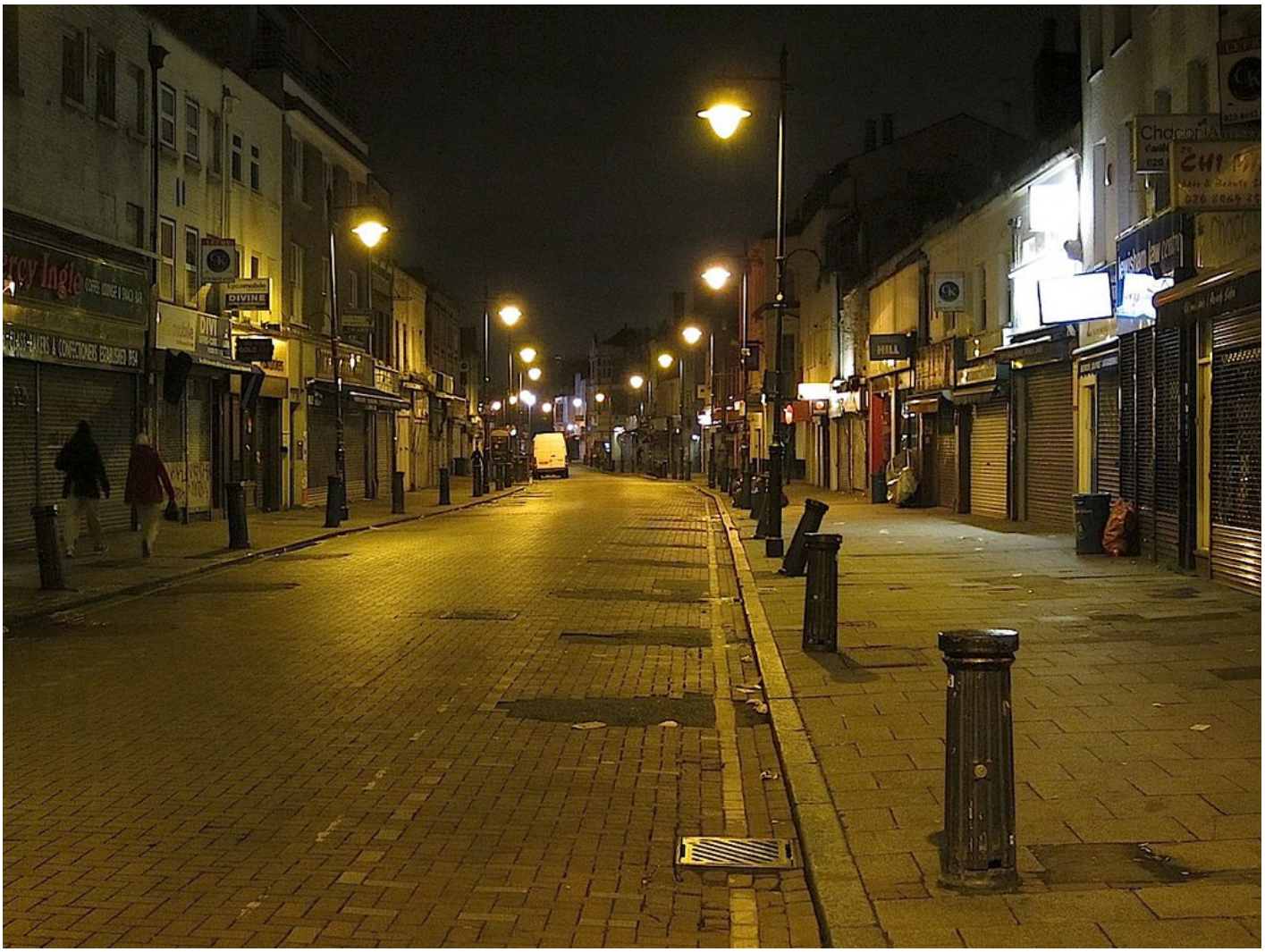


Photo: Andy Worthington, Deptford High Street at night, on Flickr

Dale a cada participante el tiempo de pensar cómo responderían a la pregunta: **“¿Cómo andarías por esta calle de noche si estuvieras a solas”**

> **Nota interseccional:** no deberías suponer que todo el mundo tiene las mismas capacidades y habilidades físicas. Es por eso que usamos “andar” en lugar de caminar.

Pídeles que escriban sus respuestas y se las guarden. Esto no debería llevar más de cinco minutos. No se trata de pensar demasiado las respuestas.

Después, invita al grupo compartir sus respuestas. Anótalas en el pizarrón.

Cuando veas algunas tendencias en las respuestas – respuestas comunes, así como respuestas únicas – **empieza a preguntarles por qué razón respondieron de esa forma.**

Estamos intentando obtener más información: empezamos con el “cómo” y ahora estamos llegando al ‘por qué’. Sondeamos los peligros – las causas del peligro – que se revelan en las respuestas al “¿cómo andarías por esta calle de noche si…?”.

Anota también las amenazas. Es buena idea mirar la fotografía otra vez para ver los elementos que podrían ser amenazadores, así como los que podrían considerarse oportunidades para sentirse a salvo al andar por esa calle.

Por ejemplo, tomando la primera fotografía:

- Señala las rejas y los arbustos bajos. ¿Hay buenos lugares para esconderse?
- ¿Qué lado de la calle usarías? ¿Por qué?
- Dado que se trata de una calle en la que hay una pequeña estación, ¿significa que la persona que anda por ahí tendrá alguien a quién llamar si algo sucede? Si es así, ¿eso hace que esta calle sea más segura?
- ¿Y en cuánto a andar por esta calle a salvo de los automóviles que pasan?

En la segunda fotografía:

- ¿Qué lado de la calle usarías? ¿Por qué?
- Señala a las dos personas que están en la calle – ¿te parece que su presencia hace la calle más segura o no?
- La camioneta que está más adelante en la calle – ¿podría ser una fuente de vulnerabilidad o de ayuda si algo sucede?

Si estás planeando sacar tu propia fotografía de una calle de noche, considera incluir los siguientes elementos:

- Una fuente de luz y una parte obviamente oscura
- Elementos que agreguen más riesgos a la calle. Por ejemplo, lugares en los que alguien podría esconderse, mucho tráfico de vehículos...

Después de destinar un tiempo a los porqués de las tácticas de seguridad y las amenazas, plantea la siguiente pregunta: “**¿Qué otras cosas necesitas saber sobre esta calle para tomar mejores decisiones para andar por ahí con seguridad?”**

Tras unos minutos para responder a las respuestas, de nuevo invita al grupo a compartirlas mientras las vas anotando en la pizarra.

Realiza una síntesis de la sesión. Destaca los puntos principales:

- Las estrategias claves – el por qué y el cómo – surgidas a partir del debate.
- La información esencial necesaria para evaluar mejor una situación.
- Relaciona esta actividad con la evaluación de riesgos: en ambos casos se analiza una situación y se toman decisiones sobre la seguridad en función del contexto, las experiencias y los conocimientos. Recalca que, esta actividad como ejemplo de la evaluación de riesgos, puede ser un proceso rápido.
- Mantenerte a salvo cuando pasas por una calle oscura de noche es una experiencia común. En ese momento, somos capaces de evaluar el riesgo con preguntas como: ¿Qué tan peligrosa es esta calle? ¿Qué tan rápido puedo correr? ¿Hay algún punto en esta calle donde podría pedir ayuda, por las dudas? ¿Voy a solas o en compañía? ¿Hay partes dónde alguien podría sorprenderme en esta calle? Y a partir de estas respuestas, aplicar estrategias y tácticas de mitigación. Recordar que ya hacemos todo esto de manera instintiva – como mecanismo de supervivencia – es significativo cuando vamos a hacer una evaluación de riesgos.
- Conocer los riesgos potenciales de esta situación específica nos dio la posibilidad de elaborar estrategias y tácticas para reducir los riesgos en una situación determinada.

Notas para la facilitación

- En la primera parte de esta actividad, es realmente importante que las personas participando piensen cómo pasarían por la calle a solas sintiéndose a salvo, pero que no reflexionen demasiado. Es por eso que basta con cinco minutos. Lo que queremos destacar aquí es el papel vital del instinto y las propias experiencias cuando evaluamos los riesgos de una situación dada.
- Si te parece que alguien reacciona muy intensamente a raíz de esta actividad, haz una pausa. Dales un respiro y la opción de salir de la actividad o mantenerse al margen.
- El objetivo de esta actividad es empezar a explorar la evaluación de riesgos. Aquí no tiene relevancia abordar esta actividad con la fórmula estándar: riesgo = amenaza/peligro x probabilidad x impacto / capacidad. Lo importante es que las personas participando sean capaces de articular las razones por las que eligieron determinadas tácticas para andar

por la calle oscura de noche.

- Recalca que no existen respuestas correctas o equivocadas, sino solamente respuestas basadas en la experiencia y el razonamiento.
- Si el conocimiento que tienes del grupo te lleva a pensar que esta actividad podría activar traumas pasados, puedes cambiar la situación a algo que creas que será menos traumático: por ejemplo, una calle llena de gente de día o de noche.

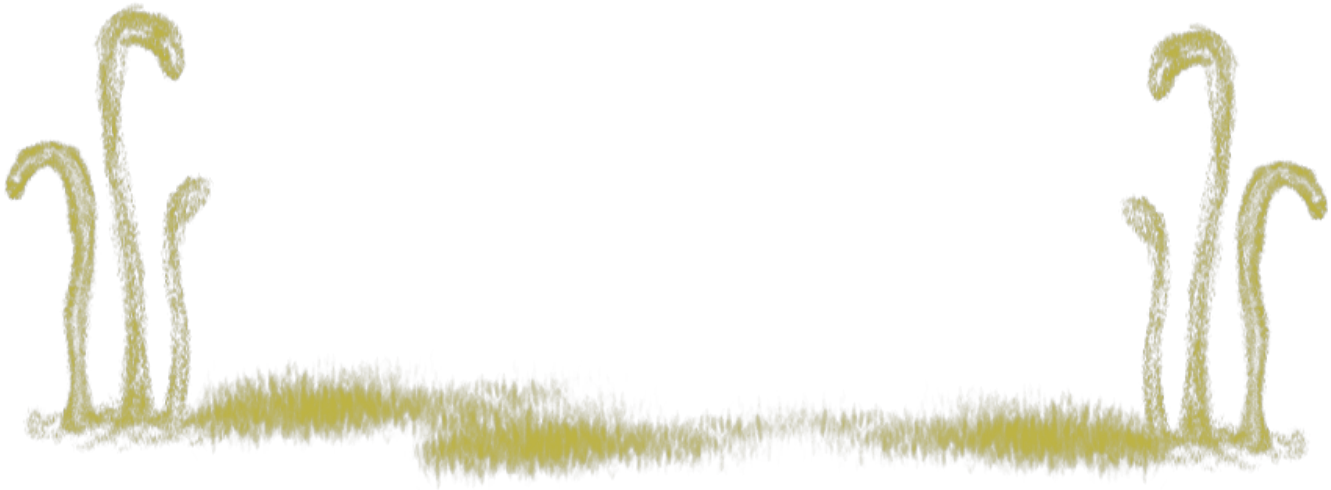
A continuación, algunos ejemplos de fotografías que puedes usar:



Foto: Carl Campbell, muchedumbres en el mercado de los sábado El Chopo, en Flickr.



Foto: Waychen C, mercado nocturno de Shilin, en Flickr.



Re-pensar el riesgo y los cinco niveles del riesgo [actividad de profundización]



Este material no tiene forma de módulo de aprendizaje aún. Por ahora son una colección de ideas sobre cómo repensar el riesgo.

Re-pensar y evaluar el riesgo

Entender el riesgo de manera realista

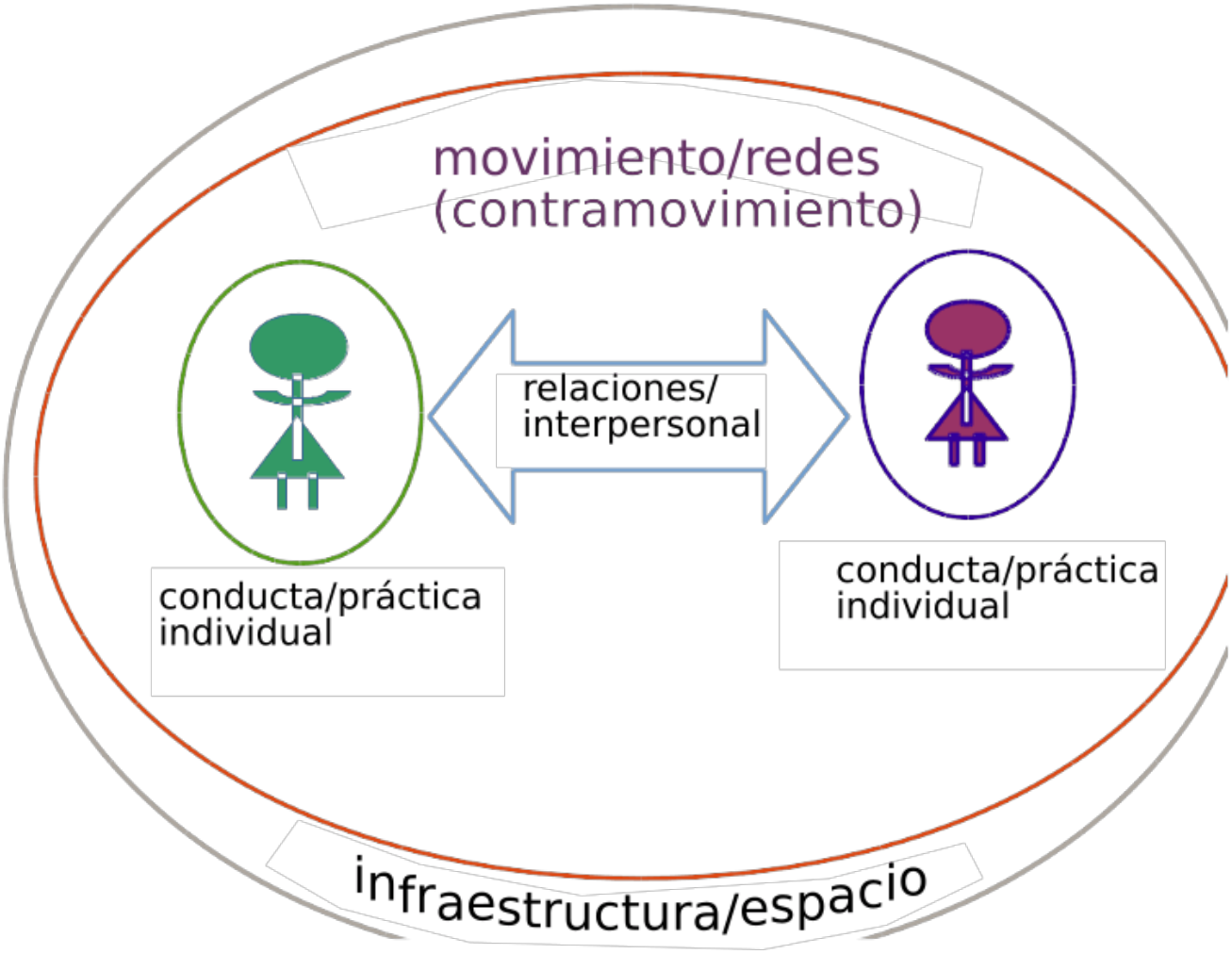
Uno de los desafíos a la hora de evaluar riesgos es la amplitud del término: pensar en el riesgo desde una perspectiva holística amplía aún más su definición (¡y con razón!). El propósito de esta evaluación es poder planear estrategias y tácticas para mitigar los riesgos que afrontamos y tomar decisiones más informadas.

Muy a menudo, el "riesgo" se ve como algo que va mal en una situación sin detallar en qué enfocarnos.

Otra manera de evaluar con más matices es tomar en cuenta 3 ángulos diferentes:

- Riesgos conocidos: amenazas que han sucedido/se han detectado adentro de la comunidad. Pon ejemplos. ¿Cuáles son las causas? ¿Cuáles son los impactos?
- Riesgos emergentes: amenazas que han sucedido afuera de la comunidad debido al contexto político actual, desarrollos tecnológicos y/o cambios en comunidades activistas más amplias/generales.
- Riesgos desconocidos: no se pueden anticipar y no hay forma de saber si van a surgir o cuándo.

También puedes examinar riesgos según diferentes niveles o dimensiones:



Espacio/infraestructura

Los espacios en los que nos movemos, comunicamos e interactuamos. Hay espacios fuera y dentro de internet donde ejercemos nuestros activismos. Independientemente de dónde nos ubicamos,

existen parámetros que pueden ser fuentes de riesgos.

Por ejemplo, se sabe que en internet no puedes borrar algo de manera definitiva. ¿Qué tipo de riesgos plantea esto para activistas en internet? ¿Cómo contribuye a un incremento/intensificación de riesgos?

Movimientos y redes (contramovimientos)

¿Cuáles son las capacidades de nuestros movimientos y redes? ¿Cuáles son nuestros adversarios? ¿Cuáles son los riesgos que enfrentamos por formar parte de movimientos feministas? ¿Quiénes son nuestras aliadas? ¿Y enemigos? ¿Qué amenazas suponen?

¿Consideras que los riesgos que existen a nivel de tus movimientos/redes expanden la idea y entendido que tienen sobre los impactos? ¿Cuáles son las consecuencias, más allá de lo individual/organizacional, del acoso de género en internet? ¿Cómo afectan la manera en que nuestros movimientos/redes son capaces de utilizar el internet para sus luchas?

Relaciones/interpersonal

Existe el supuesto que muchas personas activistas no confrontan la posible desconfianza que hay adentro de las comunidades activistas. Es importante cultivar relaciones de confianza, sí. Es igualmente importante determinar el nivel de confianza que existe entre feministas.

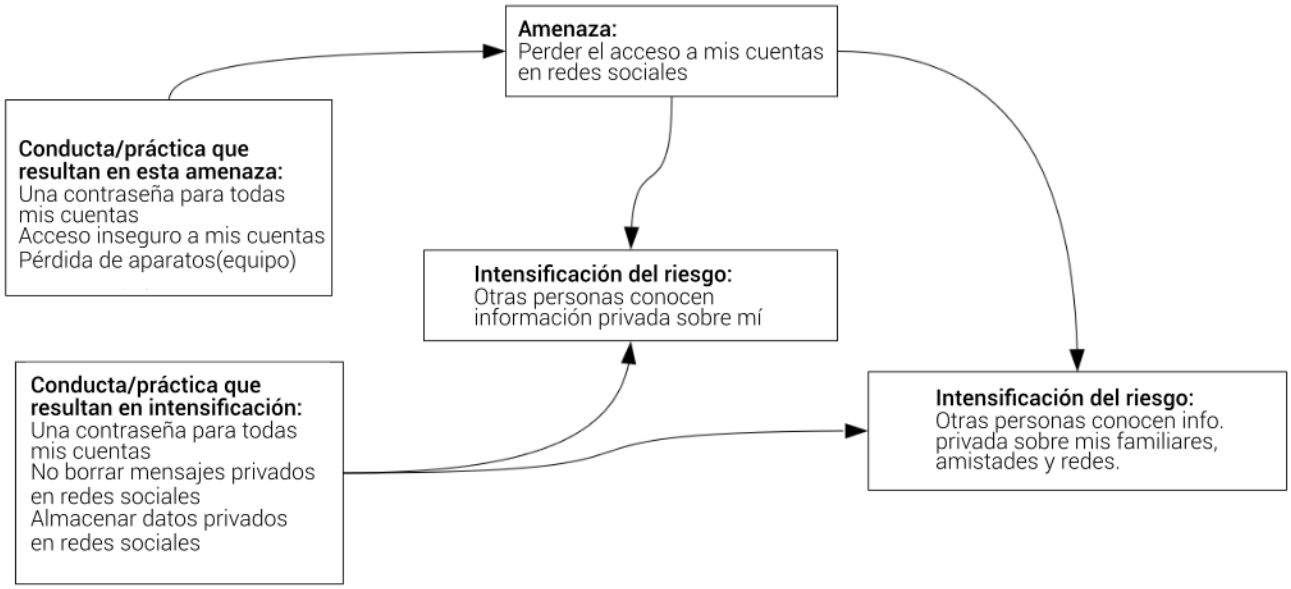
Conductas y prácticas individuales

¿Cómo nos comunicamos? ¿Cómo nos conectamos a internet? ¿De qué realidades venimos cuando interactuamos entre nosotras? ¿A qué tipos de equipo y aparatos tenemos acceso? ¿Qué tipo de herramientas utilizamos? ¿Qué habilidades tenemos? Las prácticas y conductas responden a estas preguntas.

Para entender el riesgo en mayor profundidad, es importante interrogar estas dimensiones.

Espectro conductas-prácticas y amenazas

En este marco, partimos de una amenaza conocida (o una amenaza que directamente han vivido las participantes) e interrogamos las conductas y prácticas, tanto las que influyen en que se vuelva real esta amenaza, como las que intensifican la amenaza.



El segundo nivel de este marco es identificar estrategias de mitigación y respuesta en cada punto de la imagen anterior.

image-1605451259399.png

El ciclo de vida de los datos como forma de entender el riesgo [actividad de profundización]

Esta actividad de aprendizaje consiste en entender la evaluación de riesgos desde la perspectiva del ciclo de vida de los datos. Todos las personas activistas, grupos, colectivos, organizaciones y movimientos sociales manejan datos – desde la recopilación/creación/recolección de datos hasta la publicación de información basada en datos.

Introducción



Esta actividad de aprendizaje consiste en entender la evaluación de riesgos desde la perspectiva del ciclo de vida de los datos. Todos las personas activistas, grupos, colectivos, organizaciones y movimientos sociales manejan datos – desde la recopilación/creación/recolección de datos hasta la publicación de información basada en datos.

Existen dos enfoques principales sobre la mecánica de esta actividad:

- El **taller general** funciona como un taller general de seguridad digital donde participan tanto personas que provienen de grupos y organizaciones como las que hacen activismo de manera más individual.
- El **taller organizacional** está pensado para un grupo específico. El contexto de este tipo de talleres es que los diferentes integrantes se reúnen para realizar una evaluación de riesgos de sus prácticas y procesos organizacionales de tratamiento de datos.

Los objetivos de aprendizaje y los temas generales son los mismos para ambos enfoques, pero las metodologías y técnicas de facilitación se adaptan a los distintos formatos.

Objetivos de aprendizaje

Al terminar esta actividad, serán capaces de:

- Entender qué consideraciones sobre riesgos y seguridad tener en cada etapa del ciclo de vida de los datos.
- Aplicar marcos de evaluación de riesgos a su seguridad personal y/o organizacional.

¿A quién se dirige esta actividad?

Esta actividad está pensada para activistas individuales (en una evaluación general de riesgos o un taller de seguridad digital) y para grupos (una organización, red o colectivo) que está en proceso de evaluación de riesgos. Existen dos formatos y dos enfoques en relación a esta actividad, según se trate de un taller general o un taller dirigido a un grupo específico.

También se puede utilizar como actividad de diagnóstico a fin de definir en qué prácticas o herramientas enfocarse para el resto del taller de seguridad digital.

Tiempo necesario

Esto depende del número de participantes y el tamaño del grupo. En general, esta actividad dura cuatro horas como mínimo.

Recursos

- Hojas de papelógrafo
- Marcadores
- Proyector para presentar el ciclo de vida de los datos y la guía de preguntas, además de comentarios de participantes, si es necesario.

Mecánica

(Esto se aplica a un taller de evaluación general de riesgos o de seguridad digital, donde activistas de diferentes contextos se encuentran en una capacitación. Los objetivos de aprendizaje siguen siendo los mismos, pero algunas tácticas de capacitación y facilitación difieren de las que se usarían en un taller para un grupo más establecido de personas.)

Parte 1: ¿Qué publicas?

Pregunta al grupo: **¿Qué publicas como parte de tu trabajo como activista?**

El punto es empezar con la parte más obvia del ciclo de vida de los datos – datos procesados que se comparten como información. Pueden ser investigaciones, artículos, publicaciones en blogs, guías, libros, sitios web, publicaciones en redes sociales, etc.

Pueden compartir las respuestas en el grupo grande, como si fuera una asamblea o plenaria. Sugerimos la técnica ‘palomitas de maíz’ (popcorn) donde se dan respuestas rápidas y breves – como el maíz cuando explota en la cacerola.

Parte 2: Presentación del ciclo de vida de los datos y consideraciones de seguridad

El objetivo de la presentación es recordar que existe un ciclo de vida en el manejo de datos. Los puntos esenciales de la presentación se encuentran aquí (ver presentación sobre puntos claves sobre el ciclo de vida de los datos -datalife cycle-basics-presentation.odp- y también **Presentación**).

Parte 3: Tiempo de reflexión sobre los ciclos de vida de los datos personales

Pídeles que elijan un ejemplo específico de algo que hayan publicado (un artículo, una investigación, un libro, etc) y que formen grupos pequeños en base a la similitud de sus trabajos. Cada persona tendrá 15 minutos para rastrear el ciclo de vida de los datos de su ejemplo y reflexionar. Las preguntas guía para este tiempo de reflexión serán las consideraciones de la presentación.

Posteriormente, los grupos tendrán 45 minutos para compartir cada quien sus respuestas y debatir.

Parte 4: Comentarios y consideraciones de seguridad

En lugar de pedir que cada grupo presente sus conclusiones, se planteará a cada grupo las preguntas que surgieron de la discusión en los subgrupos.

Estas son algunas preguntas que puedes utilizar para trabajar sobre el tiempo de reflexión y el debate en grupo:

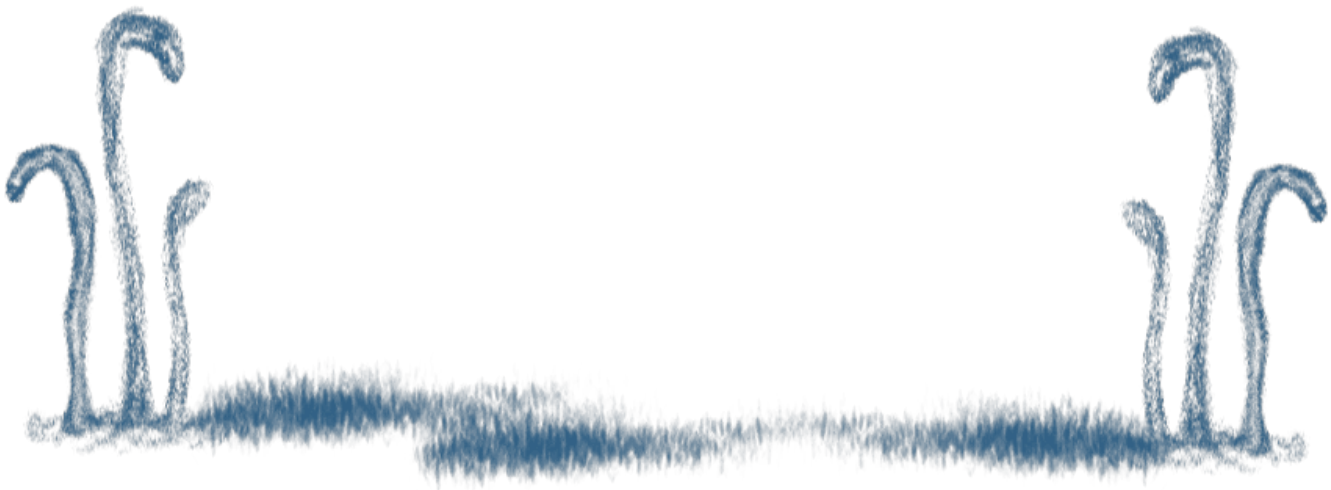
- ¿Cuáles son los dispositivos de almacenamiento de datos más comunes en tu grupo? ¿Cuáles fueron los que sólo una persona utiliza?

- ¿Cuáles fueron las diferencias y los puntos comunes en el acceso al almacenamiento de datos de tu grupo?
- ¿Qué pasa con el procesamiento de datos? ¿Qué herramientas se usaron en tu grupo?
- ¿Alguien del grupo publicó algo que le puso en riesgo directamente o a alguna persona conocida? ¿Qué fue lo que publicó?
- ¿Alguien del grupo había pensado en las prácticas de archivo y eliminación antes de hoy? Si es así, ¿qué prácticas utiliza?
- ¿Hubo algún interés en la seguridad en alguna parte del ciclo de vida de tus datos? ¿Qué tipo de interés/inquietud?

Síntesis de la actividad

Al final de las presentaciones e intercambios de los grupos, sintetiza la actividad de las siguientes maneras:

- Señala los puntos esenciales que se han detectado.
- Pide a las personas participantes señalar cuáles fueron los principales conocimientos adquiridos a través de la actividad.
- Pregúntales qué aprendieron durante la actividad en relación a los cambios que deberían introducir en su práctica de manejo de datos.



Mecánica para un taller organizacional

Pensado para un taller dirigido a una organización o grupo y sus integrantes.

Parte 1: ¿Qué tipo de información comparte cada unidad/programa/equipo/comité de la organización o grupo?

Según la configuración y la estructura de la organización o el grupo, pídele a cada equipo, área, comité o departamento que den un ejemplo de algo de lo que comparten – dentro o fuera de la organización o grupo.

Algunos ejemplos para promover una mayor respuesta:

- Para el área de comunicación – ¿qué informes publican?
- Para los equipos de investigación– ¿sobre qué investigación tienen que informar?
- Para los equipos administrativos y/o de finanzas – ¿quién tiene acceso a la planilla de sueldos de tu organización? ¿Y a los informes financieros?
- Para el departamento de recursos humanos – ¿Quién tiene acceso a las evaluaciones del personal?

Nota para la facilitación: Esta pregunta es mucho más fácil de contestar para los equipos que tienen objetivos de proyección exterior, por ejemplo, la sección de comunicación, o un programa que publica informes e investigaciones. Para las secciones de proyección más interna, como los sectores de finanzas, administración, o recursos humanos, posiblemente haya que dedicar más tiempo en la búsqueda de ejemplos de la información que comparten.

El objetivo, en esta etapa, es que cada equipo se dé cuenta de que en cualquier área se comparte información – dentro o fuera de la organización o grupo. Esto es importante porque cada equipo tiene que ser capaz de identificar uno o dos tipos de información que comparte al evaluar riesgos en su práctica de gestión de datos.

Parte 2: Presentación sobre el ciclo de vida de los datos y consideraciones de seguridad

La presentación consiste en recordar que existe un ciclo de manejo de datos. Los puntos claves de la presentación se encuentran aquí (ver la presentación sobre los puntos básicos del ciclo de vida de los datos - datalife cycle-basics-presentation.odp- y también **Presentación**).

Parte 3: Trabajo en grupos

Cada grupo tiene que identificar uno o dos tipos de la información que comparte/publica.

Con el fin de establecer prioridades, puedes sugerir que cada equipo piense en el tipo de información que le parece más importante cuidar, o qué clase de información delicada comparte.

Luego, deberán rastrear y analizar el ciclo de vida de los datos de cada uno de los tipos de información compartida o publicada. Utiliza la presentación siguiente para plantear las preguntas clave sobre la práctica de gestión de los datos que se aplica a cada pieza de datos publicada o compartida.

Al final de este proceso, cada equipo debería ser capaz de compartir el resultado de sus debates con todas las demás personas.

En general, el trabajo en grupos durará alrededor de una hora.

Parte 4: Presentaciones en grupo y reflexión sobre la seguridad

Según el tamaño de la organización o grupo y el trabajo que haya realizado cada unidad, dales tiempo para presentar las conclusiones de sus debates a sus colegas. Alienta a cada equipo a elaborar una presentación creativa y mostrar lo más destacable de sus conversaciones. No es necesario que compartan todo lo que conversaron.

Alienta a las demás personas que escuchen y tomen notas, ya que tendrán tiempo para compartir opiniones y comentarios al terminar cada presentación.

Se recomienda 10 minutos para cada grupo.

Quien facilita brinda sus comentarios al final de cada presentación, además de procurar que se respeten los tiempos y procesar los comentarios.

Algunas áreas sobre las que podrías hacer preguntas:

- Si se supone que el proceso de recolección de datos es privado, ¿no sería mejor usar herramientas de comunicación más seguras?
- ¿Quién tiene acceso al dispositivo de almacenamiento en teoría y en la realidad? En el caso de los dispositivos físicos de almacenamiento, ¿en qué parte de la oficina se encuentran?
- ¿Quién tiene acceso a los datos en bruto?

También puedes aprovechar la oportunidad para compartir algunas recomendaciones y sugerencias de prácticas más seguras de manejo de datos.

> **Nota para la facilitación:** Existe un recurso llamado Herramientas alternativas para vincular y comunicar que puede ayudarte a organizar esta actividad.

Parte 5: De vuelta a los grupos: Mejorar la seguridad

Una vez que todos los grupos hayan hecho su presentación, vuelvan a reunirse para seguir debatiendo y reflexionando cómo asegurar mejor sus datos y los procesos de gestión de los mismos.

El objetivo es que cada grupo planifique formas de operar con más seguridad en todas las etapas del ciclo de vida de los datos.

Al terminar el debate, cada equipo debe tener planes para que sus prácticas de gestión de datos se vuelvan más seguras.

> **Nota:** Partimos aquí de la suposición de que el grupo ya ha recibido una capacitación básica en seguridad para poder hacer esto. De lo contrario, quien facilita puede usar la Parte 4 para brindar algunas sugerencias de herramientas, opciones y procesos alternativos más seguros para las prácticas de almacenamiento de datos del grupo.

Preguntas guía para el debate en grupos

- De los tipos de datos que administras, ¿cuáles son públicos (cualquiera puede conocerlos), privados (sólo la organización o grupo puede conocerlos) o confidenciales (sólo el equipo y algunos grupos específicos de la organización pueden conocerlos)? ¿Y qué puede hacer tu equipo para garantizar que estos diferentes tipos de datos sean privados y confidenciales?
- ¿Qué puede hacer tu equipo para que puedas gestionar quién tiene acceso a tus datos?
- ¿Cuáles son las políticas de retención y eliminación de las plataformas que utilizan para almacenar y procesar sus datos en línea?
- ¿Cómo podría tener prácticas de comunicación más seguras el equipo, sobre todo en relación a la información y los datos privados y confidenciales?
- ¿Qué prácticas y procesos debería poner en práctica el equipo para preservar la privacidad y confidencialidad de sus datos?
- ¿Qué debería cambiar en su práctica de manejo de datos para volverla más segura? Observa los resultados del trabajo en grupo anterior y fíjate qué se puede mejorar.
- ¿Cuál sería el rol que debería tener cada uno de las integrantes del equipo para gestionar estos cambios?

Parte 6: Presentación final de los planes

Cada equipo tendrá un tiempo determinado para presentar cómo propone lograr que su práctica de gestión de datos sea segura.

Se trata de una buena oportunidad para que todos las personas dentro de la organización o grupo compartan estrategias y tácticas, y aprendan de las demás.

Síntesis de la actividad

Al final de las presentaciones y el intercambio entre los grupos, sintetiza la actividad de la forma siguiente:

- Señala los puntos claves que se plantearon;
- Pregunta cuáles son los principales conocimientos adquiridos en esta actividad;
- Llega a un acuerdo sobre los pasos siguientes para poner en marcha los planes.

Presentación

Otra forma de entender los riesgos es observar la práctica de tratamiento de datos de una organización o grupo. Todas trabajan con datos y cada una de las áreas o divisiones internas también.

Así, existen algunas consideraciones a tener para cada etapa del ciclo de vida de los datos.

Creación/recopilación/recolección de datos

- ¿Qué tipo de datos se están recopilando?
- ¿Quién crea/recopila/recolecta datos?
- ¿Acaso eso pone en riesgo a las personas? ¿Quién está en riesgo por la publicación de esos datos?
- ¿Qué tan público/privado/confidencial es el proceso de recopilación de datos?
- ¿Qué herramientas se utilizan para garantizar la seguridad del proceso de recopilación de datos?

Almacenamiento de datos

- ¿Dónde se almacenan los datos?

- ¿Quién tiene acceso al almacenamiento de datos?
- ¿Qué prácticas/procesos/herramientas utilizan para garantizar la seguridad del dispositivo de almacenamiento?
- Almacenamiento en la nube vs. almacenamiento físico vs almacenamiento en dispositivos.

Procesamiento de datos

- ¿Quién procesa los datos?
- ¿El análisis de los datos puede poner en riesgo a algún individuo, o al grupo?
- ¿Qué herramientas se utilizan para analizar los datos?
- ¿Quién tiene acceso al sistema/proceso de análisis de datos?
- En el procesamiento de datos, ¿se guardan copias secundarias de los datos en algún sitio?

Publicación/intercambio de información obtenida al procesar los datos

- ¿Dónde se publica la información/conocimiento?
- ¿La publicación de la información pone a alguien en riesgo?
- ¿Cuál es el público objetivo de la información publicada?
- ¿Tienes control sobre cómo se publica la información?

Archivo

- ¿Dónde se archivan los datos y la información procesada?
- ¿Los datos brutos se archivan, o sólo se archiva la información procesada?
- ¿Quién tiene acceso al archivo?
- ¿Cuáles son las condiciones de acceso al archivo?

Eliminación

- ¿Cuándo se eliminan de manera permanente (purgan) los datos?

- ¿Cuáles son las condiciones de eliminación?
- ¿Cómo podemos asegurarnos de que se eliminan todas las copias?

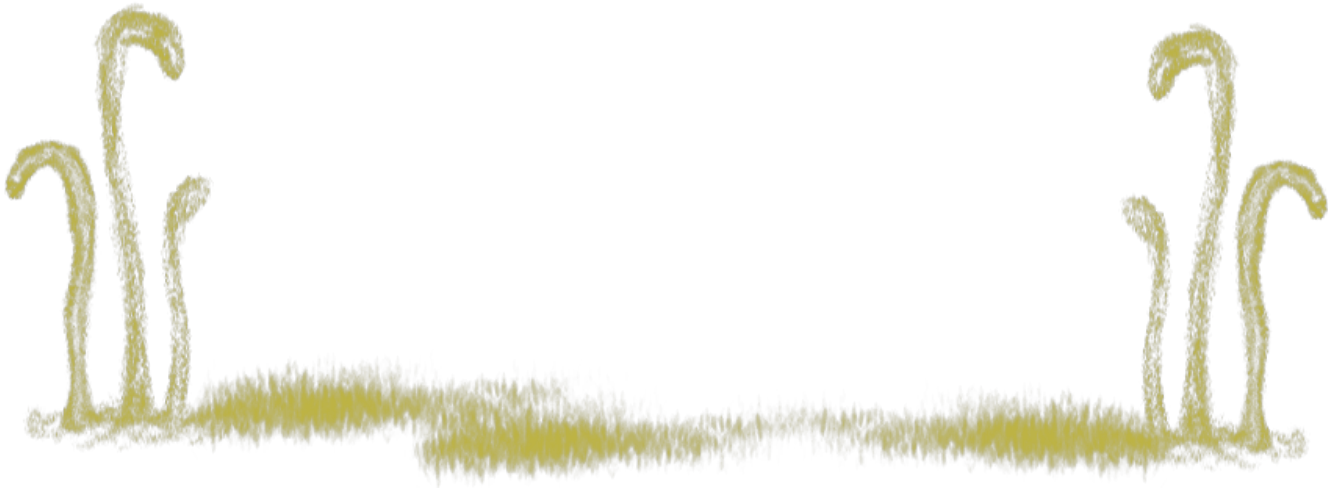
Notas para la facilitación

- Esta actividad sirve para poder conocer y evaluar los contextos, prácticas y procesos de seguridad de datos de quienes participan en este taller. Es mejor enfocarse en ese aspecto en lugar de esperar que esta actividad genere estrategias y tácticas para aumentar la seguridad digital.
- En un taller organizacional, puede ser mejor tener en cuenta los recursos humanos y los equipos/unidades administrativos. Para las nuevas personas integrantes de los grupos y organizaciones, muchas veces no cuentan con experiencia previa en talleres de seguridad digital y todos estos temas resultan muy nuevos para ellas. Por otro lado, es más difícil darse cuenta del hecho que el trabajo interno también implica “publicar datos”: datos delicados como la información sobre el equipo de trabajadores, salarios, notas sobre las reuniones del directorio, detalles bancarios de la organización, etc.
- Préstale atención también a los dispositivos físicos de almacenamiento. Si existen archivadores o armarios dónde se almacenan copias impresas de documentos, pregunta dónde están y quién tiene acceso a ellos. A veces, existe la tendencia a enfocarse demasiado en el almacenamiento en línea, olvidando así crear tácticas más seguras para el almacenamiento físico.

Lecturas recomendadas (optativo)

- Herramientas alternativas para vincular y comunicar (FTX: Reboot de seguridad)
- Seguridad móvil (FTX: Reboot de seguridad)
- Electronic Frontier Foundation's Surveillance Self-Defense (Defensa propia ante la vigilancia, de la Fundación Electronic Frontier, sólo en inglés) – a pesar de dirigirse sobre todo a un público estadounidense, esta guía contiene secciones muy útiles que explican los conceptos de vigilancia y las herramientas que se pueden usar para burlar los intentos de vigilancia.

- Guía de herramientas seguras de chat grupal y conferencias de Front Line Defenders (sólo en inglés) – una guía de gran utilidad sobre varios servicios y herramientas de chat y conferencia que cumplen con los criterios de seguridad de Front Line Defenders en relación a una aplicación o un servicio.
- Sitio web Privacy Not Included de Mozilla Foundation – analiza las diferentes políticas y prácticas de privacidad y seguridad de diversos servicios, plataformas y dispositivos para ver si cumplen con las Normas mínimas de seguridad de Mozilla, que incluyen cifrado, actualizaciones de seguridad y políticas de privacidad.



Organización de protestas y evaluación de riesgos [actividad táctica]

Esta actividad consiste en guiar la reflexión para un grupo de personas que está planificando una manifestación, a fin de que pueda prever y atender los riesgos y amenazas a los que pueda enfrentarse.

Introducción



Esta actividad consiste en guiar la reflexión para un grupo de personas que está planificando una manifestación, a fin de que pueda prever y atender los riesgos y amenazas a los que pueda enfrentarse. La actividad se aplica a protestas virtuales o presenciales y las que están dentro y fuera de internet en paralelo.

Esta no es una actividad para planificar manifestaciones o protestas, sino una evaluación de los riesgos que conlleva una acción de protesta. Se supone que antes de realizar esta actividad, el grupo ya ha realizado alguna planificación en cuanto a los motivos de la protesta y las principales estrategias, tácticas y actividades.

Objetivos de aprendizaje

En esta actividad, aprenderán a:

- Entender cuáles son los diferentes riesgos que enfrentan al llevar a cabo actividades de protesta.
- Crear un plan para responder a los riesgos identificados para llevar adelante una manifestación más segura.

¿A quién está dirigida esta actividad?

Es útil para un grupo de personas (una organización, una red o un colectivo) que haya decidido organizar una manifestación en conjunto.

El grupo tiene que contar con planes iniciales de acción, una serie de estrategias, tácticas y actividades consensuadas antes de iniciar esta actividad.

Tiempo requerido

Esta actividad dura cuatro horas, como mínimo.

Recursos

- Una pared grande en la que se pueda colgar y/o pegar el papel de papelógrafo y las notas autoadhesivas. Si no hay una pared que sirva para este propósito, es necesario liberar espacio en el suelo.
- Marcadores.
- Notas autoadhesivas (post-its)

- Dispositivos para documentar electrónicamente las conversaciones. Es importante definir qué integrantes del grupo serán responsables de documentar el diálogo y asegurar que, en caso de compartir el registro realizado, elegir canales seguros.

Dinámica de trabajo para un taller dirigido a un grupo que planea realizar una protesta compartida

Esta actividad tiene tres partes principales:

- La parte 1 consiste en analizar el riesgo desde el punto de vista de quienes organizan la protesta, la comunidad de apoyo y posibles adversarios como fuente de peligros (amenazas directas e indirectas, además de ver de qué formas puede fracasar la protesta). La parte 1 se divide en tres ejercicios diferentes, pensados para que el grupo llegue a un entendimiento común de los riesgos que puede implicar la protesta programada.
- La parte 2 se basa en la elaboración de estrategias para mitigar las posibles vulnerabilidades y fallas de la protesta, además de establecer el papel de las personas organizadoras en el plan de mitigación.
- La parte 3 se enfoca en lograr una comunicación interna segura entre las personas que participan en la protesta.

Parte 1: Evaluar posibles fuentes de riesgo

Esta parte tiene varios niveles de participación e interacción a fin de evaluar cuáles pueden ser las fuentes u orígenes de los riesgos que corre la protesta. Para que la mecánica sea más clara, los distintos niveles se señalan como “ejercicios”.

Prepara una hoja del papelógrafo para cada uno de los ítems siguientes:

- **Organizadoras de la protesta:** grupos y personas involucradas en la planificación de la protesta. También se incluye contrapartes aliadas.
- **Colaboradoras:** grupos y personas que esperas que participen de alguna manera en las acciones de protesta.
- **Adversarios de la protesta:** grupos y personas que se verán afectadas negativamente por esta protesta, además de quienes podrían llegar a apoyar en estas situaciones.
- **Actividades de la protesta:** las acciones planeadas para la protesta y dónde van a transcurrir dichas acciones. Las actividades pueden ser tanto **en línea,** como **fuera de línea.**

Ejercicio 1: Nombrar los *quiénes* y los *qué* de la protesta

Deja suficiente tiempo y espacio para completar cada una de las secciones del papelógrafo detalladas anteriormente: las respuestas se pueden escribir en post-its y pegar a los papelógrafos. O pueden escribir las respuestas directamente en el papel del papelógrafo.

> **Nota para la facilitación:** para hacer realizar el ejercicio de una forma más organizada, sobre todo si el grupo se compone de más de siete personas, se pueden formar cuatro grupos pequeños. Cada grupo trabajará primero en base a una hoja del papelógrafo. Uno puede empezar con “Organizadoras de la manifestación” y otro grupo con “Colaboradoras de la manifestación”, y así para cada grupo. Hay que dar tiempo para que escriban sus respuestas y luego pedirles que pasen a la hoja siguiente hasta que todos los grupos hayan tenido el tiempo de trabajar con todas las hojas. Esta metodología suele conocerse como World Café.

Ejercicio 2: Desglose de organizadoras, colaboradoras y adversarios

Una vez que todas las hojas del papelógrafo tengan las respuestas escritas, hay que dividirlas:

- El grupo 1 se quedará con los papelógrafos sobre organizadoras y colaboradoras.
- El grupo 2 se quedará con el papel relativo a adversarios.

La hoja del papelógrafo dedicada a las **Actividades** se dejará en el área común, como referencia.

Cada grupo tendrá su propio conjunto de preguntas guía para empezar a dilucidar dónde se encuentran los riesgos en su área focal.

En relación a organizadoras y colaboradoras, las preguntas guía son:

- ¿Quién(es) de las organizadoras es/son actualmente blanco de amenazas? ¿Qué amenazas son? ¿De qué forma pueden impactar en la manifestación o protesta?
- ¿Existen conflictos internos dentro del equipo organizador? ¿Tensiones de las que deberíamos tener conocimiento? ¿Cuál sería el posible impacto para la organización o grupo?
- Entre las colaboradoras, ¿quiénes pueden ser blanco de represalias?
- ¿Qué riesgos relativos a las represalias se pueden anticipar? ¿Ya hubo antes manifestaciones/protestas similares que generaron represalias? ¿Cuáles fueron?
- ¿Dónde tendrán lugar las reacciones o ataques? ¿Sabes qué espacios de las redes sociales constituyen el principal blanco de los adversarios? ¿Cuál sería el impacto de las represalias en la realidad fuera de internet, tanto durante como después de la manifestación/protesta?

En cuanto a los adversarios, las preguntas guía son:

- ¿Cuáles de los adversarios estarán más activos contra la manifestación/protesta?
- ¿Dónde se reúnen? ¿Dónde se reúnen tanto fuera como dentro de internet?
- ¿Cuáles son los líderes o las personas influyentes dentro del grupo de adversarios?
- ¿Qué capacidades tienen?
- ¿Qué pueden hacer contra la manifestación/protesta y contra las personas involucradas en la misma?
- ¿De qué forma los adversarios pueden afectar la planificación de la manifestación/protesta?
- ¿Cómo pueden perturbar las actividades planeadas durante la manifestación/protesta?
- ¿Qué tipo de reacciones/represalias puede generar la manifestación/protesta? ¿De qué forma los adversarios podrían tratar de alterar el mensaje de manifestación/protesta con

su reacción? ¿Quién(es) serían blanco de esa reacción? ¿Dónde se desarrollaría tal respuesta y qué papel tendrían las plataformas de redes sociales?

> **Nota para la facilitación:** la mayoría de las protestas hoy en día tienen componentes dentro y fuera de internet. Las preguntas que figuran a continuación se aplican a situaciones, manifestaciones y contextos tanto en línea, como fuera de línea. Si observas que las personas participantes se enfocan demasiado en el contexto fuera de internet, puedes ayudar a cambiar la atención haciéndoles preguntas sobre el contexto en línea de quienes están organizando y colaborando, además de posibles adversarios. Si tienen tendencia a enfocarse más bien en los factores en internet, puedes hacerles preguntas sobre el contexto fuera de línea. Invita a pensar en el impacto que pueden tener las actividades y eventos en internet sobre las actividades y eventos fuera de internet, y viceversa.

Se recomienda dedicar entre 45 minutos y una hora al intercambio grupal.

Al final de la actividad, cada grupo compartirá los resultados de su conversación, enfocándose en las siguientes preguntas:

Para el grupo que trabajó con organizadoras y colaboradoras:

- ¿Quién de las organizadoras y colaboradoras están ahora en peligro? ¿Qué peligros enfrentan?
- ¿Qué tipo de represalias supones que experimentarán las organizadoras y colaboradoras por participar en la manifestación/protesta?
- ¿Hubo conflictos o tensiones internas que puedan poner en riesgo a la manifestación/protesta? Si es así, ¿cuáles podrían ser?

Para el grupo que trabajó con adversarios:

- ¿Cuáles son los adversarios que más probablemente intentarán desbaratar la manifestación/protesta?
- ¿Qué tipo de perjuicios crees que pueden causar?
- ¿Qué diferencias supones que habrá entre las diferentes etapas de la manifestación/protesta: planificación, durante y después?

También vale la pena pedirle a los grupos que sean lo más específicos que puedan a la hora de compartir sus conclusiones.

Ejercicio 3: Reflexionar sobre las fallas posibles

Este ejercicio consiste en darle visibilidad a las fallas, o las vías por las cuales la manifestación o protesta pudieran fracasar.

Todas las personas que participan en el ejercicio tendrán el mismo tiempo para reflexionar sobre esta pregunta: **¿Qué es lo que NO quieres que suceda en esta manifestación o protesta?**

Para desglosar un poco más esta gran pregunta, puedes plantearle al grupo las siguientes preguntas a fin de incitar una reflexión más detallada:

- Piensa en las organizadoras y colaboradoras – ¿cuáles son los efectos negativos que podría tener para ellas este evento?
- Si se desarrolla dentro y fuera de internet, ¿cómo pueden perjudicar en ambos espacios los adversarios?
- Piensa en los espacios de las actividades de protesta – ¿qué es lo que *no* desearías que suceda? ¿qué puede hacer que fracasen?

Pídeles que reflexionen sobre las conversaciones que ya tuvieron y los comentarios que escucharon. Pueden escribir sus respuestas en notas autoadhesivas (post-its) separadas y pegarlas en la pared.

Junta las respuestas que tengan puntos en común para establecer temas generales que se puedan profundizar.



Parte 2: Planear estrategias y tácticas de mitigación

Ejercicio 1: Trabajo en grupos para mitigar vulnerabilidades y fallas posibles

A partir de los núcleos temáticos creados en el Ejercicio 3 de la Parte 1, forma grupos.

Cada grupo trabajará sobre las siguientes preguntas:

- ¿Qué puedes hacer para evitar resultados negativos?
- ¿Qué estrategias, enfoques y protocolos de seguridad se necesitan?
- ¿Existen diferentes estrategias para la etapa de planificación, durante la protesta/manifestación misma y después?
- ¿Qué harás si esta posible respuesta negativa se cumple? ¿Cuáles serán los pasos a dar?
- ¿Quién debe guiar estas estrategias?

Al final del intercambio de opiniones, cada grupo tendrá una lista de enfoques y estrategias, así como protocolos (reglas) de seguridad para lidiar con los resultados negativos. Escribe estas listas en el papelógrafo y/o haz una documentación electrónica. Organiza las listas según las diferentes etapas de la manifestación/protesta: antes, durante y después. Cada grupo presentará su lista a

los demás para intercambiar opiniones.

La persona facilitadora comenta los enfoques y estrategias de las participantes, sugiriendo mejoras (si es necesario) y encontrando estrategias comunes entre los grupos.

Ejercicio 2: Debate sobre roles

Organiza un debate con todo el grupo sobre los roles necesarios para mitigar consecuencias negativas, adoptar protocolos de seguridad y gestionar comunicaciones seguras – antes, durante y después de las acciones de protesta/manifestación. Es importante que el grupo defina completamente dichos roles y establezca quién va a cumplirlos.

Parte 3: Comunicarse de manera segura

Quien facilita puede presentar opciones de comunicaciones más seguras para acciones de protesta.

En caso de que sea posible, dale tiempo al grupo para instalar y probar las aplicaciones de comunicación escogidas.

Como ayuda para planificar esta parte, puedes leer Herramientas alternativas para vincular y comunicar y el Módulo de seguridad móvil.

> **Nota de seguridad:** una de las formas de poner en práctica estas nuevas herramientas más seguras es pedir a las personas responsables de hacer el registro que compartan copias de sus notas a través de canales más seguros de comunicación a las demás personas participantes.

Ajustes para un taller general

En general, las actividades de evaluación de riesgo son más eficaces cuando se realizan con grupos que tienen objetivos, contextos y escenarios de riesgos en común (por ejemplo, intervenciones de evaluación de riesgo organizacional o evaluación de riesgo para una red de organizaciones y colectivos). Por lo tanto, esta actividad fue pensada para un grupo de participantes que ya están planeando llevar a cabo una acción de protesta/manifestación. Sin embargo, la actividad se puede adaptar a un contexto de seguridad digital más general donde personas de diferentes procedencias están pensando en organizar acciones de protesta con sus propios grupos.

Para poder ajustar esta actividad para este uso más general, puede ser útil utilizar un ejemplo de protesta o manifestación para extraer aprendizajes que después puedan aplicar a sus grupos/redes/colectivos.

Algunos lineamientos para crear un ejemplo de protesta:

- **Sitúa las acciones de protesta en la realidad:** es importante situar las acciones de protesta/manifestación en un contexto real para poder realizar un análisis y diseño de estrategias práctico.

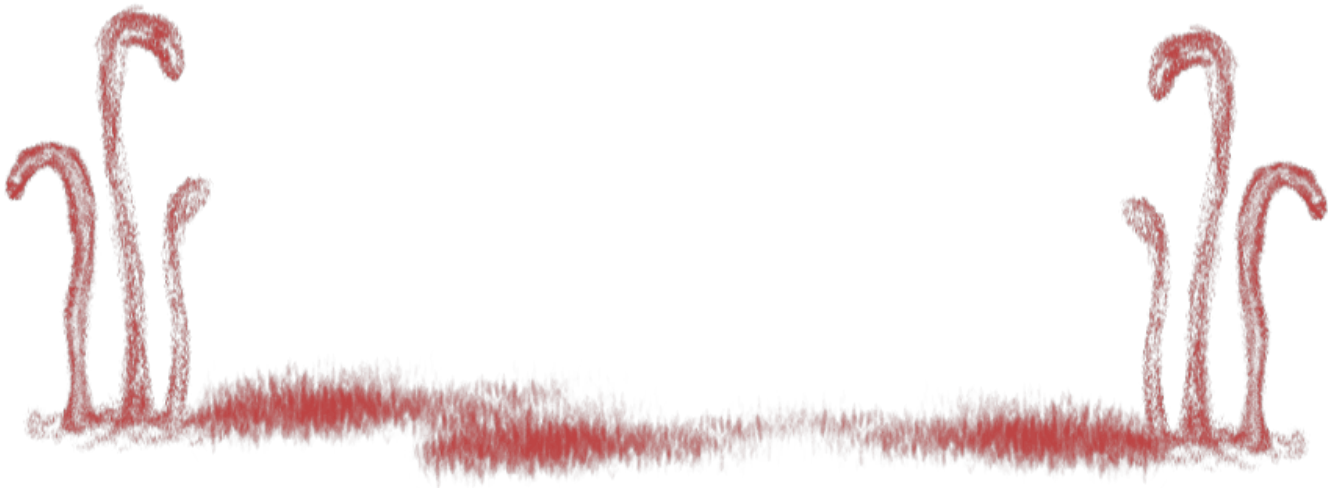
Si las personas participantes en esta actividad son del mismo país, puedes situar la protesta/manifestación en ese país. Si son de diferentes países, plantea una situación regional.

- **Diseña un modelo de protesta para un problema que resuene con las participantes:** así, les resultará familiar y lo podrán relacionar con algún evento similar.
- **Establece las demandas y los objetivos de la protesta/manifestación:** tiene que quedar claro el vínculo con el problema que esté a mano.
- **Diseña actividades de protesta/manifestación fuera y dentro de internet:** confirma que, al identificar las actividades de protesta, cuentas con una combinación de tácticas en línea y fuera de línea. Especifica los detalles de estas actividades – ¿dónde transcurrirán, cuándo, cuál será su duración?
- **Utiliza como base una protesta/manifestación real:** si conoces una protesta o manifestación que pueda funcionar para las participantes de tu taller, puedes utilizarla como ejemplo.

La clave para crear una protesta de muestra es tratar de simular lo más posible una manifestación/protesta real. Subrayamos la relevancia de la evaluación de riesgo como manera

muy eficiente para definir especificidades.

Recomendamos que encuentres formas de ajustar tus tiempos para que las personas participantes puedan aprender de la protesta de muestra y absorber lo que necesitan. Puedes compartir los detalles del ejemplo antes del taller, pero no des por sentado que todo el mundo tuvo tiempo de leer el documento por lo que recomendamos presentarlo al inicio del taller y entregarlo en papel para que cada grupo tenga la información a la mano.



Elementos básicos en la evaluación de riesgos [material de base]

Introducción

Todo el tiempo estamos evaluando riesgos. Así es como sobrevivimos. No se trata de un proceso que realizamos exclusivamente en el ámbito de la seguridad digital y/o informática.

Cuando salimos a caminar de noche por una calle tranquila, decidimos por qué acera vamos a caminar, cómo comportarnos, qué preparar y cómo caminar según nuestra lectura de la situación: *¿Esta calle es conocida por ser peligrosa? ¿Conozco a alguien en esta calle que podría venir en mi ayuda? ¿Puedo correr a toda velocidad si algo sucede? ¿Llevo pertenencias de valor con las que podría negociar? ¿Llevo objetos conmigo que podrían ponerme en peligro? ¿De qué lado de la calle es mejor caminar para evitar posibles riesgos?*

Cuando nuestro grupo empieza a planificar un nuevo proyecto, solemos pensar también en los posibles fracasos. Tomamos decisiones basándonos en lo que sabemos sobre el contexto y los factores que podrían hacer que no se cumplan los objetivos.

Al organizar manifestaciones y protestas, buscamos la forma de mantener a salvo tanto a quienes participan en la acción, como a la acción misma. Organizamos sistemas de compañerismo. Nos aseguramos de que haya un apoyo legal inmediato en caso de arrestos. Enseñamos, a quienes participan, conductas que puedan evitar abusos por parte de las autoridades y pensamos estrategias para realizar la protesta de manera pacífica a fin de minimizar potenciales riesgos. También incluimos gente dedicada específicamente a mantener la seguridad de la acción.

Si bien la evaluación del riesgo puede ser algo que hacemos instintivamente, se trata de un proceso específico que llevamos a cabo – generalmente de manera colectiva – a fin de saber cómo evitar amenazas y/o responder a dichas amenazas.

Evaluación de riesgo: Dentro y fuera de la red

Evaluar los riesgos que corremos en línea no es algo tan instintivo, por diversas razones. La mayoría ni entiende cómo funciona internet ni cuáles son los riesgos y amenazas que implica– una realidad en constante cambio y crecimiento. Hay quienes tienen la sensación de que las actividades, acciones y comportamientos en línea no son “reales” y tienen efectos menos graves que lo que nos sucede físicamente. En el otro extremo del espectro, quienes ya tuvieron la experiencia de ver cómo la vida “real” de una persona se ve afectada por sus actividades en línea (personas que fueron engañadas en los sitios de citas, gente cuyas interacciones tabúes en internet se volvieron públicas, activistas arrestadas por decir algo contra el gobierno) tienden a tener una visión paranoica de internet.

La realidad es que, para muchas personas activistas, la oposición entre el fuera y dentro de la red es falsa. El uso de dispositivos digitales (teléfonos móviles, laptops, tabletas, computadores, etc),servicios, aplicaciones y plataformas basadas en internet (Google, Facebook, Viber, Instagram, WhatsApp, etc.) es algo común y básico en su trabajo – tanto para organizarse, como para el activismo en sí mismo. El modo en que nos organizamos y realizamos nuestra labor como activistas ha evolucionado a medida que la tecnología ha ido avanzando y desarrollándose – y seguirá siendo así. Internet y las tecnologías digitales son una de las claves de nuestra infraestructura organizativa. Las utilizamos para comunicarnos, coordinar y realizar actividades y construir nuestra comunidad. Las reuniones y eventos presenciales suelen desarrollarse junto con una participación en línea, sobre todo en las redes sociales y mediante hashtags (etiquetas). Actualmente, en muchas protestas, hay un constante flujo entre la movilización, la organización y las reuniones en línea y fuera de línea.

En lugar de considerar que lo que sucede en internet es algo separado de nuestra realidad física, piensa en las realidades en línea <-> fuera de línea como planos interconectados y porosos, permeables. Existimos en ambas dimensiones de la realidad, la mayor parte del tiempo, al mismo tiempo. Lo que sucede en una, afecta nuestro modo de estar en la

Esto significa también que los riesgos y las amenazas en línea afectan nuestra integridad física fuera de línea y viceversa. Por ejemplo, las estrategias avanzadas de vigilancia estatal contra activistas y movimientos sociales que explotan el uso inseguro de las tecnologías (por ejemplo, cliquear links o descargar y abrir archivos no verificados/desconocidos potencialmente inseguros) para conseguir más información que les permita seguir vigilando también fuera de internet. . Quienes hayan tenido experiencias de violencia de género en línea conocen los efectos psicosociales de ese tipo de ataques y acoso. Hasta hay casos donde llega a afectar la seguridad física de las personas a las que estaba dirigida. Existen diferentes formas (acoso, *doxing*, hostigamiento) y se utilizan como tácticas de censura y sumisión contra activistas feministas y queer.

Pensar en la naturaleza permeable de las amenazas y los riesgos en línea <-> fuera de línea puede ser abrumador – *¿dónde empezamos a evaluar y saber cuáles son las amenazas y de dónde vienen?¿cómo elaboramos estrategias para lidiar con ellas?*

¿Qué es la evaluación de riesgos?

La evaluación de riesgos es el *inicio del proceso* de volverse más resiliente a la hora de responder ante contextos y amenazas cambiantes. Tiene como objetivo poder elaborar tácticas y estrategias para mitigar tales riesgos, y también tomar decisiones más informadas.

En términos generales, el riesgo es la exposición a posibles daños, lesiones o pérdidas.

En la evaluación de riesgos, se trata de la capacidad (o falta de capacidad) de una persona o grupo para responder a los impactos de una amenaza que se vuelve real o para evitar que suceda en primer lugar.

Existe una fórmula conocida para la evaluación de riesgos:

Riesgo = amenaza x probabilidad x impacto/capacidad

Donde:

- Amenaza es cualquier acción negativa que apunte hacia una persona o un grupo.
    - Las amenazas directas son intenciones explícitas de causar daño.

    - Las amenazas indirectas son las que suceden como resultado de un cambio en una situación.
    - Al definir cuáles son las amenazas o peligros, es importante definir de dónde vienen. Mejor aún, saber de quién vienen.

- La probabilidad es la posibilidad de que una amenaza se vuelva real.
    - Un concepto relativo a la probabilidad es la vulnerabilidad. Puede ser que el lugar, la práctica y/o la conducta del individuo/grupo incrementen las oportunidades para que un riesgo se convierta en un hecho.
    - Se trata también de la capacidad de quienes amenazan, sobre todo en relación con el individuo/grupo amenazado.
    - Para evaluar la probabilidad, pregunta si hay ejemplos reales de una amenaza de ese tipo que se haya cumplido para una persona o un grupo que conozcas – y compara la situación con la que vives de primera mano.

- El impacto es lo que sucederá cuando la amenaza se cumpla. Las consecuencias de la amenaza.
    - El impacto puede afectar al individuo, al grupo, a la red, o al movimiento.
    - Cuanto mayor sea el grado y/o el número de impactos de un peligro, mayor será el riesgo.

- Las capacidades son las habilidades, fortalezas y recursos a los que un grupo tiene acceso a fin de minimizar la probabilidad de que se cumpla la amenaza, o de responder al impacto causado por la misma.

Casos de estudio - amenazas y mitigación

Estudio de caso: Deya

A modo de ilustración, vamos a utilizar la experiencia ficticia, aunque bastante común, de Deya. Deya es una activista feminista que utiliza su cuenta de Twitter para desafiar a quienes promueven la cultura de la violación. En consecuencia, Deya ha sido acosada y amenazada en línea.

La amenaza que más le preocupa es la de quienes prometieron descubrir dónde vive y compartir la información en internet para invitar a otras personas a causarle daños físicos. En este caso, el impacto es claro – daño físico. Hay otras amenazas, como el acoso en el ámbito laboral para que la despidan de su trabajo y hacia su círculo visible de amistades en línea.

Para evaluar los riesgos, Deya tendrá que repasar todas las amenazas y analizarlas a fin de evaluar su probabilidad y el impacto que pueden causar – con el objetivo de planear cómo mitigar dichos riesgos.

Amenaza 1: Se descubre dónde vive y se comparte la información en línea

La mayoría de las amenazas proceden de cuentas en línea – y la mayoría de estas cuentas son de personas que no conoce y no puede verificar si se trata de personas de verdad o cuentas falsas. Deya reconoce a algunas de las personas que participan en las amenazas en línea: son actores conocidos que suelen participar en ataques en línea contra mujeres. Basándose en el conocimiento que tiene de ataques previos en los que a veces se publicaron detalles personales en línea, Deya siente un temor verdadero en relación a su seguridad personal.

¿Hay alguna forma de evitar que eso suceda? ¿Cuál es la probabilidad de que las personas que la acosan y atacan averigüen dónde vive ? Deya tiene que imaginar qué tan probable es que su dirección ya se encuentre disponible en internet, o que alguno de sus atacantes la ponga a disposición.

Para evaluar esta situación, Deya puede empezar realizando una búsqueda en internet sobre sí misma para ver qué información encuentra – de esta manera, sabrá si hay espacios físicos asociados a su persona y si esos espacios señalan su verdadera localización física. Si descubre que su dirección se puede encontrar en internet, ¿qué puede hacer para evitar que esté disponible públicamente?

Deya también puede evaluar qué tan vulnerable o seguro es su domicilio. *¿Vive en un edificio con vigilancia y protocolos para el acceso de quienes no residen allí? ¿Vive en un apartamento que*

debe cuidar por su cuenta? ¿Vive sola? ¿Cuáles son las vulnerabilidades de su domicilio?

Además, tendrá que evaluar cuáles son las capacidades y recursos que tiene para protegerse. *Si su domicilio se da a conocer públicamente en internet ¿puede mudarse? ¿Quién puede ofrecerle apoyo durante ese tiempo? ¿Puede llamar a las autoridades para pedir protección?*

Amenaza 2: Acoso en el ámbito laboral para que despidan a Deya de su trabajo

Deya trabaja en una ONG de derechos humanos, de modo que no hay peligro de que la despidan de su empleo. Pero el domicilio donde se encuentran las oficinas de la organización es públicamente conocido en su ciudad y está disponible en el sitio web de dicha organización.

Para Deya, el peligro de perder su empleo es escaso. Sin embargo, la información públicamente disponible sobre su ONG puede ser un flanco vulnerable para su seguridad física, así como para la seguridad del equipo.

En este escenario, la organización deberá hacer su propia evaluación de riesgo, a raíz del hecho de que una de las integrantes del equipo de trabajo es blanco de amenazas.

¿Qué hacer con los riesgos? Tácticas generales de mitigación

Más allá de identificar y analizar amenazas, probabilidades, impactos y capacidades, la evaluación de riesgos tiene que ver también con la elaboración de un plan de mitigación para todos los riesgos identificados y analizados.

Hay cinco maneras generales de mitigar riesgos:

Aceptar el riesgo y elaborar planes de contingencia

Algunos riesgos son inevitables. O ciertos objetivos hacen que valga la pena correrlos. Pero eso no significa que haya que desestimar su importancia. Hacer un plan de contingencia significa imaginar qué pasaría si sucediera el mayor riesgo y cuáles serían los impactos más graves para poder dar los pasos necesarios para lidiar con la situación.

Evitar el riesgo

Implica reducir la probabilidad de que una amenaza se vuelva un hecho. Puede significar la implementación de políticas de seguridad para mantener más seguro al grupo. También podría implicar cambios de comportamiento para incrementar las posibilidades de evitar un riesgo específico.

Controlar el riesgo

A veces, un grupo puede decidir enfocarse en el impacto causado por la amenaza, en lugar de centrarse en ella. Controlar el riesgo significa reducir la gravedad de su impacto.

Transferir el riesgo

Conseguir un recurso externo para asumir el riesgo y su impacto.

Monitorear el riesgo para estar alerta de cambios en términos de probabilidad e impacto

Suele emplearse esta táctica de mitigación para los riesgos de bajo nivel.

Estudio de caso: Deya

Para usar el ejemplo de Deya otra vez, ella tiene alternativas para actuar frente a los riesgos que enfrenta basándose en su análisis y evaluación, la probabilidad de que ocurran, los impactos y las capacidades que ya existen para lidiar con las amenazas y/o los impactos que puedan tener.

En el caso en que la dirección postal de Deya ya se pueda encontrar en internet, ella tiene que aceptar el riesgo y enfocarse en realizar planes de contingencia. Estos planes pueden ser desde mejorar la seguridad de su hogar, hasta mudarse. La medida de las posibilidades dependerá de las realidades y contextos existentes de Deya.

Otra opción que tendría Deya en este escenario sería preguntar dónde es que se encuentra su dirección postal disponible al público para eliminar ese contenido. Sin embargo, esta no es una táctica infalible. Le ayudará a eliminar el peligro si ninguna de las personas que la acosan vieron todavía la información. Pero si alguna de esas personas ya lo ha hecho y tomó una fotografía o captura de pantalla de la información, es muy poco lo que puede hacer Deya para impedir que se divulguen los datos.

Si la dirección de donde vive Deya no se conoce públicamente y no está disponible en internet, hay más espacio para pensar en cómo evitar riesgos. ¿Qué puede hacer Deya entonces para impedir que las personas que la acosan descubran la dirección de su casa? Puede eliminar sus publicaciones con etiquetas geográficas que estén cerca de su casa y dejar de enviar posts en tiempo real que contengan esta información.

En cualquiera de los dos escenarios posibles (ya sea que su domicilio esté disponible públicamente o no), Deya puede dar los pasos necesarios para controlar el riesgo enfocándose en proteger su hogar.

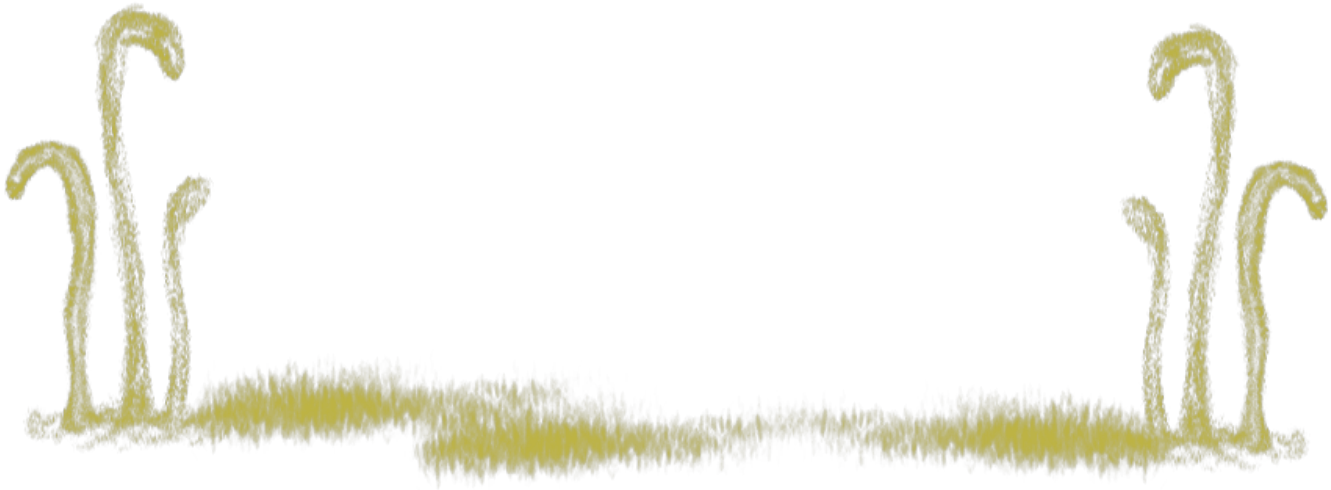
Las buenas estrategias de mitigación de riesgos implican pensar en estrategias preventivas y dar respuesta frente a incidentes – evaluar lo que se puede hacer para evitar el peligro y pensar qué se puede hacer si la amenaza se cumple.

Estrategias de prevención

- ¿Con qué capacidades cuentas para evitar que esta amenaza se vuelva un hecho?
- ¿Qué acciones llevarás a cabo para evitar que suceda? ¿Cómo cambiarás los procesos adentro de la red?
- ¿Tienes que crear políticas y procedimientos ?
- ¿Qué capacidades necesitas para prevenir esta amenaza?

Respuesta frente a incidentes

- ¿Qué harás cuando esta amenaza se torne realidad? ¿Qué pasos darás?
- ¿Cómo reducirás la gravedad del impacto de esta amenaza?
- ¿Qué capacidades se necesitan para dar los pasos necesarios para responder a esta amenaza?



Recordatorios

Las evaluaciones de riesgos están sujetas a plazos determinados

Es decir, se dan en un período de tiempo específico – en general, cuando surge una amenaza nueva (por ejemplo, un cambio de gobierno, cambios en las políticas de seguridad de alguna plataforma, etc), o se sabe de una nueva amenaza (por ejemplo, acoso en línea contra activistas, denuncia de cuentas de activistas comprometidas, etc), o se produce un cambio dentro de un colectivo (un nuevo proyecto, nuevo liderazgo). Por lo tanto, es importante revisar las evaluaciones de riesgo ya realizadas porque los riesgos van cambiando a medida que van surgiendo y desapareciendo amenazas, y a medida que van cambiando las capacidades de los grupos y las personas para responder ante una amenaza y recuperarse de sus impactos.

La evaluación de riesgos no es una ciencia exacta

Cada una de las personas que integran un grupo que está realizando un proceso de evaluación de riesgos tiene una perspectiva y una posición que afecta su capacidad de saber la probabilidad de que una amenaza se concrete, y también su capacidad de evitarla o responder a los impactos que causa. El objetivo de la evaluación de riesgos es entender colectivamente estas diferentes perspectivas adentro del grupo y llegar a tener una conciencia de los riesgos a los que se enfrenta. Las evaluaciones de riesgos son relativas. Diferentes grupos de personas enfrentados a los mismos riesgos y peligros tienen diferentes capacidades para evitarlos y/o responder ante las

consecuencias.

La evaluación de riesgos no garantiza 100% la seguridad, pero puede ayudar a un grupo a prepararse para enfrentar amenazas

Dado que no existe nada que sea 100% seguro y a salvo, las evaluaciones de riesgos no pueden garantizar total seguridad. Pero pueden ayudar a individuos y grupos a evaluar los riesgos y amenazas que pueden afectarlos.

La evaluación de riesgos tiene que ver con la capacidad de analizar riesgos conocidos y emergentes a fin de darse cuenta de cuáles son los riesgos que son impredecibles

Existen diferentes tipos de riesgos:

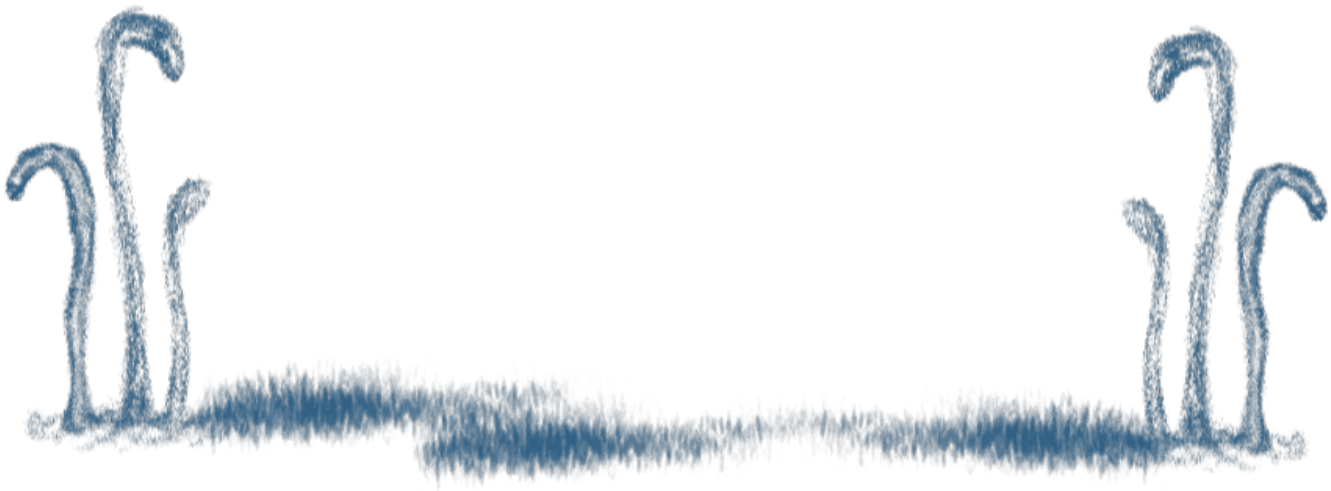
- Riesgos conocidos: peligros y amenazas que ya se han entendido en la comunidad. ¿Cuáles son sus causas? ¿Qué impactos tienen?
- Riesgos emergentes: amenazas que se han vuelto realidad pero no dentro de la comunidad a la que pertenece la persona. Pueden ser amenazas resultantes del clima político que se vive, de los desarrollos tecnológicos y/o cambios dentro de las comunidades de activistas en general.
- Riesgos desconocidos: son los riesgos imprevisibles, aquéllos cuya ocurrencia y momento de ocurrencia resulta imposible prever.

Las evaluaciones del riesgo son importantes para la planificación

Permiten que el individuo o el grupo analicen qué es lo que puede causarles daño, las consecuencias de tales daños y las capacidades con las que cuentan para mitigarlos . El desarrollo de un proceso de evaluación de riesgos ayuda a los grupos a tomar decisiones realistas sobre los riesgos que enfrentan y les permite prepararse.

La evaluación de riesgos es una forma de controlar el miedo y la ansiedad

Se trata de un buen proceso para conocerlos temores de las personas que integran un grupo – para generar equilibrio entre la paranoia y la total ausencia de miedo (pronoia) a fin de tomar decisiones colectivamente sobre qué riesgos tener en cuenta en la planificación.



Evaluación de riesgos en la organización y movilización social [material de base]

Descripción

Pensar en la evaluación de riesgos a la hora de hacer activismo y movilización social implica ampliar el alcance de nuestro análisis: incluir espacios, procesos, recursos, actividades compartidas cuya gestión es colectiva – ya sea formal o informalmente.

Los movimientos sociales son más grandes que una organización o grupo en concreto. Son un entramado de relaciones de compromiso y acciones políticas compartidas entre las diferentes partes de una red donde individuos, organizaciones, colectivos, miembros o grupos de una comunidad aportan una diversidad de conocimientos, capacidades, contextos y prioridades. Las formas de organización, de creación de roles, áreas de responsabilidad y acuerdos, son aspectos importantes en las redes activistas. En este sentido, la evaluación de riesgos también puede servir para poner en evidencia puntos de estrés potencial.

La evaluación de riesgos desde la perspectiva de un movimiento social

Suele ser más fácil identificar movimientos retrospectivamente, ya que crecen orgánicamente en el tiempo y en respuesta a inquietudes que surgen en momentos y escenarios específicos. A veces, parece que los movimientos son protestas, ya que ese suele ser el lugar desde donde se hacen visibles y crecen. Pero no todos terminan (o empiezan) en una protesta. Por ejemplo, muchos movimientos LGBTIQ++ en contextos donde la visibilidad implica un costo muy alto se organizan y actúan de maneras menos públicas, como espacios comunitarios privados en internet donde las personas se puedan encontrar, conversar, apoyarse entre si y elaborar estrategias para realizar diversos tipos de intervenciones.

Un movimiento se compone de muchos momentos o etapas diferentes tales como la vincular y difundir en comunidades, sistematizar y documentar pruebas y casos, profundizar en temas más complejos, construir acuerdos y consensos, realizar acciones, crear espacios de cuidados colectivos, distribuir recursos y mucho más.

Cada uno de estos momentos o etapas pueden ser oportunidades para que las personas a cargo de mantener un espacio o llevar a cabo un proceso realicen colectivamente una evaluación de riesgos. Puede ser útil concebir la seguridad del movimiento social como las condiciones necesarias para que las distintas etapas y componentes del trabajo del movimiento puedan funcionar y florecer.

Los estratos de un riesgo

Una forma de empezar el proceso de evaluación de riesgos desde la perspectiva de un movimiento social o red activista es distinguir los diferentes estratos que deben tomarse en cuenta. Existen tres componentes que interactúan entre sí:

1. Relaciones y protocolos
2. Espacios e infraestructura
3. Datos e información

Las secciones a continuación describen cada uno de estas dimensiones y algunos de sus componentes, incluyendo preguntas para facilitar un diálogo donde se puedan desglosar, analizar y entender los riesgos, con la intención de elaborar un plan.

1. Relaciones/protocolos

El corazón de un movimiento resiliente se compone de relaciones muy estrechas y creadas sobre la base de la confianza. Esto es de particular importancia ya que un movimiento no tiene tanto que ver con su forma como con la fuerza y la tenacidad de sus relaciones.

La evaluación de riesgos puede realizarse a nivel individual, organizacional o de grupos informales. Cuando se realiza desde la perspectiva de la construcción de movimientos sociales, hay que prestar atención a las relaciones *entre* estos niveles.

Por ejemplo, si una persona está atravesando un momento de mucho estrés porque vive de lo que cobra mes a mes, esto puede afectar su capacidad de participar plenamente, lo que a su vez puede tener impacto en la organización del trabajo en general. O si una organización está siendo blanco de un ataque del gobierno, su afiliación a otros grupos o personas del movimiento pueden exponer a las demás a ataques similares. O si hay abusos entre las personas integrantes de un colectivo, puede debilitar su proceso por estrés (interno y externo).

En otras palabras, desde la perspectiva de un movimiento social, las prácticas y el bienestar de todas las partes implicadas en una red activista afectan los riesgos que puede llegar a enfrentar. Por ello, se recomienda que su abordaje sea colectivo.

Para gestionar riesgos a nivel relacional, se pueden analizar tres áreas:

a) Cuidado colectivo

El cuidado colectivo es una responsabilidad, tanto individual como colectiva, entre las personas que integran un grupo. Esto significa que a la hora de evaluar riesgos y hacer planes para evitarlos hay que tener en cuenta la situación de bienestar de cada persona, además del bienestar interpersonal en cuanto a los espacios, plataformas, recursos y procesos compartidos.

- ¿Cuáles son algunos de los riesgos que afectan al bienestar de las diferentes personas del grupo?
- ¿Cuáles pueden ser los impactos?
- ¿Cuál es el estrato tecnológico de este asunto en relación al cuidado y al bienestar? Por ejemplo, existen protocolos sobre desconectarse de las redes sociales, limitar la cantidad de reuniones en línea, o activar acciones solidarias en red ante algún ataque contra el

grupo o sus integrantes?
- ¿Cómo pueden desarrollarse prácticas colectivas para mitigar o tratar algunos de los riesgos o impactos? ¿Existen recursos o capacidades que se pueden acumular o compartir? Por ejemplo, reunir fondos entre diferentes grupos y personas para suscribirse a un canal de comunicación o una plataforma de hosting que sea más seguro y permita controlar mejor los datos?

b) Inclusión y representación

En relación a procesos y criterios para incluir a personas a diferentes niveles de espacios organizados. A veces, se tiene en cuenta sólo cuando aparece una grieta en la seguridad, como, por ejemplo, cuando se filtra información sobre un evento organizado por WhatsApp y Facebook a grupos adversarios. Pensar en mecanismos de inclusión puede ayudarnos a desarrollar protocolos de seguridad en el intercambio de información y los canales de comunicación. Considerar la representación en las actividades del movimiento social puede ayudar también a ver algunos riesgos que pueden afectar particularmente a ciertos individuos o grupos de personas, además de preguntarse cómo mitigar, distribuir o preparase para afrontar tales riesgos.

- ¿Cuáles son los protocolos a la hora de integrar nuevas personas o cuando alguna persona se va del movimiento? Por ejemplo, listas de correo u otro tipo de espacios de intercambio y trabajo.
- ¿Tener una o varias facetas públicas a nivel del movimiento/red implica ciertos riesgos? ¿Cómo se puede planificar para evitarlos? Por ejemplo, al publicar una convocatoria, ¿existe un plan sobre las cuentas desde las cuales se debería hacer el llamado (cuentas personales, cuentas de uso único creadas para la actividad específica, cuentas organizacionales, etc.) y un plazo para que no se pueda rastrear hasta una fuente inicial?
- ¿Cuáles son algunos de los riesgos asociados a las acciones solidarias en red? ¿Cómo se puede planificar de manera segura? Por ejemplo, considerando el cuidado de identidades particularmente en riesgo ante blancos de ataque, tomar decisiones en cuanto a la documentación y la publicación de imágenes en plataformas de redes sociales y camuflando las personas en riesgo entre más participantes (de esta manera, se “distribuye el riesgo”).
- ¿Cuáles son los diferentes contextos de conectividad a internet y la capacidad técnica adentro de la red/movimiento? ¿Cómo afecta lo anterior en la participación segura de las personas integrantes?

c) Gestión de conflictos

La gestión de conflictos suele ser una de las áreas que menos se trabajan dentro de un movimiento o red, porque se suele dar por hecho que la política, los valores y los intereses son compartidos. Sin embargo, es importante hacerlos visibles, conversar y planificar de manera acorde, ya que pueden servir de apoyo a toda la misión de justicia del movimiento, además de garantizar la consideración a las vulnerabilidades y diferencias de poder internas.

Un plan no tiene que ser complejo, pero puede comenzar con un diálogo sincero, facilitado con cuidado, donde *se pone sobre la mesa* los valores compartidos. De esta manera, se pueden llegar a acuerdos y crear conjuntamente un plan que incluya a quiénes deben participar, qué medidas tomar y cómo establecer colectivamente los valores compartidos.

- ¿Cuáles son algunos conflictos que podrían suponer un riesgo para el movimiento o la red? En particular, conflictos interpersonales – ¿cuál podría ser el impacto? Por ejemplo, pérdida de confianza, fragmentación entre integrantes, pérdida de control sobre recursos como contraseñas, acceso a sitios, etc.
- ¿Cómo se puede desarrollar un plan de respuesta para diferentes tipos de conflicto? Por ejemplo, situaciones dentro del movimiento/red como acoso sexual, violencia íntima entre parejas o relaciones románticas/sexuales entre integrantes que acaban mal; toma de decisiones en relación a recursos o fondos compartidos; desacuerdos sobre valores o estrategias esenciales... Puede tratarse de mecanismos que se mantienen a largo plazo o mecanismos contingentes, relativos a actividades específicas.

2. Espacios/infraestructura

El estrato/capa digital es un componente cada vez más importante para organizar y construir movimientos sociales hoy en día. Al no ubicarse las redes activistas en un espacio institucional, la infraestructura y las plataformas digitales se han convertido en un espacio compartido fundamental para reunirse, coordinar y planear actividades, documentar decisiones, crear un archivo viviente de la historia colectiva, etc. Se trata de un componente clave del ecosistema de las redes activistas en la actualidad.

Generalmente, la infraestructura digital de los movimientos sociales se compone de diferentes plataformas, herramientas y cuentas que van cambiando a largo del tiempo. Puede haber varias

personas a cargo de diferentes tipos de espacios, cada uno con sus objetivos y comunidades particulares. Algunos pueden ser cuentas personales, otros pueden ser cuentas provisorias creadas para una actividad o algún evento; y otras pueden ser suscripciones y espacios creados específicamente para la reunión de diferentes flujos de información, contenidos y comunidades. Hay que tomarse el tiempo necesario para entender que se trata de un ecosistema: componentes interconectados de la infraestructura compartida de un movimiento. Evaluar los posibles riesgos puede ayudar a dar visibilidad a la responsabilidad y al cuidado colectivo de estos espacios, además de ayudar a desarrollar planes de seguridad.

Para evaluar riesgos relativos a espacios e infraestructura, se deben tener en cuenta las áreas a continuación:

a) Plataformas/herramientas/toma de decisiones

El trabajo de organización de un movimiento social o red activista se basa, en gran medida, en el intercambio de información, así como en una comunicación eficiente. Es necesario analizar los riesgos asociados a las plataformas y herramientas utilizadas, pensar dónde almacenar la información, dado que todo ello puede tener una gran incidencia en la seguridad de las personas, los grupos y el trabajo del movimiento. Al evaluar los riesgos relativos a las grietas de vulnerabilidad y los ataques, puede ser útil considerar si ya existen soluciones feministas/activistas desarrolladas para esa necesidad específica, ya que, en general, esas son las estrategias que más tienen en cuenta los problemas de privacidad y seguridad.

También es importante considerar la accesibilidad y facilidad de uso a la hora de escoger herramientas y plataformas. No siempre vale la pena elegir la solución técnicamente más segura si se requiere una enorme inversión de tiempo y energía para aprender a usarla, dado que muchas veces eso no es posible o no es lo preferible.

- ¿Cuáles son las plataformas, herramientas y espacios que se utilizan? ¿Con qué propósito? ¿Quién tiene acceso a tales recursos?
- ¿Cuáles son los riesgos potenciales asociados a determinadas plataformas/herramientas/hospedaje(hosting) para la necesidad del momento? ¿Cuáles son los impactos de estos riesgos?
- ¿Cuáles son los niveles de conocimientos, habilidades y capacidades necesarias para su adopción adentro del grupo? ¿Cómo se pueden compartir estos saberes y experiencias para no crear una jerarquía interna de poder?

- ¿La plataforma/herramienta es accesible para la mayoría de las personas que necesitan utilizarla? ¿Puede ser que las dificultades de uso terminen creando prácticas más inseguras? ¿Cómo se podría resolver esta situación?
- ¿Se pueden distribuir los riesgos distribuyendo también el uso de plataformas/herramientas para objetivos específicos?

b) Gestión de recursos

La gestión de infraestructura digital compartida es tanto una responsabilidad cuanto un poder y, potencialmente, un sistema de control. Cuánto mayor sea la capacidad de un movimiento o red de transformar este tema en una conversación política sobre valores y marcos compartidos de gobernanza, economía y construcción de la comunidad, más sustentables serán algunas de las prácticas de tecnología colectiva.

- ¿Cómo se gestionará el uso de infraestructura, plataformas y herramientas específicas? ¿Cuál es la economía compartida en tanto a costos derivados del uso y compromiso con determinadas tecnologías?
- ¿Cuáles son los riesgos del uso de plataformas “libres” en relación al control sobre los datos y funcionalidades? ¿Cuáles son los riesgos de los servicios pagos que implican asumir costos por un período sostenido de tiempo? ¿Qué planificación puede ayudar a manejar estos riesgos?
- ¿Y a nivel de las políticas del movimiento o red? Por ejemplo, desarrollo de herramientas en torno a los bienes comunes. ¿Se pueden hacer acuerdos flexibles de cooperación económica? ¿Cómo pueden ser sustentables y transparentes?

c) Administración y protocolos

En el contexto de la organización de movimientos sociales, concebir la infraestructura como un espacio compartido implica saber claramente cómo se gestionan dichos espacios y quién está a cargo de la gestión. Esta perspectiva puede ayudar a ver no sólo cómo ofrecer cuidado colectivo, sino también cuáles son los riesgos potenciales asociados al acceso, el cuidado y la pérdida potencial de información y espacio comunitario.

- ¿Quién tiene control sobre espacios específicos? ¿Cuánto de ello tiene que ver quién es titular del espacio (cuentas personales) o los ajustes? ¿Cuánto tiene que ver con el nivel de conocimientos, los dispositivos o las pre-condiciones de conectividad para tener

acceso?

- ¿Cuales son los riesgos potenciales si ciertos espacios se ven comprometidos? ¿Cuáles serían las fuentes de peligro (amenazas internas y externas) y cuáles serían los impactos posibles? ¿De qué manera se podría planificar para evitarlos?
- ¿Cómo se gestionan los espacios? ¿Cuáles son los protocolos – por ejemplo, cuántas personas tienen acceso administrativo? ¿Dónde están ubicadas (a nivel individual, organización, red)? ¿Qué tan a menudo cambian los protocolos? ¿Cuáles son las condiciones del cambio (por ej, cambio de claves y contraseñas)?
- ¿Existen protocolos sobre la eliminación de espacios o datos? ¿Y protocolos sobre el almacenamiento de datos? ¿Existen prácticas que se puedan discutir y convertir en protocolos?
- ¿Cómo, dónde y cuándo habrá que organizar un diálogo sobre la evaluación de riesgos de la infraestructura digital compartida?
- ¿Quién se hará responsable si hay incidentes dentro de espacios/infraestructura que afectan la seguridad del movimiento o la red?
- ¿Qué cambios en los espacios que usa el movimiento/red (por ejemplo, nuevas políticas de seguridad en plataformas, ciertas tareas de seguridad dejan de cubrirse por alguien, etc.) y en el contexto del movimiento (por ejemplo, cambios de gobierno o leyes, etc.) catalizarán un diálogo más amplio acerca de sus espacios/infraestructuras? ¿Quién dará seguimiento a estos cambios?

3. Datos/información

Producimos y generamos datos e información todo el tiempo cuando organizamos algo. Pueden tener la forma de datos formales o informales, deliberados o accidentales. Otra forma de entender riesgos incrementales es analizando la práctica de datos de una actividad o estrategia específica de alguna red activista. Piensa en este asunto ya sea desde un grupo de trabajo específico dentro de la red o desde la perspectiva de una actividad. Se puede usar también a nivel de una organización o grupo activista donde siempre se están manejando datos.

Es necesario tener en cuenta algunas consideraciones de seguridad para cada fase del ciclo de vida de los datos. La actividad “Ciclo de vida de los datos como forma de entender el riesgo” pone en práctica estos conceptos.

a) Creación/compilación/recolección de datos

- ¿Qué tipo de datos se recolectan?
- ¿Quién crea/compila/recolecta datos?
- ¿Pone en riesgo a personas? ¿Quién estará en riesgo si se dan a conocer estos datos?
- ¿Qué tan público/privado/confidencial es el proceso de recolección de datos?
- ¿Qué herramientas utilizan para garantizar la seguridad del proceso de recolección de datos?

b) Almacenamiento de datos

- ¿Dónde se almacenan los datos?
- ¿Quién tiene acceso al almacenamiento de datos?
- ¿Cuáles son las prácticas/procesos/herramientas que se utilizan para garantizar la seguridad del dispositivo de almacenamiento?
- Almacenamiento en la nube vs almacenamiento físico vs almacenamiento en un dispositivo.

c) Procesamiento de datos

- ¿Quién procesa los datos?
- ¿El análisis de los datos pone en riesgo a individuos o grupos?
- ¿Qué herramientas se utilizan para el análisis de datos?
- ¿Quién tiene acceso al sistema/proceso de análisis de datos?
- ¿En el procesamiento de datos se guardan copias secundarias de los datos en algún otro sitio?

d) Publicación/intercambio de información de los datos procesados

- ¿Dónde se publica la información/conocimiento?
- ¿La publicación de la información puede poner en riesgo a personas?
- ¿Cuáles es la audiencia de la información publicada?
- ¿Tienen control sobre cómo se publica la información?

e) Almacenamiento

- ¿Dónde se archivan los datos y la información procesada?

- ¿Los datos sin procesar se archivan, o sólo la información procesada se guarda?
- ¿Quién tiene acceso al archivo?
- ¿Cuáles son las condiciones de acceso al archivo?

f) Eliminación

- ¿Cuándo se eliminan de manera permanente (purgan) los datos?
- ¿Cuáles son las condiciones de dicha eliminación?
- ¿Cómo podemos asegurarnos de que se borraron todas las copias?

Conclusión

Este documento tiene como objetivo ayudarte a elaborar un panorama conceptual para pensar sobre la evaluación de riesgos desde la perspectiva de la organización de movimientos sociales. Muchas veces, la evaluación de riesgos se realiza desde una perspectiva individual o organizacional. Pensar en la evaluación de riesgos a nivel de un movimiento social o red activista significa ubicarnos como parte significativa, aunque parcial, de una comunidad más amplia.

Esto puede ser útil como territorio compartido para que grupos de personas organizadas de maneras diferentes puedan juntarse y pensar un plan común cuando identifican un contexto, un objetivo o una actividad compartida. También puede ayudar a facilitar procesos de reflexión colectiva sobre la sustentabilidad y la organización. Mediante la anticipación y la planificación, se pueden evitar o enfrentar riesgos relativos a grupos y dinámicas relacionales, donde las tecnologías de la información y la comunicación tienen un papel clave como infraestructura para los movimientos sociales.

Puedes compartir este material como un recurso adicional o elegir estratos específicos para profundizar.

Más lecturas

(Sólo en inglés) Para entender mejor la construcción de movimientos sociales y la organización colectiva, así como las realidades digitales:

- ICTs for Feminist Movement Building: Activist Toolkit: https://genderit.org/resources/icts-feminist-movement-building-activist-toolkit
- Making a Feminist Internet: Movement building in a digital age: https://genderit.org/editorial/making-feminist-internet-movement-building-digital-age
- Achieving Transformative Feminist Leadership: A Toolkit for Organisations and Movements: https://creaworld.org/wp-content/resources/toolkits-and-manuals/Feminist-Leadership-Toolkit.pdf

