Programa de Asesorías en Seguridad y Protección para Personas Defensoras de Derechos Humanos

Brigadas Internacionales de Paz | Proyecto México

Guía de facilitación

pbi
abriendo espacios para la paz

Programa de Asesorías en Seguridad y Protección para Personas Defensoras de Derechos Humanos

Brigadas Internacionales de Paz | Proyecto México

Título:
Programa de Asesorías en Seguridad y Protección para Personas Defensoras de Derechos Humanos – Guía de Facilitación.

Publicado por:
Brigadas Internacionales de Paz – Proyecto México, diciembre 2014.

Coordinación, investigación y edición:
Marianne Bertrand, Erick Monterrosas, Ivi Oliveira

Diseño y maquetación:
Toni Quesada

PBI – México
Medellin 33, Colonia Roma
06700 México, DF
www.pbi-mexico.org

Agradecimientos

Esta guía es el resultado del compromiso y la dedicación de muchas personas que han participado desde sus inicios en el trabajo de Brigadas Internacionales de Paz en México y lo han hecho posible.

De manera especial queremos expresar nuestra gratitud y reconocimiento a las personas defensoras en México que han compartido con PBI su tiempo, sus experiencias y sus estrategias de seguridad. Sus aportes, conocimiento y experiencias compartidas son la base de esta guía. También queremos agradecer a:

- *Los y las voluntarias e integrantes de PBI que durante los últimos 15 años han observado, replicado y mejorado los talleres de seguridad en México facilitados por PBI. En particular a Maude Chalvin, Carla Cavaretta por diseñar y revisar las bases de PASP, a Ben Leather por sus aportes para desarrollar el taller 4 de esta guía y a Elsa Pierre por revisar los contenidos de la presente publicación.*
- *Enrique Eguren y Marie Caraj por haber formado y transmitido desde los inicios del Proyecto de PBI en México la base metodológica y conceptual en seguridad y protección que seguimos divulgando a través de la presente publicación y por haber brindado consejos y asesorías puntuales a lo largo de estos años. Los talleres 1 y 2 de este manual se basan en gran medida en sus enseñanzas.*
- *Liam Mahony y Fieldview Solutions por compartir la metodología sobre la cual desarrollamos el taller 4 del PASP y por sus invaluables consejos.*
- *Este manual es también el resultado de un proceso colectivo de debates y experiencias tanto dentro de PBI como del proyecto con otras personas y organizaciones expertas en temas de seguridad y protección. En este sentido el manual no sería lo que es sin las discusiones e intercambios mantenidos a lo largo de los últimos años con Protection International, Front Line Defenders, Tactical Technology Collective, Sedem, Udefegua, el Comité Cerezo, Accudeh, la Red TdT, Serapaz, Aluna, la Red Nacional de Defensoras de DDHH en México y el Centro de Derechos Humanos Fray Bartolomé de las Casas. Sus aportaciones han sido fundamentales para elaborar y mejorar el PASP y esta guía.*

Índice

Introducción

Esta Guía de Facilitación ha sido pensada para todas aquellas personas integrantes o no de *Brigadas Internacionales de Paz* (PBI por sus siglas en inglés) que buscan compartir herramientas en seguridad y protección con personas y organizaciones defensoras de derechos humanos. Las herramientas propuestas en esta guía se basan principalmente en la experiencia que PBI ha desarrollado a lo largo de más de treinta años para garantizar la seguridad de sus propios equipos de voluntarios y poder proteger efectivamente a las personas defensoras acompañadas en los diversos países donde ha estado presente. En este sentido, el acompañamiento internacional paulatinamente ha buscado compartir herramientas a través de asesorías y talleres. Con la propuesta conceptual y práctica de los talleres presentados en esta guía, PBI busca ofrecer un espacio de intercambio para que las personas defensoras puedan desarrollar sus capacidades para gestionar a largo plazo estrategias propias de seguridad y protección.

PBI abrió su proyecto en México en 1999 y desde entonces está presente en las entidades de Oaxaca, Guerrero, Chihuahua, Coahuila y el Distrito Federal. Desde el 2002 PBI ha compartido herramientas en el tema de seguridad y protección a través de talleres y asesorías a diversos colectivos y organizaciones defensoras de derechos humanos en el país. En un inicio los talleres fueron impartidos y seguidos por la *Oficina Europea de PBI* en Bruselas (BEO). En 2007, al convertirse la BEO en la organización independiente Protection International, el proyecto México de PBI asumió progresivamente la facilitación puntual de talleres de seguridad y los integró como uno de sus ejes de trabajo. A finales del 2009, se consensuó sistematizar estos talleres y formalizarlos en el actual *Programa de Asesorías en Seguridad y Protección* (PASP). Desde entonces el PASP se ha enriquecido y evolucionado a partir de las peticiones de las personas defensoras pero también las necesidades del trabajo de acompañamiento internacional de PBI. En 2012, tras organizar tres talleres de incidencia impartidos por *Fieldview Solutions e*n el norte, sur y centro del país, se retomaron y adaptaron sus contenidos para añadir un cuarto taller enfocado en estrategias de incidencia. En mayo de 2014, un grupo de organizaciones* que comparten herramientas de seguridad y protección con personas defensoras convocaron a una formación de formadores para intercambiar experiencias en la facilitación de talleres e impulsar su efecto multiplicador. Esta guía está encaminada en el mismo sentido, recogiendo el trayecto de aprendizaje conjunto para responder a los desafíos en materia de seguridad y protección de personas defensoras.

En el contexto de creciente riesgo, agresiones y violencia que enfrentan las personas defensoras en México y la deficiente respuesta del Estado para protegerlas, uno de los objetivos principales del PASP de PBI es que las personas defensoras se apropien de los talleres, los adapten y los repliquen. Esperamos que la sistematización del PASP en esta publicación contribuya a esta meta y de esta manera coadyuve a apoyar la valiosa labor en pro de los derechos humanos que llevan a cabo las personas defensoras en México.

* La Formación para formadores fue co-convocada por Serapaz, Aluna, la Red TdT, la Red Nacional de Defensoras de DDHH en México, el Centro de Derechos Humanos Fray Bartolomé de las Casas y PBI México.

Capítulo 1:
Hacia un concepto de seguridad y protección integral: las dimensiones sociopolítica, psicosocial y de género.

1.1 La seguridad y la protección como concepto sociopolítico

Asumimos que el trabajo de las Personas Defensoras de Derechos Humanos (PDDH) es político en esencia y necesariamente conlleva un cierto nivel de riesgo porque atenta contra el status quo; es decir está encaminado a una transformación social y generalmente afecta negativamente los intereses políticos, económicos o militares de otros actores. El Programa de Asesorías en Seguridad y Protección (PASP) se enfoca por ende a riesgos ligados al contexto socio-político en el cual las personas defensoras trabajan y no a riesgos naturales como catástrofes naturales, enfermedades, accidentes, u otros de este tipo.

El contexto-socio político y su análisis son complejos debido a su naturaleza cambiante. En el caso mexicano por ejemplo este contexto se ha visto afectado por coyunturas específicas: elecciones, agendas informativas dominantes, cambios en las estrategias de seguridad federal y estatal involucrando distintos cuerpos gubernamentales armados así como su interacción con otros grupos no estatales que utilizan la violencia como recurso para defender intereses geopolíticos o de control de rutas de migrantes, trasiego de drogas o recursos naturales. Otras coyunturas incluyen la mediatización de ciertas agendas de derechos humanos y la invisibilización de otras, cambios en las relaciones de poder locales, el análisis político de aliados y potenciales agresores respecto a nuestro trabajo, cambio en nuestro perfil en relación a los intereses de otros actores y el costo político, económico o de otro tipo al atacarnos abierta o veladamente. **La seguridad y protección dependen ante todo del contexto sociopolítico particular en tiempo y espacio en el que cada persona defensora trabaja**

Entendemos por **protección** el conjunto de actividades que desarrolla una organización de derechos humanos para garantizar la seguridad de otras personas defensoras

y organizaciones con las cuales trabajan, mientras que con el de **seguridad** nos referimos a todas las medidas y estrategias enfocadas en resguardar la integridad física o psicológica de sus integrantes y que las mismas personas defensoras desarrollan e implementan hacia sí mismas.

Las estrategias de seguridad y protección buscan expandir y mantener abierto tanto nuestro propio espacio de actuación como el de las organizaciones o personas defensoras de derechos humanos con las cuales trabajamos o que acompañamos.

Grafico 1a:
Ampliando el espacio de actuación

Consideramos que el espacio de actuación[3] de una persona defensora depende primordialmente de tres elementos:

1. **Su nivel de exposición a amenazas** y hasta qué punto la PDDH y su organización priorizan políticas de seguridad y protección para reducir sus vulnerabilidades y aumentar sus capacidades.
2. **La medida en que su trabajo es aceptado o tolerado** y considerado legítimo por otros actores.
3. **La medida en que puede disuadir ataques** (porque un ataque en su contra tendría un costo político demasiado alto para el agresor) o incluso persuadir al agresor de los beneficios políticos de no atacar o violar los derechos humanos.

Por espacio de actuación entendemos la *"variedad de posibles acciones que puede realizar un defensor exponiéndose a un riesgo personal aceptable".*[1] Es decir que cada persona defensora percibe una gama de actuaciones posibles y asocia a cada una de estas un cierto costo o beneficio y una serie de consecuencias aceptables o inaceptables.[2] El "riesgo personal aceptable" es relativo y cambiante. Es una interpretación que cambia en el tiempo y según el contexto. Se basa en percepciones y proyecciones que dependen de las experiencias propias de la persona defensora y del análisis racional pero en parte también subjetivo que cada PDDH tiene de su realidad. De lo anterior se entiende que el "riesgo personal aceptable" varía de una persona defensora a otra. Nuestra experiencia en el contexto mexicano demuestra que mientras que para algunas personas defensoras las amenazas pueden ser el máximo aceptable, otras son incluso aquiescentes a no detener su trabajo político aun al precio de ser encarceladas o han continuado su labor después de ser torturadas. Esto no implica que el primer grupo esté "menos comprometido" respecto a aquellas PDDH que arriesgan más o que su análisis de riesgo es superior *per se*, sino que debemos ser sensibles y respetuosos a las diversas formas de entender lo que representa un "riesgo aceptable" para cada persona defensora y proveer elementos para que ellas mismas puedan repensar sus nociones de riesgo utilizando herramientas analíticas sólidas. Por ende, **las estrategias de seguridad y protección deben entenderse de forma amplia, tomando en cuenta estos tres elementos: cómo reducir el nivel de exposición a amenazas (reducir las vulnerabilidades y aumentar las capacidades), cómo aumentar el nivel de aceptación y cómo disuadir ataques**. Además, dichas estrategias de seguridad y protección no deben limitarse a manera de protocolos, planes o medidas aisladas sino que deben involucrar o

transversalizar otros aspectos fundamentales de nuestra labor. Otros ejes de trabajo que aparentemente no tienen un componente de seguridad intrínseco como los principios con los que trabajamos, nuestras estrategias de incidencia, nuestra forma de organizarnos interna y externamente, en realidad afectan la forma en la que el espacio de actuación puede ser ampliado.

Se puede lidiar con el riesgo de distintas formas: aceptándolo, reduciéndolo o evitándolo. **Una buena estrategia de seguridad debería sin embargo a largo plazo no limitar el trabajo sino tener como objetivo que la persona defensora haga todo lo que hace con más seguridad y permitirle incluso expandir su actividad.**

1.2 La seguridad y la protección y sus intersecciones con la esfera psicosocial

Además de la esfera sociopolítica, las estrategias de seguridad y protección se complementan con la dimensión psicosocial. Esta dimensión integra factores que abordan desde la experiencia individual, el ámbito familiar, comunitario, organizativo y social amplio de las PDDH.[4] El análisis psicosocial busca generar prácticas respetuosas del bienestar emocional así como de las construcciones socioculturales y subjetivas en todos los ámbitos de vida de las PDDH construyendo dinámicas alternativas de seguridad y protección. En un segundo plano, la dimensión psicosocial busca afrontar positivamente las afectaciones a la salud mental y el desgaste organizativo mientras impulsa estrategias de autocuidado y de reconstrucción del tejido social en las comunidades con las que trabajamos.

Gráfico 1b:
Niveles de análisis psicosocial
en seguridad y protección

La integración de la perspectiva psicosocial en seguridad y protección propone:

- **Recuperar experiencias subjetivas individuales y colectivas para que la seguridad y la protección coadyuven a resarcir el tejido social**. Implica incorporar las apropiaciones y vivencias de las PDDH en cualquier estrategia de seguridad y protección; sus búsquedas de sentido personal y su trayectoria organizativa. También se deben tener en cuenta los agravios específicos que sufren las comunidades de personas defensoras y cómo han reinterpretado estas experiencias para repensar medidas que subviertan distintas formas de violencia hacia ellas. Desde esta perspectiva, un análisis de seguridad y protección debe resaltar no sólo las consecuencias negativas de la represión, u otros tipos de violencia sino que también debe de visibilizar, valorar lo que se ha aprendido individual y colectivamente en términos de fortalezas. Esto implica rescatar las formas de afrontamiento, las distintas visiones del mundo, las construcciones y narrativas sobre la conformación grupal u organizativa e incluso los ritos que hasta ahora les han servido. Las estrategias y tácticas diversas creadas por las personas defensoras incluso antes de recibir cualquier asesoría formal sobre seguridad y protección tienen una función fundamental para romper el silencio, generar cohesión, resistencia, y solidaridad. Estas estrategias existentes en todo entramado organizativo o proceso de resistencia individual son consideradas como capacidades y por ende deben ser recuperadas para expandir los espacios de actuación de las PDDH.

- **Dimensionar la salud mental, incluyendo el bienestar emocional, la frustración o el estrés como factores cruciales que deben ser abordados de manera constante.** Los ámbitos de seguridad y protección abordan situaciones delicadas; angustias, culpas ante una "falla" en seguridad, experiencias post-traumáticas, toma de testimonios que reviven situaciones asociadas con miedos u otro tipo de sentimientos difíciles. Estas cuestiones afectan nuestro trabajo cotidiano y la forma en la que analizamos o respondemos ante incidentes de seguridad. De la misma manera quien trabaja de forma "indirecta", por ejemplo sin estar expuesto en primera persona a las experiencias de represión, amenaza etc. por el solo hecho de trabajar con estos temas tendrá también que pensar en espacios personales y colectivos para desahogar y hablar de las dificultades de "cargarse" con las historias y dificultades de los demás. Este tipo de abordaje implica establecer intervenciones no sólo en momentos posteriores a un incidente de seguridad o una situación límite de estrés o violencia, sino generar un trabajo preventivo de autocuidado que incluya el bienestar emocional, la contención y "descarga" del estrés cotidiano y el acumulativo. Un abordaje óptimo de estas dimensiones contribuye a fortalecer las capacidades de respuesta y a reducir vulnerabilidades de las personas defensoras al sentirse "cobijadas" y apoyadas.

- **Entender cómo pueden afectar tanto positiva como negativamente las medidas de protección y seguridad el entorno inmediato de las personas defensoras y sus relaciones a nivel familiar y comunitario.** En muchas ocasiones los talleres del PASP generan consciencia y cambios directos en las estrategias de las personas defensoras. Idealmente el impacto de estos cambios es positivo, sin embargo se deben contemplar también los impactos negativos de este tipo de estrategias. Por ejemplo una medida de seguridad digital que restringe ciertos canales de comunicación por su vulnerabilidad tecnológica o que propone la evacuación de una persona defensora de su comunidad para resguardar su integridad física, puede por otro lado repercutir negativamente en términos de generar aislamiento familiar o propiciar un desarraigo de la comunidad. Ponderar el beneficio de medidas de seguridad, protocolos específicos etc. en este tipo de ecuación no es una cuestión simple con respuestas automáticas. En todo momento se deberán tener en cuenta los impactos de estos cambios en relación con los hábitos y las dinámicas en varias esferas de vida de las personas defensoras.

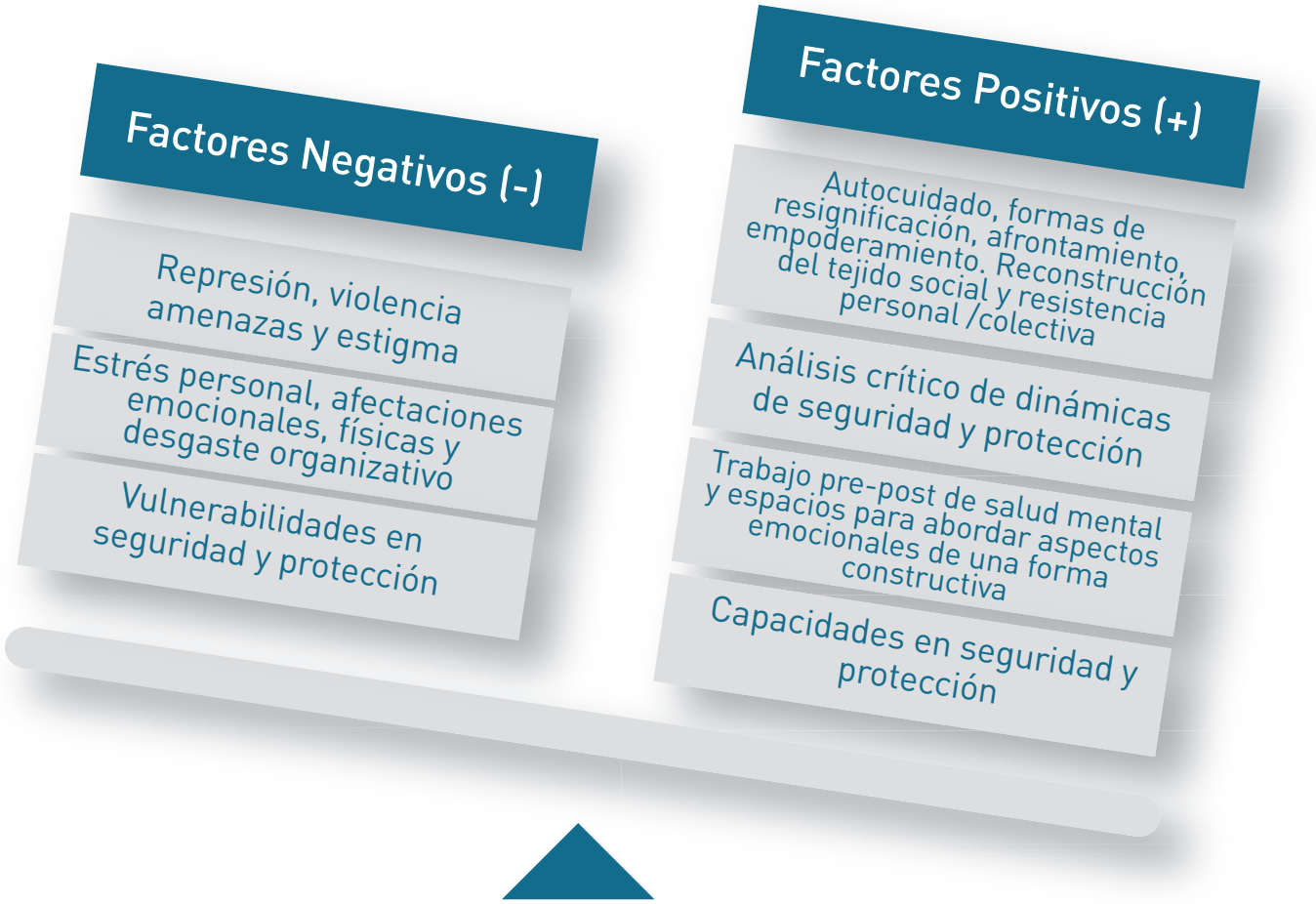
Pensar en las construcciones socioculturales en torno al trabajo que realizan las personas defensoras para que las estrategias de seguridad y protección se adapten a este entorno. El trabajo en seguridad y protección requiere de una comprensión profunda del entorno en el que viven y trabajan las PDDH. Para lograr lo anterior es necesario cuestionar nuestro propio bagaje cultural y ampliar las posibilidades de diálogo más allá de una simplificación de valores universales en los procesos de trabajo en torno a la seguridad y protección. En muchos casos los esquemas de trabajo "eficientes" o de "resolución directa de un problema" pueden ser agresivos con entornos particulares de trabajo en los que imperan cosmovisiones diferentes. El "peso específico" de ser una persona defensora en la comunidad, la construcción de la memoria histórica en las comunidades a partir del entendimiento cultural del silencio o la denuncia así como los estigmas asociados con el trabajo son factores que deben ser comprendidos. Por ejemplo mientras que ser PDDH en ciertos entornos culturales es visto por la comunidad como un orgullo, en otras existe también una deslegitimación cultural de la misma labor al ser considerados como "revoltosos" o aquellos que no quieren la paz por "andar removiendo heridas pasadas", buscar conflicto, "lavar la ropa sucia fuera de casa", etc. En algunos contextos culturales la normalización de la impunidad viene acompañada con un estigma cultural que extiende la culpa social sobre las víctimas y defensores; por ejemplo cuando hay represalias sobre una comunidad indígena entera por el trabajo de un sector de la comunidad.

Asumir la seguridad y la protección como una esfera que trabaja sobre el análisis de aspectos intra e inter organizacionales delicados. Las estrategias de seguridad y protección enfocadas al entorno organizativo operan en dos niveles: a) Intra-organizativo e b) Inter-organizativo. El primer nivel se refiere a los ámbitos al interior de una organización como la manera en que se distribuyen las responsabilidades, las funciones (formales e informales), cómo operan los procesos de toma de decisiones, los mecanismos de comunicación y los protocolos de prevención y respuesta ante incidentes de seguridad. El segundo nivel implica las relaciones de la organización con otras organizaciones, coaliciones y actores aliados, por ejemplo en la toma de decisiones colectivas más allá de una organización. Este segundo ámbito incluye por ejemplo la activación de redes de alerta, prevención y comunicación que involucran a varias organizaciones, etc. Un análisis de la operatividad en los niveles intra e inter organizativos requiere una evaluación de la horizontalidad-verticalidad en los procesos de toma de decisiones, la claridad de los roles y responsabilidades, los modelos de trabajo colaborativo y comunicación así como las fuentes de conflictos y desgaste organizativo que puedan obstaculizar esquemas de seguridad y protección. El análisis psicosocial privilegia formas constructivas de abordar conflictos o replantear las estrategias intra e inter organizativas en aras de generar formas de cooperación basadas en la transparencia, la equidad, la confianza y la solidaridad.

Cuestionar de forma crítica las dinámicas de acompañamiento en los esquemas de seguridad y protección. El acompañamiento en seguridad y protección puede dañar más de lo que beneficia si no establecemos canales de comunicación horizontales y sensibles con las PDDH quienes tienen que ser las protagonistas de su propio análisis. Los procesos de acompañamiento deben ser abordados desde una perspectiva crítica en contra de valores de superioridad o dominación derivados de ideas neocolonialistas que pugnan por "proteger", "brindar seguridad" de forma paternalista, "rescatista" o revictimista hacia las PDDH. Este punto es particularmente delicado cuando involucra interacción entre PDDH locales y extranjeros, en comunidades indígenas que históricamente han sido agraviadas o que plantean interacción entre organizaciones de entornos urbanos con acceso a más recursos y otras de entornos rurales marginados. Al conceptualizar y analizar la seguridad y protección se deben abordar las asimetrías de poder históricas y actuales, las diferencias en capacidades y las implicaciones

que estas tienen para generar un esquema de trabajo que equilibre estas condiciones. Se debe transitar hacia una posición de acompañamiento horizontal y recíproco más allá de concebir simplemente a las personas defensoras como "víctimas que reciben ayuda" o personas pasivas que carecen por completo de estrategias de seguridad y protección, ya que en todos los casos se encontrarán este tipo de estrategias propias incluso si no han sido conceptualizadas como tales previamente.

Gráfico 1c:
¿Hacia dónde queremos ir? Modelo ideal de trabajo en seguridad y protección desde la perspectiva psicosocial



1.3 La seguridad y la protección desde la transversalización de la perspectiva de género

Nuestro análisis de seguridad y protección no existe como una perspectiva neutral frente a la dimensión de género. Esto quiere decir que al aplicar el marco general analítico de seguridad y protección, debemos contemplar las inequidades estructurales y contextuales en las cuales operan patrones de exclusión, de imposición de normas distintas para lo que es aceptado como lo "masculino" y lo "femenino". Este enfoque ahonda en los patrones de violencias segmentadas y específicas para mantener esquemas de control y sus desafíos en relación con las estrategias de seguridad y protección. Además de clarificar inequidades de género a nivel analítico, la transversalización de la perspectiva de género provee herramientas prácticas en seguridad y protección para transformar las esferas individuales y organizativas de las PDDH en entornos más igualitarios e inclusivos.

La transversalización de la perspectiva de género en seguridad y protección requiere:

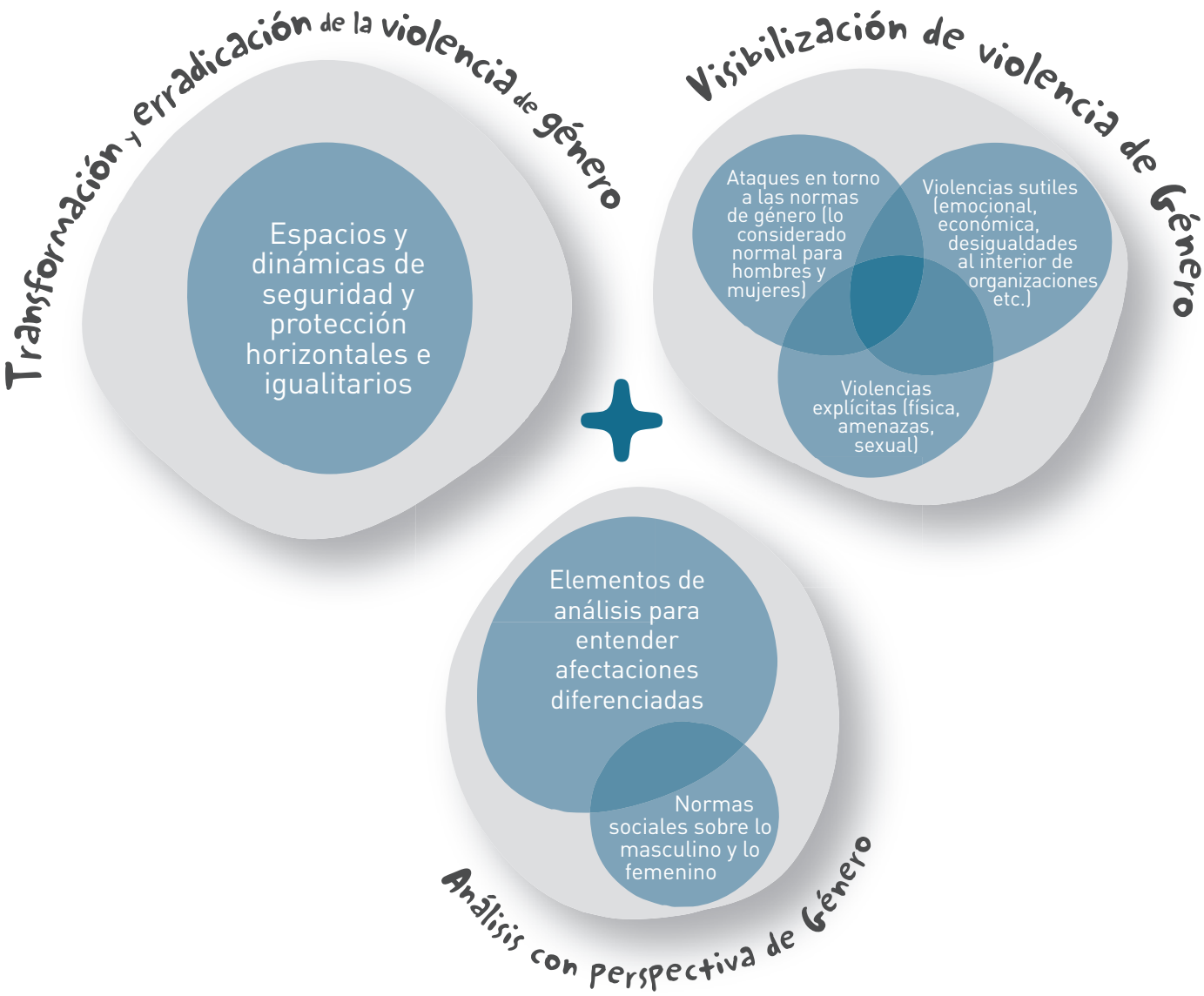
Entender el género como una construcción sociocultural que establece lo que es permisible para hombres y mujeres. Al elaborar un análisis en los ámbitos de seguridad y protección se deben tener en cuenta las normas de género imperantes en las distintas comunidades de PDDH con las que se trabaja. Estas normas de género tienen que ver con lo que se espera o se considera normal o anormal para un hombre y una mujer respectivamente; qué reacciones, comportamientos, actitudes y valores "deben" de guardar tanto en los espacios públicos como en los privados. En el caso de las defensoras por ejemplo, su involucramiento en el trabajo asociativo puede chocar con lo que se espera de ellas en la familia, la comunidad e incluso al interior de las organizaciones, etc. En el caso de los hombres un análisis de género puede ayudar a comprender mejor las nociones de riesgo asociadas culturalmente a lo que se cree que deben "soportar los hombres" por ejemplo al trabajar en un contexto en el cual hablar de los miedos es considerado signo de debilidad y por ende menoscabo de la masculinidad. En este sentido las vulnerabilidades y capacidades específicas de las PDDH están estrechamente relacionadas con estas construcciones sociales de género ya que expanden o limitan las formas de acción en contextos específicos.

Incorporar variables específicas e información con perspectiva de género al análisis de seguridad y protección tanto a nivel de indicadores como estructural. Las estrategias de protección parten de un diagnóstico de seguridad y un análisis de riesgo para tomar decisiones informadas. En la medida en que este diagnóstico incorpora información desagregada por sexo, indicadores de género en los sistemas de registro de agresiones y otra enfocada a resaltar las disparidades estructurales, se podrán tomar mejores decisiones para revertir las desigualdades y responder más adecuadamente a los desafíos en seguridad. Por ejemplo se pueden efectuar análisis de formas diferenciadas de agresiones dirigidas a mujeres y correlacionar esta violencia con su incidencia en mujeres cuyo trabajo desafía normas de género predominantes, la tolerancia de su comunidad ante este tipo de agresiones, etc. Al evaluar seguridad y protección se deben analizar los impactos de las desigualdades creadas por distintas medidas a nivel estructural. Sin un análisis de variables específicas de género o de condiciones de exclusión a nivel

macro se pueden llegar a reproducir dinámicas patriarcales. Un esquema de protección con este tipo de fallas puede llevar a la idea de "protección" estableciendo que las mujeres deben de restringir salidas a lugares públicos en comparación con los hombres, reforzando ideas falsas de debilidad o que en una organización las mujeres deberían de ser "cuidadas" por sus compañeros perpetuando de esta manera la desigualdad para tomar en sus manos cuestiones de seguridad en sus organizaciones.

Visibilizar y revertir las formas de violencia basada en normas de género. Un análisis de seguridad debe clarificar los tipos de violencia de género que sufren las comunidades de PDDH con el fin de erradicarla. Generalmente la violencia de género refuerza el mensaje de lo que es normal y anormal para hombres y mujeres y se "justifica" porque se basa en las normas de género socialmente aceptadas. Por ejemplo se dan casos de amenazas hacia las mujeres defensoras con patrones de violencia psicológica, o que van encaminadas a desprestigiar el ejercicio de su sexualidad para devaluarlas ante su comunidad representándolas como "malas mujeres" o "machorras" sea porque participan en la vida pública, porque se alejan del ideal familiar o porque desafían otras normas que son las aceptadas para las mujeres de su entorno. En otras ocasiones la

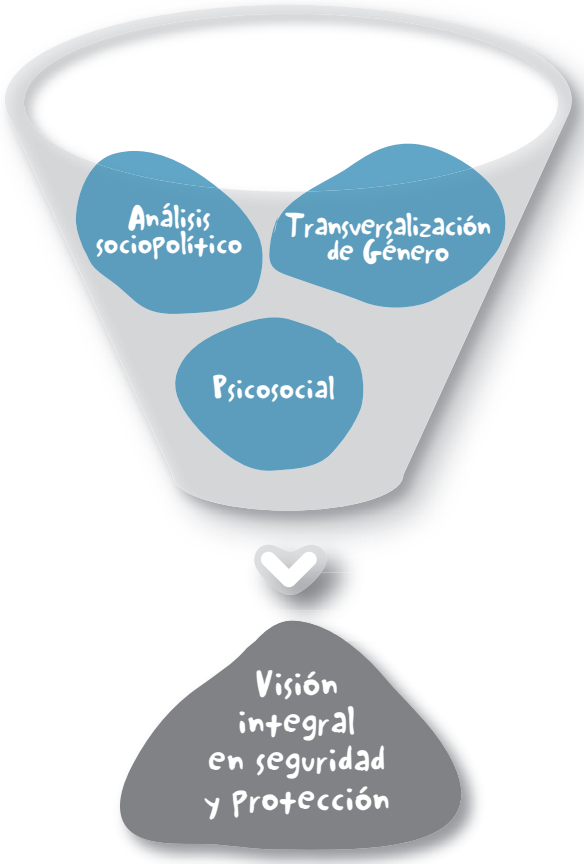
Gráfico 1d
Tranversalizar la perspectiva de género en seguridad y protección



violencia de género no sólo puede venir de fuera, sino que puede estar arraigada también al interior de las organizaciones; por ejemplo cuando las opiniones de colegas mujeres defensoras no son tomadas en cuenta de la misma manera que la de los hombres o cuando a las mujeres se les trata como subordinadas. Es importante tener en cuenta que la violencia de género puede ir también dirigida a hombres al enviar un mensaje de terror a través su "feminización", como en el caso de algunas agresiones a PDDH de grupos que luchan por derechos de minorías sexuales. Por ejemplo hombres defensores que no cumplen con normas de género asociadas a lo entendido como masculino tradicionalmente, pueden ser hostigados y violentados a través de acciones que reproducen formas o mensajes similares a los de la violencia machista. En conjunto con las personas defensoras es recomendable abordar y entender las distintas formas en que se puede ejercer la violencia de género; desde las más explícitas hasta las más sutiles para "desmenuzar" sus componentes y dejar claro cómo opera esta violencia. Al visibilizar estos patrones, sus causas y consecuencias en relación con los dominios de seguridad y protección las personas PDDH estarán en mejor posición para erradicar este tipo de violencia y sus consecuencias negativas.

Promover una transformación de las estructuras sociales y los entornos organizativos para transitar hacia la justicia y la igualdad. Las inequidades de género operan no sólo mediante la reproducción del machismo por parte de los hombres, sino que en algunas ocasiones son reproducidas también por mujeres. Por ello, además de la participación de más mujeres en organizaciones se necesitan también de liderazgos alejados de los esquemas de poder patriarcales. Este tipo de liderazgos igualitarios deben servir para desafiar estructuras de poder y catalizar el cambio social incluyendo con dignidad y respeto a los grupos tradicionalmente marginados por las estructuras de género. Procesos relacionados con el análisis, implementación y evaluación en seguridad y protección pueden detonar cuestionamientos y transformaciones positivas para generar esquemas organizativos más igualitarios, protocolos y líneas de acción más inclusivas o para que las mismas personas defensoras "pongan sobre la mesa" las asimetrías existentes tanto en su trabajo cotidiano, como en su vida privada, ambas esferas relacionadas con sus capacidades y vulnerabilidades. Para lograr transformaciones positivas se deben impulsar las soluciones y fortalezas desde el trabajo de grupos de mujeres en la comunidad o impulsando estrategias de minorías que cuestionan los modelos de masculinidad o género tradicionales. En muchos casos este tipo de estrategias relacionadas con la seguridad y la protección como la solidaridad, el autocuidado, el foco en la diversidad al interior de colectivos, etc. proporcionan una visión igualitaria que puede tener un efecto multiplicador al transformar otras formas de acción grupal. Este tipo de modelos pueden ser un referente para consolidar la seguridad organizativa al tiempo que se detonan transformaciones en las jerarquías de género tanto a nivel individual como organizativo.

Gráfico 1e
Componentes analíticos necesarios para un esquema integral de seguridad y protección



Capítulo 2:
El Programa de Asesorías en Seguridad y Protección (PASP)

2.1 Criterios del PASP

El Programa de Asesorías en Seguridad y Protección precisa de algunos criterios básicos que guían su implementación:

No injerencia

Las asesorías se realizan a petición de las organizaciones y personas defensoras y no buscan injerir en su trabajo sino más bien ofrecer un espacio de reflexión para que las PDDH participantes puedan desarrollar sus propias capacidades y autogestionar su seguridad. En otras palabras, las asesorías están pensadas como espacios para que las PDDH encuentren por sí mismas las respuestas que les sirvan. Se debe asumir que las PDDH son quienes conocen mejor su contexto, su trabajo y por ende están en la mejor posición para valorar su riesgo y definir sus propias medidas de seguridad y estrategias de protección. Todas las personas y organizaciones defensoras tienen estrategias de seguridad exitosas y rescatables y eso explica en parte que las PDDH sigan realizando su labor a pesar de obstáculos y adversidades. El PASP no busca sustituir las estrategias y tácticas ya existentes, sino ofrecer un espacio donde se puedan compartir y conocer herramientas adicionales para evaluarlas y complementarlas. En este sentido es muy importante que las asesorías eviten imponer una visión categórica o rígida sobre la seguridad y la protección. Las asesorías se deben limitar a proponer herramientas, metodologías y técnicas que puedan coadyuvar a los procesos y caminos escogidos por las PDDH.

Metodología participativa

La metodología de los talleres es participativa y requiere la implicación activa de las PDDH y de miembros de todos los niveles y áreas de la organización. La razón por la que creemos que todas las personas deben estar implicadas es porque:

- El análisis al que podemos aspirar es más completo y permite contemplar y discutir todas las ideas y soluciones posibles así como tomar en cuenta distintos puntos de vista y opiniones
- Se fomenta un buen clima de colaboración e interrelación con el grupo y se implica a todo el grupo para alcanzar los acuerdos adoptados
- Si todas las personas participan en la generación de consensos es más probable que se apropien de las decisiones que se tomen y de las reglas que se definan, además de asegurar un mayor compromiso con su implementación
- Las estrategias de seguridad son efectivas si todas y todos las implementan activamente. Cada organización tiene la responsabilidad de que sus integrantes sepan qué nivel de riesgo enfrentan. Los incidentes de seguridad y la situación general de seguridad de la organización afectan áreas incluso si estas no trabajan directamente con temas de riesgo (administración, contabilidad, servicio social, etc.).

Apego a la realidad

Los talleres son una combinación de presentaciones, trabajo sobre casos reales e hipotéticos y dinámicas en grupo que buscan acordar el nivel de riesgo enfrentado y consensuar procesos para prevenir y responder a este riesgo. Siempre intentaremos tener en cuenta las limitaciones reales que tiene el trabajo en el terreno. Buscamos que las estrategias de seguridad y protección se construyan en conjunto con PDDH se mejoren teniendo en cuenta su contexto, cultura, estrategias y tácticas que estas personas han desarrollado previamente y que les han sido útiles en su trabajo y entorno. No sirve de nada definir procesos o reglas que por el contexto en que trabajamos de antemano sabemos nunca se podrán cumplir.

¡No hay respuestas mágicas!

Los talleres buscan compartir herramientas de análisis, metodologías y métodos para analizar el riesgo y con base en ello definir procedimientos de seguridad y estrategias de protección para las personas defensoras. El riesgo depende del contexto, de las características propias y de las capacidades que cada defensor o defensora ha desarrollado con base en sus experiencias. No hay fórmulas mágicas o "recetas" predefinidas; lo que puede ser adecuado y útil en ciertos contextos puede no serlo para otros. Los talleres y reuniones del PASP buscan acompañar una reflexión y mejora de las estrategias de seguridad y protección y por ello no brindan "tips" que se puedan aplicar para resolver automáticamente una situación de riesgo. El PASP intenta abrir una serie de procesos que pueden ser tardados y también tener avances y retrocesos.

Del análisis a la estrategia

Como se mencionó en el apartado conceptual, el espacio de actuación de cada persona u organización defensoras de derechos humanos, su nivel de riesgo y aceptación al mismo son relativos y cambiantes. La metodología que usa el PASP parte de un diagnóstico de seguridad y un análisis de riesgo para tomar decisiones informadas; es decir acordar si se puede aceptar el riesgo, si es necesario mitigarlo o como última alternativa, evitarlo. Si el riesgo puede mitigarse propone herramientas para desarrollar estrategias de seguridad y protección que permitan reducirlo.

La importancia del seguimiento más allá de los talleres

Después de brindar un taller se debería procurar acordar con las PDDH participantes si necesitan seguimiento y de qué tipo. La seguridad y protección no se pueden limitar solamente a un *plan de seguridad*, sino que tienen que transitar hacia una estrategia integral de implementación. Esto requiere que todas las personas se apropien del proceso y sobre todo que se implementen las reglas, estrategias y políticas a nivel organizacional consensuadas al finalizar los talleres. Por ello es necesario reconocer de antemano que un taller no basta para lograr todo lo anterior y que para cambiar hábitos a nivel individual y organizativo se necesitan mecanismos efectivos de seguimiento a los procesos acordados. Para lograr los cambios necesarios se requiere de procesos de seguimiento posteriores al PASP que logren consolidar la transversalización de las estrategias en las labores cotidianas de defensa de derechos humanos.

2.2 Objetivos y resultados esperados del PASP

Cada taller o asesoría del PASP tiene sus objetivos propios (ver detalle de módulos), sin embargo todos parten de un piso mínimo en común para generar un espacio de reflexión y análisis que:

- **Concientice sobre la trascendencia de considerar la seguridad** como una aspecto fundamental, enfatizando su función para continuar el trabajo cotidiano de las PDDH.
- **Propicie el intercambio de experiencias, herramientas, metodologías y técnicas** tanto entre personas facilitadoras y participantes como entre participantes mismas que puedan ser retomadas para el diseño de estrategias de seguridad y protección.
- **Resulte en el diseño de estrategias de seguridad y protección sostenibles**, realistas y adaptadas a los riesgos inherentes a la defensa de los derechos humanos en México.
- **Integre transversalmente la dimensión sociopolítica, psicosocial y de género** a las estrategias de seguridad y protección en la defensa de los derechos humanos.
- **Promueva transformaciones en la gestión de la seguridad y la protección** tanto a nivel individual, grupal como a través de políticas institucionales.
- **Multiplique el impacto**, ya sea porque implica cambios positivos en la estrategias de protección al interior de la organización, con otras PDDH acompañadas u organizaciones aliadas, o bien porque las personas participantes adapten y repliquen los talleres.

2.3 Fases del PASP

El PASP es un proceso estratégico que va más allá de los talleres aislados. Por ello, el PASP implica un trabajo a mayor profundidad y requiere trabajo pre y post talleres.

Grafico 2a:
Fases del PASP

Fase 1 Antes de los talleres:
Reuniones previas a los talleres con la organización o las personas defensoras participantes para entender su contexto, conocer sus necesidades, acordar contenidos, formatos, tiempos, prioridades y compromisos mínimos para iniciar el proceso.

Fase 2 Durante los talleres:
Durante los talleres: compartir herramientas y metodologías para definir conjuntamente procesos de mejora de seguridad y protección.

Fase 3 Después de los talleres:
Después de los talleres: reuniones para dar seguimiento a la implementación de los acuerdos alcanzados durante los talleres o asesorías puntuales para profundizar el entendimiento de una herramienta en particular.

2.4 Estructura general de los talleres del PASP

El PASP propone cuatro talleres.[4] El taller 1 y 2 son considerados básicos, mientras que el 3 y 4 son autónomos y de profundización opcional. Los cuatro talleres se pueden brindar secuencialmente o de manera intercalada como se explicará más adelante.

Taller 1 — Riesgos de las personas defensoras de derechos humanos en México y diagnóstico de seguridad

Descripción general:

Taller de introducción que busca que los participantes tomen consciencia del hecho que las PPDH enfrentan situaciones de riesgo en México. Propone conceptos y herramientas para entender y analizar el riesgo particular de las PDDH participantes a través de un diagnóstico de seguridad. Este diagnóstico es importante porque a partir del mismo se podrán diseñar estrategias de seguridad adaptadas y acertadas para el perfil de las PDDH y el nivel de riesgo que estas están dispuestas a aceptar.

Al final del taller las personas participantes deberían ser capaces de:

- Ser conscientes sobre la importancia de trabajar el tema de seguridad y protección en la organización.
- Poseer una serie de herramientas para analizar su nivel y tipo de riesgo específico.
- Tener una mejor idea de qué amenazas deberían priorizar para tener en cuenta en una estrategia de seguridad.
- Decidir qué estrategia podrían adoptar ante su nivel de riesgo específico y las distintas opciones sobre el mismo (si es aceptable, se debe reducir o hay que evitarlo).

Taller 2 — Estrategia y Plan de Seguridad

Descripción general:

Taller de seguimiento que se enfoca en la gestión de la seguridad a nivel organizativo. Con base en el diagnóstico realizado en el Taller 1, durante el Taller 2 se pretende brindar conceptos y herramientas a las PDDH para que comiencen a diseñar su propia estrategia y *plan de seguridad*. Este taller aborda la importancia de desarrollar estrategias que incidan sobre la fuente misma de la amenaza y transita hacia los primeros pasos para la creación de un primer bosquejo de un *plan de seguridad*. Para ello, subraya la necesidad de establecer espacios, responsabilidades y recursos que permitan refinar la gestión organizativa de la seguridad a través de sus distintas etapas (planificación, implementación y evaluación del *plan de seguridad*).

Al final del taller 2, la organización debería:

- Tener claro que ante el riesgo se pueden adoptar varias estrategias de seguridad pero que todas buscan que el espacio de actuación en defensa de los derechos humanos sea ampliado.
- Visualizar las distintas opciones ante el riesgo como son: incidir directamente sobre la amenaza y/o trabajar la propia exposición a la amenaza.
- Esbozar un *plan de seguridad*.
- Tener un primer borrador de un Plan de Emergencia
- Realizar una evaluación de la gestión de la seguridad al nivel personal e institucional.
- Estar conscientes que todo lo anterior no sirve si no se establecen espacios, responsabilidades y recursos para planificar, implementar y evaluar la seguridad.

Taller 3 — Manejo de Información Sensible

Descripción general:

Enfocado a los tipos de riesgo específico relativos al manejo de la información sensible. Este taller condensa y adapta las herramientas y los procesos desarrollados en los talleres 1 y 2 en relación con la problemática particular del manejo y comunicación de información de forma segura. Cabe destacar que este taller no es una capacitación técnica ni un laboratorio de prácticas en seguridad digital.[5] El taller replica las herramientas para analizar el riesgo específico de la organización respecto al manejo de la información y con base en este pensar en medidas de seguridad que puedan reducirlo.

Al final del taller las personas participantes deberían ser capaces de:

- Profundizar el diagnóstico de la seguridad de la información de la organización iniciado durante el taller.
- Tener una visión amplia de la seguridad de la información: desde las sedes, hasta el almacenamiento y las comunicaciones.
- Elaborar una política sobre comunicación y manejo de información sensible, considerando tanto la seguridad física de los integrantes de la organización como la protección de la información.

Taller 4 — Generando estrategias de incidencia que coadyuven a la seguridad de la organización

Descripción general:

Se enfoca en una herramienta específica que toda estrategia de seguridad debería valorar: la incidencia. Este taller surge de las necesidades del acompañamiento internacional, y fue pensado para que PBI y las PDDH acompañadas pudieran coordinar y acordar sus estrategias de incidencia con el fin de maximizar la protección que brinda el acompañamiento de PBI. El taller busca compartir buenas prácticas y herramientas para crear estrategias de incidencia exitosas que amplíen el espacio de actuación de la organización participante. Este taller puede enfocarse directamente en la seguridad y protección (por ejemplo ¿cómo influenciar potenciales agresores o responsables de la protección de las PDDH?) o en otros objetivos políticos (por ejemplo lograr que el Gobierno implemente una consulta en una comunidad afectada por un megaproyecto). Los aspectos de incidencia a trabajar en el taller no están restringidos exclusivamente al ámbito de seguridad y protección sino que abordan las estrategias más amplias de trabajo político de las PDDH.

Al final del taller las personas participantes deberían ser capaces de:

- Identificar buenas prácticas de incidencia.
- Poseer una metodología para desarrollar estrategias de incidencia que contemple mapeos de actores y de pistas de influencia.
- Tener la base de una estrategia de incidencia (en el tema que hayan decidido previamente).
- Ser capaces de identificar a los actores más relevantes para el fortalecimiento político, técnico y de seguridad de la organización a nivel nacional e internacional.

Adicionalmente, si el taller se da con el objetivo de establecer una incidencia conjunta entre la organización facilitadora y la organización peticionaria, al final de este taller se debería establecer la base de una estrategia coordinada.

La lógica secuencial de los talleres.

Los talleres básicos (1 y 2) comparten metodologías para mejorar y gestionar la seguridad dentro de una organización en cuatro fases.[6] El Taller 1 brinda herramientas para la primera fase del proceso (diagnóstico) y el Taller 2 para las tres fases subsecuentes (planificación > implementación > evaluación). Se recomienda brindar ambos talleres de forma consecutiva.

Se debe advertir a las PDDH que si deciden tomar los talleres 1 y 2 ¡no saldrán automáticamente con el proceso hecho! Como explicamos anteriormente, los talleres proponen herramientas pero no aportan soluciones mágicas para gestionar la seguridad. El trabajo de desarrollo y mejora de una política de seguridad toma tiempo y solo lo puede llevar a cabo la misma organización. La persona facilitadora está allí para brindar las asesorías, apoyar ese proceso, clarificar o profundizar las herramientas compartidas en los talleres pero no para sustituir el proceso o "hacer" el trabajo de la organización.

Los talleres 3 y 4 están pensados para profundizar y aplicar las herramientas básicas en temas específicos, concretamente en incidencia y manejo de información. Los talleres opcionales 3 y 4 son independientes de los primeros talleres básicos a pesar de que se basan en el mismo piso conceptual.

Grafico 2b
Método de Gestión de la seguridad

Gráfico 2c
Sugerencias sobre la secuencia de los talleres

Capítulo 3:
Facilitación del PASP

3.1 Antes de los talleres

Sondeo y preparación conjunta de las asesorías con las PDDH peticionarias

Es importante tener al menos una reunión previa con las PDDH peticionarias para entender la audiencia, el contexto en el que trabajan y con base en ello poder proponer un taller adaptado a las necesidades específicas de las y los participantes. Durante la reunión previa se puede realizar una breve presentación del PASP; sus módulos, objetivos y metodología, así como enfatizar el proceso de seguimiento posterior a los talleres y la necesidad de compromiso por parte de la organización o las PDDH peticionarias. Hay que acordar la confidencialidad y dejar claro que toda la información que se intercambie antes, durante y después del taller será tratada como información sensible y no será publicada o divulgada con otras partes.

En este punto también hay que definir canales de comunicación y quién será la persona de contacto y enlace para la preparación y seguimiento de los talleres. En general es bueno que la persona de enlace sea una persona con capacidad de decisión en la organización o en la comunidad (líder, puesto directivo o de coordinación, encargado de seguridad o de formación, etc.). Sin embargo esto no debe limitar la participación en los talleres exclusivamente a las personas de este perfil. Como se ha explicado previamente, es importante que toda la organización se sienta implicada y participe en el proceso de trabajo sobre seguridad y protección.

Algunas preguntas básicas antes de los talleres:

Es fundamental que en esta reunión previa obtengamos información que nos pueda ser útil para bosquejar una asesoría adaptada a las necesidades de las PDDH peticionaras y entender cómo se gestiona la seguridad desde su perspectiva organizativa.

* ¿Quiénes son las personas defensoras con quiénes trabajaremos; cuál es su contexto de trabajo? ¿Cuáles son sus principales temas o ejes de trabajo en derechos humanos?

* ¿Cuál es el nivel de conocimiento previo de las personas participantes en temas de seguridad y protección? ¿Han recibido capacitaciones previas de este tipo? ¿Tienen estrategias de incorporación de perspectiva de género en su organización? ¿Desarrollan algún tipo de trabajo psicosocial o de salud mental al interior de la organización? ¿Cuál es su nivel de sensibilización y compromiso en relación con estos temas?

* ¿Todos y todas saben por qué se ha pedido o porque se necesita el taller o esta petición refleja una necesidad de una persona o sector dentro de la organización? ¿Se ha identificado a una persona responsable dentro de la organización (punto focal) en seguridad y protección?

* ¿Están en un momento de sobrecarga de trabajo? ¿Existe la posibilidad de que perciban las asesorías como una carga más en sus agendas? ¿Cómo pretenden darle seguimiento al taller de introducción?

* ¿Qué idioma hablan los participantes? ¿Es necesario tener traducción simultánea?

* ¿Qué necesidades y expectativas tiene la organización o las PDDH peticionarias del PASP? ¿Qué situación motiva la petición; existe algún incidente de seguridad, nuevos riesgos, un cambio en la situación de seguridad? ¿Cómo conocieron al PASP? ¿Por qué consideran que requieren una asesoría y qué pretenden lograr? ¿Cuáles son las principales amenazas, las vulnerabilidades prioritarias etc. que deben ser atendidas desde su perspectiva?

* ¿Qué estrategias de seguridad y protección existen a nivel organizativo previas a las asesorías? ¿Tienen alguna medida de seguridad? ¿Todas las PDDH de la organización peticionaria la conocen? ¿Se implementa? ¿Cómo se gestiona la seguridad en la organización? ¿Han enfrentado obstáculos o resistencias para implementar dichas medidas de seguridad con las personas integrantes de su organización?

* ¿Cómo se ha tomado la decisión de mejorar la seguridad de la organización? ¿Es algo que decidieron en asamblea o fue algo decidido por una persona dentro de la organización? ¿Existe un consenso entre las personas de la organización sobre la idoneidad de participar e invertir recursos (tiempo, personal, cambios de dinámicas de trabajo etc.) en asesorías en seguridad y protección? ¿Quién estará en contacto para organizar el primer taller y darle seguimiento? ¿Todas las personas integrantes de la organización en todos sus niveles estarán presentes durante las asesorías y talleres o solo algunas?

Elaboración conjunta de una propuesta consensuada de taller

Tras una primera reunión de sondeo, se puede construir una propuesta tentativa de taller priorizando de forma realista las necesidades de las PDDH. Es importante consensuar esta propuesta con las PDDH peticionarias a través de una segunda reunión y revisar conjuntamente la agenda, los tiempos y los contenidos generales del taller. La organización o personas peticionarias tienen la responsabilidad de valorar la propuesta y en conjunto con las personas facilitadoras, adaptarla a sus necesidades.

Una propuesta básica de taller debe incluir:

Definición de las personas participantes en los talleres

En general es preferible organizar el taller con una organización y no mezclar PDDH de varias organizaciones. De esta manera es más fácil crear un ambiente de confianza y tratar información sensible o fomentar diálogos con franqueza entre participantes de una misma organización. El focalizarse en una organización sienta las bases para el seguimiento posterior y la integración de estrategias de seguridad y protección a nivel organizativo. Se puede considerar también llevar a cabo talleres con varias organizaciones si estas trabajan en red o si su objetivo es crear una coalición de organizaciones. De cualquier forma se debe tener en cuenta que las condiciones de confianza son más complicadas en la medida que se mezclan organizaciones y que esto puede tener un impacto importante al compartir información sensible la cuál es la materia prima para los análisis de seguridad y protección.

En la medida de lo posible se debe intentar que todas las personas de una misma organización sin importar sus funciones y sus puestos puedan participar en el taller. De ser posible se debe involucrar a los puestos de dirección, coordinación o con capacidad de toma de decisiones pero también al personal administrativo, operativo, de coordinación, apoyo en limpieza y acceso a instalaciones, etc. para que se entienda la importancia de incorporar las estrategias de seguridad y protección entre la todas las personas que hacen posible el trabajo organizativo.

Para que todas las personas puedan participar activamente y se genere una buena dinámica de grupo, el número ideal de participantes en un taller debe fluctuar entre 5 personas (en este caso una persona facilitadora es suficiente) y 25 personas (en este caso al menos 2 personas facilitadoras son necesarias y 3 máximo).

Definición del tiempo y calendarización para los talleres

Cada taller está pensado para darse en un día y medio (8 horas mínimo sin contar pausas). Un día y medio es lo ideal para tener el tiempo suficiente para procesar la información, dar espacio a los debates y entrar en profundidad en å actividad. Si se decide acortar el taller y darlo en un día, ese tiempo muchas veces solo da para socializar las herramientas con ejemplos de cómo funcionan y no para aplicar la herramienta conjuntamente con los participantes. Si la organización tiene más tiempo se puede cubrir un taller en dos días enteros y en este caso aplicar cada herramienta.

En cuanto a la planeación de las horas de comienzo y término de los talleres se deben contemplar distintos contextos e ideas diversas sobre la temporalidad, por ejemplo en algunos entornos rurales las ideas sobre puntualidad son distintas, o los procesos para generar confianza o "romper el hielo" suelen tomar más tiempo, lo cual privilegia dinámicas de trabajo distintas respecto a otros entornos en los cuales "se va al grano".

Definición del lugar para los talleres

El lugar en el cual se darán las asesorías es de crucial importancia. El espacio ideal debe proveer condiciones materiales para trabajar como son: ventilación e iluminación adecuada, sillas suficientes, espacios de distención y descanso, servicios sanitarios accesibles sin condiciones de hacinamiento y amplitud mínima para realizar las dinámicas planeadas. Dentro del espacio se puede contemplar también un área con café, té, agua, galletas etc. para que la gente pueda tener un refrigerio y se hidrate constantemente. Antes de comenzar se puede revisar el espacio donde se trabajará para repensar la distribución más adecuada del mobiliario.

Normalmente para las organizaciones lo más fácil es ofrecer su centro de trabajo para los talleres, en este caso se debe contemplar un espacio aislado de las oficinas de las personas participantes con el fin de evitar posibles distracciones cotidianas de su organización. Si la facilitación se hace en un espacio distinto de su centro de trabajo se debe velar por que sea accesible para todas las personas y no implique tiempo o gastos económicos excesivos para el traslado. Un espacio adecuado debe también brindar condiciones de privacidad y seguridad para que la gente se sienta cómoda abordando temas sensibles (ver el apartado sobre cómo generar un espacio seguro desde la perspectiva psicosocial).

Material y recursos para los talleres

- ✓ Un plan del taller para ubicar los módulos, las fechas, horarios y su distribución temática.
- ✓ Un documento base que resuma los conceptos clave y los lineamientos para los ejercicios.
- ✓ Insumos y materiales para la facilitación (*post-its*, fotocopias de los documentos de apoyo suficientes, plumones, papelógrafos, etc.).
- ✓ Recursos tecnológicos opcionales (computadora, proyector, extensiones, etc.).
- ✓ Otras publicaciones relevantes sobre temas relacionados con las asesorías a la mano.

Repaso final de la metodología

Antes de comenzar los talleres se recomienda repasar cuidadosamente la metodología, la secuencia lógica de las actividades para hacer adecuaciones si es necesario en caso que el número de participantes u otras condiciones obliguen a improvisar.

3.2 Durante los talleres

El rol de la persona facilitadora durante el taller

La persona facilitadora es una guía y como su nombre lo indica facilita la interacción y reflexión conjunta entre las personas participantes. Una de las claves para una facilitación exitosa es tener receptividad para catalizar lo más positivo del trabajo grupal y ser adaptable a distintos grupos de personas. La persona que facilita debe evitar dar una ponencia, una simple presentación o cátedra o posicionarse como una autoridad con mayor conocimiento ya que esto puede truncar la interacción y participación activa de las personas. La facilitación se debe esforzar por generar aprendizajes conjuntos de formas multidireccionales en vez de privilegiar una idea de "transmisión" de conocimiento en un sentido unidireccional (limitada al conocimiento de la persona que facilita). La persona responsable del proceso de facilitación debe dejar claro que como facilitadores no tenemos respuestas únicas y que no existe una sola verdad cuando de seguridad se habla.

Habilidades y experiencia requeridas para la facilitación de talleres

Conocimiento a profundidad de los objetivos y resultados esperados en cada proceso de facilitación.

Nociones avanzadas sobre seguridad y entendimiento de los retos que enfrentan las PDDH en sus contextos de trabajo.

Conocimiento mínimo de las PDDH participantes.

Dominio de los conceptos fundamentales de los talleres.

Capacidad para propiciar una reflexión colectiva en los paradigmas de las personas.

Poseer sensibilidad cultural y emocional e involucrar la perspectiva de género al facilitar.

Entender rápidamente como funciona un grupo y de adaptar el contenido y el estilo del taller a las necesidades de las personas participantes.

Saber "leer" el estado de ánimo de un grupo y detectar gestos sutiles de desánimo, contrariedad, aburrimiento, etc. para poder revertir este tipo de situaciones e involucrar en todo momento a todas las personas participantes.

Flexibilidad y apertura para aprender de los demás.

Experiencia en procesos de facilitación de talleres y en diálogos con toma de decisiones por consenso.

Ser capaz de ponerse en los zapatos del otro, de inspirar empatía, respeto y escucha activa.

Ser capaz de establecer procesos de aprendizaje colectivo a nivel cognitivo y actitudinal.

Uso de herramientas complementarias: *Metaplán*

PBI usa también en general la herramienta y metodología del *Metaplán*, la cual promueve que todo el grupo participe, interactúe, visualice lo que se está discutiendo y llegue conjuntamente y estructuradamente a una conclusión. Se trabaja con un panel, pizarrón, pared o una gran manta visible para todas las PDDH. Los miembros del grupo pueden aportar mediante tarjetas en las cuales van escribiendo o dibujando (con marcadores) sus aportes y pegándolos y ordenándolos en el panel. El *Metaplán* permite mover y reagrupar los elementos lo cual brinda claridad conceptual y versatilidad.

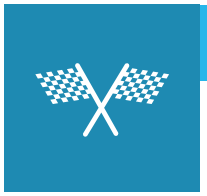
Funciones más importantes de la persona que facilita

- Explicar claramente los objetivos, el proceso, los tiempos.
- Explicitar su propia función a las PDDH participantes.
- Promover un ambiente de inclusión, confianza y respeto para todas las personas.
- Sintetizar las ideas claves, las discusiones y argumentos claves.
- Plantear objetivos, enfocar las discusiones evitar la redundancia y las divagaciones fuera de los temas cruciales.
- Proponer diversos métodos de debate, dinámicas de trabajo y procesos de toma de decisión conjunta.
- Integrar al debate las preocupaciones, opiniones e inquietudes de todas las personas integrantes del grupo.
- "Destrabar" argumentos o discusiones que generan fricción innecesaria o empantanan el debate.
- Tomar como punto de partida las vivencias, procesos y reflexiones de las personas participantes en los talleres usando varios ejemplos relacionados al ámbito de trabajo de las personas participantes.
- Fomentar la participación equitativa de todas las personas en el grupo dando prioridad al proceso de construcción de conocimiento y reflexión grupal por encima de protagonismos individuales.
- Cuidar que todas las personas tengan el mismo nivel de entendimiento para participar plenamente.
- Intersectar las tres dimensiones conceptuales del PASP (sociopolítica, psicosocial y de género) y relacionar dichas dimensiones con ejemplos prácticos que tengan sentido en el trabajo cotidiano de las PDDH.
- Asegurar la exposición de ideas, propuestas nuevas y aportes diferentes a lo ya expresado.
- Establecer consensos y privilegiar acuerdos grupales
- Velar por el cumplimiento de las fases del taller en los tiempos acordados y en caso de necesidad proponer reajustes a la agenda.

Claves para imprimir dinamismo a la facilitación y asegurar la comunicación efectiva durante la facilitación

- Explicar conceptos complejos a través de formas sencillas que ejemplifiquen de lo que estamos hablando: se pueden usar metáforas, historias y analogías que tengan sentido para las personas participantes.
- Prescindir de los monólogos privilegiando procesos de diálogo e interpelación con las personas participantes.
- Evitar abusar de la jerga conceptual (se puede hacer una "pelota de jerga" que sea arrojada cada que alguien menciona un concepto que los demás no entienden para parar y explicarlo).
- Modular la voz adecuadamente.
- Utilizar comunicación más allá de lo verbal (oral o escrito) apoyándose en diversas herramientas pedagógicas para evitar la monotonía.
- Implicar el propio cuerpo para enfatizar ideas y generar asociaciones fácilmente a través de ademanes, expresión facial, acompañamiento corporal, etc.
- Ocupar y moverse entre el espacio disponible para estar cerca de las personas y no permanecer estático ni distante.
- Incorporar técnicas vivenciales durante los talleres como juegos de rol, puestas en escena, dinámicas corporales para revitalizar, energizar, romper el hielo, generar confianza y cercanía, etc.
- Evitar leer en demasía o hacer uso excesivo de presentaciones de *power point*.

- ✓ Incluir diversos elementos para trabajar los talleres: apuntes tipo tablero donde se puedan reacomodar y añadir visualmente las ideas a lo largo de los talleres, carteles, dibujos, videos, canciones, moldeado con plastilina, etc.
- ✓ Promover discusiones en grupos pequeños y plenarias, charlas entre los participantes, rondas, presentación de debates sintetizados por grupos.
- ✓ Rotar la facilitación si se pierde dinamismo.
- ✓ Establecer contacto visual con las personas participantes mientras se facilita.
- ✓ Reforzar ideas con comunicación no verbal y sensorial como ademanes, pantomima, representaciones y juegos de rol.



Apertura de los talleres

La apertura es un momento crucial en el proceso pedagógico por lo que hay que dedicarle el tiempo adecuado.

En la apertura del taller procuraremos:

- Presentar a los participantes y su trabajo brevemente.
- Romper el hielo" y establecer alguna dinámica para generar confianza *ver sección de recursos para dinámicas de presentación y confianza.*
- Establecer grupalmente normas de convivencia mínimas antes de comenzar los talleres *(ver sección Generar espacio seguro desde la perspectiva psicosocial).*
- Brindar una introducción general de los objetivos generales y específicos del taller.
- Identificar las expectativas de los participantes.
- Revisar y consensuar los objetivos del taller de forma realista.
- Plantear el tipo de metodologías y participación que se quieren trabajar a los largo del taller.
- Sondear los conocimientos previos de los participantes .
- Revisar los horarios.

Uso de herramientas complementarias: Cuaderno del participante.

Se recomienda brindar un *Cuaderno del Participante* que incluya: una presentación del taller, la agenda y fotocopias de los anexos referidos para cada taller de este manual. Tener material de apoyo como este puede ser positivo ya que representa un documento físico que se queda la organización y que apoya las tareas de desarrollo o implementación de estrategias de seguridad posteriores al taller. El cuaderno sirve para: **1)** resumir los conceptos y definiciones usados durante el taller, **2)** incluir las actividades, ejercicios y sus indicaciones y **3)** funcionar como un cuaderno para tomar actas y recoger los principales acuerdos alcanzados durante el taller.

¡Cuidar la terminología y conceptos que usamos!

La persona que está a cargo de la facilitación debe **tener claro cuáles son los conceptos claves que se discutirán durante los talleres.** Para estos conceptos (i.e. incidentes, amenazas, ataques, riesgos, vulnerabilidades, capacidades, normas de género, estrés acumulativo, etc.) se debe tratar de usar siempre las mismas palabras para facilitar el diálogo y el seguimiento posterior, se pueden también usar tarjetas que por un lado contengan el concepto y por el otro las definiciones. Para otro tipo de conceptos conviene más **usar los términos que proponen los participantes** al taller: usar su vocabulario, sus ejemplos, su manera de explicar en aras de facilitar la apropiación de los contenidos por parte de las PDDH participantes.

Ser flexible y estar listo a cambios de último minuto

Las personas que facilitan tienen que estar listas para replantear partes del taller de último momento en el caso de que lo que se preparó no sea idóneo para la audiencia. Hay que **ser capaces de adaptar sobre la marcha** la forma en que se explican los conceptos o las actividades mismas para satisfacer las necesidades de las personas participantes en la medida de lo posible.

Generar espacios con equidad

Una labor fundamental durante los talleres es la de generar espacios equitativos y libres de toda forma de discriminación, ya sea esta explícita o implícita. Para lograr lo anterior la persona que facilite requiere atender los detalles y propiciar que todas las personas se sientan tratadas de forma equitativa en su dignidad, sus posiciones y opiniones independientemente de su sexo, etnia, función en la organización o cualquier otro factor que pudiese dar pie a distinciones discriminatorias.

Algunos consejos para fomentar que los talleres sean espacios con equidad:

- ✓ **Distribuir los espacios de trabajo durante la facilitación de tal manera que "equilibren" las posiciones de poder** (por ejemplo no poner al personal de ciertas organizaciones en lugares privilegiados respecto a otras, o a las personas de la dirección de una ONG en lugares especiales respecto a las demás personas integrantes).

- ✓ **Ser consciente de la composición de los grupos de trabajo por variables de distribución de poder (clase, etnia, sexo, nacionalidad, posición de mando etc.)** ¿Es un grupo multiétnico? ¿Hay personas que trabajan en contextos urbanos y rurales en el mismo grupo? ¿Hay organizaciones que trabajan en condiciones asimétricas de acceso a fondos respecto a otras? ¿Existen liderazgos autoritarios o equitativos por parte de las personas que coordinan o dirigen las organizaciones con las que trabajamos?

- ✓ **Atender las necesidades especiales que puedan tener las personas** ¿Se necesita algún mobiliario o disposición especial para personas con motricidad reducida? ¿Se requiere mejor visibilidad o audibilidad para algunas personas? ¿Hay personas que necesitan un intérprete o traducción de ciertos términos?

- ✓ **Comprender las asimetrías de género en el trabajo organizativo y de facilitación para poder revertirlas durante el taller** ¿La distribución de hombres/mujeres y sus labores en el grupo es equilibrada? ¿Quiénes tienen las posiciones de liderazgo son mayoritariamente hombres? ¿En caso de que sean mujeres quienes tienen liderazgos importantes, incluyen también a otras mujeres o reproducen formas de exclusión patriarcales? ¿Qué implica que la facilitación esté a cargo de una mujer en ese contexto grupal por ejemplo?

- ✓ **Administrar balanceadamente las intervenciones** (turnos de palabra, dar prioridad a las personas que hablaron menos o no han participado todavía).

- ✓ **Abordar las implicaciones de lenguaje discriminatorio** de antemano con el fin de que la gente reflexione no sólo el fondo de sus mensajes sino en las formas en que los expresa y las implicaciones que esto tiene en términos de inclusión o exclusión.

- ✓ **Estar preparados para revertir o tratar una situación de exclusión por parte de algún participante:** comentario sexista, designación con implicaciones clasistas, racistas, etc. sin que la persona que participó en dicha acción se sienta juzgada, planteando una solución constructiva a partir de la reflexión conjunta *(ver la sección de ejemplos de retos y situaciones complicadas).*

Generar un espacio seguro desde la perspectiva psicosocial

Las personas que facilitan tienen que procurar construir la dimensión de la seguridad más allá de condiciones materiales. Esto conlleva a poner de relieve la importancia de la subjetividad y emocionalidad para construir un "espacio seguro" en el que las emociones, inseguridades, estrés y otras formas sutiles de interacción grupal sean abordadas positivamente. Un espacio seguro genera confianza, solidaridad y apertura a lo largo de la interacción incluso al hablar de temas personales en relación con el trabajo o al expresar emociones que en ocasiones son difíciles de abordar.

Cómo generar un espacio seguro desde la perspectiva psicosocial:

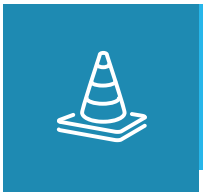
- ✓ **Aportar condiciones para cuidar en todo momento el respeto** entre las personas integrantes del grupo.
- ✓ **Acordar desde un principio las reglas de participación y convivencia** ¿Cómo se va a pedir la palabra? ¿Qué pasa cuando se interrumpe?
- ✓ **Establecer reglas de confidencialidad** ¿Se pueden tomar fotos? ¿Se puede grabar? ¿Cómo se va a tratar lo que se hable dentro de este espacio en relación con comentarios fuera de este grupo?
- ✓ **Promover la escucha activa entre todas las personas participantes** (se puede por ejemplo acordar dejar computadoras y celulares en un rincón apartado del cuarto).
- ✓ **Limitar el número de entradas y salidas del recinto donde se lleva a cabo la facilitación** ya que esto puede interrumpir procesos clave y dar la sensación a quien está participando de que a las personas que salen o entran constantemente no les interesa.
- ✓ **Estar especialmente atentos a las reacciones y omisiones de las personas participantes** para detectar posibles dificultades en la comunicación, incomodidades, miedos, conflictos entre las personas, etc.
- ✓ **Establecer a priori que hay distintas formas de enfrentar las situaciones y sentimientos**
- ✓ **Brindar garantías para que la gente no se sienta juzgada por expresar sus emociones durante el taller** (ver la sección de ejemplos de retos y situaciones complicadas).
- ✓ **Buscar un espacio físico que facilite la intimidad, la empatía y la privacidad**.
- ✓ **Hablar desde lo sensible en ocasiones para expresar opiniones**, cuidando no invalidar ningún tipo de manifestación emocional (por ejemplo decir "yo me siento", "yo considero" "para algunas PDDH es difícil porque...").
- ✓ **Cuidar la inclusión de las personas a nivel emotivo y recalcar el carácter positivo de los talleres** para abordar de manera constructiva temas delicados.
- ✓ **Sondear condiciones de estrés previo y establecer dinámicas de distención emocional** (puede ser al comienzo o si surge algo que "traba" los talleres).
- ✓ **Garantizar condiciones comunicativas y dialógicas francas evitando la negación de problemas, pero teniendo cuidado de abordar con delicadeza las situaciones complicadas para las demás personas** (por ejemplo estrés acumulativo, alcoholismo, conflictos laborales o de poder al interior la organización, etc.).
- ✓ **No revictimizar ni culpabilizar a las personas** ya sea por juzgar sus sentimientos o por descalificar sus reacciones derivadas de experiencias personales o de trabajo en derechos humanos.
- ✓ **Evitar establecer comparaciones innecesarias entre las experiencias y emociones de las personas** ya que esto puede malinterpretarse como una invalidación sutil de ciertas formas de reaccionar ante emociones y situaciones diferentes (por ejemplo al comparar las reacciones de dos personas en una organización ante IdS.

Sensibilidad Cultural

Los procesos de facilitación en seguridad y protección suelen llevarse a cabo en contextos distintos. Cada taller debe adecuarse a este contexto: actitudes, gestos o palabras que en ciertos talleres son insignificantes pueden tener un impacto o generar impresiones muy distintas y de mayor trascendencia en diferentes condiciones culturales.

Aspectos importantes a considerar para la sensibilidad cultural:

- ✓ **Conocer los códigos culturales básicos, las trayectorias organizativas y la historia de las comunidades con las que se trabaja.**
- ✓ **Evitar estereotipar o reproducir prejuicios culturales** a través de generalizaciones y reduccionismos (por ejemplo al afirmar que una cultura es necesariamente de una forma, o al imponer una visión negativa de antemano sobre aspectos culturales concretos).
- ✓ **Reconocer las implicaciones de diferencias culturales y connotaciones en mensajes y representaciones para distintas culturas** (por ejemplo si la persona que facilita pertenece a una cultura diferente entender qué puede representar su posición, nacionalidad, cultura, posición social, color de piel etc. para la cultura del grupo con el que se trabaja).
- ✓ **Entender y adaptarse a las formas de gestión de conflicto en cada cultura** ¿Las PDDH expresan directamente su negativa o prefieren formas más sutiles para manifestar la renuencia? ¿Plantean abiertamente las discusiones o prefieren evadir los temas? ¿Cuál es la implicación de que se expresen opiniones divergentes al interior del grupo, se ve como una disputa a evitar o como una situación constructiva positiva?
- ✓ **Comprender los procesos autóctonos de toma de decisiones y su relación con las jerarquías** ¿Las personas con las que realizamos los talleres están más arraigadas a una cultura colectivista o a una individualista? ¿Existen liderazgos alrededor de una figura central o se promueve la horizontalidad? ¿Se toman las decisiones por consenso, por votación o se sigue la postura de las personas líderes? ¿Si se cuestiona la opinión de una persona líder en la comunidad cómo se toma este cuestionamiento; como afrenta o cómo algo constructivo? ¿Los debates son igualitarios o las jerarquías de posición generacional, de género etc. determinan la forma en que se toman las decisiones?
- ✓ **Distinguir los tipos de narrativas prevalentes en las comunidades de PDDH con las que trabajamos** ¿El silencio es habitual o es percibido con incomodidad? ¿Cómo se comunican los acuerdos y las negociaciones? ¿Los compromisos se hacen de forma reiterada? ¿Las menciones a los acuerdos son percibidas como débiles si no son reiteradas? ¿Se va al grano y se expresa de forma directa lo que se piensa o es una comunicación que privilegia formas indirectas? (p. ej. Se usan frases ambiguas o eufemismos "tal vez" o "sería bueno" para expresar una negativa o estuvo "bastante bien" para referirse a algo que en realidad no cubrió las expectativas, se usan metáforas, dichos o historias para hacer referencias a una situación) .
- ✓ **Diferenciar las distintas formas de entender el tiempo en las comunidades con las que se trabaja** ¿Los horarios son entendidos de forma exacta o en un sentido aproximado? ¿La cultura de trabajo tiene horarios estrictamente definidos o se acostumbra a trabajar sin horarios fijos? ¿La memoria histórica del pasado se ve como algo distante o se tiene muy presente en el imaginario colectivo de la comunidad?
- ✓ **Entender los códigos y rituales sociales** ¿Cómo manejan la proximidad corporal? ¿Es importante el contacto físico como apretones de manos, abrazos etc.? ¿Hay diferencias entre estos códigos de contacto entre hombres y mujeres? ¿Están acostumbrados a ver a colegas con familiaridad o prefieren mantener una relación estrictamente formal? ¿Marcan o desdibujan los límites entre vida privada y perfil público como PDDH? ¿Cuánta importancia dan al preludio o presentación para abrir el espacio previo a las sesiones "formales" de trabajo? ¿En su cultura es importante convivir al terminar sesiones de trabajo? (fiestas, convivios, bailes, etc.).
- ✓ **Entender el papel de la religión y la espiritualidad en la cultura y el trabajo de las PDDH** ¿Su cultura está vinculada a alguna(s) religión(es) en particular? ¿Existen algunos rituales o creencias espirituales que sean importantes para las PDDH en relación con su trabajo? ¿En caso de que la religión no sea abiertamente importante en el trabajo, qué valores asociados a la misma están presentes en su cultura?



Algunos ejemplos de retos y situaciones complicadas que pueden surgir durante el proceso de facilitación y cómo afrontarlos

Como se ha mencionado los talleres son momentos que pueden implicar situaciones complicadas al abordar tantos temas delicados. La interacción de bagajes, emociones, ideas, conocimientos y contextos culturales distintos entre las personas facilitadoras y otras personas participantes pueden suponer retos en algunas de estas situaciones. En seguida se abordan algunos ejemplos paradigmáticos para sortear algunos de estos tipos de situaciones y cómo aprovecharlas para crear una situación positiva.

1 Cuestionamiento del rol de la persona facilitadora o descalificación de lo que presenta durante la facilitación

En ocasiones algunos talleres pueden verse desestabilizados por cuestionamientos excesivos o descalificaciones a la forma o contenido de los talleres incluyendo en los casos más extremos ataques directos a la persona que facilita. Estos cuestionamientos pueden deberse ya sea a un cuestionamiento de la posición de la persona o lo que representa ante los ojos de ciertas personas participantes (por ser joven, por ser extranjera, por ser mujer en un grupo que privilegia el conocimiento de los hombres, etc.) o por que los planteamientos de la facilitación son percibidos como un desafío a los esquemas de trabajo, creencias o la cultura del grupo con el que se trabaja. Este tipo de cuestionamiento puede ser abierto (crítica al esquema de trabajo, descalificación de la información que se maneja etc.) o más sutil (interrumpiendo la facilitación con intervenciones excesivas, haciendo bromas pesadas o simplemente ignorando a la persona que facilita). Para prevenir o desactivar este tipo de situaciones es importante explicar detalladamente lo que se trabajará de antemano con las organizaciones. Cuando una persona interrumpe demasiado o propone siempre "mejores soluciones" se le puede reclutar en actividades de mesas o subgrupos de trabajo con un rol más protagónico para encauzar positivamente su energía (por ejemplo proponerlo como presentador de una actividad o relator de una mesa de trabajo, dándole algunas responsabilidades adicionales dentro del taller) pero siendo claros en que esta participación se debe enmarcar dentro de los esquemas de trabajo necesarios para el cumplimiento de los objetivos de los talleres. Es importante trabajar con humildad y reconocer de forma pública los saberes y experiencia de las personas con las que se trabaja en todo momento. Se debe también diferenciar las ideas y posiciones de las personas (no convertir las opiniones en algo personal) para propiciar el respeto mutuo independientemente de las posiciones ideológicas o conceptuales. En casos extremos es importante tener temple para no caer en provocaciones ni entrar en conflicto innecesario y sin embargo tener la franqueza suficiente para exigir reciprocidad en el respeto al trabajo propio. Si todo lo anterior no funciona se debe plantear abiertamente la imposibilidad de continuar los talleres en dichas condiciones ya que no existen las condiciones mínimas de respeto para desarrollarlos. Una vez hecho este planteamiento se puede proponer un espacio aparte para buscar una solución con la organización involucrando a todas las partes.

2 Situaciones en que los tiempos se salen de control

Muy a menudo es difícil controlar los tiempos. Hay que saber ser flexibles para dar tiempo suficiente a las dinámicas y si se está en medio de un ejercicio o debate importante no necesariamente truncar el proceso aunque esto implique alargar un poco al final. Por otro lado hay que saber discernir cuando los procesos no son fundamentales y en estos casos preguntar respetuosamente al grupo si se quieren extender en este punto, si es necesario pasar a otro punto o si se puede dejar en una lista pendiente para tratar después o en otro espacio específico. Se puede tener un papelógrafo o espacio en el salón donde se puedan ir punteando los temas que se desvían del objetivo de los módulos pero que de acuerdo al grupo sean importantes de tratar. Se puede también reprogramar otro día para dar lo que falta o extender ese mismo día dedicando un tiempo especial si hay consenso. Antes de comenzar los talleres se aconseja pedir a la gente con la que se tiene más confianza en la organización ayuda en la moderación de los tiempos ya que puede ser complicado para la persona que facilita tener que detener o apurar las participaciones de las personas, e incluso muchas personas participantes pueden tomar esta situación como una falta de respeto o un cuestionamiento a su posición por lo que es un tema delicado.

3 Alguna persona participante se torna excesivamente nerviosa o se pone a llorar durante el taller

Por el tipo de discusiones y la dificultad que entrañan temas en temas de seguridad y protección no es atípico que alguna persona o varias del grupo se encuentren en una posición de vulnerabilidad emocional, estrés o llanto durante las discusiones o dinámicas. Lo primero que hay que hacer es escuchar activamente a la persona que está afectada y brindar un espacio de contención el cual habrá de garantizarle apoyo y empatía. Una vez que se haya preguntado por el bienestar de la persona la persona facilitadora puede poner ejemplos sobre cómo las cuestiones emocionales pueden afectar el trabajo de las PDDH remarcando el mensaje de que este tipo de espacios abren también las emociones y que es válido expresarlas de distintas maneras, hay gente que desahoga el estrés con el silencio o introversión, mientras que otras personas requieren hablarlo o llorar para desahogar la tensión. La validación de las expresiones de los demás es importante para que la persona no se sienta avergonzada de mostrar sus emociones. Se debe ser particularmente atento a no revictimizar ni poner a la persona en una posición de vulnerabilidad extrema, también resaltando el hecho de que el afrontamiento de las emociones es un paso muy importante. Si se aborda positivamente este tipo de episodios pueden servir para abordar la importancia de la relación entre las emociones y nuestro trabajo cotidiano y cómo la seguridad y la protección deben abarcar estas esferas. Se puede hacer una pequeña pausa para retomar este punto e incluso abrir alguna pequeña dinámica para abordar el papel de las emociones en nuestro trabajo o para que todas las personas se sientan cobijadas y en confianza (como las dinámicas de "vitaminas", para "construir equipo" o para rebajar tensiones).

4 Dos o más participantes o facciones entran en conflicto y comienzan a atacarse

Lo primero es detectar este tipo de situaciones tempranamente, generalmente las expresiones más abiertas o incluso violentas en un grupo se dan después de una escalada global de agresiones. Por ello es importante abordar desde los primeros momentos el conflicto de forma constructiva y no simplemente dejarlos de lado como si no existiesen. En dado caso que las expresiones de hostilidad sean abiertas se debe de mantener la calma y utilizar dinámicas para bajar la tensión. Hay que tener en cuenta que muchas de estas situaciones están fundamentadas en roces previos de las personas participantes derivados de experiencias ajenas a los talleres y en la ausencia de espacios para abordar los conflictos. También el estrés acumulativo puede catalizar este tipo de conflictos por lo que es importante explicar la relación entre desgaste personal y organizativo y cómo eso puede afectar nuestro trabajo colaborativo, lo cual sucede en muchas organizaciones. Es importante estar atentos y en dado caso que la situación se salga de control se puede hacer una pausa y retomar con un poco de más calma. También se pueden utilizar los tiempos muertos de los talleres para hablar en privado con alguna persona que se sienta ostensiblemente incómoda con alguna situación o comentario. Existen distintas dinámicas y ejercicios para bajar la tensión, en general aquellas dinámicas que resaltan las similitudes por encima de las diferencias (por ejemplo los objetivos por los que se trabaja, los valores, etc.) ayudan a subrayar la importancia de resaltar la colaboración y ver más allá de las diferencias.

5 Actitudes o expresiones machistas

En ocasiones surgen comentarios con connotaciones machistas o que perpetúan estereotipos sobre hombres y mujeres. Es fundamental dejar en claro la importancia de integrar la dimensión de género para el trabajo cotidiano de derechos humanos y establecer que este es un proceso que no es lineal sino que requiere cuestionarnos desde la forma en la que hablamos, nos comportamos con nuestros compañeros y compañeras, etc. Se deben abordar directamente estos episodios sin propiciar una "guerra de sexos" durante el taller sino plantear que todas las personas, tanto hombres como mujeres hemos sido educados con ciertas visiones sobre las normas de género socialmente aceptadas y que como PDDH es nuestro deber trabajar gradualmente por desarraigar prejuicios e ideas que perpetúan la desigualdad y afectan la equidad ya sea en la vida privada como en el trabajo.

6 Generar apertura entre hombres defensores de DH

En algunos casos al realizar los análisis de seguridad por el contexto cultural algunos hombres tienden a ver amenazas, riesgos, incidentes de seguridad y vulnerabilidades como un cuestionamiento de su hombría. Esto se debe a que en muchas ideas sobre la masculinidad el aceptar por ejemplo una vulnerabilidad o que se experimenta miedo, cansancio o frustración es visto como un síntoma de debilidad, lo que a su vez va en contra de las cualidades asociadas a la masculinidad hegemónica, o

en otras palabras, las formas como "se debe" ser varón. En otras ocasiones al trabajar la dimensión psicosocial de la seguridad y la protección en contextos culturales patriarcales los hombres son más reacios a expresar frustraciones, miedos, emociones, etc. Se debe garantizar un espacio que genere confianza para que los hombres y mujeres puedan expresarse y abordar amenazas, riesgos, incidentes de seguridad y vulnerabilidades sin sentirse juzgados. Se deben aportar ejemplos de cómo el trabajo de defensa de los DH afecta a todas las personas y de la importancia de abordar estas cuestiones desmantelando analíticamente concepciones de "hombría tradicionales" para fortalecer su trabajo.

7 La impuntualidad durante los talleres afecta el trabajo

Si el grupo es impuntual a la hora de iniciar los talleres se pude proponer recuperar el tiempo perdido al final de la sesión. Si es imposible alargar los talleres al final se puede proponer recortar los recesos u horas de comida en concordancia con los desfases temporales. Esto generalmente disuade los retrasos aunque es importante que no se imponga esta medida de manera autoritaria sino que se haga ver a las personas participantes la importancia de recuperar el tiempo de trabajo perdido.

Conclusión y cierre del taller

La conclusión de los talleres es un momento crucial porque sirve para resumir, atar cabos que hayan quedado sueltos y cerrar el proceso de facilitación.

Al momento de concluir un taller procuraremos:

- ✓ Hacer una revisión somera del contenido del taller relacionando los diferentes conceptos claves explorados.
- ✓ Cerciorarnos que no hayan quedado dudas sobre los aspectos fundamentales del taller.
- ✓ Dar una oportunidad para que la gente que quiera aportar algo o no pudo a lo largo de los talleres pueda hacerlo.
- ✓ Abordar las expectativas de seguimiento y acordar si se necesita seguimiento, de qué tipo y cómo se podría dar.
- ✓ Revisar los acuerdos alcanzados y establecer los compromisos con los participantes en cuanto a las estrategias de seguridad y protección que serán desarrollados a nivel organizativo.
- ✓ Evaluar el cumplimiento de los objetivos de los talleres individualmente.
- ✓ Evaluar colectivamente los talleres y compartir las valoraciones.
- ✓ Clausurar el taller, despedir y agradecer.

3.3 Después de los talleres

Como facilitadores debemos autoevaluarnos después de cada taller o asesoría. Es bueno discutir entre facilitadores o reflexionar sobre los puntos positivos y negativos de los talleres, los momentos más complicados que se experimentaron y si se conciben ajustes necesarios para mejorar facilitaciones subsecuentes. También se deben retomar los puntos fundamentales de la evaluación que rellenaron los participantes al final de taller y ver si es necesario efectuar cambios. Es aconsejable guardar un registro o memoria de estas evaluaciones.

Seguimiento de los talleres

El tipo de seguimiento dependerá de la organización, de sus disponibilidades, de su compromiso con la seguridad y de los cambios en sus necesidades.

Después de los talleres, y en acuerdo con la organización peticionaria, se recomineda:

- ✓ Reiterar que la persona facilitadora está disponible para cualquier consulta a distancia relativa a la implementación de las herramientas de seguridad compartidas con la organización.
- ✓ Recordar a las organizaciones que el PASP no está solo para momentos de emergencia. Los talleres y asesorías se pueden pedir también cuando hay más tiempo y tranquilidad.
- ✓ Definir la fecha y el lugar para una reunión de seguimiento con la organización para establecer en conjunto cómo quieren seguir y qué esperan de la persona que facilita.
- ✓ Acordar reuniones bimensuales, trimestrales o semestrales para saber cómo va la organización y cómo la persona que facilita puede apoyarles, resolver dudas, ver si otro taller o asesoría es necesaria.
- ✓ Para brindar otra asesoría o taller esperamos que la organización la pida proactivamente y que demuestre un cierto grado de compromiso (cumplimiento de las tareas identificadas durante los talleres por ejemplo).
- ✓ En cualquier momento del proceso se pueden tener asesorías puntuales para profundizar alguna herramienta en particular compartida en alguno de los talleres ya brindados.
- ✓ Tener en mente la lógica y orden de los talleres (ver capitulo 2, sección 4)

Uso de herramientas complementarias: *Herramienta de monitoreo del Manejo de la Seguridad*

Durante el seguimiento usamos la *Herramienta de monitoreo del Manejo de la Seguridad*[7] (ver sección posterior a los talleres y anexos). Con esta herramienta se pretende monitorear el proceso de seguridad desarrollado por la organización a lo largo del PASP. La herramienta recopila los criterios que deberían estructurar y guiar las reuniones de seguimiento ulteriores. Se sugiere revisar la herramienta conjuntamente con la organización al menos tres veces durante el programa. La idea con esta herramienta no es juzgar o evaluar externamente a la organización, sino aplicar conjuntamente la herramienta con la organización para que las PDDH identifiquen mejor sus necesidades y que las personas facilitadoras detecten dónde podría seguir apoyando el proceso de mejora de seguridad. La herramienta se puede compartir tal cual con la organización o adaptar. Lo importante es poder trabajar los criterios principales que contiene y llegar a un consenso sobre qué herramientas o apoyo posterior necesita la organización.

Herramienta de monitoreo del Manejo de la Seguridad (Actitudinal)

	Manejo básico		Manejo estratégico	
	"instintivo/ informal" en ausencia de un compromiso institucional		Política institucional con definición de espacios, responsabilidades y recursos. Adaptación constante de la estrategia y del plan de seguridad a la situación de riesgo (diagnóstico).	
	Mínimo	**Bajo**	**Medio**	**Alto**
Conciencia	La mayoría de las personas integrantes de la organización no perciben los riesgos y por lo tanto no ven la necesidad de la estrategia y del plan de seguridad.	Algunas personas integrantes de la organización empujan el tema de la seguridad, compartiendo su conciencia de los riesgos. No reciben el apoyo institucional necesario.	Las personas responsables de la organización perciben los riesgos y empujan el tema de la seguridad. Sin embargo esta conciencia no es compartida, existen resistencias.	La organización tiene la capacidad de compartir su conciencia de los riesgos y de la necesidad de seguridad con todas sus personas integrantes incluyendo las nuevas.
Experiencia	Pocas personas integrantes de la organización tienen experiencia práctica con situaciones de riesgo y/o pocas tienen conocimiento práctico sobre el manejo de la seguridad.	Algunas personas integrantes de la organización tienen una buena experiencia en gestión de riesgos. No logran compartir estos conocimientos prácticos.	La organización tiene una "memoria histórica" en cuanto al manejo del riesgo pero no todas sus personas integrantes tienen experiencia práctica.	La organización tiene una "memoria histórica" en cuanto al manejo del riesgo y todas sus personas integrantes tienen experiencia práctica sobre manejo de la seguridad. La organización tiene la capacidad de compartir su conciencia de los riesgos y de la necesidad de seguridad con todas sus personas integrantes incluyendo las nuevas.
Conclusiones	**El manejo de la seguridad es insuficiente.**	**El manejo de la seguridad es informal.** **No hay compromisos claros institucionales/ existen resistencias.**	**Existe un compromiso institucional por parte de la organización en favor de la seguridad. Aún falta concretarlo.**	**El compromiso institucional en favor de la seguridad se manifiesta en la práctica.** **Hay una gestión integral de la seguridad al nivel individual e institucional.**

Herramienta de monitoreo del Manejo de la Seguridad (diagnóstico y planificación)

	Manejo básico		Manejo estratégico	
	"instintivo/ informal" en ausencia de un compromiso institucional		Política institucional con definición de espacios, responsabilidades y recursos. Adaptación constante de la estrategia y del plan de seguridad a la situación de riesgo (diagnóstico).	
	Mínimo	**Bajo**	**Medio**	**Alto**
Diagnóstico	Sólo algunas personas integrantes de la organización identifican los diferentes elementos del diagnóstico de seguridad. Este análisis no se comparte con las demás lo que no permite tener una estrategia de seguridad apegada al contexto y riesgo de la organización.	Los pasos del diagnóstico se realizan de manera informal, no de forma sistemática y sin contar con herramientas sistematizadas ni procesos claros para compartir la información. Varias personas integrantes de la organización identifican y analizan los elementos del diagnóstico de seguridad pero hay discrepancias en las conclusiones y no se ha dado espacio para debatirlas.	Los pasos del diagnóstico o sus elementos están incluidos en el trabajo de la organización (política institucional de seguridad). Sin embargo no todos las personas integrantes de la organización poseen una visión amplia del riesgo de la organización. Los diferentes elementos del diagnóstico se analizan de forma independiente y desvinculada (por ejemplo no se relaciona el mapeo de actores con la bitácora de IdS o con las estrategias de incidencia). Hacen falta espacios de análisis en conjunto y evaluar/ajustar periódicamente la política y estrategia de seguridad para que se apegue mejor a la situación de riesgo.	Los pasos del diagnóstico o el análisis de sus elementos están incluidos en el trabajo de la organización (política institucional de seguridad) y se refleja totalmente en la estrategia y el plan de seguridad. Las metodologías, responsabilidades y espacios están totalmente definidos.
Plan de seguridad y diseño de estrategias	No existe planificación sino acciones individuales instintivas. Algunas personas integrantes de la organización adoptan medidas de seguridad, reaccionan a emergencias o implementan estrategias de incidencia sin que previamente y colectivamente se hayan decidido y planificado.	Hay acciones colectivas de prevención y reacción así como normas tácitas para la ejecución. Falta ponerlos por escrito y compartirlos/acordarlos entre todos.	Se han identificado los protocolos, políticas y planes necesarios y existe un compromiso institucional para ponerlos por escrito. Hace falta completar el plan de seguridad y relacionarlo y vincularlo con el trabajo más amplio de la organización y en específico con la estrategia de incidencia política.	La organización tiene un plan de seguridad completo que presenta protocolos de prevención, políticas permanentes y planes de reacción en caso de emergencia. Este plan de seguridad se inscribe en una estrategia de seguridad más amplia que considera la incidencia política.
Conclusiones	**El manejo de la seguridad es insuficiente.**	**El manejo de la seguridad es informal. No hay compromisos claros institucionales/ existen resistencias.**	**Existe un compromiso institucional por parte de la organización en favor de la seguridad. Aún falta concretarlo.**	**El compromiso institucional en favor de la seguridad se manifiesta en la práctica. Hay una gestión integral de la seguridad al nivel individual e institucional.**

Herramienta de monitoreo del Manejo de la Seguridad (implementación y evaluación)

	Manejo básico		Manejo estratégico	
	"instintivo/ informal" en ausencia de un compromiso institucional		Política institucional con definición de espacios, responsabilidades y recursos. Adaptación constante de la estrategia y del plan de seguridad a la situación de riesgo (diagnóstico).	
	Mínimo	**Bajo**	**Medio**	**Alto**
Formación	La mayoría de las personas integrantes de la organización nunca ha recibido una formación sobre seguridad.	La mayoría de las personas integrantes de la organización han recibido una formación sobre seguridad pero no existen recursos sistematizados para los y las nuevas integrantes o para los que nunca han recibido una formación.	La mayoría de las personas integrantes de la organización han recibido la debida capacitación y hay recursos didácticos accesibles para todos (pe. Manual de seguridad para defensores). Sin embargo no existe una política de formación para los y las nuevas integrantes.	Las personas integrantes de la organización han recibido la debida capacitación. Hay recursos didácticos accesibles para todos. La orientación de los y las nuevas integrantes incluye una capacitación sobre temas de seguridad.
Participación	Cuando se planifica la seguridad y se evalúa la estrategia y el plan de seguridad no se busca la participación de todas las personas integrantes de la organización.	En el desarrollo del proceso de seguridad y su evaluación se pretende involucrar a todas las personas integrantes y buscar el consenso. Sin embargo, en la práctica no hay participación activa.	La organización tiene como política buscar la participación activa de todas las personas integrantes para diseñar el plan y la estrategia de seguridad, facilitar su implementación efectiva y evaluarlos. Sin embargo hay fallos a ciertos niveles (diagnóstico, planificación, implementación, evaluación).	La organización logra una participación integral de todas y todos sus miembros en el proceso de seguridad y su evaluación. Se les consulta y se toman en cuenta las preocupaciones y valoraciones de todas y todos.
Cumplimiento de normas	Las normas no se cumplen porque no están establecidas.	Algunas personas integrantes de la organización cumplen con unas normas tácitas. Otras ni siquiera conocen la existencia de normas.	Todas las personas integrantes de la organización conocen las normas. Sin embargo no todas cumplen con todas las normas.	Todas las personas integrantes de la organización conocen y cumplen con todas las normas.
Conclusiones	**El manejo de la seguridad es insuficiente.**	**El manejo de la seguridad es informal. No hay compromisos claros institucionales/ existen resistencias.**	**Existe un compromiso institucional por parte de la organización en favor de la seguridad. Aún falta concretarlo.**	**El compromiso institucional en favor de la seguridad se manifiesta en la práctica. Hay una gestión integral de la seguridad al nivel individual e institucional.**

Herramienta de monitoreo del Manejo de la Seguridad (implementación y evaluación)

	Manejo básico		Manejo estratégico	
	"instintivo/ informal" en ausencia de un compromiso institucional		Política institucional con definición de espacios, responsabilidades y recursos. Adaptación constante de la estrategia y del plan de seguridad a la situación de riesgo (diagnóstico).	
	Mínimo	Bajo	Medio	Alto
Responsabilidades	No hay claridad sobre la división de responsabilidades.	En la práctica, existe una división de responsabilidades entre las personas integrantes de la organización. Esta asignación se realiza de manera informal.	La organización contempla en su política de seguridad la necesidad de asignar responsabilidades claras para todas las etapas del proceso. Sin embargo, hace falta asignar unas responsabilidades o la división de responsabilidades no se manifiesta totalmente en la práctica.	La política de seguridad de la organización define las responsabilidades claras para todas las etapas del proceso. En la práctica, se cumple con esta asignación de responsabilidades
Recursos	Los recursos identificados según las necesidades de seguridad no están disponibles porque no se les da prioridad.	Unos recursos están disponibles porque algunas personas integrantes de la organización los han adquirido.	La organización se ha comprometido a adquirir los recursos necesarios para la seguridad. Estos recursos no están disponibles porque no se les dio prioridad en la gestión financiera.	La organización se ha comprometido a adquirir los recursos necesarios para la seguridad y estáhaciendo lo necesario para adquirirlos y poderlos ejercer.
Espacios	Existen espacios informales sobre todo en tiempo de crisis donde las personas integrantes de la organización comparten sus preocupaciones.	Existen espacios informales donde algunas personas integrantes de la organización comparten sus análisis y propuestas y ponen en común su evaluación de la estrategia de seguridad.	La política de seguridad de la organización define espacios para las etapas del proceso y su evaluación. En la práctica, estos espacios son insuficientes o no se priorizan.	La política de seguridad de la organización define espacios para todas las etapas del proceso y su evaluación. En la práctica se cumplen y el tiempo dedicado es adecuado para lograr una gestión integral de la seguridad.
Conclusiones	**El manejo de la seguridad es insuficiente.**	**El manejo de la seguridad es informal. No hay compromisos claros institucionales/ existen resistencias.**	**Existe un compromiso institucional por parte de la organización en favor de la seguridad. Aún falta concretarlo.**	**El compromiso institucional en favor de la seguridad se manifiesta en la práctica. Hay una gestión integral de la seguridad al nivel individual e institucional.**

Algunas preguntas para guiar las reuniones de seguimiento

- ¿Cuál es la situación de seguridad de la organización? ¿Hay nuevos IdS, nuevas amenazas, cambios en sus vulnerabilidades y capacidades, cambio en el contexto o en el trabajo que llevan? ¿Estos cambios les exponen a nuevos riesgos?

- ¿Han servido las herramientas compartidas durante el/los taller(es)? ¿Ha cambiado algo en la organización en cuanto a la importancia de la seguridad a nivel individual y organizativo? ¿Han logrado replicar/adaptar/usar otras herramientas y profundizar en el análisis de su seguridad? ¿Han institucionalizado un espacio y designado responsables para actualizar periódicamente este análisis?

- ¿Han logrado implementar algunas de las medidas de seguridad consensuadas en el/los taller(es)? Si no fue así ¿Cuáles han sido los obstáculos? ¿Las medidas estaban mal formuladas? ¿No eran realistas? ¿Las PDDH de la organización no las conocen? ¿Las personas integrantes de la organización experimentan resistencias para implementarlas?

Además de preguntar sobre los criterios presentes en la *Herramienta de monitoreo del Manejo de la Seguridad*, en las reuniones de seguimiento podemos trabajar con las PDDH para responder las siguientes preguntas:

- ¿Cuáles han sido las medidas de seguridad más eficientes de su plan de seguridad? ¿Han logrado desarrollar un poco más el plan de seguridad? ¿Han institucionalizado espacios y designado responsables para desarrollar/implementar/evaluar el plan y/o su estrategia de seguridad?

- ¿Han incorporado cuestiones específicas de género o de bienestar psicosocial en sus esquemas de seguridad y protección? ¿Han experimentado dificultades o tienen alguna barrera para integrar esquemas de trabajo con perspectiva de género y psicosocial que respondan a las necesidades de seguridad y protección?

- ¿Han desarrollado estrategias de seguridad aparte de las trabajadas en los talleres? ¿Han sido exitosas? ¿Han conseguido influenciar el comportamiento de otros actores? ¿Tienen buenas prácticas para compartir? ¿Estas estrategias responden a sus necesidades y los protegen eficazmente? ¿Se pueden adaptar o rectificar si la situación cambia?

- ¿Qué vacíos siguen identificando y dónde necesitan apoyo?

El proceso completo del Programa de Asesorías en Seguridad y Protección puede cerrarse de dos formas:

1 Se han brindado todas las herramientas posibles y de común acuerdo con las PDDH se decide cerrar el ciclo.

En este caso, la persona facilitadora organiza una reunión con las personas responsables del manejo de la seguridad para realizar conjuntamente una evaluación general del programa y del rendimiento de la organización en cuanto al manejo de su estrategia de seguridad y protección.

Durante la reunión de cierre:

- Se rellena conjuntamente una última *Herramienta de monitoreo del Manejo de la Seguridad* ya sea directamente sobre el formato (ver anexo) o se crea una herramienta específica basada en sus criterios evaluativos.

- Se llega conjuntamente a una conclusión acerca de si se puede cerrar el proceso o si más bien se necesita reabrir otro ciclo (existe la posibilidad de que organizaciones que han cerrado un proceso puedan pedir más adelante reaperturas de ciclos).

2 Si la organización no entra en contacto con la institución a cargo de la facilitación durante el año que sigue, el PASP se cierra automáticamente.

Notas

1 EGUREN/CARAJ, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, Protection International, 2010, p.71.

2 Este concepto fue desarrollado por Enrique Eguren y Liam Mahony en 1997. Véase: MAHONY/EGUREN, *En buena compañía: el Acompañamiento Internacional para la Protección de losDerechos Humanos*, 2ª ed., España, Universidad de Cantabria, 2006, pp.164-172.

3 Peace Brigades International, *Política de Seguridad*, Noviembre 2009.

4 El taller 1 y 2 fueron desarrollados con base en la metodología de Enrique Eguren y de la antigua Oficina Europa de PBI (BEO) que desde 2007 se convirtió en la organización independiente *Protection International*. El taller 3 se construye en base al "Taller Centroamericano Ampliando la Libertad de Expresión: Herramientas para la colaboración, información y comunicación seguras", (Hivos, SEDEM, SIMAS, 2006) así como a la *Guía de protección para defensores de derechos humanos, periodistas y operadores de justicia*, SEDEM, Guatemala, 2005. El taller 4 fue desarrollado primordialmente a partir de la metodología de Liam Mahony y de *Fieldview Solutions*. Dichas bases metodológicas han sido adaptadas y retroalimentadas a partir de reflexiones de ex voluntarios de PBI con trabajo de terreno con PDDH en México. Si bien los talleres 1 y 2 comparten un mismo piso conceptual con los talleres 3 y 4, cabe resaltar que son independientes. Los enfoques de los talleres 3 y 4 fueron determinados en gran medida por las necesidades particulares del acompañamiento internacional que PBI México y las PDDH acompañadas detectaron para mejorar este proceso.

5 PBI-México no ha ampliado el PASP a un trabajo enfocado exclusivamente en Seguridad Digital. Sin embargo si se han desarrollado asesorías prácticas y puntuales que responden a la necesidad de comunicar de forma más segura con las organizaciones acompañadas. Dichas asesorías están basadas en el material producido por *Tactical Technology Collective y Frontline Defenders*. Consúltese la Caja de Herramientas de Seguridad (*Security in a Box*), disponible en : https://securityinabox.org/es

6 Basado en: EGUREN, *Beyond Security Planning: Towards a Model of Security Management*, 2000.

7 Esta herramienta está basada en el método de evaluación con ejes cruzados de Enrique Eguren (EGUREN, *Beyond Security Planning : Towards a Model of Security Management,* 2000).

Taller 1
Riesgos de las Personas Defensoras de Derechos Humanos en México y diagnóstico de seguridad

El taller de introducción crea conciencia sobre los riesgos específicos que enfrentan las PDDH en México. Este taller clarifica conceptualmente las nociones de riesgo y aporta herramientas analíticas para consensuar el nivel y características del riesgo dentro de la organización que sirvan de base para una posterior elaboración de estrategias de seguridad apegadas a la realidad específica de las personas con las que trabajamos. Para lograr lo anterior, este taller trabaja sobre los siguientes elementos: análisis de contexto y actores, incidentes de seguridad y el entendimiento del riesgo a través de las amenazas las capacidades y las vulnerabilidades.

Objetivos generales del taller y resultados esperados:

- Sensibilizar sobre la importancia de los ámbitos de la seguridad y la protección y su relación con el trabajo cotidiano de defensa de los derechos humanos que llevan a cabo las personas defensoras.
- Impulsar una "toma de conciencia" sobre los riesgos relacionados con el trabajo de defensa de los DDHH en México.
- Presentar una metodología para la planificación de la seguridad dentro del trabajo de la organización.
- Compartir diferentes herramientas para analizar y valorar conjuntamente el tipo y nivel de riesgo al que se enfrentan en su trabajo cotidiano las PDDH.
- Entender las capacidades y vulnerabilidades y su relación con el riesgo.
- Identificar qué estrategia pueden adoptar las PDDH ante su nivel de riesgo específico y las distintas opciones sobre el mismo (si es aceptable, se debe reducir o hay que evitarlo).
- Identificar las amenazas que la organización debería priorizar y tener en cuenta antes de poder desarrollar una estrategia de seguridad.

Lo que el taller NO pretende:

- Asesorar o proponer a la organización sus estrategias internas.
- Brindar "tips" o medidas de seguridad genéricas.
- Emitir valoraciones sobre las estrategias, visiones o análisis de la organización con la cual se trabaja.
- Hacer planes, estrategias o protocolos de seguridad.

Duración total

***8 a 10 horas** (sin contar pausas).*

Calendarización

Considerar dar el taller en un día y medio. Contar al menos 2 horas de pausa en un día repartidas a lo largo del día. En caso de necesidad puede acortarse a un día ya que se trata de una introducción y completarse luego con asesorías de medio día para profundizar alguna herramienta (por ejemplo: análisis de una amenaza declarada o de IdS, mapeo de actores, análisis del riesgo, etc.).

Plan General del Taller:

Módulo 1: Bienvenida e introducción

Sesión 1 Presentación, expectativas, revisión de agenda y acuerdos de convivencia

Sesión 2 Situación de riesgo de las personas defensoras en México: concientización

Sesión 3 Entender qué es el riesgo y los pasos del diagnóstico de seguridad

Módulo 2: El Diagnóstico de Seguridad

Sesión 1 El análisis de contexto

Sesión 2 El mapa de actividades

Sesión 3 El análisis de actores

Sesión 4a Análisis de los Incidentes de Seguridad

Sesión 4b Análisis de amenazas declaradas *(opcional)*

Sesión 5 Análisis de vulnerabilidades y capacidades

Sesión 6 Acordar el nivel de riesgo e identificar las amenazas prioritarias

Módulo 3: Conclusión

Sesión 1 Compromisos de seguimiento, evaluación y cierre

Material y recursos:

- Hojas blancas
- Plumones
- Papelógrafos
- Una manta pegajosa o una superficie amplia y visible para todo el grupo que pueda servir de *Metaplán* *[ver Uso de herramientas complementarias en Cap. 3]*
- Cartulinas de colores
- Papelitos adheribles de colores
- Gafetes o etiquetas adhesivas
- Hilos de colores
- Papel foamy de colores
- Chinches
- Cinta adhesiva
- Anexos del Taller 1
- Computadora y proyector u otro equipo de proyección audiovisual (opcional)

Consejos generales para este taller:

Este taller es un taller de introducción que comparte conceptos y herramientas analíticas básicas. En esencia desarrolla seis pasos para analizar el entorno y las características propias de la organización y poder valorar su tipo y nivel de riesgo específico.

Hay que puntualizar que la seguridad no es una ciencia exacta y por ende no existen certezas absolutas, resaltando que lo único que propone este taller son una serie de herramientas para intentar analizar la seguridad de forma ordenada y metódica.

Las expectativas al entrar a este primer taller suelen ser muy altas y es común que las personas participantes esperen que se les enseñen tips o medidas genéricas de seguridad que puedan aplicar saliendo del taller. Ante este escenario se debe dejar claro que el proceso de seguridad toma tiempo y que no podemos comenzar una fase de planeación en seguridad sin compartir conceptos y un análisis (o diagnóstico) colectivo de la situación de seguridad de la organización. Este análisis debería ser la base previa para cualquier planificación o toma de decisión posterior en seguridad.

En un inicio los conceptos compartidos en el taller pueden ser difíciles de comprender. La persona que facilita debe simplificar las definiciones y en la medida de lo posible transcribirlas o plantearlas en las palabras de las personas participantes.

Cada paso del diagnóstico se puede hacer de forma independiente y darse bajo la forma de una asesoría puntual fuera del taller con el afán de profundizar alguna de las herramientas o conceptos (por ejemplo se podría dedicar medio día para analizar una amenaza declarada, una serie de incidentes de seguridad o un día entero para hacer un mapeo de actores).

Bienvenida e introducción

Presentación, expectativas, revisión de agenda y acuerdos de convivencia

50min

Objetivos específicos:

- Conocerse entre participantes y facilitadores.
- Presentar el PASP, sus criterios y marco conceptual básico.
- Conocer qué esperan las personas participantes del taller y consensuar los objetivos del mismo.
- Clarificar el rol de la persona que facilita, sus posibilidades y limitaciones.
- Aclarar la metodología que se usará durante el taller.
- Sondear el conocimiento previo del grupo y ajustar taller si es necesario.
- Revisar la agenda con base en los puntos anteriores. Presentar las diferentes partes del taller y acordar tiempos y pausas.
- Acordar las normas de convivencia que servirán de base para generar un espacio seguro desde la perspectiva psicosocial y garantizar condiciones de equidad durante todas las sesiones subsecuentes.
- Distribuir materiales complementarios y roles de apoyo para la facilitación.

Puntos clave:

- Generar una apertura del taller que facilite la confianza y conocimiento de todas las personas participantes.
- Subrayar que la persona que facilita está para catalizar la participación y que se está construyendo un espacio conjunto de conocimiento. Por ello la participación de todas las personas es crucial para el proceso.
- Visualizar cómo se intersectan las tres dimensiones del análisis del PASP para una visión integral de la seguridad.
- Dar definiciones básicas de seguridad y protección: "*Entendemos por protección el conjunto de actividades que desarrolla una organización de derechos humanos para garantizar la seguridad de otras personas defensoras y organizaciones con las cuales trabajan, mientras que con el de seguridad nos referimos a todas las medidas y estrategias enfocadas en resguardar la integridad física o psicológica de sus integrantes y que las mismas personas defensoras desarrollan e implementan hacia sí mismas.*"
- Abordar ideas más allá de lo convencional en seguridad (normalmente surgen cuestiones materiales de seguridad o ideas asociadas a represión o formas de violencia más explícitas). Hablar por ejemplo también del bienestar emocional, el estrés y la importancia de tener espacios para abordar dichos temas en relación con la seguridad.
- Enfatizar la necesidad de compromisos y seguimiento por parte de la organización ya que el programa de asesorías plantea impulsar y acompañar el propio proceso de seguridad que las PDDH desarrollen.
- Explicar los pasos del método de gestión de la seguridad usados por PBI. Diagnóstico > Planificación > Implementación > Evaluación.
- Consensuar normas de convivencia que promuevan las condiciones necesarias de respeto, diálogo e inclusión durante todo el taller. La persona que facilita debe estar segura que toda la gente se siente cómoda con los acuerdos alcanzados.

Materiales

- Papelógrafos
- Plumones
- Fotocopias con objetivos y agenda del taller
- Papelógrafo o diapositivas con definiciones de los conceptos de seguridad y protección y su relación con el espacio de actuación *[Gráfico 1a, cap.1]*, Componentes analíticos necesarios para un esquema integral de seguridad y protección *[Gráfico 1e, cap.1]* y con el gráfico del *Método de gestión de seguridad [Anexo T1.M1.S1]*
- Papelitos adheribles de colores
- Gafetes o etiquetas adhesivas
- Computadora y proyector (opcional solo en caso que la actividad 3 no se lleve a cabo con papelógrafo o pizarrón)

Recursos adicionales y lecturas de apoyo:

Para distintas dinámicas de presentación e integración grupal y distención:

- BERISTAIN & SORIANO, *La Alternativa del Juego I: Juegos y Dinámicas de Educación para la Paz. [RA1]*

Para comenzar adecuadamente con la construcción de un espacio seguro en un trabajo grupal sobre seguridad con PDDH:

- BARRY & NANIAR. *Integrated Security the Manual*, cap. 1.2, 1.3 y 3.4. *[RA4]*

Para entender los conceptos de seguridad y protección:

- Capítulo 1 de esta Guía.

Para entender el PASP, sus criterios y marco conceptual básico:

- Capítulo 2 de esta Guía

Actividades

Actividad 1: Ronda de presentación y expectativas del grupo.

Dinámica de presentación y discusión en plenaria* *10 min

Abrir con una ronda de presentación. Acompañar su nombre de pila por un adjetivo positivo con el que cada persona se describa a sí misma. P. ej. "Simón simpático". El adjetivo debe empezar con la misma letra que el nombre de pila para que se facilite la asociación entre cualidad y nombre.

Se pueden utilizar otras dinámicas de presentación pero independientemente de la dinámica de presentación utilizada es importante que las personas participantes comuniquen si ya han recibido talleres previos, y qué esperan del taller.

Se pueden apuntar motivaciones y expectativas en papelitos adheribles de colores para agruparlos en un lugar visible durante todo el taller. Estas expectativas se retomaran más adelante y al final del taller se revisarán para evaluar qué hemos cumplido y qué no.

Actividad 2: Lo que entendemos por "Seguridad".

Lluvia de ideas y discusión en plenaria a partir de preguntas detonadoras* *10 min

Plantear al grupo las siguientes preguntas:

> *¿Al mencionar "seguridad", cuáles son las palabras o ideas que nos vienen en mente?*
>
> *¿De qué se debería hablar dentro de una formación sobre seguridad?*

Apuntar las palabras y conceptos usados por las PDDH en un papelógrafo plenamente visible. Usar y hacer referencia a las palabras y conceptos retomándolos durante las fases subsecuentes del taller.

Actividad 3: Presentación del PASP.

Presentación oral con apoyo de elementos visuales (se puede usar papelógrafo, pizarrón o diapositivas en power point)* *10 min

Presentar de forma concisa en qué consiste el PASP, sus criterios y metodología. Bosquejar visualmente las tres dimensiones conceptuales que sustentan el programa de asesorías y los conceptos de seguridad y protección. *[ver definiciones conceptuales y gráficas de cap. 1 sección 1 y gráficos sobre estructura del PASP en cap. 2 sección 3 y 4 de esta guía]*

Explicar que el taller 1 es el primer paso del método de gestión de la seguridad usado por PBI. *[Anexo T1.M1.S1]*

Actividad 4: Revisión de expectativas y adaptación de agenda y contenidos del taller en caso de ser necesario.

Discusión en plenaria* *10 min

Presentar los objetivos y contenidos del taller consensuados previamente con la organización. Revisar junto con el grupo las expectativas expresadas en relación con los objetivos y la metodología del taller presentadas.

A partir de una perspectiva realista de las limitaciones en términos de tiempo, objetivos y contenidos del taller así como de las expectativas previamente

expresadas por las PDDH, explicar lo que podemos hacer en este taller y lo que no es posible o que puede ser abordado sólo en talleres posteriores.

Realizar ajustes si es necesario.

Pegar la agenda general del taller consensuada en un papelógrafo a la vista de todas las personas participantes.

Actividad 5: Acuerdos de convivencia, distribución de material complementario y roles de apoyo.

Discusión en plenaria y/o dinámica participativa ***10 min***

Acordar en conjunto las normas de convivencia: cómo pedir la palabra, cómo expresar con respeto nuestros desacuerdos, cómo garantizar condiciones de igualdad, confidencialidad de los aspectos tratados durante el taller, uso de celulares, computadoras y cámaras, entradas y salidas de participantes, puntualidad, etc. *[ver apartado sobre espacios con equidad y espacios seguros desde la perspectiva psicosocial en el apartado 3.2 y recursos de apoyo RA4]* Se puede realizar la "Dinámica de la Estrella" o alguna variante: Se pide a las personas participantes pararse en círculo y que vayan enunciando reglas que les parecen importantes. Cada vez que alguien enuncia una regla el resto de las personas muestran su acuerdo (acercándose al centro del círculo) o su desacuerdo (alejándose del centro del círculo). Si hay fuertes desacuerdos se busca el consenso. Después se hace un breve recuento de los acuerdos mínimos para la convivencia.

Después de las normas de convivencia se puede entregar material complementario (por ejemplo: un cuaderno del participante). Pedimos que no se lea inmediatamente ya que este se trabajará a lo largo del taller.

Dejar claro el rol de la persona que facilita y sus posibles limitaciones.

Distribuir roles de apoyo a la facilitación, preguntar a las personas participantes quién quiere ser voluntario/a para tomar actas y apuntar los consensos, para anotar otros pendientes y tareas que surjan durante el taller.

Consejos de facilitación:

- Se pueden utilizar distintas dinámicas de presentación para "despertar" o espabilar al grupo *[ver RA1]*. Si el grupo es numeroso y no se conocían previamente, también se pueden usar gafetes o adhesivos con el nombre de las personas para facilitar dirigirse a las personas por su nombre de pila y recordar los nombres.
- Se puede también pedir a las personas que además de las palabras y conceptos realicen un dibujo sobre su idea de seguridad y luego todo el grupo dice una lluvia de ideas sobre los dibujos de sus demás compañeros.
- En las partes con mayor carga conceptual se recomienda aprovechar al máximo los recursos gráficos propuestos.
- Con base en la actividad 1 y 2, puede ser necesario bajar las expectativas o ajustar la agenda para dedicar más tiempo a algunos temas, quitar otros etc. ¡Hay que ser flexibles y receptivos a la hora de tratar las expectativas del taller e ideas sobre seguridad y protección!
- Se puede consensuar un espacio para dejar los aparatos electrónicos como celulares y computadoras durante el taller (por ejemplo en la esquina de la sala o en una bolsa resguardada). Se puede consensuar cómo retribuirá al grupo alguien que llegue tarde a las sesiones o que pase por alto algún acuerdo de convivencia (por ejemplo puede traer dulces para todas las personas la siguiente sesión, o relevar al relator de acuerdos).
- ¡Atención con el control del tiempo! Este módulo es susceptible a extenderse demasiado.

Bienvenida e introducción

Situación de riesgo de las personas defensoras en México: concientización

30min

Objetivos específicos:

- Asumirse como defensor/a de DDHH.
- Asegurarse que participantes y facilitadores compartimos la visión que ser persona defensora de los DDHH en México entraña riesgos.
- Generar una "conciencia de la seguridad".
- Listar las amenazas latentes relacionadas al trabajo de defensa de DDHH en México y proponer una clasificación de estas según el objetivo que persiguen y su *modus operandi* para facilitar su identificación y análisis.

Recursos adicionales y lecturas de apoyo:

Sobre PDDH, su reconocimiento y el marco normativo nacional e internacional que les respalda:

- OACNUDH, Video Campaña "*Yo me declaro*".
- ONU, *Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos.* ***[RA7]***
- *Ley Federal de Protección para Personas Defensoras y Periodistas.* ***[RA8]***

PDDH en México y su situación en seguridad y protección:

- PBI-Proyecto México, *Panorama de la Defensa de los Derechos Humanos en México: Iniciativas y Riesgos de la Sociedad Civil Mexicana.* ***[RA8, puede consultar también otros informes de la sociedad civil o la OACNUDH referidos en esta sección]***

Puntos clave:

- Dar la definición y características de una PDDH.
- Dejar claro que el estado tiene una obligación de no atacar a las PDDH ni deslegitimizarles, de protegerles de ataques por parte de otros actores y de crear instituciones que prevengan, investiguen, sancionen y reparen los ataques en su contra. Aclarar que en México existe un marco legal que debería proteger a los defensores y que su actuación es legal y legítima.
- Dejar claro que ser defensor implica un riesgo.
- Definir lo que entendemos por amenaza latente: "*Una fuente de daño potencial o los peligros en nuestro entorno/contexto*" (causados por actores hostiles u otros factores hostiles).
- Proponer clasificación/tipología de amenazas latentes. Dejar claro que pueden haber distintas tipologías además de la propuesta por esta guía.
- Puntualizar que las amenazas pueden variar según el sexo, las normas de género que imperan en la comunidad donde trabajan las PDDH, la edad, las actividades, el tipo de derechos que se defienden y otros factores (por ejemplo, defensores comunitarios podrían enfrentar más criminalización, mientras mujeres defensoras podrían enfrentar más agresiones físicas de carácter sexual).

Actividades

Actividad 1: Definiendo a las Personas Defensoras de DDHH. *Lluvia de ideas y discusión en plenaria a partir de preguntas detonadoras* *10 min*

Escoger una de las dos actividades siguientes:

a) Plantear al grupo las siguientes preguntas:
¿Quiénes son las personas defensoras de derechos humanos?
¿Qué hacen?
¿Hay criterios o requisitos para ser una persona defensora?

b) Proyectar video "Yo me declaro" ***[ver enlace en RA7]*** plantear al grupo las siguientes preguntas:
¿Qué tienen en común estas personas?
¿Dónde trabajan?
¿Su trabajo es parecido al nuestro?

Al terminar la actividad elegida apuntar las ideas en el pizarrón o papelógrafo que surjan de las respuestas. Resumir las ideas y sacar conclusiones. Presentar una definición conjunta que englobe las ideas propuestas. Se puede apoyar también en las definiciones de la ONU o de la *Ley Federal de Protección para Personas Defensoras y Periodistas.* ***[RA8]***

Materiales

- Papelógrafos
- Plumones
- Papelógrafo o diapositivas con *Tipología de las amenazas latentes para personas defensoras de los DDHH* *[Anexo T1.M1.S2]*
- Computadora y proyector (opcional solo en caso que se decida proyectar el video "Yo me declaro")

Actividad 2: Amenazas latentes para las PDDH en México.

Lluvia de ideas y discusión en plenaria a partir de preguntas detonadoras

20 min

Plantear al grupo las siguientes preguntas y debatir:

> *¿Qué amenazas latentes enfrentan los y las defensoras de DDHH en México? o ¿Qué peligros corre una persona defensora en México?*

Apuntar ideas, agruparlas y proponer clasificación/tipología de estas amenazas latentes. Se puede proponer una clasificación construida grupalmente o utilizar la que propone esta guía

Consejos de facilitación:

Actividad 1:

- Algunos grupos o participantes no estarán acostumbrados al concepto de PDDH, incluso el concepto de "Derechos Humanos" puede resultarles extraño a algunas personas. Otras pueden tener dificultad para asumirse como PDDH. En estos casos se debe explicar el concepto con términos más próximos: *¿Quiénes son las personas que buscan conseguir mejoras para sus familias y la comunidad? ¿Qué hacen y cómo lo hacen? ¿Qué quieren para sus comunidades?* Relacionar estas "esperanzas" con los derechos humanos que tiene la comunidad para luego hacer ver que, persiguiendo estos objetivos, todos se vuelven PDDH. Legitimizar esa categoría mostrando que incluso la reconoce la ley nacional e internacional aunque en la realidad les falten garantías de reconocimiento.
- Puede ser buena idea también compartir otros ejemplos de defensores o su propia experiencia. En vez de usar la definición se puede dibujar un personaje e ir añadiéndole características.
- Si por el contrario las personas participantes ya manejan estos conceptos, la sesión se puede enfocar en compartir el concepto de amenaza latente y la clasificación de amenazas latentes.

Actividad 2:

- No asumir que todas las personas del grupo tienen conciencia o la misma conciencia sobre los riesgos de ser defensor/a. Es importante darse cuenta si hay gente que no está muy enterada (personas de administración, servicio social, etc. a veces están presentes y muchos realmente no tienen esta conciencia). Puede ser útil tener las últimas cifras sobre agresiones a defensores disponibles en distintos informes de fuentes confiables sobre DDHH ***[Ver RA8]*** y ver si la organización es de un estado en donde se considera especialmente peligroso defender los derechos humanos.
- Es difícil explicar lo que es una amenaza latente (y luego diferenciarla con las amenazas declaradas y el riesgo que se explican más adelante en el taller). Una opción puede ser referirse a ellas como peligros.
- Es aconsejable no perder tiempo en definiciones muy técnicas y explicar cada concepto con las propias palabras de las personas participantes. Abogados de la ciudad por ejemplo tienden a apreciar las definiciones más técnicas mientras que con defensores comunitarios puede ser mejor usar términos más simples, dibujos, metáforas. ¡Hay que pensar en la terminología según el público!
- Atención con las cuestiones psicosociales delicadas! Durante esta actividad pueden empezar a surgir historias personales o de la organización muy específicas. Hay que saber encauzar y evitar que se salgan de control sobre todo si fueron experiencias difíciles o que abordan aspectos delicados desde la perspectiva psicosocial. Se debe recalcar que en esta sesión se abordan las amenazas a nivel general sobre PDDH para entender su relación con la seguridad en general y que por otro lado debe haber otros tiempos y espacios adecuados para abordar este tipo de experiencias a nivel individual y organizativo.

Bienvenida e introducción

Entender qué es el riesgo y los pasos del diagnóstico de seguridad

35min

Objetivos específicos:

- Entender el riesgo y sus componentes.
- Dar a conocer los pasos del Diagnóstico de Seguridad.

Materiales

- Papelógrafos
- Plumones
- Papelógrafo o diapositivas con gráficos según las opciones elegidas en la Actividad 1 *[Anexo T1.M1.S3a y/o Anexo T1.M1.S3b]* y con *Los pasos del Diagnóstico de Seguridad [Anexo T1.M1.S3c]*

Recursos adicionales y lecturas de apoyo:

Sobre el Riesgo y dinámicas alternativas para trabajar el concepto:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.2. ***[RA5]***
- Front Line Defenders, *Manual sobre seguridad: Pasos prácticos para defensores/as de derechos humanos en riesgo*, cap. 2. ***[RA5]***
- Protection International, *Guía de facilitación para el nuevo manual de protección para los defensores de derechos humanos*, pp. 63-70. ***[RA2]***
- Centro de Derechos Humanos Fray Francisco de Vitoria-Comité Cerezo, *Manual de Introducción: Seguridad en las organizaciones civiles y sociales*, cap. 3. ***[RA5]***

Puntos clave:

Sobre el riesgo:

- Definir el riesgo: "*La posibilidad de que nos pase algo que nos cause daño*"
- Entender que el riesgo se compone de varios elementos sobre los cuales podemos trabajar independientemente: amenazas, vulnerabilidades y capacidades.
- Definir qué es una amenaza: "*La posibilidad de que alguien dañe la integridad física o moral de otra persona, o su propiedad, mediante una acción intencionada y a menudo violenta*"
- La amenaza es algo externo a nosotros. Podemos intentar incidir sobre ella pero no es seguro que lo logremos.
- Definir qué es una capacidad (puntos fuertes o fortalezas: "*puntos fuertes y recursos a los que puede acceder un/a defensor/a para lograr un nivel respetable de seguridad*") y una vulnerabilidad (puntos débiles o debilidades: "*grado en que los/las defensores/as son susceptibles a pérdida, daños, sufrimiento o la muerte en caso de un ataque*")
- Las vulnerabilidades y capacidades son características nuestras, propias, internas, sobre las cuales podemos trabajar.
- Las vulnerabilidades y capacidades comprenden también factores emocionales, de bienestar emocional y de lazos sociales de más o menos solidaridad.
- El riesgo es dinámico (varía en el tiempo), circunstancial (depende del contexto) y subjetivo (porque cada persona en la organización puede percibirlo de forma diferente).
- El riesgo depende de la amenaza pero también de las capacidades y vulnerabilidades ante esta amenaza. Aun en el mismo contexto o amenaza no todas las PDDH tienen el mismo riesgo porque cada quien tiene vulnerabilidades y capacidades diferentes y se involucra de distinta manera en la organización.
- Si uno de los componentes del riesgo cambia, el riesgo también cambia (se mueve toda la balanza). Para bajar el riesgo debemos reducir nuestras vulnerabilidades, aumentar nuestras capacidades e incidir sobre la fuente de la amenaza.
- Como vimos antes, las PDDH en México podrían enfrentar muchísimas amenazas latentes, sin embargo el que estas amenazas se cumplan depende de las características y el contexto de cada organización. Lo que haremos ahora es seguir unos pasos de análisis para saber cuáles amenazas son reales y cuáles deberíamos considerar de forma prioritaria en un *plan de seguridad*.

Sobre el Diagnóstico de Seguridad:

- El diagnóstico es un proceso que a su vez consiste en una serie de pasos para analizar la situación de seguridad.
- Es la base sobre la cual se definirá la estrategia y las medidas de seguridad adaptadas a la organización o a cada grupo de PDDH específico.
- Como todo análisis ¡el diagnóstico no es estático! Al depender de la coyuntura, cambia con el tiempo y por eso se debe reevaluar periódicamente.
- Idealmente debería involucrar a todas las personas en la organización.

Consejos de facilitación:

- Actividad 1: Se recomienda utilizar la metodología más adaptada al público; la dinámica A suele ser más abstracta y es apta para público familiarizado con fórmulas. Las dinámicas B, C y D son más gráficas y se pueden adaptar a contextos comunitarios o no alfabetizados.
- La seguridad y la protección no son una ciencia exacta y por ello se debe remarcar que la fórmula es sólo aproximativa. Evitar una presentación cargada de fórmulas y conceptos sin interacción con las personas participantes. Las definiciones hasta cierto punto son secundarias; lo que importa es que cada concepto quede claro y que todo el grupo tenga un piso común para empezar a trabajar. Los conceptos pueden ir profundizándose a lo largo del taller.
- Es común que exista confusión entre el concepto de riesgo y el de amenaza. Explicar en este caso que las amenazas son los peligros y el riesgo es el punto en que estos peligros pueden llegar a suceder y afectar a la organización y sus integrantes. Explicar que el riesgo depende de la amenaza pero también de qué tan expuestos estamos a esa amenaza i.e. *¿Qué tan probable es que la amenaza nos haga daño según nuestros puntos fuertes y débiles?*
- Es común que exista confusión entre vulnerabilidades y elementos del contexto. En este caso clarificar con ejemplos: subrayar que las vulnerabilidades son internas a la organización y los hábitos y condiciones personales. Remarcar que las vulnerabilidades cambian según el contexto.
- Al afirmar que un Diagnóstico de Seguridad debería involucrar a todas las personas de la organización suele suceder que algunas organizaciones no compartan este esquema de trabajo. Para entrar en este diálogo podemos dar una explicación más amplia de porqué consideramos importante que sea hecho por todas y todos en la organización, cuál es el valor añadido de cada persona y también la responsabilidad que tiene una organización con sus integrantes para que sepan que están en riesgo si es que aún no lo saben. Recordamos el tema de los puntos débiles y podemos dar ejemplos de IdS con personas de administración, servicio social o puestos/personas que no están en contacto directo con la defensa de los derechos humanos o no tienen un rol tan visible en la organización.

Actividades

Actividad 1: Entender el riesgo y los factores que lo conforman.

Presentación oral con apoyo de elementos visuales (se puede usar papelógrafo, pizarrón o diapositivas en power point) 20 min

Definir el riesgo y explicar sus componentes. Para lo anterior se pude escoger una de las siguientes opciones o combinar varias de ellas:

a) La ecuación del riesgo: R= (A x V) / C y la ponderación de sus componentes: *[Anexo T1.M1.S3a]*

b) Analogía del riesgo: *El Niño y la enfermedad*

Dibujamos 2 niños, uno gordito feliz con buena salud y el otro muy flaco, débil. Explicamos que hay una epidemia de gripe en la región (= *Amenaza*) y por ende existe la posibilidad de que se enfermen (= *Riesgo*). Vamos inventando con las personas participantes las *fortalezas* y *debilidades* que tienen estos dos niños para evaluar la *probabilidad* que uno de los dos se enferme y las consecuencias para este niño si se enferma (= *Impacto*). Por ejemplo, el gordito tiene buena alimentación (probabilidad más baja de agarrar el virus) y vive en una comunidad donde hay servicios de salud y medicamentos gratuitos para las familias (impacto bajo: se podrá curar), mientras que el niño flaquito sufre de malnutrición (más probabilidad de enfermarse), no tiene acceso a servicios de salud y no puede comprarse medicamentos (consecuencias más graves si se enferma). El riesgo para el primero es por ende más bajo que para el segundo.

c) Analogía del riesgo: *La Milpa*

Dibujamos una milpa. Abordamos en plenaria:

¿Cuáles son los problemas que pueden dañar a la cosecha? (= *Amenaza*), ver las características de la milpa que la hace más vulnerable a éstas amenazas (p. ej. Tiene o no sistema de agua, fertilizante, tierra fértil, etc.) y que podría por ende ocurrir (= *Riesgo*).

d) Mostramos el gráfico del anexo *Debatir sobre riesgos y amenazas en comunidades [T1.M1.S3b]* o lo replicamos en el papelógrafo Abordamos con el grupo cuáles serían las amenazas, vulnerabilidades, capacidades y cómo cambiaría el riesgo en las distintas situaciones.

e) Dinámica Alternativa: "*El riesgómetro*". *[Ver Centro de Derechos Humanos Fray Francisco de Vitoria-Comité Cerezo, p.40-45, referencia en RA5]*

Actividad 2: Los pasos del Diagnóstico de Seguridad.

Presentación oral con apoyo de elementos visuales (se puede usar papelógrafo, pizarrón o diapositivas en power point) 5 min

Explicar que el diagnóstico está conformado por 6 pasos *[ver Anexo T1.M1.S3c]* y puntear cada uno de ellos someramente para hilar este módulo con el siguiente.

El Diagnóstico de seguridad

El análisis de contexto

25min

Objetivos específicos:

- Identificar y explicar los fenómenos sociales, políticos, económicos, legales, las normas de género, etc. que impactan en el trabajo de las PDDH.

Materiales

- Papelógrafos
- Rótulos o tarjetas de colores
- Plumones
- *Metaplán*

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos,* cap. 1.1.
- Front Line Defenders, *Manual sobre seguridad: Pasos prácticos para defensores/as de derechos humanos en riesgo*, cap. 6 ***[RA5]***
- Consejo de Educación Popular de América Latina y el Caribe, *Guía para hacer análisis de coyuntura*, ***[RA11]***

Consejos de facilitación:

- Es necesario conocer previamente un mínimo del contexto de las PDDH para poder dar ejemplos concretos que les sean familiares o hacer preguntas que guíen las discusiones si estas se estancan.
- En general las PDDH llevan a cabo un análisis de contexto de manera informal. Si la organización ya hace formalmente análisis de contexto, no extenderse tanto en el análisis, sino destacar su impacto en la seguridad.
- Evitar que redunden sobre el contexto ya que puede extenderse demasiado esta discusión.

Puntos clave:

- Dejar claro que el análisis de contexto es importante porque los riesgos dependen del contexto.
- Ver que el contexto afecta de manera diferente a defensoras y a defensores y que existen diferencias de género que están relacionadas con el riesgo específico de las PDDH.
- Resaltar la importancia de contar con fuentes fiables y diversas.
- Enfatizar que el contexto es dinámico y está en constante cambio. Por ende los riesgos también cambian y es importante analizar el contexto regularmente.
- Es imposible saber el futuro, sin embargo se pueden entender mejor los actores y condiciones que nos pueden llegar a afectar si llevamos a cabo un análisis del contexto periódicamente.

Actividades

Actividad 1: Entender el contexto y las fuentes de información.

Discusión en plenaria o trabajo en grupos a partir de preguntas detonadoras

25 min

Plantear al grupo las siguientes preguntas y debatir:

> *¿Cuáles son los elementos económicos, sociales y políticos del contexto que tienen un impacto sobre la seguridad de la organización y de sus integrantes? ¿Este impacto es diferente para hombres y mujeres?*
>
> *¿De dónde obtenemos nuestra información?* (fuentes: rumores, comunidad, informes, prensa, etc.) *¿Qué tan fiables son nuestras fuentes?*

Para otros ejemplos de preguntas que pueden guiar la discusión: ver Protection International, *Nuevo Manual…*, pp.20-21 ***[RA5]***

Escoger una de las siguientes dinámicas:

a) Dividir a las personas en dos grupos; uno que trabaje sobre los elementos contextuales y otro que trabaje sobre las fuentes de información. Al terminar la discusión cada grupo presenta en papelógrafos los elementos más relevantes de su discusión (pueden valerse de dibujos, palabras o mapas conceptuales en los papelógrafos).

b) *Metaplán*; Alternativamente, se pueden distribuir cartulinas de dos colores distintos para cada segmento (un color para los elementos del contexto y otro para las fuentes) y dividir el *Metaplán* en dos partes (elementos de un lado y fuentes del otro). Las personas participantes identifican y apuntan respuestas en los rótulos que van pegando en el *Metaplán*. La persona que facilita ordena las cartulinas según el tipo de fuentes/elementos. Acabamos en plenaria escogiendo algunas de las respuestas y pidiendo al participante que la colocó que explique su respuesta.

El Diagnóstico de seguridad

El mapa de actividades

15min

Objetivos específicos:

- Identificar las principales actividades de la organización que podrían tener consecuencias sobre su seguridad.
- Valorar si se necesitan formalizar espacios y responsables dentro de la organización para actualizar periódicamente el análisis de contexto y el mapa de actividades.

Materiales

- Pizarrón o papelógrafo
- Plumones

Puntos clave:

- Hay que considerar el impacto de las medidas/actividades que se toman y cómo podrían reaccionar los diferentes actores.
- Puntualizar que no todas las actividades de la organización conllevan riesgos. No todas molestan a actores con capacidad de acción.
- Rescatar las iniciativas y acuerdos en cuanto a espacios para compartir y analizar la información dentro de la organización.

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.1. ***[RA5]***

Actividades

Actividad 1: Identificar los intereses de agresores y situaciones potenciales de riesgo.

Discusión en plenaria a partir de preguntas detonadoras 15 min

Guiar la discusión con las siguientes preguntas y debatir en plenaria:

> *¿Cuáles son las principales actividades de la organización que pueden ir en contra de los intereses de los potenciales agresores?*
>
> *¿Hay eventos planeados que pueden alterar la situación de riesgo de la Organización? (actividad pública, publicación de informe, etc.)*
>
> *¿Cuándo es más probable que las personas integrantes de la organización puedan sufrir una agresión?*

Actividad 2: Identificar espacios para compartir y analizar la información.

Discusión en plenaria y toma de acuerdos por parte de la persona designada como relatora 5 min

Guiar la discusión con las siguientes preguntas y debatir en plenaria:

> *¿Quién busca la información en su organización, quién la analiza?*
>
> *¿Hay un espacio para compartir y analizarla conjuntamente?*

Valorar si hay que formalizar el análisis de contexto y de actividades dentro de la organización. Intentar llegar a compromisos si el grupo valora relevante el ejercicio.

Consejos de facilitación:

- Esta sesión se hace antes del análisis de actores porque puede brindar un ejemplo (de actividad, de objetivo) para luego realizar el ejercicio de las flechas y el mapeo de actores. En el caso de PDDH que realizan su trabajo en organizaciones menos estructuradas puede evitar que se pierdan y que reafirmen qué actividades les implican riesgos y porqué.
- Este módulo es útil también para el ejercicio posterior sobre incidentes de seguridad que liga los IdS con las actividades de la organización.
- Invitar a las personas participantes a que valoren si necesitan formalizar el análisis de contexto definiendo responsables y espacios para llevarlo a cabo periódicamente. Si existe voluntad, intentar llegar a un acuerdo y pedir a la persona que apoya con la relatoría que tome nota ¡Ojo con no forzar compromisos!

El Diagnóstico de seguridad

El análisis de actores

1h 40min

Objetivos específicos:

- Compartir herramientas que permiten identificar y mapear los actores que pueden afectar positivamente o negativamente la seguridad de la organización
- Identificar a los actores que podrían amenazar o atacar a la organización: sus intereses, relaciones y capacidades.

Materiales

- Papelógrafos
- Plumones
- *Metaplán*
- Papelógrafo o diapositivas con *Análisis del campo de fuerzas [Anexo T1.M2.S3a]* y *Mapeo y análisis de actores [Anexo T1.M2.S3b]*
- Rótulos o tarjetas de colores
- Papelitos adhesivos de colores
- Hilos gruesos de colores
- Figuras de cartón (estrellas y burbujas)

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.1.
- Front Line Defenders, *Manual sobre seguridad: Pasos prácticos para defensores/as de derechos humanos en riesgo*, cap. 6. *[RA5]*

Puntos clave:

- Los actores y las relaciones que mantienen el uno con el otro no son estáticas, cambian con el tiempo y por eso hay que actualizar nuestros mapeos de actores regularmente.
- Las relaciones entre actores pueden no estar bien definidas.
- Hay que analizar los actores a nivel macro (a nivel de país o región) y micro (en la zona que trabaja la organización). Es necesario ser detallistas (por ejemplo en una misma secretaría de gobierno pueden haber actores a favor y en contra). Intentar poner nombre y apellido a los actores en la medida de lo posible.
- El análisis de actores nos permite ver qué actores están dispuestos y tienen la capacidad de protegernos; qué actores tienen la voluntad y capacidad de oponerse a nuestro trabajo, amenazarnos y atacarnos y cómo se relacionan todos estos actores entre sí.
- El análisis de actores también nos permite ver de dónde pueden provenir las amenazas y qué capacidad tienen estos actores para dañarnos y si son sensibles o no al costo político. Podemos establecer también las cadenas de responsabilidad.
- Debemos ser conscientes sobre la necesidad de tener un análisis e información más completa sobre los diferentes actores que pueden afectar nuestro trabajo.

Actividades

Actividad 1: Analizar el campo de fuerzas.

Discusión en plenaria y/o trabajo en grupos* *30 min

Recrear en un papelógrafo o *Metaplán* el *Análisis del campo de fuerzas. [ver anexo T1.M2.S3a]* Dividir en grupos o elaborar en plenaria según el tamaño del grupo.

Identificar el mandato (objetivo general) de la organización rellenando el óvalo con las ideas aportadas por el grupo. También se puede hacer con una campaña, un proyecto o un caso específico de la organización.

Rellenar el esquema de campo de fuerzas situando a distintos actores dentro de las grandes flechas. Se pueden usar papelitos adhesivos para los distintos actores; instituciones, empresas, grupos del crimen organizado, instituciones y personas de gobierno, de otras organizaciones, de organismos internacionales, medios de comunicación, etc.) El ejercicio asume que los problemas de seguridad podrían venir de fuerzas o actores opuestos a los objetivos de la organización. Por el contrario, las fuerzas de apoyo podrían ser aprovechadas para mejorar su seguridad.

Identificar las fuerzas (actores) de apoyo, de oposición y de dirección desconocida

(usar papelitos de distintos colores). Pedir que señalen con un símbolo distintivo *cuáles actores tienen una obligación o un interés en proteger a las personas defensoras*. Tomar actas de esta parte porque sirve de base para una parte del Taller 2.

Compartir conclusiones en plenaria, pedir a las personas participantes que no expliquen todo el diagrama sino:

1) *¿Fue difícil hacer el ejercicio?*
2) *¿Hubo debate?* en caso afirmativo *¿sobre qué fuerzas/actores no estaban de acuerdo?*
3) Si pueden evaluar resultados a partir de las siguientes preguntas: *¿cuáles actores tienen una obligación o un interés en proteger a las personas defensoras? ¿pueden eliminar el riesgo generado por las fuerzas de oposición con la ayuda de las fuerzas de apoyo?*

*Actividad alternativa 1b: Analizar el campo de fuerzas con defensores de base.

Ejercicio en grupos y discusión en plenaria** **60 min

Se recomienda para sustituir la actividad 1, especialmente para trabajar con PDDH comunitarios.

En pequeños grupos, las PDDH comparten sus esperanzas:

¿Qué queremos legar a nuestros hijos e hijas?

¿Cómo quisiéramos que sea la comunidad?

Cada grupo debe acordar 3 metas para el futuro de la comunidad. Una persona escribe o dibuja una idea por cartón.

Cada grupo presenta sus ideas y las pega en la manta del *Metaplán*. Se eliminan luego las ideas que se repiten para tener una lista de los objetivos de la organización.

Preguntamos:

¿Quiénes son las gentes, organizaciones, gobiernos, etc. que tienen influencia sobre la vida de la comunidad?

Para ser más específico: ¿Quiénes nos ayudan a cumplir con nuestros objetivos? ¿Quiénes están en contra de estos objetivos? ¿Quiénes nos crean problemas? Pedimos que escriban o dibujen los actores en cartulinas.

En el *Metaplán* hemos agrupado los objetivos en la actividad precedente. Pegamos dos flechas grandes de cartón (una verde hacía los objetivos y una roja en el sentido contrario). Pegamos las cartulinas de actores al lado o dentro de las grandes flechas (en pro o en contra).

Actividad 2: Mapeo de actores.

Trabajo en grupos sobre Metaplán y presentación en plenaria** **70 min

Preguntar antes del taller si la organización prefiere hacer un mapeo general o un mapeo de actores relacionados a una actividad en particular (puede ser que hayan detectado que el riesgo viene de esa actividad particular). Puede surgir también del módulo anterior.

El ejercicio consta de cuatro partes:

1) *Identificar los actores agresores (actores cuyos intereses se ven negativamente afectados por el trabajo de la organización).*

   Se ponen a disposición de las personas participantes tarjetas de colores

Consejos de facilitación:

- Preguntar antes de la actividad 1 qué prefiere la organización (a lo mejor ya han ubicado que el riesgo viene de una actividad en particular y prefieren enfocar el diagnóstico de seguridad en dicha actividad y no en el objetivo general de su organización).
- Es necesario conocer previamente un mínimo del contexto de las personas participantes para poder dar ejemplos concretos que les son familiares o hacer preguntas que guíen las discusiones si estas se estancan.
- Las PDDH suelen decir "gobierno", "policía" o actores genéricos. Es importante que pidamos un análisis más detallado (i.e. *¿Todos dentro de esa institución? ¿No hay nadie que podría ser aliado?*) para mostrar que el Estado no es monolítico y que es importante diferenciar las personas de las instituciones y ponerle nombres y apellidos.
- La idea con el ejercicio 2 es no solo identificar los potenciales actores agresores, sino su interés real o voluntad en atacar y su capacidad en llevar a cabo un ataque concreto.
- Se pueden guardar los papelógrafos o tomar fotos del *Metaplán* para que la organización profundice el ejercicio después con más tiempo. Se debe guardar una copia del resultado del ejercicio para el Taller 2. ¡Ojo, son documentos sensibles por lo cual los registros documentales deben ser resguardados adecuadamente!
- Al final de la sesión todos deberían compartir un mejor entendimiento del entorno en el que trabajan. Esto permitirá tomar decisiones informadas y conscientes sobre seguridad y protección en las sesiones y talleres futuros.

diferentes (un color por nivel; local, estatal, federal). En las cartulinas las personas participantes van escribiendo nombres de actores (un actor por tarjeta) y los van pegando en el *Metaplán*.

2) *Identificar sus intereses (económicos, militares, políticos, territoriales, impunidad, etc.).*

Se ponen a disposición papelitos adheribles de colores diferentes (un color por interés, pe. económicos legales o ilegales, políticos, impunidad, control territorial, militar, etc.). Las personas participantes van pegándolos en las cartulinas de actores.

3) *Identificar las redes de intereses y relaciones entre los actores.*

Se utilizan hilos gruesos de colores (mismo color que los papelitos adhesivos) para relacionar a los actores entre ellos según sus intereses. Al final se obtienen redes de diferentes colores según los intereses (ej: red de hilos amarillos para todos los actores que tienen intereses económicos).

4) *Distinguir entre autores intelectuales y autores materiales e identificar la cadena de mando.*

Se ponen a disposición del grupo estrellas de cartón (para autor material de las agresiones) y burbujas de cartón (para los autores intelectuales) que las personas participantes tendrán que posicionar sobre las cartulinas de actor. *[ver ejemplo en anexo T1.M2.S3b]*

Compartir conclusiones en plenaria guiando la discusión con las siguientes preguntas: 1) *¿podría haber un costo político para los actores si les atacan?* (evaluación de la racionalidad del actor y su cálculo de costos políticos) A partir de las respuestas a la pregunta anterior pedir que el grupo reflexione 2) *¿Sobre qué actores se puede ejercer un poder de disuasión?*

*Actividad alternativa 2b: Mapeo de actores con defensores de base.

Discusión en plenaria 30 min

Se recomienda para sustituir la actividad 2, especialmente para trabajar con PDDH comunitarios.

Preguntamos:

¿Quién es aliado de quién?

¿Quién manda a quién?

¿Quién nos atacó o nos podría atacar?

En el *Metaplán* trabajamos con las cartulinas "en contra"; agrupamos a los que son aliados entre sí, que tienen intereses similares y con un hilo vamos dibujando la "cadena de mando" para ilustrar quién manda a quién. Finalmente resaltamos a los actores que podrían atacar directamente con adheribles de colores.

**Actividad alternativa: Matriz para el análisis de actores.

Trabajo en grupo 10 min

Opcional, se sugiere para complementar las actividades 1 y 2 ya que la matriz toma en cuenta no solo los actores agresores sino los actores que deberían o podrían proteger a la organización.

Llenar en un papelógrafo o *Metaplán* en conjunto con el grupo una Matriz para el análisis de actores. *[ver ejemplo en anexo T1.M2.S3c]*

El Diagnóstico de seguridad

Análisis de los Incidentes de Seguridad

1h

Objetivos específicos:

- Compartir herramientas para la identificación y el análisis de los incidentes de seguridad.
- Realizar un breve análisis de los incidentes de seguridad.

Materiales

- Rótulos o tarjetas de colores
- Plumones
- *Metaplán*
- Papelógrafo o diapositivas con anexos sobre análisis de IdS *[T1. M2.S4a, T1.M2.S4b y T1.M2.S4c]*

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.3 y 1.4.
- Front Line Defenders, *Manual sobre seguridad: Pasos prácticos para defensores/as de derechos humanos en riesgo*, cap. 3. ***[RA5]***
- BARRY & NANIAR. *Integrated Security the Manual*, cap. 3.2. ***[RA4]***

Puntos clave:

- Definir lo que es un Incidente de Seguridad (IdS): "*Cualquier hecho o acontecimiento fuera de lo común que pensamos podría afectar a nuestra seguridad personal o como organización*".
- Explicar que los IdS son indicadores de nuestra situación de seguridad. Nos permiten medir el impacto de nuestro trabajo.
- Clarificar las diferencias entre distintos tipos de IdS (internos, externos, provocados, fortuitos, de origen político, incidental o relacionado con la delincuencia común).
- Cuando tenemos duda de si es o no es un IdS intencionalmente provocado y debido a nuestro trabajo, es mejor considerarlo como tal.
- Puntualizar los pasos a seguir para registrar los IdS y recalcar la importancia de mantener una bitácora actualizada de registro detallado (qué, cuándo, dónde, quién, fuente información, etc.).
- Enfatizar la importancia de definir formalmente al interior de la organización las responsabilidades y espacios de análisis conjunto en torno a los IdS como son compartir y analizar (destacar pautas y patrones como repetición, aumento; determinar el tipo y origen de IdS, si hay violencias específicas de género) y reaccionar ajustando las medidas de seguridad.
- Explicar que algunos IdS, pueden llegar a ser amenazas declaradas. Sin embargo no todos los IdS son amenazas. Las amenazas declaradas provienen necesariamente de actores externos, son intencionales y debidas a nuestro trabajo. Incluyen necesariamente una indicación de que pretenden hacernos daño, deben ser reales y concretas. Su propósito es infundir miedo y paralizar nuestro trabajo (dar ejemplo de una amenaza de muerte).
- Explicar que aunque no existe una regla universal, muchos de los ataques a personas defensoras ocurren tras una serie de señales. Normalmente las personas defensoras se dan cuenta de eso cuando miran una agresión en retrospectiva.

Actividades

Entender los incidentes de seguridad.

Presentación 30 min

Explicar qué es un incidente de seguridad (IdS) ver *Definición y análisis básico de los Incidentes de Seguridad [Anexo T1.M2.S4a].*

Explicar que las amenazas declaradas pueden ser un tipo de IdS, características y pasos a seguir ver *Pasos a seguir para registrar un IdS [Anexo T1.M2.S4b]* y *Bitácora de registro de IdS [Anexo T1.M2.S4c].*

Actividad 2: Identificar los IdS de la organización.

Trabajo individual y presentación en plenaria 30 min

Disponer rótulos o tarjetas de colores:

Tarjeta roja: IdS externos intencionales.

Tarjeta amarilla: IdS no se sabe si fue provocado o fortuito.

Tarjeta azul: IdS interno o fortuito.

Cada participante tiene derecho a tres cartulinas, deberá pensar en tres IdS que hayan pasado en los últimos 12 meses y escribirá en cada tarjeta un IdS y el mes en el que ocurrió.

Se escoge el color de la tarjeta en función del tipo u origen del IdS.

Las personas participantes pegan sus cartulinas en el *Metaplán*. 2 o 3 participantes presentan sus IdS al grupo.

La persona que facilita puede preguntar detalles de algunos de los IdS (qué, cuándo, dónde, quién, fuente información). Se puede preguntar al grupo si hay algunos IdS ahí que sorprenden o que no se entienden como IdS.

Analizar los IdS de la organización con el grupo de la siguiente manera:

1) *Análisis temporal:* Colocamos las cartulinas sobre una línea del tiempo, según el mes en el que se dieron. Preguntamos: *¿Se puede relacionar el aumento de IdS con una actividad o un contexto específico?*

2) *Análisis según el origen:* Apartamos los IdS internos o fortuitos (tarjetas azules) *¿De qué actor podrían venir los demás IdS?* (origen político, delincuencia común, incidentales). Se pueden recuperar las cartulinas de actores del Mapeo de Actores de la sesión anterior y pegarlas al lado de los Incidentes.

3) *Análisis de las amenazas latentes:* Intentamos colocar los IdS bajo los tipos de amenazas que identificamos al inicio y se pregunta al grupo por indicios sobre cuáles son las más probables de enfrentar. Guardamos las amenazas donde hay IdS o amenazas declaradas a un lado y de forma visible para todos.

Actividad alternativa: Pensar medidas y estrategias básicas a partir de IdS.

Trabajo en grupos y presentación en plenaria 60 min

Opcional para trabajar después de las actividades 1 y 2, se sugiere en caso de que sea una asesoría independiente y exclusiva sobre IdS.

A partir del análisis de la actividad previa dividir en tres grupos cada uno trabajando una de las siguientes preguntas:

¿Hay acciones que podemos tomar?

¿Qué comportamientos/infraestructura deberíamos cambiar?

¿Qué medidas o estrategias podríamos adoptar?

Cada grupo presenta conclusiones y el grupo debate. Es recomendable que la persona relatora del grupo tome notas sobre los consensos.

Consejos de facilitación:

- Es probable que en el grupo exista confusión entre IdS, amenazas declaradas y amenazas latentes. En este caso usar ejemplos:

  a) *Amenaza latente:* es el peligro que tienen todos los defensores en México de que sus oficinas sean víctimas de robo.

  b) *IdS:* es que encuentre por la mañana la puerta de la oficina abierta o que documentación sensible se haya extraviado.

  c) *Amenaza declarada:* que una persona en la calle me diga que si no paro de molestar robarán la oficina.

- Usar ejemplos para mostrar la necesidad de percibir, registrar, compartir y analizar los IdS. Por ejemplo:

  Patricia sale el lunes de la oficina el miércoles y ve un Tsuru blanco estacionado frente a la oficina con dos hombres dentro mirándola pero no le da importancia. El viernes Ricardo llegando a la oficina ve lo mismo pero tampoco le da importancia. El martes siguiente, parqueando su coche cerca de la oficina, David se da cuenta que ha perdido o le han robado las llaves de la oficina. Lo minimiza y no avisa a sus compañeros. Al día siguiente todos se dan cuenta que alguien se ha metido a la oficina y llevado archivos confidenciales.

- Durante la actividad 2 es común que se socialicen algunos IdS. Hay que fomentar ese intercambio. Guiar la discusión con los pasos a seguir para los IdS.

- En caso de que en la preparación previa al taller se haya visto que la organización recibió una amenaza declarada o que al compartir los IdS surja la necesidad de analizar amenazas declaradas específicas con mayor profundidad y si existe tiempo suficiente se puede trabajar adicionalmente la sesión 4b opcional del siguiente apartado.

- Se debe tener cuidado al abordar IdS, algunos incidentes traen a la memoria momentos muy complicados de estrés y ansiedad para las PDDH. La persona que facilita debe estar lista para una eventual situación de estrés, llanto, asociada a evocar o recordar situaciones traumáticas, etc. Ver cómo abordarlo en consejos de facilitación y buscar herramientas de distención (respiración, manejo de emociones, etc.) en ***[RA4]*** especialmente CAPACITAR y BARRY & NANIAR.

- Se debe entender cuando las PDDH son reacias a dar detalles de IdS asociados a experiencias traumáticas o que no se han trabajado previamente desde la perspectiva psicosocial o de género. Nunca se debe forzar a las personas a dar más detalles si no quieren hacerlo.

- Al trabajar IdS se debe evitar revictimizar a la gente haciéndola sentir culpable por IdS, particularmente al explicar los IdS internos. Se debe evitar juzgar las actitudes como "errores" haciendo énfasis de que sin un análisis de seguridad es muy fácil y común pasar por alto estos incidentes y que a cualquiera le puede suceder.

El Diagnóstico de seguridad

Análisis de amenazas declaradas (opcional) *1h30min a 2h*

Objetivos específicos:

- Compartir herramientas para la identificación y el análisis de los incidentes de seguridad y de las amenazas declaradas.
- Analizar una amenaza declarada. Concluir evaluando la probabilidad de que se cumpla.
- Valorar cambios en las medidas de seguridad.

Materiales

- Papelógrafos
- Plumones
- Papelógrafo o diapositivas con anexos sobre amenazas declaradas *[Anexo T1.M2.S4bis a, T1.M2.S4bis b y T1.M2.S4bis c]*

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.4.
- Front Line Defenders, *Manual sobre seguridad: Pasos prácticos para defensores/as de derechos humanos en riesgo*, cap. 3. ***[RA5]***

Puntos clave:

- Definir lo que es una amenaza declarada: *"Acción de dar a entender con actos o palabras que se quiere hacer algún mal al otro/a"*. Incluyen necesariamente una indicación de que pretenden hacernos daño, deben ser reales y concretas. Indican claramente que el peligro se podría materializar.
- Reiterar que algunos IdS pueden llegar a ser amenazas declaradas, sin embargo no todos los IdS son amenazas.
- Clarificar diferencia entre amenazar y constituir una amenaza real: importante entender para valorar la probabilidad que la amenaza se lleve a cabo.
- Las amenazas declaradas provienen necesariamente de actores externos, son intencionales y debidas a nuestro trabajo.
- Tienen un propósito: infundir miedo y paralizar nuestro trabajo. Paradójicamente denotan el miedo de los actores adversarios respecto a nuestra labor de DDHH. No suele suceder que existan amenazas si nuestro trabajo es inefectivo o inútil respecto a los intereses de las fuerzas opositoras.
- Comúnmente se refieren no sólo a nuestro trabajo en DDHH sino que aluden a cuestiones profundamente personales o relacionadas con la forma como nos ven los actores que representan fuerzas de oposición.
- Las amenazas declaradas pueden contener un fuerte componente de violencia de género, ya sea al hacer uso de la amenaza de violencia sexual o de otro tipo. También al atacar la dignidad de los hombres con mensajes que aluden a la "falta de hombría" o que denuestan a las mujeres por su trabajo fuera de la esfera doméstica.
- Explicar sus componentes (origen, blanco, medio de expresión, fondo del mensaje, objetivo y se dan en un contexto).
- Explicar pasos a seguir con amenazas declaradas: 1) Recoger los hechos; 2) destacar pautas y patrones; 3) determinar el objetivo; 4) determinar la fuente y 5) evaluar la probabilidad que la amenaza se cumpla.
- Las conclusiones a la que llegaremos nunca pueden ser 100% seguras. Siempre nos hará falta información. La falta de información también nos brinda pistas sobre lo que no sabemos y nuestras vulnerabilidades.
- Siempre es mejor prevenir considerando el peor escenario posible, sin embargo se debe evitar que cunda el pánico.

Actividades

Actividad 1: Entender las amenazas declaradas y sus componentes.

Presentación 20 min

Explicar qué es una amenaza declarada, sus componentes *[Anexo T1.M2.S4bis a]* y los pasos a seguir para su análisis. *[Anexo T1.M2.S4bis b]*

Actividad 2: Análisis de amenazas declaradas específicas.

Trabajo en grupos y presentación en plenaria 70 min

Pedir a las personas participantes que escriban en una tarjeta un ejemplo de amenaza declarada que han sufrido ellos o su organización. Se comparten las amenazas declaradas en plenaria. Se corrobora si efectivamente los ejemplos dados son amenazas declaradas.

Dependiendo del tamaño del grupo, retomar uno o dos ejemplos de amenazas declaradas y analizarlas en grupos más reducidos siguiendo los pasos del análisis expuesto anteriormente. Si no hay ejemplos en la organización se pueden también usar ejemplos ficticios. *[ver Anexo T1.M2.S4bis c]*

Seguir los pasos de análisis: hechos, patrones, objetivo, fuente y probabilidad de ataque.

Pedir a cada grupo que presente en plenaria:

> *¿Cuál es su conclusión? ¿Qué tan probable es según el grupo que se lleve a cabo la amenaza?*
>
> *¿Por qué? ¿Cuál fue el razonamiento que siguieron?*
>
> *¿Fue difícil? ¿Hubo mucho debate? ¿Por qué?*
>
> *¿Qué comportamientos o infraestructura deberíamos cambiar? (medidas de seguridad que reduzcan las vulnerabilidades ante esta amenaza).*

Presentar conclusiones.

*Actividad alternativa: Pensar medidas y estrategias a partir de amenazas declaradas.

Trabajo en grupos y presentación en plenaria 30 min

Opcional después de las actividades 1 y 2, se sugiere sólo para trabajar cuando hay tiempo extra o en caso de que la sesión sea una asesoría independiente.

Adaptar las medidas y estrategias de seguridad. En grupos responder a las siguientes preguntas:

> *¿Qué estrategia seguir?*
> *¿Se puede reducir el riesgo o hay que evitarlo?*
> *¿Podemos intentar incidir en la amenaza?*
> *¿Qué acciones proponen?*
> *¿Qué comportamientos o infraestructura deberíamos cambiar? (medidas de seguridad que reduzcan las vulnerabilidades ante esta amenaza).*

Presentar conclusiones.

Consejos de facilitación:

- Las personas participantes pueden llegar a confundir IdS, amenazas declaradas y amenazas latentes. En este caso retomar las definiciones a través de ejemplos. Dejar claro que una amenaza declarada es real y concreta.
- Si se usa un ejemplo de una amenaza declarada real tener en cuenta que puede tener implicaciones emocionales sobre las personas que las abordan. Estar seguros de que existen las condiciones para que las personas que brindan su experiencia personal con amenazas declaradas se sienten cómodas compartiéndolo con el grupo y no forzarlas a compartir dicha información si no se sienten cómodas. Enfatizar al grupo que este trabajo es delicado y que no es fácil abordar una amenaza que nos ha ocurrido en primera persona o a nuestra propia organización.
- La persona que facilita debe estar lista para una eventual situación de estrés, llanto, asociada a evocar o recordar situaciones traumáticas, etc. Ver cómo abordarlo en consejos de facilitación y buscar herramientas de distención (respiración, manejo de emociones, etc.) en *[RA4]* especialmente CAPACITAR y BARRY & NANIAR.
- Mientras trabajan los grupos puede ser necesario intervenir para plantear posibilidades que el grupo no haya visto o animar el debate.
- Verificar que se siguen todos los pasos de análisis y que no se omite alguno.
- Cuidar la diferencia entre hecho e interpretación en el grupo. Hay que partir de los hechos (*¿a quién va dirigida? ¿por quién? ¿dónde? ¿cómo?, ¿cuándo? ¿patrones?*). A partir de los hechos se puede pasar a la interpretación (*¿cuál podría ser la fuente? ¿cuál podría ser el objetivo? ¿cuál es la probabilidad?*).
- Reflexionar sobre qué capacidad tiene la persona que amenaza para pasar a la acción *¿Hay información que nos da indicios?* (por ejemplo: dejar un papelito con una amenaza de muerte en el parabrisas de un coche o dejarlo dentro del coche no es lo mismo. En el segundo ejemplo el perpetrador ha demostrado tener más capacidad).
- Cerciorarnos que durante las actividades se tomen en cuenta múltiples escenarios posibles.

El Diagnóstico de seguridad

Análisis de vulnerabilidades y capacidades *30min*

Objetivos específicos:

- Identificar las capacidades y vulnerabilidades de la organización y de sus integrantes.
- Priorizar las áreas que deberían ser fortalecidas y potenciar las capacidades.

Materiales

- Rótulos o tarjetas de colores
- Plumones
- *Metaplán*
- Papelógrafo, fotocopias o diapositivas con *Análisis de Vulnerabilidades y Capacidades [Anexo T1.M2.S5]*

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.2.
- Front Line Defenders, *Manual sobre seguridad: Pasos prácticos para defensores/as de derechos humanos en riesgo*, cap. 2. *[RA5]*

Puntos clave:

- Dejar claros los conceptos de capacidad: *"Los puntos fuertes y recursos a los que puede acceder un/a defensor/a para lograr un nivel mínimo de seguridad. Estas capacidades siempre son mejorables."* y vulnerabilidad: *"El grado en que los/las defensores/as son susceptibles a pérdida, daños, sufrimiento o la muerte en caso de un ataque".*
- Las vulnerabilidades y capacidades son características nuestras, propias, internas, sobre las cuales podemos trabajar.
- Las capacidades y vulnerabilidades son las dos caras de una misma moneda. Podemos convertir una vulnerabilidad en una capacidad.
- Las capacidades y vulnerabilidades se pueden analizar a nivel individual, familiar-comunitario y organizativo.
- Vulnerabilidades y capacidades tienen una dimensión de género, por ello en una misma comunidad u organización sucede que las vulnerabilidades y capacidades sean diferentes para hombres y mujeres.
- Algo que podría ser una capacidad para una persona puede ser una vulnerabilidad para otro: ¡dependen del contexto!
- Hay que considerar las vulnerabilidades y capacidades que tenemos en muchos ámbitos: la oficina, la casa, el transporte, cómo nos comunicamos y guardamos la información, nuestro conocimiento de la coyuntura, relación con las autoridades, acceso al sistema legal, el estatus legal y la contabilidad de la organización, nuestro grado de organización social, el manejo de salud mental, recursos materiales y financieros, acceso a una red de apoyo, etc.
- Es importante considerar las vulnerabilidades y capacidades en su relación amenazas concretas. Sin embargo como no podemos estar seguros de la totalidad de amenazas que enfrentamos y como las vulnerabilidades afectan también la probabilidad y el impacto de una amenaza, hacemos un primer análisis de las vulnerabilidades y capacidades del grupo para poder priorizar las amenazas latentes posteriormente.

Actividades

Actividad 1: Identificar las capacidades y vulnerabilidades.

Trabajo en grupos y presentación en plenaria 30 min

Dar las definiciones de capacidades y vulnerabilidades y dejarlas a la vista de todas las personas en papelógrafo o diapositivas. *[T1.M2.S5]* Poner a disposición de las personas participantes cartulinas de dos colores diferentes (por ejemplo verdes para las capacidades y rojas para las vulnerabilidades). Separar el *Metaplán* en dos columnas para cada una de las categorías. Pedir al grupo que rellene las columnas escribiendo o dibujando en las tarjetas de colores sus propias vulnerabilidades y capacidades. Pueden apoyarse y guiarse en fotocopias del Anexo *Análisis de Vulnerabilidades y Capacidades [T1.M2.S5]* en su sección de componentes.

Al final la persona que facilita intenta quitar elementos repetidos de las columnas. Se pueden debatir algunas de las cartulinas y mostrar que algunas capacidades en un contexto pueden volverse vulnerabilidades o al revés.

*Actividad alternativa 1b: Identificar las capacidades y vulnerabilidades con defensores de base.

Trabajo en grupos y discusión en plenaria 30 min

En plenaria recordar lo que es una capacidad y una vulnerabilidad. Se pueden brindar de nuevo ejemplos y ligarlos a las amenazas previamente identificadas. Pedimos que se formen grupos a quienes repartiremos las amenazas mencionadas. Tomando en cuenta la amenaza que les tocó, en una hoja grande de papelógrafo se pide que hagan un dibujo de su comunidad o pueblo y señalen las fortalezas y las debilidades que identifican en sus comunidades, en particular:

- Zonas de peligro o dónde se sienten seguros.
- Vecinos o actores que hemos identificado a favor/ en contra de nuestra labor de defensa de los DDHH.
- Qué fortalezas y debilidades tienen los hombres y las mujeres en su labor de defensa de DDHH (personal, familiar, organización).
- Puntos estratégicos: teléfono público, carretera hacia comunidad vecina amiga, cuartel de la policía.

Cada grupo pasa a presentar su dibujo y explicarlo en plenaria.

Consejos de facilitación:

Para tener certeza de que las PDDH piensan en todas las vulnerabilidades y si los componentes de vulnerabilidades y capacidades trabajados resultan demasiado complejos, se puede plantear pensar en los puntos fuertes y débiles de la organización y de sus miembros desde la perspectiva de los espacios donde se puede estar en riesgo (casa, trabajo, calle, traslados, tiempo libre, etc.).

El Diagnóstico de seguridad

Acordar el nivel de riesgo e identificar las amenazas prioritarias

1h 45min

Objetivos específicos:

- Priorizar las amenazas latentes que enfrenta la organización con base en los pasos previos del diagnóstico de seguridad.
- Valorar el riesgo para estas amenazas latentes: evaluar la probabilidad que las amenazas latentes se cumplan y determinar el nivel de daño que podrían producir.
- Acordar qué amenazas conllevan mayor riesgo y deberían ser tratadas prioritariamente.
- Verificar que el riesgo se puede reducir.
- Empezar a elaborar el *plan de seguridad* para las amenazas que conllevan mayor riesgo.

Materiales

- *Metaplán*
- Cartulinas blancas u hojas grandes de papelógrafo
- Plumones de colores
- Papelógrafos o diapositivas con los anexos *Análisis de Riesgo [T1.M2.S6]* y *Matriz de Priorización de Amenzas [T1. M2.S6b]*
- Fotocopias del Anexo *Pensar medidas de Seguridad para amenazas prioritarias*. *[T1.M2.S6c]*
- Tarjetas de cartón o *foamy* verdes, amarillas y rojas
- Rótulos o tarjetas de cartón con las amenazas identificadas previamente en el análisis de los IdS (Módulo 2; sesión 4a)
- Papelógrafos con las vulnerabilidades y capacidades identificadas previamente (Módulo 2; sesión 5)
- Chinches
- Cita adhesiva

Puntos clave:

- El riesgo depende de componentes externos (amenaza) y propios (capacidades y vulnerabilidades).
- Para valorar el riesgo debemos analizar primero: 1) si existe la posibilidad que alguien nos haga daño intencionalmente (amenaza); 2) qué tan factible es que esto suceda en la realidad (probabilidad) y 3) qué tanto daño provocaría en nosotros si se llevara a cabo la amenaza (impacto).
- Analizar el riesgo es complicado porque necesariamente nos enfrenta a nuestros miedos (personales, en la organización, respecto a nuestras familias y comunidades. En ocasiones estos miedos son irracionales, pero en otras están plenamente justificados por la probabilidad de que sucedan las amenazas y su impacto en el trabajo y vida de las PDDH.
- El riesgo es subjetivo. Cada persona percibe el riesgo de forma diferente.
- Los niveles aceptables de riesgo varían de persona a persona y por eso debemos ponernos de acuerdo sobre qué nivel de riesgo aceptan de forma consensuada las personas integrantes de una organización.
- Como el riesgo depende en parte de las capacidades y vulnerabilidades que son distintas para defensoras y defensores, el riego también varía en función del género.
- Hay diferentes formas de responder al riesgo: se puede 1) aceptar; 2) reducir (intentando incidir sobre la fuente de las amenazas, o trabajando nuestras capacidades y vulnerabilidades) o 3) evitar (bajando el perfil, suspendiendo o cambiando nuestras actividades o escondiéndose). Puede ser que el riesgo sea tan alto que se tenga que salir y trabajar para reducirlo y poder regresar en el medio plazo. O puede ser que el riesgo se pueda reducir con acciones y medidas de corto plazo.
- Para reducir nuestra exposición al riesgo, intentaremos proponer medidas de seguridad que puedan reducir nuestras vulnerabilidades y aumentar nuestras capacidades para *prevenir* que las amenazas (prevención) se materialicen o aumentar la capacidad de *reaccionar* a las consecuencias si se llegasen a materializar (reacción). También podemos incidir sobre la fuente de la amenaza (por ejemplo disuadiendo al perpetrador de atacarnos o convenciendo a las autoridades de cumplir con su obligación de protegernos).
- El riesgo es dinámico y cambia en el tiempo, por ello es crucial analizarlo periódicamente en la organización incluyendo la perspectiva de todas las PDDH integrantes.
- Enfatizar la importancia de haber hecho todo el análisis previo para tener mejores elementos de análisis de riesgo.

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.2, 1.5 y p. 79.
- Front Line Defenders, *Manual sobre seguridad: Pasos prácticos para defensores/as de derechos humanos en riesgo, cap. 2.* *[RA5]*

Para abordar miedos, preocupaciones y amenazas desde la perspectiva psicosocial con PDDH:

- BARRY & NANIAR. *Integrated Security the Manual.*
- BERISTAIN, *Manual sobre la Perspectiva Psicosocial en la investigación de derechos humanos.*
- CAPACITAR, *Herramientas de Capacitar que nos pueden ayudar en casos de emergencia.*
- CONSTANZA & AGILAR, *Introducción a la Salud Mental.* *[RA4]*

Actividades

Actividad 1: Priorización inicial de amenazas en función de los pasos previos del diagnóstico de seguridad.

Trabajo en plenaria 15 min

Pedir que en función del análisis de contexto, el mapeo de actores, los IdS identificados y de las amenazas declaradas (si existen) anoten en tarjetas de cartón las amenazas latentes que detectan para su persona y organización.

Junto con el grupo se revisan los diferentes papelógrafos que dejamos en la pared; en particular el de vulnerabilidades y capacidades que habíamos trabajado previamente para verificar si deberíamos añadir otras amenazas latentes.

Se anota cada amenaza que identifiquen en una tarjeta.

*Actividad 1b: Priorización inicial de amenazas a partir de preocupaciones y miedos ligados a nuestro trabajo en DDHH.

Trabajo en grupos y/o plenaria 30 min

Se recomienda para sustituir la actividad 1, especialmente para trabajar con PDDH comunitarios.

Dividir en grupos de 3 a 5 personas. Se brinda una hoja de papelógrafo a cada grupo y se les pide que dibujen la figura de un defensor/a.

Pedir que cada persona dibuje en tarjetas aparte las principales preocupaciones y miedos en el trabajo y la comunidad que podría tener esta persona defensora (lo que le preocupa que le pase a su persona, a sus compañeros, a sus familias, a la oficina, a sus tierras si son defensores comunitarios, etc.). Se recomienda que mínimo un grupo se concentre en dibujar una defensora para abordar amenazas específicas que enfrentan las mujeres en su trabajo de DDHH.

Pedir que peguen alrededor de las personas defensoras dibujadas los cartones con las preocupaciones y miedos que dibujaron. Concluir explicando que el miedo nos puede paralizar y dañar nuestra integridad y nuestro trabajo pero también nos puede enseñar cuales son las amenazas que enfrentamos y eso a su vez nos va a ayudar a tomar mejores decisiones sobre cómo protegernos como veremos a continuación.

Actividad 2: valorar la probabilidad e impacto de las amenazas detectadas.

Discusión en plenaria 30 min

Cada persona determina cuáles son las amenazas que representan mayor probabilidad e impacto. Para ello se llena con el grupo una *Matriz de Priorización de Amenazas* sobre el *Metaplán* *[ver anexo T1.M2.S6b]*:

En la columna izquierda "Amenazas latentes" se adhieren las tarjetas con las amenazas detectadas en la actividad precedente (dibujos o amenazas escritas según la actividad previa elegida).

En la columna central "Probabilidad" cada persona escogerá una sola tarjeta

de color (Roja-probabilidad alta; Amarilla-probabilidad media; verde-probabilidad baja). Para ello tendrá que valorar la siguiente pregunta:

> *¿Qué tan probable es que pase una situación semejante a nuestra persona, en nuestra comunidad u organización?*

En la columna derecha "Impacto" y como producto del debate escogerá una sola tarjeta de color (Roja-impacto alto; Amarilla-impacto medio; Verde-impacto bajo). Para ello tendrá que valorar la siguiente pregunta:

> *¿Si sucediera algo similar en nuestra persona, comunidad u organización qué tan grave sería el impacto en nuestras vidas y nuestro trabajo?*

Al final cada participante habrá pegado para cada amenaza de la Matriz una tarjeta de probabilidad y una de impacto. Como resultado cada amenaza tendrá varias tarjetas de valoración para probabilidad e impacto. Es normal que haya divergencias sobre las valoraciones de cada amenaza.

Otra forma de hacer la matriz es colocar el listado de amenazas y poner un semáforo con los tres colores en cada espacio de las columnas para probabilidad e impacto. Pedir que cada persona pegue dos chinches (una para probabilidad y otra para impacto) en el color que considere para todas las amenazas.

Actividad 3: Consensuar el nivel de riesgo aceptable a partir de la priorización de amenazas.

Presentación y discusión en plenaria ***15 min***

El grupo intenta acordar en discusión plenaria cuáles son las amenazas que representan mayor probabilidad e impacto (se recomienda seleccionar de 3 a 5 amenazas prioritarias). A partir de la *Matriz de Priorización de Amenazas* rellenada previamente mostramos que puede haber varias percepciones del riesgo pero lo importante es llegar a un consenso sobre cómo valorar las amenazas latentes.

Explicar que esas amenazas latentes que fueron detectadas en la matriz con probabilidad e impacto medio y sobre todo alto, son las que deberíamos abordar de forma prioritaria ya que según el análisis que trabajamos son las más probables y las que dañarían más nuestro trabajo e integridad física y psicológica si llegasen a suceder.

Hacer notar que hay amenazas de un riesgo tan bajo que podría ser aceptado. Explicar que otras amenazas entrañan un nivel de riesgo medio pero importante a considerar ante el cual hay que tomar medidas para reducirlo. Puede ser que haya amenazas que impliquen un riesgo tan alto que se deban evitar.

De preferencia se deja por escrito el consenso sobre las amenazas prioritarias.

Actividad 4: Reaccionar y prevenir ante las amenazas.

Trabajo en grupos y presentación en plenaria ***45 min***

Dividir en grupos de 3 a 5 personas. Cada grupo trabajará sobre una amenaza prioritaria específica de la siguiente manera:

- Retomar las vulnerabilidades y capacidades que se trabajaron previamente, detectar las que estén relacionadas con la amenaza.
- Pensar en posibles medidas de seguridad que sean realistas para su situación

y que coadyuven a disminuir las vulnerabilidades al tiempo que aumentan sus capacidades.

- Anotar las medidas de seguridad propuestas en tarjetas de cartón.

Se pide que coloquen las tarjetas de cartón de las medidas de seguridad bajo cada amenaza latente y se presenten en plenaria.

Para guardar una memoria escrita de esto se puede rellenar el anexo *Pensar medidas de seguridad para amenazas prioritarias [T1.M2.S6c].*

**Actividad alternativa 4b: Reaccionar y prevenir ante las amenazas con defensores de base.

Trabajo en grupos 30 min

Se recomienda para sustituir la actividad 4, especialmente para trabajar con PDDH comunitarios.

Con base en las amenazas prioritarias identificadas previamente, organizamos grupos de 3 a 5 personas, repartimos las distintas amenazas y pedimos que para cada una de ellas el grupo a cargo arme una pequeña actuación con juego de roles para presentar:

¿Cómo se puede prevenir la amenaza?

¿Cómo reaccionaría en caso de que sucediera la amenaza?

A partir de la presentación se pide a las demás personas que aporten más ideas.

La persona facilitadora intenta buscar un consenso sobre cuáles serían las medidas de seguridad más realistas de acuerdo a sus posibilidades para responder a las amenazas efectivamente en términos de reacción y prevención.

Se recomienda que la persona que sea relatora deje por escrito las medidas propuestas o que rellene un formato similar al anexo *Pensar medidas de seguridad para amenazas prioritarias [T1.M2.S6c]* ya que este registro se utilizará en el taller 2.

Consejos de facilitación:

Puede ser difícil valorar la probabilidad y el impacto en la ecuación del riesgo. Dejar claro que no podemos ser 100% exactos. Es una valoración subjetiva y el objetivo es que todas las PDDH lleguen a un *acuerdo* sobre cuál es el nivel de riesgo para cada una de las amenazas identificadas. Al momento de valorar la probabilidad e impacto de las amenazas latentes es probable que cada participante piense de forma diferente (ante el robo de información por ejemplo un participante puede poner una tarjeta amarilla mientras otra considerará que debe tener una tarjeta verde). La actividad hace patente la subjetividad del riesgo. La función de la persona que facilita es la de impulsar un consenso para permitir llegar a una visión compartida del riesgo y acordar como lo valora la organización en su conjunto.

Para valorar el impacto, analizar para cada amenaza latente:

- *Impacto alto:* limita excesivamente el funcionamiento organizativo y nuestro trabajo. Implica un daño irreversible o excesivo sobre la integridad física y/o psicológica de las personas defensoras o de su círculo cercano (familia, comunidad).
- *Impacto Medio:* limita parcialmente el funcionamiento organizativo, pero permite seguir trabajando sobre las líneas estratégicas de DDHH que se ha planteado la organización. Afecta moderadamente la integridad física y/o psicológica de las personas defensoras o de su círculo cercano (familia, comunidad).
- *Impacto Bajo:* no limita de forma considerable ni el funcionamiento organizativo ni sus líneas de trabajo. No conlleva afectaciones a la integridad física de las PDDH y/o implica afectaciones leves a las personas defensoras (dichas afectaciones son capaces de ser superadas y manejadas con un trabajo cotidiano básico desde la perspectiva psicosocial).
- Para valorar la probabilidad, analizar si la posibilidad que se concretice la amenaza es inmediata o remota y si la fuente de la amenaza tiene capacidad para llevarla a cabo (según el mapeo de actores, los IdS, las vulnerabilidades y si ya ha habido alguna amenaza declarada).
- La persona que facilita debe tener especial cuidado al trabajar la parte sobre miedos y amenazas ya que es un tema delicado desde la perspectiva psicosocial, no se debe forzar el proceso bajo ninguna condición ni

obligar a hablar a quien no quiera. Se debe estar listo para una eventual situación de estrés, llanto, cuando se abordan las amenazas. Ver cómo abordarlo en consejos de facilitación y buscar herramientas de distención (respiración, manejo de emociones, etc.) en ***[RA4]*** especialmente CAPACITAR y BARRY & NANIAR.

- Pueden haber vulnerabilidades y capacidades que se repiten para diferentes amenazas latentes
- Puede ser complicado para el grupo pasar de las vulnerabilidades/capacidades a medidas de seguridad. En vez de pensar en la amenaza como un simple suceso (por ejemplo robo de información), pensar en ella en términos de *¿qué es lo que quieren evitar?* Quieren evitar la posibilidad que ocurra algo y quieren evitar que en el caso de que ocurra el impacto sobre la organización no sea tan grave (por ejemplo queremos evitar que roben información sensible y que nos quedemos sin archivos para continuar nuestro trabajo). Queremos que sea más difícil llevar a cabo la amenaza y queremos también que sí se lleva a cabo, las consecuencias negativas para la organización sean menores, *¿qué medidas podemos tomar para esto?*
- Otra manera de trabajar las amenazas es enfatizar en qué medida trastocan el espacio de actuación de las PDDH. Por ejemplo cómo el robo de información sensible comprometería su trabajo o su seguridad al punto que ya no podrían continuar su trabajo adecuadamente.
- Considerar también si la amenaza toca todos los espacios de la PDDH (casa, trabajo, traslados etc.) y analizar si están cubiertos por las medidas propuestas en esos ámbitos. También se puede hacer el ejercicio inverso, es decir, tomar cada medida de seguridad y ver en qué espacio protegen al defensor o reducen la posibilidad de que la amenaza se concretice.
- Las personas suelen elegir medidas generales de seguridad y poco aplicables, es importante hacerlas ver que tienen que ser específicas para que realmente sean medidas. Por ejemplo, suelen decir cosas como "una medida es tener una política de acceso a la organización", en este caso alentarlos a pensar cuáles serían los componentes de esta política entonces y qué mecanismos específicos necesitarían para que se implemente.
- Las personas suelen preguntar sobre medidas generales que sirvan de antemano (preguntan por ejemplo si es bueno "cambiar de ruta constantemente"). En este caso, explicar que no opinamos específicamente sobre este tipo de medidas (ni las recomendamos ni las rechazamos *a priori*, sino que las deben consensuar a la luz de su contexto específico. Una medida apropiada para una organización no necesariamente sirve para otra.
- Las medidas deben ser realistas y apegadas al contexto de la organización. Hay organizaciones que han estudiado y observado que en un contexto de defensa de derechos humanos, ciertas medidas han funcionado para la mayoría de organizaciones y son vistas como buenas prácticas (i.e. no viajar solo, cambiar de rutas, etc.). Estas posibles medidas y/o buenas prácticas no deben menguar la creatividad de la organización para buscar formas alternas de protegerse. Es decir, al usar un catálogo de buenas medidas existe el riesgo de caer en una fórmula única que en caso de no poder ser cumplida deja en desprotegida a la organización.
- La creatividad es un elemento de protección ante actores agresores que han estudiado y estudian el comportamiento de las organizaciones de derechos humanos. Medidas de protección tomadas sin basarse en un análisis del riesgo y un diagnóstico previo como el que se propone pueden crear una falsa sensación de protección y poner en mayor vulnerabilidad a las PDDH. Si las PDDH insisten en tener alguna lista base que las oriente, para comenzar a imaginar sus propias medidas se pueden referir a Front Line Defenders, Manual sobre seguridad: *Pasos prácticos para defensores/as de derechos humanos en riesgo*, apéndices 5 a 15. ***[RA5]***
- Se pueden guardar los papelógrafos o tomar fotos del *Metaplán* para que la organización profundice el ejercicio después con más tiempo. ¡Ojo, son documentos sensibles por lo cual los registros documentales deben ser resguardados adecuadamente!

Conclusión

Compromisos de seguimiento, evaluación y cierre

45min

Objetivos específicos:

- Revisar el contenido y los conocimientos adquiridos.
- Identificar tareas y responsabilidades para darle seguimiento al taller e implementar lo que se trabajó.
- Acordar el seguimiento.
- Evaluar el taller.

Materiales

- Papelógrafos
- Plumones
- *Metaplán* o palelógrafo con Anexo *Tareas del diagnóstico pendientes [Anexo T1.M3.S1]*
- Hojas
- Papelógrafo con un punteo de los *Objetivos generales del taller y resultados esperados*
- Fotocopias con *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b]*
- Urna o caja de cartón con una ranura

Puntos clave:

- Enfatizar que este taller fue sólo la piedra base para posteriormente llevar a cabo una estrategia y *plan de seguridad* integral.
- Dejar claro que si la organización no le destina los recursos (responsables, espacios, tiempo,etc.) al ámbito de seguridad y protección no se podrán llevar a cabo estrategias ni planes integrales.
- Abordar las expectativas de seguimiento y acordar si se necesita seguimiento, de qué tipo y cómo se podría dar.
- Revisar los acuerdos alcanzados y establecer los compromisos con las personas participantes en cuanto a las estrategias de seguridad y protección que serán desarrolladas a nivel organizativo.
- Hay que revisar las tareas apuntadas e identificar plazos, espacios, recursos y responsables con un nivel aceptable de detalle y claridad.
- Cerciorarnos que no hayan quedado dudas sobre los aspectos fundamentales del taller.
- Evaluar el taller y la facilitación.

Actividades

Actividad 1: Revisión de "Actas y Acuerdos".

Discusión en plenaria* *15 min

En un *Metaplán* o papelógrafo rellenar una matriz sobre las *Tareas del diagnóstico pendientes [Anexo T1.M3.S1].* Recuperar las notas de la relatoría.

Mientras las personas participantes hacen un punteo para identificar las tareas pendientes, queremos resaltar las necesidades de asesoría por parte de la organización:

¿Cuándo podríamos llevar a cabo una entrevista de seguimiento?

¿Quién será la(s) persona(s) que serían nuestro punto de contacto?

En caso de haber un consenso al respecto y de que se dieran avances después del taller en las *Tareas del diagnóstico pendientes*:

¿Cuándo podríamos llevar a cabo un taller de seguimiento? [para más detalles sobre la lógica secuencial y el seguimiento de talleres ver capítulo 2]

¿Quién debería asistir a dicho taller?

Consejos de facilitación:

- Si el grupo no quiere llegar a acuerdos en términos del seguimiento no hay que forzarlo.
- Si se tiene más tiempo al final se puede optar por la evaluación en fotocopias que permite sistematizar mejor la información y retroalimentaciones. Algunos grupos prefieren rellenar las evaluaciones sin el facilitador presente. Se pueden poner cajitas a modo de urnas para que se depositen las evaluaciones individuales dobladas y de forma anónima.

Actividad 2: Evaluación del cumplimiento de los objetivos del taller y expectativas.

Trabajo en plenaria* *10 min

Retomar las expectativas de las personas participantes trabajadas al inicio del taller. En un papelógrafo se pegan las expectativas iniciales del grupo del lado izquierdo y a la derecha se hacen tres columnas para evaluar el cumplimiento de las mismas: 1) se cumplió 2) se cumplió parcialmente y 3) no se cumplió. Para cada una de las expectativas se pide que cada persona pegue un papelito adherible en la columna que considere.

En otro papelógrafo se tiene listo un punteo de los *Objetivos generales del taller* y resultados esperados. Enfrente de cada aspecto del punteo se hacen tres columnas al igual que para las expectativas y se pide que las personas peguen un papelito adherible en la columna que consideren. También pueden escribir sobre el papelito que peguen si gustan ahondar en algún objetivo específico si sienten que hubo aspectos del objetivo que se les dificultaron o que fueron no se cumplieron a cabalidad.

La persona que facilita hace un recuento y revisa especialmente aquellos objetivos y expectativas que faltó cumplir a cabalidad. Se contrasta si dichos objetivos y expectativas estaba en las posibilidades planteadas por el taller o si se pueden abordar en talleres subsecuentes.

Actividad 3: Evaluación del taller y la facilitación.

Trabajo individual o plenaria* *10 min

Escoger una de las siguientes formas de evaluación:

a) En un papelógrafo se hacen dos columnas: 1) adecuado y 2) puede mejorar. Se reparten papelitos con los distintos criterios adaptados de las 2 tablas del *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b]*

Se les pide que cada quien tome 3 criterios de evaluación del taller y 3 criterios de evaluación de la facilitación (de preferencia aquellos donde tengan más que aportar o que les llamaron la atención para evaluar) y que escriban sobre los papelitos con sus opiniones, críticas y sugerencias. Luego se les pide que adhieran los papelitos en una de las dos columnas según corresponda a su punto de vista.

b) Se distribuyen individualmente fotocopias del *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b].* Se pide a las personas que lo llenen y lo depositen doblado y de forma anónima en una caja o urna.

Actividad 4: Conclusión.

Discusión en plenaria* *10 min

Se da una oportunidad para dudas y comentarios al grupo, se comentan las apreciaciones y se hace una última ronda de críticas y sugerencias.

Se recuerda la confidencialidad de lo abordado en los talleres.

Se dan los agradecimientos y se clarifica que se deja la posibilidad abierta para futuros talleres.

Taller 1

Anexos

Anexo T1 M1 S1

Método de gestión de la seguridad

T1 M1 S2

Tipología de las amenazas latentes para personas defensoras de los DDHH

1. Acciones de intimidación

- Amenazas telefónicas, por correo o recados, verbales, etc.
- Vigilancia y seguimientos demostrativos

2. Acciones de Control

- Espionaje a través de escuchas telefónicas con micrófonos ocultos
- Infiltración dentro de la Organización, uso de "orejas", etc.
- Vigilancia sobre locales, violación de la correspondencia electrónica

3. Robo de información

- Cateo y allanamiento a oficinas o domicilios, robo de maletines o mochilas, robo de computadoras portátiles, unidades extraibles, celulares, etc.
- Extracción de objetos dejados en vehículos, examen de la basura, etc.

4. Agresiones Físicas y ejecuciones

- Golpes, tortura, violencia de género en forma física (incluyendo violencia sexual), ejecuciones.

5. Criminalización

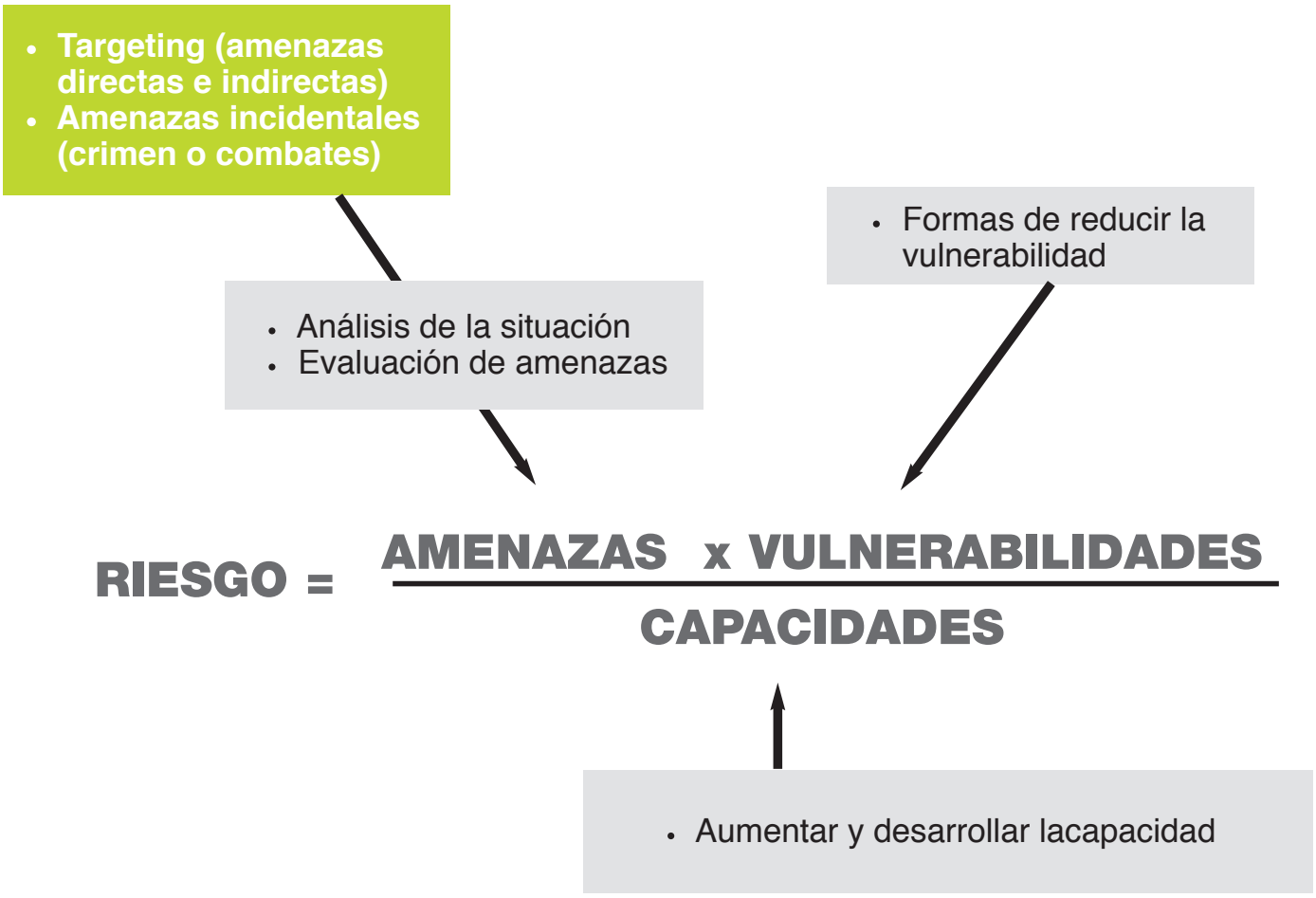
- Difamación pública, montajes judiciales, uso arbitrario del sistema penal

Anexo T1 M1 S3a

Ecuación y ponderación del riesgo*

Para reducir los riesgos a niveles aceptables (principalmente, para protegerse) debemos:

· Reducir los factores que nos hacen vulnerables
. Aumentar nuestra capacidad
. Reducir las amenazas posibles



* Tomado de Peace Brigades International (Oficina Europea) & Frontlinde Defenders, *Manual de Protección para los Defensores de Derechos Humanos*, 2005, cap. 2.

Anexo T1 M1 S3a continuación

Ecuación y ponderación del riesgo*

Cuantas más amenazas y vulnerabilidades tenemos, más riesgo corremos.

Fig. 1

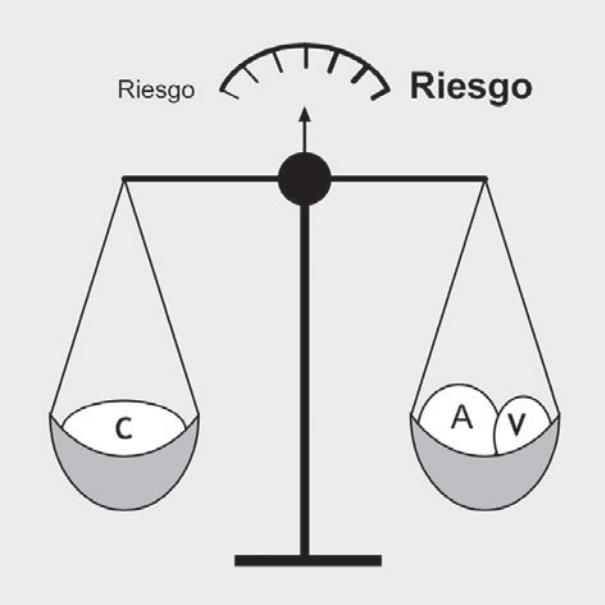


Fig. 2

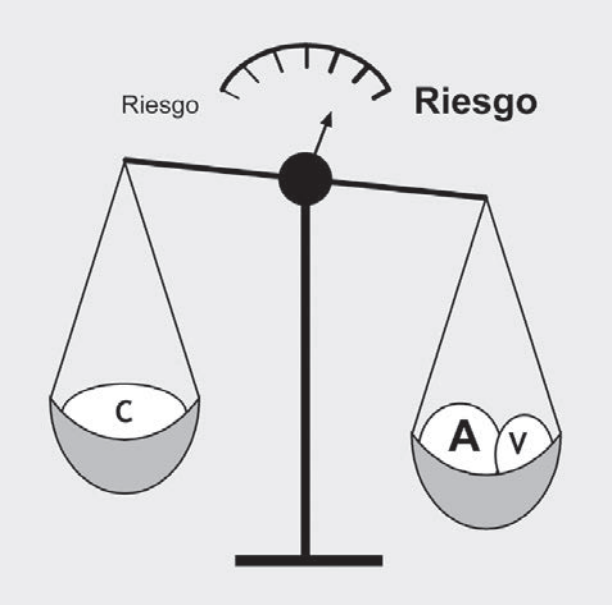


Fig. 3

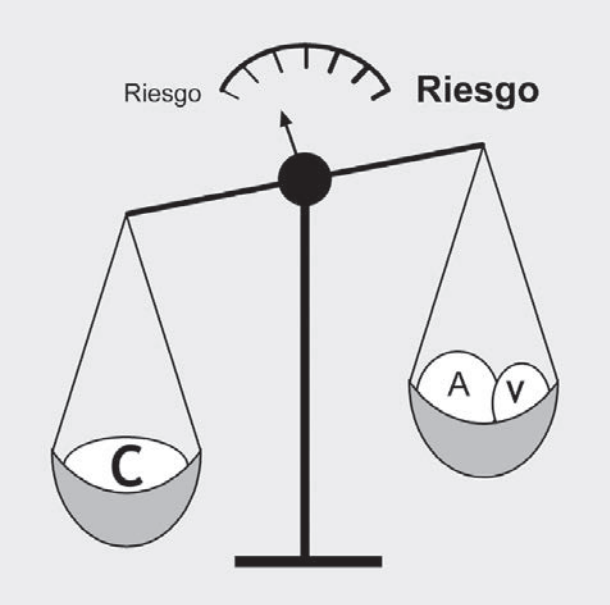
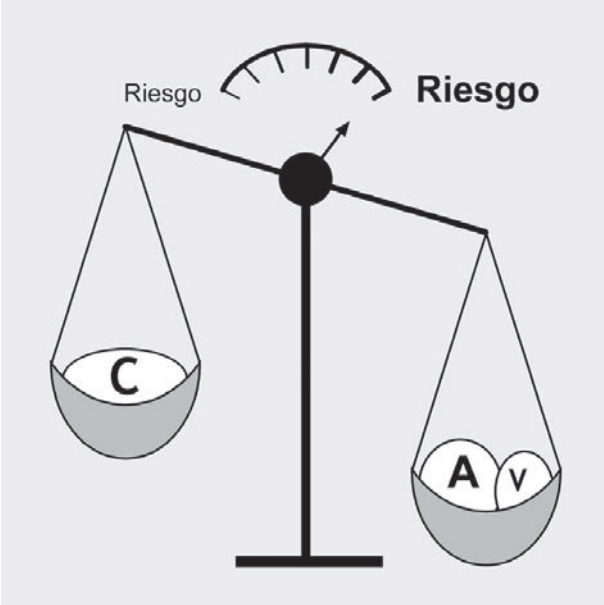


Fig. 4



* Tomado de Peace Brigades International (Oficina Europea) & Frontlinde Defenders, *Manual de Protección para los Defensores de Derechos Humanos*, 2005, cap. 2.

Anexo T1 M1 S3b

Debatir sobre Riesgos y amenazas en comunidades*

*Autora; Lina Selano Defensora de DDHH en Ecuador. Tomado de: *Front Line Defenders, Manual sobre seguridad: Pasos prácticos para defensores/as de derechos humanos en riesgo*, 2011, p. 70.

Anexo T1 M1 S3c

Los pasos del Diagnóstico de Seguridad

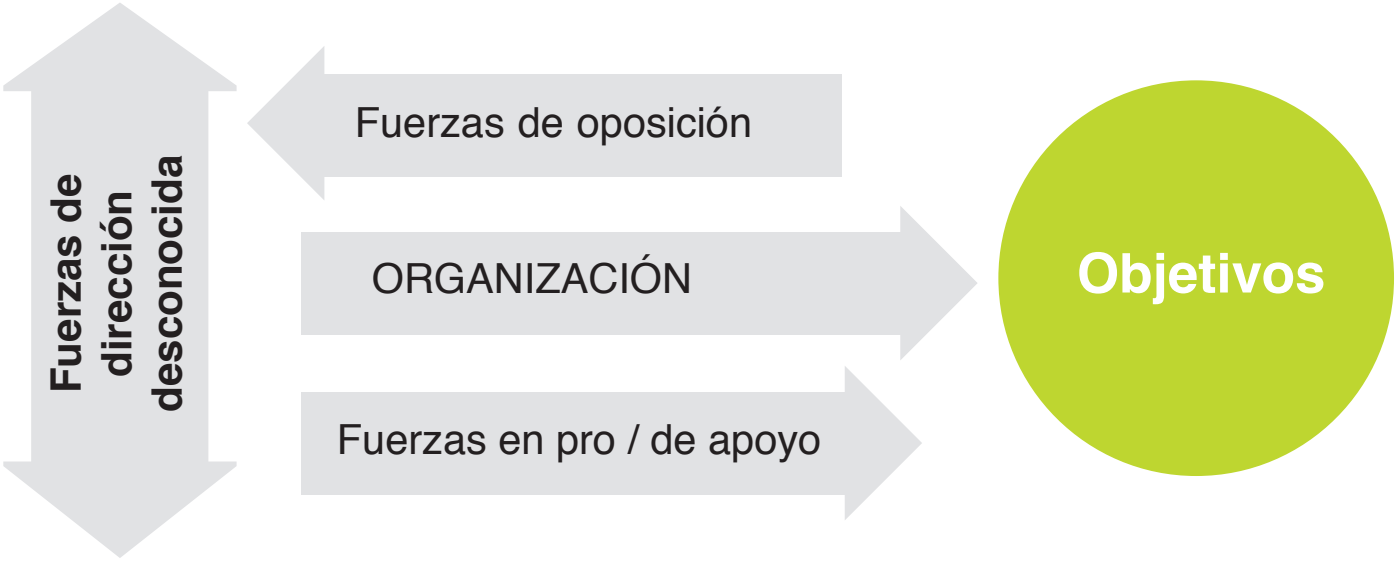
Análisis de CONTEXTO	**Identificar y explicar los fenómenos sociales, políticos, económicos, legales, las normas de género, etc. que impactan en el trabajo de la organización.**
Mapa de ACTIVIDADES	**Identificar las principales actividades que van en contra de los intereses de los potenciales agresores.**
Análisis de ACTORES	**Identificar los actores (locales, nacionales e internacionales) sus intereses y relaciones.** **Evaluar sus capacidades para llevar a cabo ataques.**
Análisis de INCIDENTES	**Identificar los tipos de incidentes de seguridad y analizarlos.** **Si existen, analizar un tipo particular de IdS: las amenazas declaradas.**
Análisis de CAPACIDADES y VULNERABILIDADES	**Identificar las capacidades y vulnerabilidades de la organización y de sus integrantes. Considerar diferenciaciones por género y a nivel individual, familiar, comunitario y organizacional (psicosocial).** **Priorizar las áreas que deberían ser fortalecidas y potenciar las capacidades.**
Análisis de RIESGO	**Priorizar las amenazas latentes en función de los pasos previos.** **Evaluar la probabilidad de que ocurra cada una de estas amenazas y su impacto.** **Definir cuáles deberían ser prioritariamiente abarcadas por un plan de seguridad.**

Anexo T1 M2 S3a

Análisis del campo de fuerzas*

Análisis de ACTORES

Identificar los actores (locales, nacionales e internacionales) sus intereses y relaciones. Evaluar sus capacidades para llevar a cabo ataques.



*Adaptado de Peace Brigades International (Oficina Europea) & Frontlinde Defenders, *Manual de Protección para los Defensores de Derechos Humanos*, 2005, p. 11.

Anexo **T1 M2 S3b**

Mapeo y análisis de actores (ejemplo de *Metaplán*)

Uso de herramientas complementarias: *Metaplán*

PBI usa también en general la herramienta y metodología del *Metaplán*, la cual promueve que todo el grupo participe, interactúe, visualice lo que se está discutiendo y llegue conjuntamente y estructuradamente a una conclusión. Se trabaja con un panel, pizarrón, pared o una gran manta visible para todas las PDDH. Los miembros del grupo pueden aportar mediante tarjetas en las cuales van escribiendo o dibujando (con marcadores) sus aportes y pegándolos y ordenándolos en el panel. El *Metaplán* permite mover y reagrupar los elementos lo cual brinda claridad conceptual y versatilidad.

Anexo T1 M2 S3c

Matriz para el análisis de actores* (ejemplo)

	GOBIERNO	EJÉRCITO	POLICÍA	GRUPO DE OPOSICIÓN ARMADA	ONGS DE DDHH NACIONALES	IGLESIAS	OTROS GOBIERNOS	ORGANISMOS DE LA ONU	ONG S INTER - NACIONALES
GOBIERNO	(actor)								
EJÉRCITO		(actor)						B	
POLICÍA			(actor)						
GRUPO DE OPOSICIÓN ARMADA				A					
ONGS DE DDHH NACIONALES					(actor)				
IGLESIAS						(actor)			
OTROS GOBIERNOS							(actor)		
ORGANISMOS DE LA ONU								(actor)	
ONG S INTER - NACIONALES									(actor)

Casilla A

PARA CADA ACTOR :
. objetivos e intereses
. estrategias
. legitimidad
. poder

Casilla B

RELACIONES
ENTRE ACTORES :
(relaciones que afectan al tema de protección y relacionadas con temas estratégicos, para ambas partes)

*Tomado de Peace Brigades International (Oficina Europea) & Frontlinde Defenders, *Manual de Protección para los Defensores de Derechos Humanos*, pp. 15-16.

Anexo T1 M2 S4a

Definición y análisis básico de los Incidentes de Seguridad

Análisis de INCIDENTES

Identificar los tipos de incidentes de seguridad y analizarlos. Si existen, analizar un tipo particular de IdS: las amenazas declaradas.

INCIDENTES DE SEGURIDAD
« un evento fuera de lo común que afecta mi seguridad o la seguridad de los demás »

Internos o Externos	**Interno**	Asociado a actos de los integrantes de la organización: no respeto de las medidas de seguridad, olvido, distracción, etc.
	Externo	Provocado por agentes externos a la organización
Provocados o Fortuitos	**Provocado**	Incidente provocado de manera intencional para dañar a la Organización
	Fortuito	Evento fuera de control, no provocado por actores hostiles
Origen del incidente	**Delincuencia común**	No relacionado al trabajo del/a defensor/a
	Incidental	Consecuencia del contexto de violencia, el/la defensor/a no es el blanco directo
	Político	El/la defensor/a es el blanco. Origen político.

Anexo T1 M2 S4b

Pasos a seguir para analizar un IdS

Incidente	¿Qué pasó?
Fecha	¿Cuándo?
Lugar	¿Dónde?
Víctima	¿Quién fue la persona afectada?
Violencia de género	¿Existe violencia de género? (psicológica, física, etc.)
Victimario	Para Provocado - Externo: ¿Quién es responsable?
¿Actividad relacionada?	¿Por qué? (por qué ahora, aquí, con esta víctima)
I / E	¿Interno o Externo?
P / F	¿Provocado o Fortuito?
Origen	¿Delincuencia común / Incidental / Político?

Anexo T1 M2 S4b continuación

Pasos a seguir para analizar un IdS

Responsabilidades y espacios de análisis conjunto de Ids dentro de la organización

Anexo T1 M2 S4c

Bitácora de registro de IdS

Incidente de seguridad	idS 1	idS 2	idS 3	idS 4	idS 5	idS 6
Responsable:						
Fecha						
Lugar						
Víctima						
Violencia de género						
Victimario						
¿Actividad relacionada?						
I / E						
P / F						
Origen						

Anexo T1 M2 S4bis a

Análisis de Amenazas Declaradas

AMENAZAS DECLARADAS

Acción de dar a entender con actos o palabras que se quiere hacer algún mal a otro
La mayoría de las amenazas declaradas son actos de intimidación.
Las amenazas declaradas son el medio mas "económico" para neutralizar las actividades de una organización.

Origen	Actor afectado por el trabajo de la persona defensora u organización. Autor (intelectual y/o material.)
Objetivo	La mayoría de las amenazas suceden por el impacto del trabajo de la persona defensora o el de su organización. En general tienen el objetivo de interrumpir lo que están haciendo o forzarlos a hacer algo.
Medio de expresión	Forma en la que llega al conocimiento de la persona defensora u organización. Medio de expresión (escrito, verbal, por tercera persona...)
Fondo del mensaje	Contenido del mensaje, tipo de amenaza (pe. Muerte, robo, etc), formas específicas de violencais de género (insultos basados en normas de género, amenazas de violencia sexual etc.)
Contexto	Actividad relacionada. Coyuntura. Análisis de riesgo.
Acceso	Defensor/a expuesto y vulnerabilidad específica.

Anexo T1 M2 S4bis b

Pasos para analizar Amenazas Declaradas

Paso 1

Recoger todos los hechos

Origen de la amenaza
Medio de expresión y tipo de amenaza
Contexto: ¿había/hay riesgos específicos ahora ? ¿Por qué?

Paso 2

Destacar patrones

Establecer si hay factores comunes a las amenazas y tendencias en las amenazas: si han bajado o aumentado en intensidad, qué medios se han usado repetidamente, frecuencia, etc. Circunstancias comunes a varias amenazas y/o incidentes de seguridad de otras ONG.

Medios utilizados para amenazar, el momento en el que las amenazas aparecen, los símbolos, el contenido del mensaje, violencias específicas basadas en normas de género, etc.

Paso 3

Determinar el objetivo ¿por qué?

En vista de que la amenaza suele tener un claro propósito relacionado con el impacto del trabajo, es posible que analizando ese impacto se pueda establecer qué pretende conseguirse con la amenaza.

Paso 4

Determinar la fuente ¿quién esta detrás?

De la manera mas específica posible. Identificar autor intelectual y material y sus posibles intereses.

Paso 5

Evaluar la probabilidad de ataque

Evaluar el nivel de amenaza según el origen, el objetivo, el blanco expuesto.

Análisis de riesgos de la organización para determinar si hay vulnerabilidades especificas al contexto de la amenaza que pueden aumentar su probabilidad e impacto.

Anexo T1 M2 S4bis c

Casos ficticios para analizar Amenazas Declaradas

CASO A

Tras la desaparición de su hijo, una mujer con poca trayectoria organizativa, comienza a trabajar con una asociación de familiares que le da seguimiento a desapariciones forzadas y a la impunidad en las que quedan estos casos.

Al poco tiempo, la mujer empieza a notar vigilancia por coches y hombres armados a fuera de su casa. Una mañana recibe una llamada a su celular de un tipo que dice ser del Cártel del Golfo y que pide "que se dejen de chingaderas y que no anden más con sus pendejadas. Si siguen buscando a su gente les va a ir muy mal".

Unos días después, camino a su trabajo, un hombre empieza a seguirla e intenta agredirla sexualmente pero la mujer se escapa corriendo. Logra escuchar al hombre decirle que "lo mismo podría pasarle a tu hija".

CASO B

Una mujer campesina, con amplia trayectoria organizativa, comienza a trabajar con una comunidad que planea un plantón contra una minera que ha empezado a excavar el subsuelo cerca de la comunidad sin su consentimiento. Logra conseguir que una delegación de ONGs internacionales visite la zona y denuncie lo que está pasando.

A las semanas, el presidente municipal junto con un ejidatario a favor de la minera se acercan a la milpa donde trabaja su marido y le reprochan que no sabe mantener a su esposa en casa, y que la cuide. El ejidatario lleva arma y se la muestra ostentosamente al esposo.

Unos días después, ella encuentra posada en frente de la puerta de su casa una calaverita de azúcar con su nombre. A los pocos días, al regresar a la casa, encuentran la puerta abierta y varias cosas rotas en el interior. La noche siguiente amanece degollado su perro en el patio de la casa.

Amenaza escrita: "Mejor te vas ya del estado. Te crees mucho con tus internacionales pero de nada sirbe (sic). Si no vas a acabar como tu pinche perro."

Firmado: Los Pelones

CASO C1

Un albergue para migrantes decide tomar la defensa legal de un caso de un migrante extorsionado y torturado por elementos de la policía estatal. Desde entonces, el albergue es constantemente blanco de ataques. Se ha visto gente rondando en vehículos con actitudes intimidatorias, sabotaje de la línea de teléfono y de la luz e incluso allanamiento de las oficinas del albergue.

El personal del albergue ha recibido en varias ocasiones amenazas escritas dónde se les avisa que si siguen con el caso jurídico se les va a matar. Se han dado cuenta que estas amenazas surgen generalmente después de algún trámite en cuanto al caso.

En consecuencia, el albergue ha pedido medidas cautelares a la CIDH que le fueron otorgadas pero tras meses de negociación con el Estado no se notan avances aparte de dos aparatos celulares entregados que nunca tienen saldo.

Próximamente, tendrá lugar la audiencia final del caso.

CASO C2

Un albergue para migrantes decide tomar la defensa legal de un caso de un migrante extorsionado y torturado por elementos de la policía estatal. Unos meses después, se ha visto gente rondando en vehículos con actitudes intimidatorias (incluso uno enseñando una pistola). A veces la línea telefónica o la de la luz se corta pero no saben la razón. Una mañana el director del albergue entra en su oficina, siempre cerrada con llave y se da cuenta que ha desaparecido una laptop con información valiosa.

En consecuencia, el albergue ha pedido medidas cautelares a la CIDH que le fueron otorgadas pero tras meses de negociación con el Estado no se notan avances aparte de dos aparatos celulares entregados que nunca tienen saldo.

Una mañana les llega un papelito: "ya párenle con su desmadrito y de andar defendiendo a mugrosos, se nos está acabando la paciencia".

Anexo T1 M2 S5

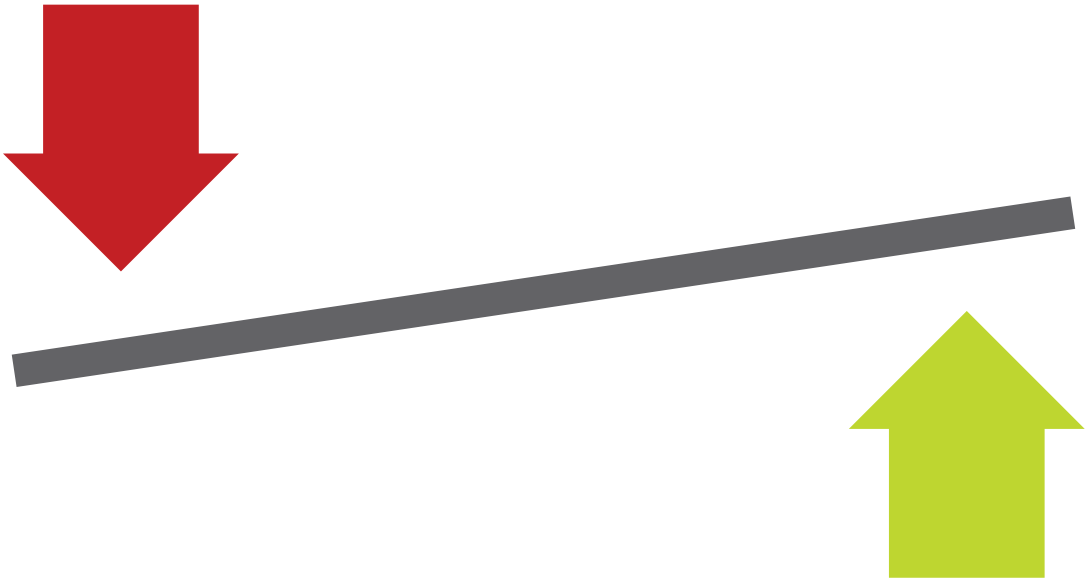
Análisis de Vulnerabilidades y Capacidades

Análisis de CAPACIDADES y VULNERABILIDADES

- **Identificar las capacidades y vulnerabilidades de la organización y de sus integrantes.**
- **Considerar diferenciaciones por género y a nivel individual, familiar, comunitario y organizacional (psicosocial).**
- **Priorizar las áreas que deberían ser fortalecidas y potenciar las capacidades.**

Vulnerabilidades

El grado en que los/las defensores/as son susceptibles a pérdida, daños, sufrimiento o la muerte en caso de un ataque



Capacidades

Los puntos fuertes y recursos a los que puede acceder un/a defensor/a para lograr un nivel mínimo de seguridad. Estas capacidades siempre son mejorables.

Anexo T1 M2 S5 continuación

Análisis de Vulnerabilidades y Capacidades*

Componentes de vulnerabilidades y capacidades geográficos , físicos y técnicos		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
EXPOSICIÓN	La necesidad de cruzar o quedarse en zonas peligrosas para levar a cabo actividades rutinarias u ocasionales, con actores amenazantes en esas zonas.	**V o C**
ESTRUCTURAS FÍSICAS	Las características de la vivienda (oficinas, casas, refugios); materiales de construcción, puertas, ventanas, armarios. Barreras protectoras. Alumbrado nocturno.	**V o C**
OFICINAS Y LUGARES ABIERTOS AL PÚBLICO	¿Están tus oficinas abiertas al público? ¿Existen áreas reservadas únicamente al personal? ¿Debes tratar condesconocidos que acuden a tus oficinas?	**V o C**
ESCONDITE, RUTAS DE ESCAPE	¿Existe algún lugar para esconderse? ¿Son accesibles? (distancia física) y ¿para quién? (para personas específicas o para el grupo entero) ¿Podrías salir momentáneamente del lugar si fuera necesario?	**V o C**
ACCESO A LA ZONA	¿Con qué dificultades se pueden encontrar los visitantes de fuera (funcionarios del gobierno, ONGs, etc.) para acceder a la zona? (en el caso de un vecindario peligroso, por ejemplo) ¿Con qué dificultades de acceso se encuentran los actores que generan amenazas?	**V o C**
TRANSPORTE Y ALOJAMIENTO	¿Existe algún acceso a transporte seguro (público o privado) para las PDDH? Estos transportes, ¿representan alguna ventaja o desventaja en particular? ¿Disponen las PDDH de un alojamiento seguro durante sus desplazamientos?	**V o C**
COMUNICACIÓN	¿Hay sistemas de telecomunicaciones (radio, teléfono)? ¿Disponen las PDDH de un buen acceso a éstos? ¿Funcionan correctamente en todo momento? ¿Podrían los actores amenazadores cortarlos antes de un posible ataque?	**V o C**

*Salvo los componentes de género, los demás componentes fueron tomados de Peace Brigades International (Oficina Europea) & Frontlinde Defenders, *Manual de Protección para los Defensores de Derechos Humanos*, 2005, cap. 2.

Anexo T1 M2 S5 continuación

Análisis de Vulnerabilidades y Capacidades

Componentes de vulnerabilidades y capacidades relacionados con el conflicto		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
VÍNCULOS CON LAS PARTES CONFLICTIVAS	¿Existe algún vínculo entre las PDDH y las partes en conflicto (parientes, vienen de la misma zona, intereses comunes) que pudiera ser utilizado injustamente contra las PDDH?	**V o C**
ACTIVIDADES DE LAS PDDH QUE AFECTAN A UNA PARTE CONFLICTIVA	La labor de las PDDH, ¿afecta de forma directa a los intereses de algún actor? (Como por ejemplo en el caso de la protección de recursos naturales valiosos, el derecho a la propiedad) ¿Trabajas en algún asunto delicado de cara a los actores con poder? (como por ejemplo el derecho a la propiedad de la tierra)	**V o C**
TRANSPORTE DE OBJETOS Y MERCANCÍAS INFORMACIÓN ESCRITA	¿Poseen las PDDH objetos o mercancías que puedan ser valiosos para los grupos armados, y que por lo tanto aumenten el riesgo de targeting o de robo? (Gasolina, ayuda humanitaria, pilas, manuales de salud, etc.) ¿Tienen las PDDH que llevar consigo información escrita sensible o comprometedora?	**V o C**
CONOCIMIENTO DE LAS ZONAS DE ALTO RIESGO	¿Posees algún tipo de información sobre lo que sucede en las zonas donde se producen combates e ataques que pudiera causarte algún riesgo? ¿Y sobre posibles zonas seguras para contribuir a tu seguridad?	**V o C**

Anexo T1 M2 S5 continuación

Análisis de Vulnerabilidades y Capacidades

Componentes de vulnerabilidades y capacidades del el sistema jurídico y político		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
ACCESO A LAS AUTORIDADES Y A UN SISTEMA JURÍDICO PARA RECLAMAR SUS DERECHOS	¿Pueden las PDDH iniciar un procedimiento legal para reclamar sus derechos? (Acceso a una representación legal, presencia física en juicios o reuniones, etc.) ¿Pueden las PDDH obtener una asistencia apropiada de las autoridades de cara a su labor y sus necesidades de protección?	**V o C**
CAPACIDAD PARA OBTENER RESULTADOS DE LAS AUTORIDADES	¿Tienen las PDDH derecho a reclamar sus derechos? ¿O ¿Están sujetos a leyes internas represivas? ¿Pueden adquirir suficiente poder/influencia para hacer que las autoridades tomen nota de sus reclamaciones?	**V o C**
CAPACIDAD DE MANTENER CRITERIOS LEGALES	¿Se les niega a las PDDH un registro legal o están éstos sujetos a largos retrasos? ¿Es tu organización capaz de mantener la contabilidad en orden según los requerimientos legales nacionales? ¿Emplean programas informáticos pirateados?	**V o C**

Anexo T1 M2 S5 continuación

Análisis de Vulnerabilidades y Capacidades

Componentes de vulnerabilidades y capacidades de gestión de la información		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
FUENTES Y PRECISIÓN DE LA INFORMACIÓN	¿Poseen las PDDH fuentes de información fidedignas en las que basar sus acusaciones? ¿Publican las PDDH información precisa y siguiendo métodos adecuados?	**V o C**
MANTENER, ENVIAR Y RECIBIR INFORMACIÓN	¿Pueden las PDDH guardar información en un lugar seguro y de confianza? ¿Podría ser robada? ¿Está protegida de virus y piratas informáticos? ¿Puedes enviar y recibir información de forma segura?	**V o C**
SER TESTIGOS O POSEER INFORMACIÓN CLAVE	¿Son las PDDH un testigo clave para presentar cargos contra un actor con poder? ¿Poseen las PDDH información única y relevante sobre un caso o proceso específicos?	**V o C**
TENER UNA EXPLICACIÓN COHERENTE Y ACEPTABLE SOBRE LA LABOR Y SUS OBJETIVOS	¿Tienen las PDDH una explicación clara, sostenible y coherente sobre su labor y objetivos? ¿Es esta explicación aceptable, o por lo menos tolerable, por parte de la mayoría o de todos los actores? (sobre todo los armados) ¿Están todos los miembros del grupo capacitados para proporcionar esa explicación cuando se les solicite? (en un retén o en una entrevista)	**V o C**

Anexo T1 M2 S5 continuación

Análisis de Vulnerabilidades y Capacidades

Componentes de vulnerabilidades y capacidades de género		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
CONDICIONES DE IGUALDAD DENTRO DE LA ORGANIZACIÓN	¿Existen diferencias salariales, en la distribución de responsabilidades y toma de decisiones entre hombres y mujeres al interior de la organización? ¿Se les asignan actividades, misiones de terreno, casos o labores distintas a hombres y a mujeres? ¿La organización tiene consideraciones especiales para apoyar a las mujeres que por su situación personal tienen actividades demandantes además del trabajo (llevar a sus hijos a la escuela, prepararles alimentos, llevar a cabo estudios, etc.)? ¿Todas las personas saben manejar y están listas para hacerlo en caso de emergencia o los viajes de trabajo son conducidos primordialmente por hombres? ¿Se tiene una visión en la organización de que hay que cuidar a las mujeres o que las actividades de riesgo son solo para los hombres? ¿Se considera que la seguridad y la protección deben ser un asunto de hombres?	**V o C**
CONDICIONES DE IGUALDAD EN LA FAMILIA Y COMUNIDAD	¿La labor de las PDDH desafía normas de género que imperan en la comunidad? ¿Se ve a las defensoras como "mujeres raras" que deberían renunciar a su labor pública o hay un sector de la comunidad que las ve con admiración por su rol transformador y en pro de la justicia? ¿Además de las labores en su organización, las mujeres enfrentan mayor carga de trabajo en sus hogares y el cuidado de los hijos? ¿Existen espacios en la comunidad o la familia donde las mujeres puedan empoderarse, hablar de sus problemas y buscar soluciones entre todas? ¿La comunidad considera que un defensor debe sacrificarse por su comunidad? ¿Es mal visto que un hombre hable de sus riesgos o miedos en la comunidad?	**V o C**
VIOLENCIA DE GÉNERO	¿La violencia hacia las mujeres (sexual, económica, emocional, física, etc.) es comúnmente aceptada o callada en su contexto? ¿Existen directrices internas en la organización sobre acoso sexual y las formas de abordarlo? ¿Ha habido entrenamientos de autodefensa para responder a un ataque físico tanto para hombres como para mujeres? ¿Existe una red de apoyo o refugio que la organización conozca para casos de violencia de género que puedan suceder a cualquiera de sus integrantes?	**V o C**

Anexo T1 M2 S5 continuación

Análisis de Vulnerabilidades y Capacidades

Componentes de vulnerabilidades y capacidades sociales y organizativas		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
EXISTENCIA DE UNA ESTRUCTURA DE GRUPO	¿Está el grupo organizado o estructurado de alguna forma? ¿Proporciona dicha estructura un grado aceptable de cohesión al grupo?	**V o C**
HABILIDAD DE TOMAR DECISIONES CONJUNTAS	¿Es la estructura del grupo un reflejo de intereses particulares o representa al grupo entero (incluyendo afiliados)? ¿Quién asume las principales decisiones y responsabilidades, una única persona o varias? ¿Se han creado sistemas de emergencia para la toma de decisiones y asunción de responsabilidades? ¿En qué grado es la toma de decisiones participativa? ¿La estructura del grupo permite las siguientes opciones ? a) toma de decisiones conjuntas e implementación de éstas ; b) debatir los temas en grupo ; c) reuniones esporádicas e inefectivas ; d) ninguna de las arriba mencionadas	**V o C** **a** **b** **c** **d**
PLANES DE SEGURIDAD Y PROCEDIMIENTOS	¿Se han puesto en marcha normas y procedimientos de seguridad? ¿Existe un buen conocimiento y apropiación de los procedimientos de seguridad? ¿Se cumplen las normas de seguridad?	**V o C**
GESTIÓN DE LA SEGURIDAD FUERA DEL ÁMBITO LABORAL	Familias. Tiempo libre. ¿Cómo manejan las PDDH su tiempo fuera del ámbito laboral (familia y tiempo libre)? El consumo de alcohol y drogas representan grandes vulnerabilidades. Las relaciones personales también pueden convertirse en vulnerabilidades (al igual que ventajas).	**V o C**
CONDICIONES LABORALES	¿Tiene todo el mundo un contrato laboral adecuado? ¿Se tiene acceso a fondos de emergencia? ¿Y a seguros?	**V o C**
CONTRATACIÓN DE PERSONAL	¿Se sigue el procedimiento adecuado en la contratación de personal o miembros? ¿Se sigue un *plan de seguridad* apropiado con los voluntarios ocasionales (como los estudiantes, por ejemplo) o los visitantes de la organización?	**V o C**
TRABAJAR CON GENTE O CON ORGANIZACIONES CONJUNTAS	¿Se trabaja de cara al público? ¿Se conoce bien a la gente? ¿Se trabajas conjuntamente con alguna organización como intermediaria ante la gente?	**V o C**
CUIDAR DE LOS TESTIGOS O VÍCTIMAS CON LAS QUE TRABAJAMOS	¿Evaluamos los riesgos de las víctimas y testigos, etc., cuando trabajamos en casos concretos? ¿Tomamos medidas de seguridad específicas cuando les vemos o cuando vienen a nuestra oficina? ¿Cómo reaccionamos si reciben amenazas?	**V o C**
VECINDARIO Y ENTORNO SOCIAL	¿Están las PDDH bien integrados socialmente en el área local? ¿Algunos grupos sociales consideran la labor de las PDDH como algo bueno o nocivo? ¿Están las PDDH rodeadas de gente presuntamente hostil? (vecinos que actúan de informadores, por ejemplo)	**V o C**
CAPACIDAD DE MOVILIZACIÓN	¿Pueden las PDDH movilizar a la gente en actividades públicas?	**V o C**

Anexo T1 M2 S5 continuación

Análisis de Vulnerabilidades y Capacidades

Componentes de vulnerabilidades y capacidades psicosociales (grupo /individuos)		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
CAPACIDAD PARA MANEJAR EL ESTRÉS Y EL MIEDO	Las personas clave, o el grupo en conjunto, ¿confían en su propio trabajo? ¿Expresan los individuos sentimientos de unidad y de tarea común (tanto en palabras como en actos)? ¿Existen espacios organizativos para abordar el estrés asociado al trabajo? ¿Existen fondos de atención psicológica o de sostén psicosocial permanente en la organización? ¿El nivel de estrés afecta en la comunicación y las relaciones interpersonales?	**V o C**
SENTIMIENTOS DE DESALIENTO O DE "SENTIRSE PERSEGUIDO"	¿Se expresan claramente (tanto en palabras como en actos) los sentimientos de desaliento o de pérdida de esperanza?	**V o C**

Anexo T1 M2 S5 continuación

Análisis de Vulnerabilidades y Capacidades

Componentes de vulnerabilidades y capacidades de análisis y contexto del trabajo		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
HABILIDAD DE COMPRENDER EL CONTEXTO Y EL RIESGO DEL TRABAJO	¿Tienen las PDDH acceso a una información precisa de su contexto de trabajo, de los actores involucrados y de sus intereses? ¿Son las PDDH capaces de procesar esa información y valorar las amenazas, las vulnerabilidades y las capacidades?	**V o C**
CAPACIDAD PARA DEFINIR PLANES DE ACTUACIÓN	¿Pueden las PDDH definir e implementar planes de acción? ¿Hay previos ejemplos de ello?	**V o C**
CAPACIDAD PARA OBTENER CONSEJO DE FUENTES BIEN INFORMADAS	¿Puede el grupo obtener consejo fiable? ¿De las fuentes apropiadas? ¿Puede el grupo decidir independientemente qué fuentes utilizar? ¿Se tiene acceso a organizaciones específicas o se posee un estatus que apoye las capacidades de protección?	**V o C**
PERSONAL Y CANTIDAD DE TRABAJO	¿Es el número de personas o trabajadores proporcional a la cantidad de trabajo existente? ¿Es posible organizar las visitas al terreno en equipos (de un mínimo de dos personas)?	**V o C**
RECURSOS FINANCIEROS	¿Se dispone de suficientes recursos financieros para la seguridad? ¿Se maneja el dinero de una forma segura?	**V o C**
CONOCIMIENTO DE IDIOMAS Y ZONAS	¿Se dominan los idiomas necesarios para trabajar en esta zona? ¿Se conoce bien la zona? (carreteras, pueblos, teléfonos públicos, centros de salud, etc.)	**V o C**

Anexo T1 M2 S5 continuación

Análisis de Vulnerabilidades y Capacidades

Componentes de vulnerabilidades y capacidades para el acceso a contactos nacionales e internacionales y a los medios de comunicación		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
ACCESO A REDES NACIONALES E INTERNACIONALES	¿Tienen las PDDH contactos nacionales e internacionales? ¿Con delegaciones, embajadas, otros gobiernos, etc. visitantes? ¿Con líderes de la comunidad, líderes religiosos, u otros personajes influyentes? ¿Se pueden emitir acciones urgentes a través de otros grupos?	**V o C**
ACCESO A LOS MEDIOS Y RESULTADOS	¿Tienen las PDDH acceso a los medios de comunicación (nacional, internacional)? ¿Y a otros medios (medios independientes)? ¿Saben las PDDH relacionarse con los medios de comunicación correctamente?	**V o C**

Anexo T1 M2 S6

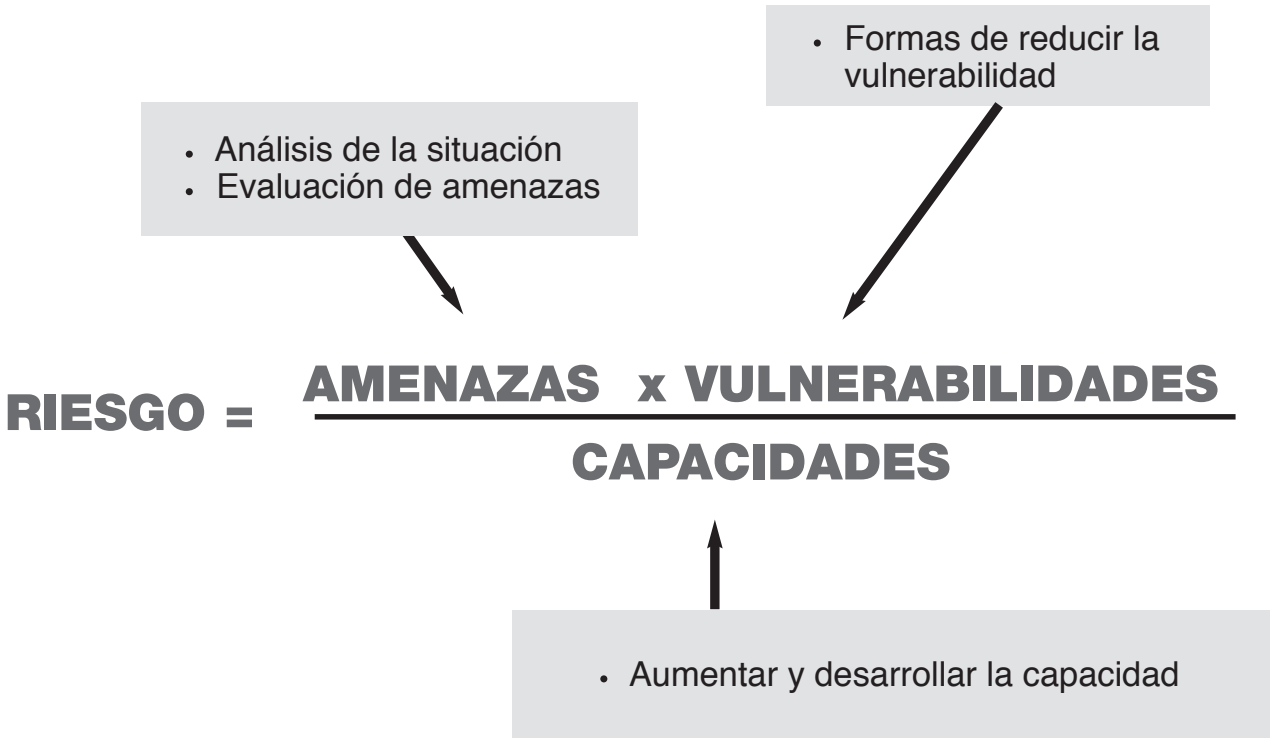
Análisis del riesgo*

Análisis de RIESGOS

Priorizar las amenazas latentes en función de los pasos previos.

Evaluar la probabilidad de que ocurra cada una de estas amenazas y su impacto.

Definir cuáles deberían ser prioritariamente abarcadas por un plan de seguridad.



*Tomado de Peace Brigades International (Oficina Europea) & Frontlinde Defenders, *Manual de Protección para los Defensores de Derechos Humanos*, p. 20.

Anexo T1 M2 S6b

Matriz de Priorización de Amenazas

Amenazas latentes	Probabilidad ¿Qué tan probable es que pase una situación semejante a nuestra persona, en nuestra comunidad u organización?	Impacto ¿Si sucediera algo similar en nuestra persona, comunidad u organización qué tan grave sería el impacto en nuestras vidas y nuestro trabajo?
Amenazas identificadas	¿Alta?	¿Alta?
	¿Media?	¿Media?
	¿Baja?	¿Baja?

Consenso sobre amenazas prioritarias identificadas:

1)

2)

3)

...

Anexo T1 M2 S6c

Pensar medidas de seguridad para amenazas prioritarias

CAPACIDADES	VULNERABILIDADES	MEDIDAS DE SEGURIDAD

Anexo T1 M3 S1

Tareas del diagnóstico pendientes

Etapas	Responsable(s) dentro de la organización ¿Quién será punto focal ?	Espacio para Compartir ¿Se harán reuniones especiales o se aprovecharán otros espacios existentes	Plazo de revisión y evaluación ¿Fechas importantes, fechas límites?	Recursos Necesarios ¿Qué insumos se necesitan para llevarlo a cabo? ¿se tiene lo necesario o se necesitan insumos adicionales
Análisis de Contexto Documentación, análisis de la información y de la coyuntura				
Mapa de actividades Planificación, identificación de riesgos potenciales, elaboración de medidas de seguridad especificas				
Análisis de actores Mapeo de actores, estrategia de persuasión / disuasión				
Análisis de Incidentes Identificar, registrar, compartir, analizar				
Análisis de Capacidades y Vulnerabilidades Identificarlas y proponer medidas para reducir las debilidades y potenciar las capacidades				
Análisis de riesgos Identificar las amenazas prioritarias y proponer medidas para reducir su probabilidad e impacto				

Anexo T1 M3 S1b

Formato de evaluación individual de taller y la facilitación

Evaluación del taller (Marque con una X la casilla con la que esté de acuerdo y brinde su opinión sobre los siguientes criterios)	Totalmente de acuerdo	Parcialmente de acuerdo	No estoy de acuerdo	Por favor explique o brinde más detalles al respecto
Conocí y comprendí conceptos nuevos que puedo aplicar a mi trabajo cotidiano de derechos humanos				
La secuencia con que fueron presentados los temas facilitó mi comprensión				
Las estrategias didácticas empleadas para abordar cada tema fueron las adecuadas				
El material que recibí me será de gran utilidad				
Obtuve herramientas y recursos teórico-prácticos que puedo emplear y compartir para mejorar mi seguridad				
El taller cumplió los objetivos planteados				
La logística del taller fue adecuada				
El espacio escogido para trabajar fue adecuado para que nos sintiéramos cómodos				
Evalúa del 1 al 10 los talleres en general (10 como evaluación máxima)				

Evaluación de la facilitación (Marque con una X la casilla con la que esté de acuerdo y brinde su opinión sobre los siguientes criterios)	Totalmente de acuerdo	Parcialmente de acuerdo	No estoy de acuerdo	Por favor explique o brinde más detalles al respecto
La persona facilitadora realizó en cada sesión alguna dinámica que despertara el interés en el tema				
La persona facilitadora mencionó los objetivos de la sesión y dio instrucciones claras al momento de realizar dinámicas				
La persona facilitadora fomentó la participación del grupo de manera inclusiva				
La persona facilitadora nos ayudó a generar confianza y apertura durante las sesiones de trabajo				
La persona facilitadora mostró empatía con lo que las personas participantes expresaron				
La persona facilitadora se preocupó por el bienestar de todas las personas del grupo				
La persona facilitadora retomó los comentarios y experiencias del grupo para integrarlos al tema				
La persona facilitadora expuso empleando un lenguaje claro y accesible que facilitara la comprensión de los temas				
La persona facilitadora respondió satisfactoriamente a las preguntas que se le plantearon				

Taller 2
Estrategia y Plan de Seguridad

El taller Estrategia y el Plan de Seguridad se enfoca en las fases posteriores al diagnóstico del *Método de gestión de la seguridad* (planificación > implementación > evaluación). Con base en el diagnóstico realizado en el Taller 1, este taller brinda herramientas para que las PDDH piensen en formas de incidencia sobre las fuentes de las amenazas con el objetivo de reducir su riesgo. La mayor parte del taller se enfoca posteriormente en el desarrollo de un Plan de Seguridad en tres ámbitos: en el trabajo cotidiano de la organización (ejecución); en situaciones particulares (prevención) y en situaciones de emergencia (reacción). En la etapa subsiguiente a la de planificación se trabaja para sentar las bases de una adecuada implementación y evaluación de la gestión de la seguridad a nivel personal y organizativo desde la propia perspectiva de las PDDH. Finalmente el taller trabaja en los consensos básicos para establecer espacios, responsabilidades y recursos que mejoren la gestión de la seguridad.

Objetivos generales del taller y resultados esperados:

- Impulsar la gestión de la seguridad dentro del trabajo de la organización.
- Visualizar distintas opciones para disminuir el riesgo a través de la reducción de vulnerabilidades, el aumento de capacidades y la incidencia sobre las amenazas.
- Identificar pistas para incidir sobre las amenazas identificadas en el Taller 1.
- Abordar los puntos de entrada para la elaboración de un *Plan de Seguridad* y un Plan de Emergencia en la organización.
- Evaluar la gestión de la seguridad a nivel personal y organizativo desde la propia perspectiva de las PDDH (autoevaluación).
- Llegar a consensos básicos sobre la definición de espacios, responsabilidades y recursos específicos para implementar y gestionar la seguridad (política de seguridad de la organización). priorizar y tener en cuenta antes de poder desarrollar una estrategia de seguridad.

Lo que el taller NO pretende:

- Proponer a la organización sus estrategias internas.
- Brindar "tips" o medidas de seguridad genéricas.
- Emitir valoraciones sobre las estrategias, visiones o análisis de la organización con la cual se trabaja.
- Juzgar el nivel de seguridad de la organización.

Duración total

***8 horas** (sin contar pausas).*

Calendarización

Se puede considerar dar el taller en un día y medio. Contar al menos 2 horas de pausa en un día repartidas a lo largo del día.

Plan General del Taller:

Módulo 1: Bienvenida e introducción

Sesión 1 Presentación, expectativas, revisión de agenda y acuerdos de convivencia

Sesión 2 Revisión de conceptos e introducción a las estrategias de seguridad

Módulo 2: Planificación

Sesión 1 El *Plan de Seguridad*: componentes y primeros pasos

Sesión 2 Marco general de actuación en caso de emergencia

Módulo 3: Implementación

Sesión 1 Niveles, Espacios, Recursos y Responsabilidades

Módulo 4: Evaluación

Sesión 1 La Rueda de la seguridad

Módulo 5: Compromisos de seguimiento, evaluación y cierre

Sesión 1 Compromisos de seguimiento, evaluación y cierre

Material y recursos:

- Hojas blancas
- Plumones
- Papelógrafos
- Una manta pegajosa o una superficie amplia y visible para todo el grupo que pueda servir de *Metaplán* *[ver Uso de herramientas complementarias en Cap. 3]*
- Cartulinas de colores
- Papelitos adheribles de colores
- Gafetes o etiquetas adhesivas
- Pizarrón
- Hilos de colores
- Papel *foamy* de colores
- Chinches
- Cinta adhesiva
- *Anexos Taller 2*
- *[Anexo T1.M2.S6c] Pensar medidas de seguridad para amenazas prioritarias* completado por las PDDH participantes durante el taller 1
- *[Anexo T1.M1.S1] Método de gestión de seguridad*
- *[Anexo T1.M1.S3c] Los pasos del Diagnóstico de Seguridad*
- *[Anexo T1.M1.S3a] Ecuación y ponderación del riesgo*
- Fotocopias para llenar del *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b]*
- Computadora y proyector u otro equipo de proyección audiovisual (opcional)

Consejos generales para este taller:

En la reunión previa es importante aclarar que este taller si bien aborda la incidencia sobre las fuentes de las amenazas identificadas previamente en el Taller 1, se enfoca principalmente en compartir herramientas para trabajar las vulnerabilidades y capacidades de la organización ante estas amenazas. Se puede recordar que el Taller 4 aporta herramientas de mayor profundidad para definir estrategias de incidencia.

Es importante aclarar que desarrollar un *Plan de Seguridad* y conseguir que las normas consensuadas se cumplan toma tiempo. Como todo proceso organizativo el cumplimiento de un *plan de seguridad* desde su concepción pasando por su implementación y evaluación tiene sus altibajos. Por ello se debe de hacer patente que el tiempo dedicado a este taller no será suficiente para desarrollar un *Plan de Seguridad* completo en todas sus fases, sino que cada organización deberá destinarle los espacios, tiempo y recursos necesarios posteriores al taller. El taller solo brinda un espacio inicial de bosquejo de estos elementos y comparte herramientas para empezar con el proceso, en este sentido el taller es solo el primer paso para el *Plan de Seguridad*.

Bienvenida e introducción

Presentación, expectativas, revisión de agenda y acuerdos de convivencia

50min

Objetivos específicos:

- Conocerse entre participantes y facilitadores.
- Recapitular la estructura del PASP, sus criterios y marco conceptual básico.
- Conocer qué esperan las personas participantes del taller y consensuar los objetivos del mismo.
- Clarificar el rol de la persona que facilita, sus posibilidades y limitaciones.
- Aclarar la metodología que se usará durante el taller.
- Sondear el conocimiento previo del grupo y ajustar taller si es necesario.
- Revisar la agenda con base en los puntos anteriores. Presentar las diferentes partes del taller y acordar tiempos y pausas.
- Acordar las normas de convivencia que servirán de base para generar un espacio seguro desde la perspectiva psicosocial y garantizar condiciones de equidad durante todas las sesiones subsecuentes.
- Distribuir materiales complementarios y roles de apoyo para la facilitación.

Puntos clave:

- Generar una apertura del taller que facilite la confianza y conocimiento de todas las personas participantes.
- Subrayar que la persona que facilita está para catalizar la participación y que se está construyendo un espacio conjunto de conocimiento. Por ello la participación de todas las personas es crucial para el proceso.
- Recapitular cómo se intersectan las tres dimensiones del análisis del PASP para una visión integral de la seguridad.
- Enfatizar la necesidad de compromisos y seguimiento por parte de la organización ya que el programa de asesorías plantea impulsar y acompañar el propio proceso de seguridad que las PDDH desarrollen.
- Explicar los pasos del *Método de gestión de la seguridad* usados por PBI. Diagnóstico > Planificación > Implementación > Evaluación.
- Señalar que el taller 2 trabaja sobre las 3 últimas fases del *Método de gestión de la seguridad* retomando la fase de diagnóstico trabajada en el taller 1.
- Consensuar normas de convivencia que promuevan las condiciones necesarias de respeto, diálogo e inclusión durante todo el taller. La persona que facilita debe estar segura que toda la gente se siente cómoda con los acuerdos alcanzados.

Actividades

Actividad 1: Ronda de presentación y expectativas del grupo.

Dinámica de presentación y discusión en plenaria* *10 min

Abrir con una ronda de presentación. Se puede pedir que participantes hablen en parejas y que cada quien presente a su pareja. También se pueden utilizar las dinámicas de presentación propuestas en el taller 1.

Independientemente de la dinámica de presentación utilizada es importante que las personas participantes comuniquen si ya han recibido talleres previos, y qué esperan del taller.

Se pueden apuntar motivaciones y expectativas en papelitos adheribles de colores para agruparlos en un lugar visible durante todo el taller. Estas expectativas se retomaran más adelante y al final del taller se revisarán para evaluar qué hemos cumplido y qué no.

Materiales

- Pizarrón
- Papelógrafos
- Plumones
- Fotocopias con objetivos y agenda del taller
- Papelógrafo o diapositivas con *Componentes analíticos necesarios para un esquema integral de seguridad y protección [Gráfico 1e, cap. 1]* y con el gráfico del *Método de gestión de seguridad [Anexo T1.M1.S1]*
- Papelitos adheribles de colores
- Gafetes o etiquetas adhesivas
- Computadora y proyector (opcional solo en caso que la actividad 3 no se lleve a cabo con papelógrafo o pizarrón)

Recursos adicionales y lecturas de apoyo:

Para distintas dinámicas de presentación e integración grupal y distención:

- BERISTAIN & SORIANO, *La Alternativa del Juego I: Juegos y Dinámicas de Educación para la Paz.* ***[RA1]***

Para comenzar adecuadamente con la construcción de un espacio seguro en un trabajo grupal sobre seguridad con PDDH:

- BARRY & NANIAR. *Integrated Security the Manual*, cap. 1.2, 1.3 y 3.4. ***[RA4]***

Para entender los conceptos de seguridad y protección:

- Capítulo 1 de esta Guía.

Para entender el PASP, sus criterios y marco conceptual básico:

- Capítulo 2 de esta Guía

Actividad 2: Lo que entendemos por "Plan de Seguridad".

Lluvia de ideas y discusión en plenaria a partir de preguntas detonadoras 10 min

Plantear al grupo la siguiente pregunta:

> *¿Al mencionar "Plan de Seguridad", cuáles son las palabras o ideas que nos vienen en mente*

Apuntar las palabras y conceptos usados por las PDDH en un papelógrafo plenamente visible. Usar y hacer referencia a las palabras y conceptos retomándolos durante las fases subsecuentes del taller. Retomar conceptos y discusiones del Taller 1.

Actividad 3: Recapitulación del PASP.

Presentación oral con apoyo de elementos visuales (se puede usar papelógrafo, pizarrón o diapositivas en power point) 10 min

Recordar en qué consiste el PASP, sus criterios y metodología. Bosquejar visualmente las tres dimensiones conceptuales que sustentan el programa de asesorías y los conceptos de seguridad y protección. *[ver definiciones conceptuales y gráficas de cap. 1 sección 1 y gráficos sobre estructura del PASP en cap. 2 sección 3 y 4 de esta guía]*

Explicar que el taller 1 fue el primer paso del método de gestión de la seguridad usado por PBI y que en el Taller 2 abordaremos los últimos tres pasos siguientes. *[Anexo T1.M1.S1]*

Actividad 4: Revisión de expectativas y adaptación de agenda y contenidos del taller en caso de ser necesario.

Discusión en plenaria 10 min

Presentar los objetivos y contenidos del taller consensuados previamente con la organización. Revisar junto con el grupo las expectativas expresadas en relación con los objetivos y la metodología del taller presentadas.

A partir de una perspectiva realista de las limitaciones en términos de tiempo, objetivos y contenidos del taller así como de las expectativas previamente expresadas por las PDDH, explicar lo que podemos hacer en este taller y lo que no es posible o que puede ser abordado sólo en talleres posteriores.

Realizar ajustes si es necesario.

Pegar la agenda general del taller consensuada en un papelógrafo a la vista de todas las personas participantes.

Actividad 5: Acuerdos de convivencia, distribución de material complementario y roles de apoyo.

Discusión en plenaria y/o dinámica participativa 10 min

Acordar en conjunto las normas de convivencia: cómo pedir la palabra, cómo expresar con respeto nuestros desacuerdos, cómo garantizar condiciones de igualdad, confidencialidad de los aspectos tratados durante el taller, uso de celulares, computadoras y cámaras, entradas y salidas de participantes,

puntualidad, etc. *[ver apartado sobre espacios con equidad y espacios seguros desde la perspectiva psicosocial en el apartado 3.2 y recursos de apoyo RA4]* Se puede realizar la "Dinámica de la Estrella" o alguna variante: Se pide a las personas participantes pararse en círculo y que vayan enunciando reglas que les parecen importantes. Cada vez que alguien enuncia una regla el resto de las personas muestran su acuerdo (acercándose al centro del círculo) o su desacuerdo (alejándose del centro del círculo). Si hay fuertes desacuerdos se busca el consenso. Después se hace un breve recuento de los acuerdos mínimos para la convivencia.

Después de las normas de convivencia se puede entregar material complementario (por ejemplo: un cuaderno del participante). Pedimos que no se lea inmediatamente ya que este se trabajará a lo largo del taller.

Dejar claro el rol de la persona que facilita y sus posibles limitaciones.

Distribuir roles de apoyo a la facilitación, preguntar a las personas participantes quién quiere ser voluntario/a para tomar actas y apuntar los consensos, para anotar otros pendientes y tareas que surjan durante el taller.

Consejos de facilitación:

- Se pueden utilizar distintas dinámicas de presentación para "despertar" o espabilar al grupo *[ver RA1].* Si el grupo es numeroso y no se conocían previamente, también se pueden usar gafetes o adhesivos con el nombre de las personas para facilitar dirigirse a las personas por su nombre de pila y recordar los nombres. La parte de presentación de las personas participantes se puede reducir si ya hemos tenido un taller con el mismo grupo y las personas se conocen bien entre sí y a la persona que facilita.
- Se puede también pedir a las personas que además de las palabras y conceptos realicen un dibujo sobre su idea de *plan de seguridad* y luego todo el grupo dice una lluvia de ideas sobre los dibujos de sus demás compañeros.
- En las partes con mayor carga conceptual se recomienda aprovechar al máximo los recursos gráficos propuestos.
- Con base en la revisión de expectativas puede ser necesario bajar las expectativas o ajustar la agenda para dedicar más tiempo a algunos temas, quitar otros etc. ¡Hay que ser flexibles y receptivos a la hora de tratar las expectativas del taller e ideas sobre seguridad y protección!
- Se puede consensuar un espacio para dejar los aparatos electrónicos como celulares y computadoras durante el taller (por ejemplo en la esquina de la sala o en una bolsa resguardada). Se puede consensuar cómo retribuirá al grupo alguien que llegue tarde a las sesiones o que pase por alto algún acuerdo de convivencia (por ejemplo puede traer dulces para todas las personas la siguiente sesión, o relevar al relator de acuerdos).
- ¡Atención con el control del tiempo! Este módulo es susceptible a extenderse demasiado.

Bienvenida e introducción

Revisión de conceptos e introducción a las estrategias de seguridad

60min

Objetivos específicos:

- Revisar los conceptos y conclusiones del taller 1.
- Entender que una estrategia de seguridad debería considerar reducir las vulnerabilidades y aumentar las capacidades discutidas en el taller 1 pero también incidir en la fuente de la amenaza.
- Entender la relación entre el espacio de actuación y las posibles formas de incidir en la fuente de la amenaza.
- Tener un punteo básico sobre los actores que se necesitaría considerar en el futuro al intentar *incidir sobre las* fuentes de las amenazas.

Materiales

- Papelógrafos
- Plumones
- Papelógrafo o diapositivas con las definiciones básicas de *seguridad* y *protección* y su relación con el espacio de actuación *[Gráfico 1a, cap. 1]*, Los *pasos del Diagnóstico de Seguridad [Anexo T1.M1.S3c]* y la *Ecuación y ponderación del riesgo y sus componentes [Anexo T1.M1.S3a].*
- *Metaplán*
- Fotos del *Metaplán* o copias del Mapeo de Actores hecho en el Taller 1 y rótulos de cartón de color para completarlo.

Puntos clave:

- Revisar la definición y elementos del riesgo (amenazas, vulnerabilidades y capacidades).
- Recordar las distintas opciones ante el riesgo: aceptarlo, reducirlo (intentando incidir sobre la fuente de las amenazas, o trabajando nuestras capacidades y vulnerabilidades) o evitarlo (reduciendo, suspendiendo, cambiando nuestras actividades, escondiéndose, exiliándose).
- El objetivo de una estrategia de seguridad es mantener abierto el espacio de actuación.
- Una estrategia de seguridad debería contemplar dos opciones que no son excluyentes, sino complementarias: 1) disminuir nuestra exposición al riesgo proponiendo medidas que puedan reducir nuestras vulnerabilidades y aumentar nuestras capacidades y 2) incidir sobre la fuente de la amenaza.
- Para incidir sobre la fuente de la amenaza se debe primero identificar a los actores que podrían agredir y a los actores que podrían o deberían proteger.
- Las estrategias de incidencia se basan en la disuasión al elevar los costes políticos de atacarnos o convenciendo a ciertos actores de cumplir con su obligación internacional de protegernos.
- Dejar claro que el taller 2 se enfoca principalmente en reducir la exposición al riesgo mediante un *Plan de Seguridad* y cubre por ende solo una parte de una estrategia de seguridad integral. Si se quiere trabajar a mayor profundidad las estrategias de incidencia se deberá recurrir al taller 4.
- Al terminar la sesión, explicar que a continuación trabajaremos un *Plan de Seguridad* que reduzca las vulnerabilidades de la organización ante las amenazas prioritarias identificadas en el Taller 1.

Actividades

Actividad 1: Repaso de los conceptos básicos del Taller 1.

Presentación* *30min

Recordar y repasar los conceptos básicos del Taller 1, como las definiciones básicas de seguridad y protección y su relación con el espacio de actuación *[Gráfico 1a, cap. 1]*, *Los pasos del Diagnóstico de Seguridad [Anexo T1.M1.S3c]* y la *Ecuación y ponderación del riesgo y sus componentes [Anexo T1.M1.S3a].*

Recursos adicionales y lecturas de apoyo:

- Peace Brigades International (Oficina Europea) & Frontlinde Defenders, *Manual de Protección para los Defensores de Derechos Humanos*, cap. 6.
- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.6. *[RA5]*

Consejos de facilitación:

- Lo que deberíamos transmitir con el dibujo del niño y el perro, o con cualquier otro que se elija es que cada defensor tiene un espacio de actuación y que para mantenerlo abierto se pueden seguir varias estrategias ante las amenazas. Hay que evitar ser demasiado conceptuales y usar muchas definiciones. Por eso se propone explicar el concepto de espacio de actuación y ejemplificar diferentes estrategias de seguridad a través de un dibujo.
- La Actividad 3 es solo una introducción para comenzar a pensar posibles actores sobre los que se puede incidir. Esta actividad se puede desarrollar a profundidad más adelante en el taller 4. Con esta actividad debemos enfatizar que además de un *Plan de Seguridad*, una estrategia de seguridad debería incluir un componente de *Incidencia*.
- Puede ser necesario incluir también una pequeña diferenciación entre medidas de seguridad, estrategia de seguridad y *Plan de Seguridad* (tener cuidado de no confundir y no dar a pensar que son lo mismo). Una definición útil es que la estrategia es un plan con vistas a alcanzar un objetivo a largo plazo y un plan son los pasos concretos que deben ser dados para alcanzar el objetivo (ver definición de *Plan de Seguridad* en la sesión siguiente). Las medidas de seguridad por ejemplo, como las que se trabajaron en el taller 1 son sólo acciones básicas de reacción, ejecución y prevención. Si estas medidas no están incluidas dentro de un plan, ni responden a una estrategia, no podremos saber si tienen el efecto que necesitamos.

Actividad 2: Analogía sobre el espacio de actuación "El niño y el perro".

Discusión en plenaria* *10 min

Para introducir el concepto de estrategia de seguridad y de espacio de actuación dibujamos sobre un papelógrafo o pizarrón un niño y en un patio cerrado una pelota y un perro de grandes colmillos.

Se explica que el niño quiere jugar con su pelota pero para esto necesitaría entrar en el patio donde el perro amenaza con morderlo. El patio representa el espacio del niño (= *espacio de actuación*). Pedir a las personas participantes que identifiquen la amenaza (=*el ataque del perro*).

Preguntarles qué piensan que puede hacer el niño para recuperar su espacio e ir a jugar, ligar las respuestas con estrategias de seguridad. Por ejemplo el niño podría:

a) lanzarle un hueso al perro (lo convence de que no representa una amenaza sino algo positivo – aceptación/tolerancia)

b) entrar acompañado de un perro protector más grande o con un adulto (disuasión)

c) entrar con un escudo al patio (reducción de vulnerabilidades)

d) tomar un entrenamiento para domar perros (aumento de capacidades)

e) hablar con el dueño para que controle, amarre o le ponga un bozal al perro (incidencia sobre la fuente de la amenaza, puede ser que lo convence o lo disuade)

Actividad 3: Retomar el análisis de actores para nuestra estrategia de seguridad.

Discusión en plenaria* *20 min

Retomar el Mapeo de Actores realizado el taller 1 (utilizar las fotos del *Metaplán* o en su defecto una reproducción o las tarjetas de los actores analizados)

A partir de los actores analizados se realizan las siguientes preguntas:

¿Cuáles actores tienen una obligación o un interés en protegernos?

¿Cuáles actores tienen el poder de ejercer influencia sobre los perpetradores?

¿Todos los actores son racionales y evalúan los costes políticos de un ataque antes de actuar?

¿Sobre qué actor se puede ejercer un poder de disuasión?

Con base en las respuestas hacer junto con el grupo una lista de actores que podrían ser influenciados (mediante acciones para disuadirlos de agredir o acciones encaminadas a persuadirlos de proteger a las PDDH).

Discutir en plenaria:

¿Qué acciones se están ya tomando o se podrían tomar para influenciar a estos actores? (tanto para convencer a los actores con obligación o interés de protección que nos protejan como para disuadir a actores agresores de agredirnos).

Planificación

El Plan de Seguridad: componentes y primeros pasos

45min

Puntos clave:

- Definición del *Plan de Seguridad*: *Conjunto de pasos concretos y realistas que deben ser dados para reducir las vulnerabilidades y aumentar las capacidades de la organización ante una amenaza.*
- El plan sirve para tener acordadas reglas mínimas de comportamiento que todas las personas adoptarán para minimizar el riesgo.
- Explicar que el *Plan de Seguridad* es una estrategia de reducción del riesgo y por ende no siempre es la respuesta adecuada (puede ser que el riesgo sea tan grande que deba ser evitado en un primer momento).
- Recordar que una estrategia global de seguridad debería, aparte del *Plan de Seguridad*, *incluir estrategias de incidencia* para poder actuar directamente sobre la amenaza: disuadiendo los potenciales agresores de agredirnos o convenciéndolos de protegernos.
- El *Plan de Seguridad* reduce las vulnerabilidades y potencia las capacidades pero rara vez influye sobre la voluntad del agresor para concretar la amenaza (para eso hay estrategias de incidencia). A pesar de que el plan no actúa directamente sobre la fuente de la amenaza, busca disminuir la probabilidad de que la amenaza se cumpla o de mitigar el impacto en caso de que ocurra.
- Componentes del *Plan de Seguridad*:

  Prevención: Protocolos para situaciones específicas o actividades "extraordinarias". Por ejemplo: preparación de viajes en zona de alto riesgo, negociación con actores armados, cómo llevar a cabo manifestaciones o preparar conferencias de prensa, protocolos para abordar el estrés antes de audiencias o eventos clave, protocolos de prevención de violencia de género, etc.

  Ejecución: Políticas permanentes que rigen el día al día de la organización. Por ejemplo: medidas para el manejo de la información, la comunicación, la seguridad de las sedes, la selección del personal, los espacios de trabajo políticas de salud mental, etc.

  Reacción: Planes en caso de emergencia. Por ejemplo: marco general en caso de emergencia o cómo reaccionar ante un problema concreto (cateo, ataque, desaparición, detención, estrés acumulativo excesivo por un evento violento o estado de *shock* etc.)
- Es mejor tener un *Plan de Seguridad* simple y realista que tener uno muy elaborado que sabemos nunca se cumplirá. Un buen *Plan de Seguridad* es un plan cuyas medidas se cumplen.
- El *Plan de Seguridad* debe revisarse periódicamente.
- Los IdS pueden visibilizar vulnerabilidades que se nos ha olvidado cubrir en el *Plan de Seguridad* por ello pueden abordarse como una oportunidad para mejorar el Plan.
- Hay un mínimo de 3 espacios donde una persona defensora está en riesgo: en su trabajo, en su casa y en el traslado entre uno y otro (por eso es un mínimo, dependiendo de las actividades que desarrolla la persona defensora, tanto en su tiempo libre como en lo laboral, los espacios aumentan).
- Cuando pensamos las medidas de seguridad debemos reflexionar sobre los espacios que abarcan ya que puede haber otros espacios en los cuales hay vulnerabilidades y tendremos que adoptar otras medidas.
- Hacer un sinnúmero de medidas de seguridad que no estén vinculadas con un análisis de las amenazas, las vulnerabilidades y las capacidades puede dar una falsa impresión de seguridad ya que al no tener un plan que responda al nivel de riesgo real, las medidas pueden resultar contraproducentes.

Objetivos específicos:

- Definir lo que es un *Plan de Seguridad*
- Recordar que un *Plan de Seguridad* solo actúa sobre algunos componentes del riesgo y que se necesitan estrategias más amplias para incidir sobre las fuentes de las amenazas.
- Presentar los componentes que puede tener un *Plan de Seguridad*: Protocolos, Políticas y Planes de emergencia.
- Clarificar que la función de dichos componentes puede tener una función de prevención, ejecución o reacción.
- Identificar los protocolos, políticas o planes que la organización debe implementar de manera prioritaria.

Materiales

- Papelógrafo o diapositivas con los Elementos básicos de un *Plan de Seguridad*. *[Anexo T2.M2.S1]*
- Fotocopias o papelógrafos con el anexo Formato de preparación de un *Plan de Seguridad*. *[Anexo T2.M2.S1b]*
- Amenazas prioritarias detectadas en el taller 1, Módulo 2 Sesión 6 y Anexo completado en el taller 1 por las personas participantes. *[Anexo T1.M2.S6c]*

Recursos

Actividades

Actividad 1: Definir qué es un Plan de Seguridad.

Presentación 10 min

Explicar los *Elementos básicos de un Plan de Seguridad [Anexo T2.M2.S1]* sus alcances y limitaciones.

Actividad 2: Introducción a la preparación del Plan de Seguridad.

Ejercicio en grupos y discusión en plenaria 35 min

Recordar en plenaria las amenazas prioritarias ubicadas en el Taller 1, en caso de haberse rellenado recuperar el anexo completado por las personas participantes *[Anexo T1.M2.S6c]*

Dividir en grupos de 3 a 5 personas. Cada grupo trabajará sobre una de las amenazas prioritarias identificadas en el taller 1. Para cada amenaza prioritaria un grupo completará un formato como el del anexo *Formato de preparación de un Plan de Seguridad. [Anexo T2.M2.S1b]*

Pedir a cada grupo que retome las capacidades y vulnerabilidades para cada amenaza prioritaria y que tomen los primeros 5 minutos de la actividad para pensar si quieren agregar algo importante en estos campos respecto a lo que habían trabajado en el taller 1.

Pedir que rellenen las columnas de "Medidas de Seguridad" pensando las acciones básicas que deberían ser llevadas a cabo para abordar las capacidades y vulnerabilidades. Pedir también que especifiquen el componente del plan al cual corresponden dichas medidas.

Por el momento no deberán rellenar los espacios sobre responsabilidades y recursos necesarios, estos se trabajarán más adelante.

Utilizar los últimos diez minutos de la plenaria para socializar los distintos formularios de los grupos y discutir en plenaria los principales hallazgos.

Consejos de facilitación:

- Manejar de forma realista las expectativas de las personas participantes! Elaborar un *Plan de Seguridad* toma mucho tiempo y es una actividad que la organización debe hacer posteriormente invirtiendo recursos en términos de tiempo, responsabilidades, seguimiento, etc. Por ello no podemos completar esta actividad del todo en un taller. La sesión actual sirve como introducción y comparte una propuesta de metodología que se puede seguir para desarrollar posteriormente un *Plan de Seguridad* más acabado.
- Para la Actividad 2 pueden haber vulnerabilidades y capacidades que se repiten para diferentes amenazas prioritarias.
- Puede ser complicado para el grupo pasar de las vulnerabilidades/capacidades a medidas de seguridad. En vez de pensar en la amenaza como un simple

adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos,* cap. 1.7.
- Front Line Defenders, *Manual sobre seguridad: Pasos prácticos para defensores/as de derechos humanos en riesgo*, cap. 5. *[RA5]*

Para una forma alternativa de trabajar el bosquejo de un *Plan de Seguridad* con organizaciones ver:

- Protection International, *Guía de facilitación para el nuevo manual de protección para los defensores de derechos humanos*, pp. 97-102. *[RA2]*

suceso (por ejemplo robo de información), pensar en ella en términos de *¿qué es lo que quieren evitar?* Quieren evitar la posibilidad que ocurra algo y quieren evitar que en el caso de que ocurra el impacto sobre la organización no sea tan grave (por ejemplo queremos evitar que roben información sensible y que nos quedemos sin archivos para continuar nuestro trabajo). *Queremos que sea más difícil llevar a cabo la amenaza y queremos también que sí se lleva a cabo, las consecuencias negativas para la organización sean menores, ¿qué medidas podemos tomar para esto?*

- Considerar si la amenaza toca todos los espacios del defensor (casa, trabajo, traslados etc.) y verificar si están cubiertos por las medidas propuestas. Al revés, se puede tomar cada medida y ver en qué espacio protegen a las PDDH o reducen la posibilidad de que la amenaza se materialice.
- Las personas suelen elegir medidas generales de seguridad y poco aplicables, es importante hacerlas ver que tienen que ser específicas para que realmente sean medidas. Por ejemplo, suelen decir cosas como "una medida es tener una política de acceso a la organización", en este caso alentarlos a pensar cuáles serían los componentes de esta política entonces y qué mecanismos específicos necesitarían para que se implemente.
- Las personas suelen preguntar sobre medidas generales que sirvan de antemano (preguntan por ejemplo si es bueno "cambiar de ruta constantemente"). En este caso, explicar que no opinamos específicamente sobre este tipo de medidas (ni las recomendamos ni las rechazamos *a priori*), sino que las deben consensuar a la luz de su contexto específico. Una medida apropiada para una organización no necesariamente sirve para otra.
- Las medidas deben ser realistas y apegadas al contexto de la organización. Hay organizaciones que han estudiado y observado que en un contexto de defensa de derechos humanos, ciertas medidas han funcionado para la mayoría de organizaciones y son vistas como buenas prácticas (i.e. no viajar solo, cambiar de rutas, etc.). Estas posibles medidas y/o buenas prácticas no deben menguar la creatividad de la organización para buscar formas alternas de protegerse. Es decir, al usar un catálogo de buenas medidas existe el riesgo de caer en una fórmula única que en caso de no poder ser cumplida deja en desprotegida a la organización.
- Si las PDDH insisten en tener alguna lista base que las oriente, para comenzar a imaginar sus propias medidas se pueden referir a Front Line Defenders, *Manual sobre seguridad: Pasos prácticos para defensores/as de derechos humanos en riesgo*, apéndices 5 a 15. *[RA5]*
- Dejar claro que hasta ahora hemos seguido cuatro pasos para construir un *Plan de Seguridad*:

  1) Hemos priorizado las amenazas prioritarias en el Taller 1.

  2) Hemos identificado las vulnerabilidades y capacidades relacionadas a cada una de estas amenazas.

  3) Hemos definido medidas que puedan disminuir las vulnerabilidades y aumentar las capacidades.

  4) Hemos identificado en qué apartado de un *Plan de Seguridad* podría ir cada medida (protocolo, política o plan de emergencia)

Planificación

Marco General en caso de Emergencia

2h

Objetivos específicos:

- Que las PDDH desarrollen un Plan para reaccionar ante cualquier tipo de emergencia.
- Llegar a un acuerdo sobre la definición de una emergencia entre las personas integrantes de la organización.
- Presentar los elementos de reacción y prevención de una emergencia: "guardia", "primer contacto", "red de apoyo", "apoyo emocional", etc. y valorar su utilidad para la organización.
- Consensuar marco general de actuación en caso de emergencia.

Materiales

- Pizarrón o papelógrafos
- Plumones
- Fotocopias con Anexos para la sesión *[T2.M2.S2; a,b,c,d,e,f]*

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.7. ***[RA5]***

Puntos clave:

- Antes de empezar con las actividades dejar claro que en esta sesión empezaremos a desarrollar un plan para reaccionar ante cualquier tipo de emergencia. Es decir que escogemos trabajar sobre un componente específico del *Plan de Seguridad* (Reacción). ¡Esto no quiere decir que no haya que cuidar los otros componentes! Sin embargo con la actividad 2 de la sesión anterior ya hemos visto un ejemplo de metodología para desarrollar los otros componentes.
- Para desarrollar un Plan de Emergencia se seguirán tres pasos:

  1) Intentar llegar a una definición consensuada y compartida de qué es una emergencia

  2) Definir qué personas deberíamos contactar en caso de emergencia (lista de contactos de emergencia).

  3) Definir los pasos a seguir en caso de emergencia (marco general de actuación)
- Dar ejemplos de una definición de emergencia: *Emergencias son aquellos hechos o situaciones que, por su gravedad para las personas o /y organizaciones implicadas, tienen una repercusión directa con el trabajo de la organización (a cualquier nivel). Ante estas situaciones se requieren acciones rápidas y no siempre previsibles. Por hechos graves nos referimos a cualquier tipo de incidente o situación que genera riesgos para la seguridad de los integrantes o que pone en peligro la integridad física o el bienestar emocional de las PDDH.*
- Al trabajar los tres elementos del plan de emergencia (definición, contactos y marco general de actuación) dejar claro que ninguna definición ni lista es perfecta. No hay respuesta correcta o incorrecta. Lo importante es que se llegue a un acuerdo entre las personas integrantes de la organización y que la definición y propuestas sean efectivas para responder a sus necesidades.
- Facilitar un formato que sirva de guía a las organizaciones para documentar emergencias *[Anexo T2.M2.S2f]*
- Recordar por qué es importante contar con un plan de emergencia antes de que esta suceda: por el grado de estrés que implica y la rapidez de respuesta que requiere, tener pasos pre definidos ayuda, tanto a que no se escape ningún detalle importante, como para que la persona directamente afectada por la emergencia y sus colegas sepan los primeros pasos que se han de seguir.

Actividades

Actividad 1: Definir conjuntamente una emergencia.

Lluvia de ideas y discusión en plenaria a partir de preguntas detonadoras 20 min

Plantear al grupo las siguientes preguntas:

¿Qué es una emergencia?

¿Qué criterios usamos para calificar un suceso como una emergencia?

¿Podríamos dar algunos ejemplos?

Apuntar las ideas en el pizarrón o papelógrafo que surjan de las respuestas. Resumir las ideas para llegar a una definición o criterios mínimos consensuados.

Tomar nota de los acuerdos alcanzados en la relatoría o en el formato propuesto en la sección de definición de emergencia y ejemplos. *[Anexo T2.M2.S2a]*

Actividad 2: Definir los elementos de una lista de contactos de emergencia y un marco general de actuación en caso de emergencia.

Presentación 20 min

Proponer criterios que podría tener una lista de contactos de emergencia ver *Propuesta de criterios para contactos de emergencia*. *[Anexo T2.M2.S2b]* Por ejemplo Guardia, red de apoyo, autoridades locales y federales, servicios públicos, asesor legal, atención psicológica, etc. estos criterios deben servir de ejemplo y las personas pueden adaptarlos a las necesidades que identifiquen.

Proponer criterios que podría tener un Marco general de actuación en caso de emergencia: *¿Quién es el primer contacto? ¿Quién y cómo se documenta y analiza lo ocurrido? ¿Quién toma las decisiones? ¿Quiénes podrían abordar el impacto psicosocial en la organización para gestionar los efectos de una emergencia? ¿Cómo se reacciona se contactan a las autoridades? ¿Se contactan aliados? ¿Se contacta a la prensa o es más seguro mantener la confidencialidad? [Ver Anexo T2.M2.S2c]*

Actividad 3: Realizar el directorio de contactos de emergencia y trabajar los pasos a seguir en caso de emergencias.

Ejercicio en grupos 40 min

Se divide a las personas en dos grupos:

El grupo 1 debe pensar en los contactos iniciales para los casos de emergencia en sus distintos rubros. *[Ver Anexo T2.M2.S2d]*

El grupo 2 debe definir los pasos a seguir para reaccionar en caso de emergencia. *[Ver Anexo T2.M2.S2e]*

Cada grupo debe escoger algunos ejemplos de emergencia para probar sus propuestas.

Actividad 4: Debate y consensos sobre propuesta inicial para actuar en casos de emergencia.

Discusión en plenaria 40 min

Se pide que cada grupo elija una persona para explicar su propuesta en plenaria.

Se debaten las propuestas de ambos grupos.

Se intentan consensuar pasos a seguir en caso de emergencia o al menos acordar quién podría afinar la propuesta y cuándo se podría retomar la discusión (espacio y momento concreto).

La persona relatora toma nota de los acuerdos alcanzados en las secciones de "Contactos de Emergencias" y "Marco General de Actuación" *[Anexo T2.M2.S2a]* y se facilita un *Formato para analizar y documentar una emergencia [Ver Anexo T2.M2.S2f]* que les pueda servir de base para su trabajo ulterior para casos de emergencia.

Consejos de facilitación:

- Para facilitar la Actividad 1 se puede dar el ejemplo de definición de emergencia dada en los puntos clave, sin embargo esta definición es solo un ejemplo y es preferible que las PDDH acuñen su propia definición.
- Si no se logra con el grupo llegar a listas de contactos o pasos concretos de reacción intentar al menos acordar quién afinará ambas propuestas y cuándo y dónde se retomarán las discusiones.
- Para cada uno de los conceptos que presentamos y/o proponemos, es siempre bueno retomar emergencias previas que ya hayan tenido en la organización y ver cómo funcionaron sus propios procesos.
- No se deben forzar dinámicas que la estructura organizacional no esté preparada para asumir. Es decir, hay estructuras en donde la toma de decisiones y los primeros contactos siempre pasan por un cierto comité directivo o ciertos liderazgos. Si es así, ya hay una parte predefinida y solo habría que pensar qué harían estas personas si estuvieran involucradas como afectadas directamente en la emergencia. Lo importante es que todas las demás personas tengan esta claridad.
- Es común que surja la pregunta de si vale la pena establecer lenguaje codificado. Nuestro rol facilitando no es aprobarlo o desaprobarlo, pero hacerles pensar en los pros y contras con algunos ejemplos. El uso de códigos puede funcionar bastante bien en organizaciones que se mantienen constantes con su personal y tienen tiempo para memorizarlos y volverlos parte de su rutina (siendo entonces utilizado en general y no solo en caso de emergencia). Por otro lado, hay que tener en cuenta que durante una emergencia las personas olvidan incluso cosas básicas por el nivel de estrés al que son expuestas. En el caso de otras organizaciones, en una emergencia otras reglas de seguridad relativas a los códigos y comunicación son ignoradas porque lo más importante desde su punto de vista es la claridad de la información y la resolución de la emergencia (es decir, usan códigos en su día a día, pero si hay una emergencia prefieren no usarlos).
- Cuidar que la lista de contactos de emergencia no se vuelva un directorio de la organización. La lista debe limitarse a contactos importantes, relevantes y cada persona que esté en la lista debe tener una función. Una lista también es importante para detectar relaciones que nos hacen falta construir Por ejemplo: *¿tenemos un abogado/a al que llamar? ¿tenemos relación con especialistas u organizaciones para atender casos de violencia de género o de impacto psicosocial organizativo?*
- Hacer énfasis en que en muchas ocasiones las emergencias implican situaciones complicadas e intereses contrapuestos. Por ejemplo puede ponderarse denunciar en medios una agresión sexual a una integrante de la organización para exigir justicia pero por otro lado sin su consentimiento para hacerlo puede provocar una revictimización de la persona afectada. En otros casos de emergencia se puede decidir evacuar a una PDDH, pero si no se evalúa el impacto psicosocial de exiliar a esa persona de su comunidad los efectos contraproducentes de dicha medida pueden ser mayores que los beneficios. ***[ver RA4 para recursos en caso de emergencia con perspectiva psicosocial y de salud mental]*** Por ejemplo algunas organizaciones prefieren contactar con autoridades, mientras que otras no. Este tipo de situaciones complicadas es el que se deben de ir planteando al clarificar los procesos en el marco general de actuación.
- Los anexos referidos en esta sesión no suelen ser útiles para todos los perfiles de PDDH como defensores comunitarios o defensores de base. En este caso, se puede definir una lista de situaciones en las que las personas participantes consideran que ameritan dar una respuesta de emergencia: *¿puede esperar o tiene que resolverse en el momento que se da? ¿dejarías lo que estás haciendo para ir a resolver la situación?* etc. y trabajar los mismos elementos propuestos en la actividad 3 (contactos y pasos a seguir). La persona que facilita puede también formular preguntas basadas en los anexos para guiar la actividad trabajando con un *Metaplán* o papelógrafos dónde las personas participantes escriban/dibujen los acuerdos alcanzados (a quienes contactar y qué pasos seguir). Puede ser útil usar ejemplos de emergencias pasadas y evaluar qué funcionó o no.

Implementación

Niveles, Espacios, Recursos y Responsabilidades

1h 15min

Objetivos específicos:

- Sensibilizar sobre la interconexión de los tres niveles de implementación del *Plan de Seguridad*.
- Promover el compromiso institucional a favor de la seguridad.
- Identificar las necesidades de espacios, recursos y definición de responsabilidades dentro de la organización para definir el *Plan de Seguridad* en tres fases: 1) planificación, 2) implementación y 3) evaluación.
- Llegar a un acuerdo sobre las actividades pendientes que la organización deberá trabajar ulteriormente para definir su *Plan de Seguridad* con mayor detalle.

Materiales

- Pizarrón
- Plumones
- Papelógrafo o diapositivas con los *Niveles de Implementación de la política de Seguridad*. *[Anexo T2.M3.S1]*
- *Formato de preparación de un Plan de Seguridad [Anexo T2.M2.S1b]* Trabajado en el Módulo 2, Sesión 1 de este taller

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 2.2 y 2.3. ***[RA5]***

Puntos clave:

- Los planes, protocolos etc. son inútiles si no son implementados y respetados.
- Las reglas de seguridad no se deben entender como reglas "duras" que hay que imponer. Por el contrario, las reglas suelen respetarse cuando las personas integrantes de la organización las entienden, se las apropian y se sienten partícipes del proceso de manejo de la seguridad en la organización.
- Para que una Política de seguridad se pueda implementar se necesita de compromiso en tres ámbitos:

  1) *Individual*: La seguridad es un asunto que incumbe a todas las personas integrantes de la organización y cuyas medidas tocan incluso a sus relaciones con sus familias, comunidades, etc. fuera del trabajo. Para que un *Plan de Seguridad* funcione todas las personas de la organización deben internalizar y seguir las medidas consensuadas e incorporar estas medidas a sus funciones cotidianas.

  2) *Institucional*: La organización debe tomar medidas para que se implemente el plan integrando la seguridad en los planes y agendas de trabajo atribuyendo recursos y distribuyendo responsabilidades. En este sentido la organización tiene que dedicar espacios para el análisis, supervisión, formación, etc. y asegurar que hay mecanismos para que todas las personas integrantes conozcan las medidas de seguridad. No menos importante es el rol de la organización para evaluar la implementación de los planes, protocolos y políticas para mejorarlos.

  3) *Inter-organizacional*: Se debe trabajar por un mínimo de coordinación con organizaciones aliadas u otras organizaciones con las que trabajamos de cerca y de las cuales depende en gran medida nuestra seguridad. Por ejemplo no sirve tener protocolos de encriptación de la información sensible a nivel interno si al compartirla con organizaciones aliadas éstas no tienen los mismos protocolos. De la misma manera es bueno saber cómo reaccionarían las organizaciones pertenecientes a nuestras redes de apoyo si los llamamos en caso de emergencia.
- La política de seguridad debería aparecer como una introducción al *Plan de Seguridad* de la organización ya que define los espacios, recursos y responsabilidades y detalla los procedimientos para el diagnóstico, la planificación, la implementación y la evaluación del Plan.

Actividades

Actividad 1: Explicar los Niveles de Implementación de la política de seguridad.

Presentación* *30 min

Explicar que la seguridad es un asunto que implica la participación de todas las personas integrantes de la organización y debe ser implementada en tres niveles: individual, institucional e inter-organizativo.

Explicar que al interior de la organización el compromiso hacia la seguridad pasa por una política institucional que define espacios, recursos y responsabilidades para implementar el *Plan de Seguridad*.

Actividad 2: Consensuar responsabilidades y recursos necesarios.

Discusión en plenaria y trabajo en grupos* *45 min

Se plantean al grupo las siguientes preguntas:

> *¿Qué protocolos, políticas o planes de emergencia están entonces pendientes de desarrollar?*
>
> *¿Quién o quienes tienen la responsabilidad de desarrollar esto?*
>
> *¿Qué recursos se necesitan para desarrollar esto?*
>
> *¿Cuándo se va a desarrollar esto (espacio en la agenda de trabajo) con qué plazos?*

Se toma nota de los acuerdos. Se explica que quedan como una tarea para la organización, es importante definir, espacios, responsables y plazos concretos para estas tareas.

A partir de los consensos se intenta completar el *Formato de preparación de un Plan de Seguridad* *[Anexo T2.M2.S1b]* que ya se había trabajado. Un grupo trabaja la columna de responsabilidades y otro grupo la de recursos necesarios.

Consejos de facilitación:

- Si la primera parte de la sesión resulta muy conceptual para el grupo puede omitirse. Por ejemplo con defensores comunitarios podemos comenzar a trabajar directamente con las definiciones de: 1) *¿Qué necesitan para implementar cada medida?* (recursos) 2) *¿Cuándo y dónde la van a implementar?* (espacios) y 3) *¿Quién está encargado de hacer posible que se implemente la medida?* (responsabilidades).
- No hay que confundir el respeto de todas las personas por las reglas de seguridad, con que todas las personas de la organización tendrán exactamente las mismas medidas de seguridad. Hay personas que se desplazan con el trabajo, hay personas que son más o menos visibles, que tienen diferentes perfiles, que manejan información sensible, hay grupos dentro de una organización que son susceptibles a violencias específicas de género como la agresión sexual, etc. Hay que reconocer el riesgo de todas las personas tomando en cuenta sus capacidades y vulnerabilidades específicas. Esto implica que sin minimizar el riesgo de ningún integrante, se debe reconocer que cada persona dentro de la organización tiene roles y niveles de riesgo diferentes. Por ejemplo puede haber reglas de convivencia dentro de la oficina o ciertas reglas específicas del tiempo libre que todos deberán aplicar, pero reglas de comunicación diferenciadas para aquellas personas que documentan casos o que acompañan directamente a víctimas de violaciones de DDHH.
- Recordar que como se vio en el taller 1, ser PDDH en México conlleva un nivel de riesgo que trasciende los espacios de trabajo. Cada persona tiene el derecho de decidir si está o no y hasta qué punto dispuesta a asumir su nivel de riesgo específico con los consiguientes cambios que eso implica en su vida profesional y privada. A pesar de lo anterior se debe recordar que las decisiones de cada persona en este sentido también pueden afectar la seguridad de otras personas (en el círculo cercano de la familia y la comunidad, PDDH de nuestra y de otras organizaciones así como a las víctimas de violaciones de DDHH con las que trabajamos). Por eso es necesario el compromiso de todas las personas en la organización y una conciencia colectiva sobre el riesgo al que están expuestas o cómo sus acciones u omisiones pueden influir en la seguridad de terceras personas.

Evaluación

La Rueda de la Seguridad

45min

Objetivos específicos:

- Explorar los diferentes componentes de la seguridad a través de la rueda de la seguridad para revisar el contenido del taller y recordar que la seguridad se debe implementar a nivel individual y organizacional.
- Promover una reflexión individual, sobre el manejo de la seguridad fuera y dentro del trabajo.
- Compartir las valoraciones sobre el manejo de la seguridad por parte de la organización.
- Identificar los puntos que quedan por fortalecer.

Materiales

- Plumones o colores
- Fotocopias y/o Papelógrafo o diapositivas con la *Rueda de la Seguridad (nivel individual) [Anexo T2.M4.S1]* y Rueda de la Seguridad (nivel organizativo) *[Anexo T2.M4.S1b]*

Consejos de facilitación:

- Para rellenar la rueda es bueno colorear el área de la rueda que se valora cumplir. *[Ver Anexo T2.M4.S1c]*
- Generalmente las ruedas rellenadas no son uniformes ni perfectamente redondas. Se puede hacer una analogía con las ruedas de un carro y mostrar que si no son uniformes el carro no puede rodar adecuadamente.
- Se recomienda guardar o fotografiar algunas ruedas o tomar notas de esta sesión en la relatoría para poder revisar con la organización si ha habido progresos en las reuniones posteriores de seguimiento.

Puntos clave:

- Para lograr una buena gestión de la seguridad tenemos que lograr cumplir a cabalidad con todos los componentes de la rueda de la seguridad tanto a nivel individual como organizativo: 1) Experiencia y cohesión adquiridas, 2) Formación, 3) Sensibilización y actitud, 4) Planificación, 5) Reparto de responsabilidades, 6) Respeto a las reglas y compromiso, 7) Análisis de los incidentes de seguridad y respuestas a los mismos y 8) Evaluación de la gestión.

Actividades

Actividad 1: La rueda de la Seguridad.

Presentación* *10 min

Explicar los 8 componentes de la rueda de seguridad.

Actividad 2: Llenar nuestra Rueda de la Seguridad a nivel individual.

Ejercicio individual* *10 min

Pedir que cada persona del grupo rellene una *Rueda de la Seguridad (nivel individual.) [Anexo T2.M4.S1]*

Pedir a algunas personas que se ofrezcan de voluntarias para compartir sus puntos fuertes y sus aspectos por fortalecer.

Actividad 3: Llenar nuestra Rueda de la Seguridad a nivel organizativo.

Ejercicio en grupos y presentación en plenaria* *25 min

Explicamos cómo se adaptan esos 8 radios de la rueda individual a la organización.

En grupos de 3 a 5 personas, las personas participantes rellenan una *Rueda de la Seguridad* (nivel organizativo) *[Anexo T2.M4.S1b]*

En plenaria se presentan las distintas ruedas que llenaron a nivel organizativo y se debate hasta llegar a un consenso sobre qué puntos quedan por fortalecer de forma prioritaria.

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 2.1. ***[RA5]***

Conclusión

Compromisos de seguimiento, evaluación y cierre

45min

Objetivos específicos:

- Revisar el contenido y los conocimientos adquiridos.
- Identificar tareas y responsabilidades para darle seguimiento al taller e implementar lo aprendido.
- Acordar el seguimiento.
- Evaluar el taller.

Materiales

- Papelógrafos
- Plumones
- *Metaplán*
- Hojas
- Papelógrafo con un punteo de los *Objetivos generales del taller y resultados esperados*
- Fotocopias con *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b]*
- Urna o caja de cartón con una ranura

Puntos clave:

- Enfatizar que si la organización no le destina los recursos (responsables, espacios, tiempo, etc.) al ámbito de seguridad y protección no se podrán llevar a cabo estrategias ni planes integrales.
- Abordar las expectativas de seguimiento y acordar si se necesita seguimiento, de qué tipo y cómo se podría dar.
- Revisar los acuerdos alcanzados y establecer los compromisos con las personas participantes en cuanto a las estrategias de seguridad y protección que serán desarrolladas a nivel organizativo
- Hay que revisar las tareas apuntadas e identificar plazos, espacios, recursos y responsables con un nivel aceptable de detalle y claridad.
- Cerciorarnos que no hayan quedado dudas sobre los aspectos fundamentales del taller.
- Evaluar el taller y la facilitación.

Actividades

Actividad 1: Revisión de "Actas y Acuerdos".

Discusión en plenaria* *15 min

Mientras las personas participantes van identificando las tareas pendientes, sondear las necesidades y voluntad para una asesoría ulterior (tener en cuenta las posibilidades de los talleres 3 y 4 del PASP).

Plantear al grupo las siguientes preguntas:

¿Cuándo podríamos realizar una entrevista de seguimiento?

¿Sienten que necesitan otras asesorías?

Actividad 2: Evaluación del cumplimiento de los objetivos del taller y expectativas Seguridad.

Trabajo en plenaria* *10 min

Retomar las expectativas de las personas participantes trabajadas al inicio del taller. En un papelógrafo se pegan las expectativas iniciales del grupo del lado izquierdo y a la derecha se hacen tres columnas para evaluar el cumplimiento de las mismas: 1) se cumplió 2) se cumplió parcialmente y 3) no se cumplió. Para cada una de las expectativas se pide que cada persona pegue un papelito adherible en la columna que considere.

Consejos de facilitación:

- Si el grupo no quiere llegar a acuerdos en términos del seguimiento no hay que forzarlo.
- Si se tiene más tiempo al final se puede optar por la evaluación en fotocopias que permite sistematizar mejor la información y retroalimentaciones. Algunos grupos prefieren rellenar las evaluaciones sin la persona que facilita presente. Se pueden poner cajitas a modo de urnas para que se depositen las evaluaciones individuales dobladas y de forma anónima.

En otro papelógrafo se tiene listo un punteo de los *Objetivos generales del taller y resultados esperados*. Enfrente de cada aspecto del punteo se hacen tres columnas al igual que para las expectativas y se pide que las personas peguen un papelito adherible en la columna que consideren. También pueden escribir sobre el papelito que peguen si gustan ahondar en algún objetivo específico si sienten que hubo aspectos del objetivo que se les dificultaron o que no se cumplieron a cabalidad.

La persona que facilita hace un recuento y revisa especialmente aquellos objetivos y expectativas que faltó cumplir a cabalidad. Se contrasta si dichos objetivos y expectativas estaba en las posibilidades planteadas por el taller o si se pueden abordar en talleres subsecuentes.

Actividad 3: Evaluación del taller y la facilitación.

Trabajo individual o plenaria 10 min

Escoger una de las siguientes formas de evaluación:

Plantear al grupo las siguientes preguntas:

a) En un papelógrafo se hacen dos columnas: 1) adecuado y 2) puede mejorar. Se reparten papelitos con los distintos criterios adaptados de las 2 tablas del *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b]*

Se les pide que cada quien tome 3 criterios de evaluación del taller y 3 criterios de evaluación de la facilitación (de preferencia aquellos donde tengan más que aportar o que les llamaron la atención para evaluar) y que escriban sobre los papelitos con sus opiniones, críticas y sugerencias. Luego se les pide que adhieran los papelitos en una de las dos columnas según corresponda a su punto de vista.

b) Se distribuyen individualmente fotocopias del *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b]*. Se pide a las personas que lo llenen y lo depositen doblado y de forma anónima en una caja o urna.

Actividad 4: Conclusión.

Discusión en plenaria 10 min

Se da una oportunidad para dudas y comentarios al grupo, se comentan las apreciaciones y se hace una última ronda de críticas y sugerencias.

Se recuerda la confidencialidad de lo abordado en los talleres.

Se dan los agradecimientos y se clarifica que se deja la posibilidad abierta para futuros talleres.

Taller 2

Anexos

Anexo T2 M2 S1

Elementos básicos de un Plan de Seguridad

PREVENCIÓN

Situaciones Específica o Actividades Extraordinarias

Protocolos

Por ejemplo:

- Protocolo para los viajes en zonas de alto riesgo,
- Protocolo para la protección de testigos y víctimas en riesgo,
- Protocolo para la organización de eventos públicos,
- Protocolo de salud mental y manejo de estrés previo a un careo o audiencia judicial clave, protocolos de prevención de violencia de género, etc.

EJECUCIÓN

Actividades Ordinarias/ Normas para El día al día

Políticas permanentes

Por ejemplo:

- Manejo de la información, sistema de comunicación,
- Control del acceso a espacios clave, seguridad de las sedes, selección del personal, política de seguridad digital, política de salud mental, transversalización de género en las políticas permanentes, etc.

REACCIÓN

Emergencias Incidentes

Planes de emergencia

Por ejemplo:

- Plan en caso de cateo & allanamiento
- Plan en caso de secuestro
- Plan en caso de detención
- Plan en caso de estrés acumulativo excesivo o estado de *shock*
- Plan en caso de robo de información sensible
- Plan en caso que una persona no se reporte, etc.

Anexo T2 M2 S1b

Formato de preparación del plan de seguridad

Amenaza prioritaria:

Trabajadas en el Taller 1, Módulo 2, Sesión 6		Trabajar en el Taller 2, Módulo 2, Sesión 1				Trabajar en el Taller 2, Módulo 3, Sesión 1		
		Plan de seguridad *Conjunto de pasos concretos y realistas que deben ser dados para reducir las vulnerabilidades y aumentar las capacidades de la organización ante una amenaza.*				**Responsabilidades** *Personas puntos focales o unidades dentro de la organización.*		
Capacidades	**Vulnerabilidades**	**Medidas de seguridad** *Acciones básicas y concretas de prevención, ejecución y reacción.*	**Componente del plan** *Identificar si es de prevención (protocolos), ejecución (políticas permanentes) o reacción (planes de emergencia o respuesta).*			**Implementación** *Nivel individual/institucional/entre orgs. ¿Quién debe seguir esta medida y en qué plazos?*	**Elaborar y Supervisar** *¿Quién asegurará la supervisión de estas medidas de seguridad?*	**Recursos necesarios** *Necesidades materiales, financieras, de capacitación y asesorías, etc.*
			Prevención	*Ejecución*	*Reacción*			

Anexo T2 M2 S2a

Acuerdos sobre el Plan de Emergencia

Acuerdos sobre el Plan de Emergencia

DEFINICIÓN DE UNA EMERGENCIA

o criterios para determinar cuándo se trata de una "emergencia":

Ejemplos de emergencias:

Contactos de emergencia

Contactos:

Redacción y actualización ¿Quién?	**Plazo de actualización**	**¿Quién debe tenerlos? ¿Cuándo?**

Marco general de actuación

Pasos:

Primer contacto	**Análisis / Documentación**	**Toma de decisiones**
Contactos con red de apoyo, autoridades, apoyo psicosocial, abogada/o, etc.	**Apoyo emocional**	**Evaluación de los resultados / Memoria**

Anexo T2 M2 S2b

Propuesta de criterios para contactos de emergencia

Primer Contacto dentro de la organización y persona de "Guardia" designada	Persona de la organización disponible fuera de las horas de oficina. Se encarga de responder ante cualquier situación de emergencia. Lleva consigo los contactos de emergencia y conoce muy bien el Plan General de Emergencia así como los diferentes planes de reacción para poder ofrecer una repuesta rápida.
Red de Apoyo	Contactos de confianza con quien se puede comunicar fuera de las horas de oficina. Organizaciones aliadas, familiares, personajes influyentes, difusión de denuncias, acciones urgentes, etc.
Autoridades	Funcionario/a público/a con quien se puede comunicar fuera de las horas de oficina para obtener una asistencia apropiada
Servicio públicos	Servicio médicos de emergencia, bomberos, policía local, taxi de confianza, etc.
Asesor legal	Con quien se puede comunicar en cualquier momento para asesorías puntuales o iniciar procedimientos legales.
Atención psicológica	Personal especializado para eventos traumáticos, situaciones que generen *shock* o que requieren especial atención desde la perspectiva psicosocial, tanto para las personas directamente afectadas por la emergencia como para sus colegas y círculo cercano afectados/as.

Anexo T2 M2 S2c

Propuesta de Marco general de actuación en caso de emergencia

Primer Contacto

Comunicación de la emergencia dentro de la organización. ¿Cómo y a quiénes se comunica la emergencia?

Documentación y Análisis

En el "primer contacto" se nombra la emergencia, las personas afectadas, el lugar, etc. pero muchas veces no se puede dar muchos detalles por lo que puede ser necesario documentar mejor la situación antes de seguir con la activación (pe. antes de contactar a las autoridades, de avisar a medios de comunicación, etc.) ¿Procedimiento para la documentación y el análisis?

Coordinación / toma de decisión

Las responsabilidades en cuanto a la toma de decisión (tipo de reacción, contacto con autoridades, medios, red de apoyo, procedimiento legal o no) deben estar definidas de antemano de manera clara para todas y todos. ¿Quiénes coordinarían o tomarían las decisiones en caso de emergencia?

Apoyo emocional

Las personas directamente afectadas por la emergencia, sus colegas y círculo cercano afectados/as pueden requerir asesoría o intervención de personal especializada. ¿A quién se puede recurrir para el apoyo psicológico de emergencia? ¿Quiénes podrían abordar el impacto psicosocial en la organización para gestionar los efectos de una emergencia? ¿Quién se comunica con dicho personal?

Contacto con la Red de Apoyo

¿A cuáles organizaciones aliadas / personas de confianza se tiene que avisar?
¿Con qué objetivo? ¿Quién se comunica con ellos?

Contacto con las autoridades

¿Queremos contactar con autoridades? Si decidimos contactar: ¿Cuáles funcionarios públicos se tiene que avisar? ¿Con qué objetivo? ¿Quién se comunica con autoridades?

Contacto con las autoridades

¿Queremos hacer pública la emergencia? ¿El hacer pública la información podría revictimizar a las personas o comunidades afectadas? Si decidimos avisar: ¿A quiénes avisamos? ¿Con qué objetivo? ¿Quién se comunica con medios de comunicación?

Memoria de la emergencia

Puede ser útil documentar o que sucede partir del momento inicial en el cual se identifica la emergencia. (Por ejemplo autoridades contactadas y sus respuestas, otros incidentes de seguridad, actuación de la red de apoyo, etc.) ¿Quién llevaría la sistematización de la respuesta a la emergencia y analizaría lo sucedido para aprender de ella?

Anexo T2 M2 S2d

Definición de contactos de emergencia

Primer Contacto	¿A quién se tiene que avisar primero dentro de la organización? ¿Con quién se tiene que comunicar si esta persona no está disponible? ¿Hay siempre una persona "de guardia"?
Red de Apoyo	En caso de emergencia ¿hay que avisar a otras organizaciones / personas de confianza? Fuera del horario de oficina, ¿se puede contactar con la gente de las organizaciones que forman parte de la Red de Apoyo? ¿Tenemos los números de unos familiares de los integrantes? ¿se tienen que avisar?
Autoridades	¿Hay autoridades locales, estatales o federales que conocen del trabajo de la organización y podrían generar un coste político para reducir las amenazas y/o que se deberían avisar para responsabilizarles de la seguridad de los integrantes? ¿Quién de la organización se puede comunicar con estas autoridades? ¿Se necesita de una decisión dentro de la organización para contactar a estas autoridades? ¿Tenemos los números personales de estas autoridades para comunicarse con ellos en cualquier momento?
Apoyo legal	¿La organización tiene un abogado? ¿Está disponible en cualquier momento para todas las personas de la Organización?
Apoyo emocional	A quién se puede recurrir para el apoyo psicológico de emergencia? ¿Quiénes podrían abordar el impacto psicosocial en la organización para gestionar los efectos de una emergencia?
Apoyo Mediático	¿Qué medios de comunicación periodistas o redes mediáticas serían útiles para difundir información que nos ayude en caso de una emergencia?
Servicios públicos	Policía, Ambulancia, Bomberos. Taxi de confianza. Otros.

Pendientes (contactos/ acuerdos que hacen falta)	**Responsabilidades** Redacción y actualización: ¿Quién y cuándo? ¿Quién debe tener esta lista consigo y cuándo?

Anexo T2 M2 S2e

Definición de los pasos a seguir en caso de emergencia

Primer Contacto	¿A quién se tiene que avisar primero dentro de la organización? ¿Hay siempre una persona "de guardia"? ¿Con quién se tiene que comunicar si ésta persona no está disponible? ¿Es tarea de la gente en situación de emergencia contactarse con esta persona o tarea de la "guardia"? ¿La persona que sirve de "primer contacto" debe avisar a los demás miembros de la Organización? Quién. ¿Es necesaria una reunión de emergencia o solo un contacto telefónico entre los miembros?
Análisis y documentación	¿Quién se encarga de documentar y analizar el incidente? ¿A quién y cómo se comunicará esta información? ¿Todos los integrantes saben cómo documentar y analizar una situación de emergencia? ¿Es necesario crear un formato o revisar en conjunto los pasos de análisis?
Coordinación / toma de decisión	Dentro de la organización ¿quién toma la decisión sobre la respuesta a esta emergencia? ¿Hay un proceso de consulta? ¿Quién decide si se deben iniciar procedimientos legales?
Apoyo emocional	¿Quién se queda en contacto con la/s persona/s afectada/s para atender sus necesidades? ¿Quiénes podrían abordar el impacto psicosocial para gestionar los efectos de una emergencia a nivel individual y organizativo (estrés, miedo, ansiedad, *shock*, etc.)?
Memoria evaluación	¿Quién se encarga de documentar todo lo que sucede partir del momento inicial en el cual se identifica la emergencia? pe. Autoridades contactadas y sus respuestas, otros incidentes de seguridad, actuación de la red de apoyo, etc. ¿Existen espacios para evaluar en conjunto la reacción y sus resultados?
Red de Apoyo	En caso de emergencia ¿hay que avisar a otras organizaciones / personas de confianza / familiares? ¿Quién y con cuál objetivo? ¿Quién toma la decisión de contactarlos? ¿Quién se comunica con ellos?
Autoridades	¿Hay autoridades locales, estatales o federales que conocen del trabajo de la organización y podrían generar un coste político para reducir las amenazas y/o a quienes se deberían avisar para responsabilizarles de la seguridad de los integrantes? ¿Se necesita de una decisión dentro de la organización para contactar a estas autoridades? ¿Quién puede tomar semejante decisión? ¿Quién se comunica con ellos?
Prensa	¿Se contacta automáticamente a la prensa en caso de emergencia o más bien se necesita una decisión dentro de la organización antes de contactarla? ¿Quién decide el mensaje? ¿Quién se comunica con ellos?

Pendientes:
(contactos/ acuerdos que hacen falta / otras tareas).

Responsabilidades:
Redactar el Plan general de Emergencia.
(Poner por escritos los pasos y darlos a conocer a todos los integrantes y definir quién y cuándo).

Anexo T2 M2 S2f

Formato para analizar y documentar una emergencia

1) Establecer los hechos y analizarlos

Resumen de lo que pasó (o está pasando)	**Cuándo.** Fecha. Hora	**Dónde**	**Actores involucrados**	
			Víctima	Agresores
Fuente de información		**Fiabilidad de la información**		

2) Análisis y reacción de las contra partes locales implicadas

¿Cuál es su análisis e interpretación de los hechos?

¿Cuál va a ser su reacción y estrategia frente a lo sucedido?

3) Análisis de los acontecimientos: por qué ha sucedido esto

¿Por qué sucedieron los hechos?
¿Por qué a ésta persona/comunidad/ONG?
¿Por qué en ese momento?
¿Por qué de esta manera?

4) Tipo de reacción

Inmediata o posterior ¿Cuándo?	**Autónoma o implicando otros actores** ¿Quién?	**Acción legal o se decidirá no usar las vías judiciales** ¿Cuál?	**Denuncia pública o se mantendrá el evento confidencial** ¿Cómo?

5) Definir los objetivos de la reacción y las actuaciones concretas

Acción	Objetivo	Responsable	Plazo

6) Documentar y evaluar la reacción

Acción	Resultado	Seguimiento

Anexo T2 M3 S1

Niveles de Implementación de la política de seguridad

Individual (cada integrante sigue el plan de seguridad).

Institucional (la organización en conjunto sigue el plan).

Inter-organizativo (cooperación con orgs. aliadas para la seguridad).

Compartir y analizar los IdS y las medidas de seguridad.

Analizar Identificar nuevas amenazas y ajustar las medidas de seguridad.

Supervisar la implementación del plan de seguridad.

Evaluar la efectividad del plan.

Asignar responsabilidades para el diagnóstico, la planificación, la implementación y la evaluación.

Asignar responsabilidades para puntos focales de cooperación con otras organizaciones, contacto con autoridades, etc.

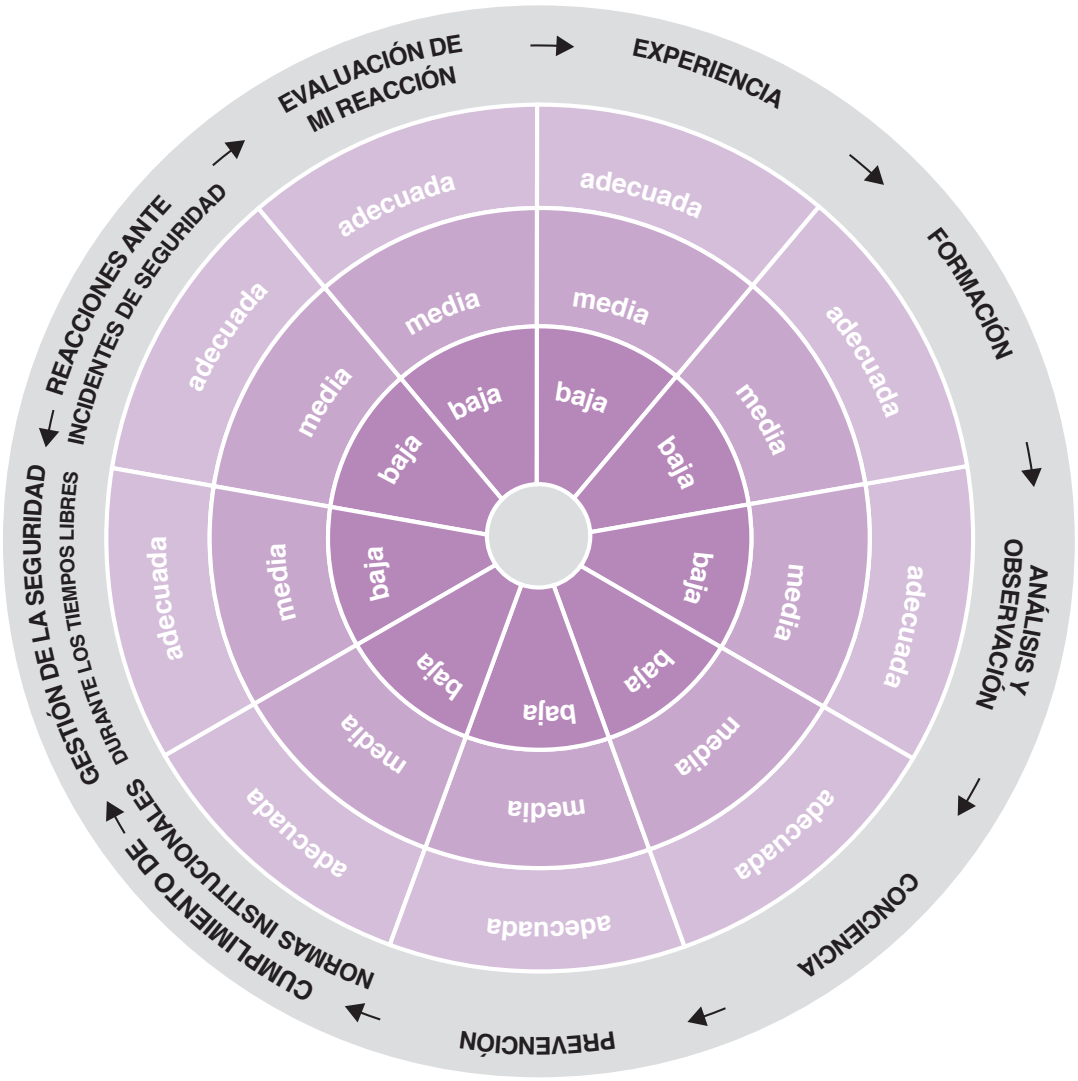
Recursos de capacitación y asesorías necesarias.

Recursos laborales y tiempos para la planificación y evaluación.

Recursos materiales como inversión en insumos y destinación de recursos económicos (fondos de emergencia, seguridad de las sedes, etc.).

Anexo T2 M4 S1

La rueda de la seguridad (nivel individual)*



EXPERIENCIA
¿Tengo experiencia previa en manejo de seguridad?

FORMACIÓN
¿Recibí una buena capacitación?
¿Tengo acceso a material, lecturas, etc.?

ANÁLISIS Y OBSERVACIÓN
¿Estoy atento a mi entorno?
¿Identifico los incidentes?
¿Tomo tiempo para analizar elcontexto, los riesgos, etc.?

CONCIENCIA
¿Soy consciente de los riesgos y de mi necesidad de protección?

PREVENCIÓN
Cuando planeo actividades, viajes, etc. ¿Integro medidas de prevención?

CUMPLIMIENTO DE NORMAS INSTITUCIONALES
¿Entiendo y cumplo con todas las normas de mi organización?

GESTIÓN DE LA SEGURIDAD DURANTE LOS TIEMPOS LIBRES
¿Platico de los incidentes con mi entorno social, busco conocer su interpretación, comparto mis propuestas de reacción? ¿Tengo la capacidad de involucrar a mi red social en la reacción ante estos incidentes?

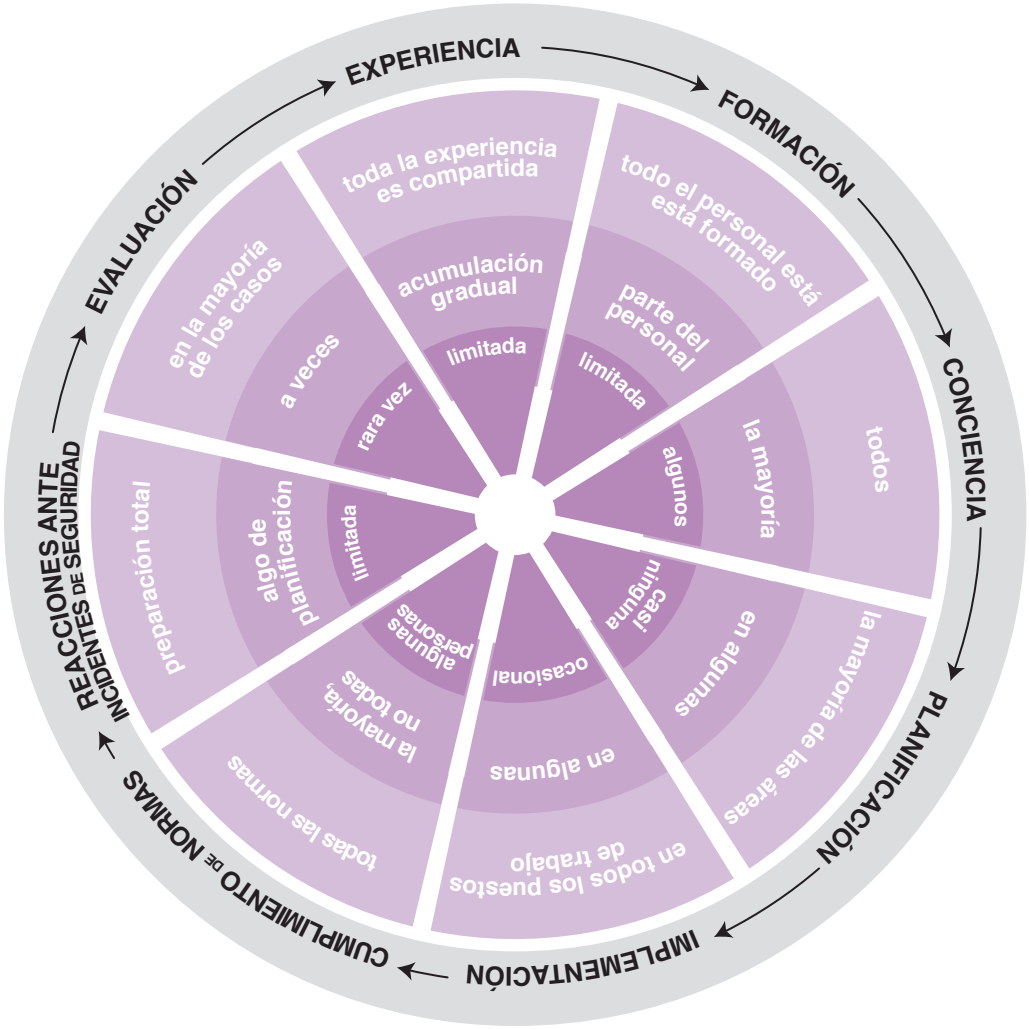
REACCIONES ANTE INCIDENTES DE SEGURIDAD
¿Se contacta automáticamente a la prensa en caso de emergencia o más bien se necesita una decisión dentro de la organización antes de contactarla? ¿Quién decide el mensaje? ¿Quién se comunica con ellos?

EVALUACIÓN DE MI REACCIÓN
Después de una situación de riesgo, una emergencia o un incidente, ¿Tomo el tiempo de valorar mi reacción y compartir mi valoración con los demás? ¿Evalúo también la reacción de mi familia u otros conocidos involucrados?

* Adaptada de Peace Brigades International (Oficina Europea) & Frontlinde Defenders, *Manual de Protección para los Defensores de Derechos Humanos*, cap 7.

Anexo T2 M3 S1b

La rueda de la seguridad (nivel organizativo)*



EXPERIENCIA
¿Tengo experiencia previa en manejo de seguridad?

FORMACIÓN
¿Recibí una buena capacitación?
¿Tengo acceso a material, lecturas, etc.?

CONCIENCIA
¿Estoy atento a mi entorno?
¿Identifico los incidentes?
¿Tomo tiempo para analizar elcontexto, los riesgos, etc.?

PLANIFICACIÓN
¿Soy consciente de los riesgos y de mi necesidad de protección (estrés, miedo, ansiedad, *shock*, etc.)?

IMPLEMENTACIÓN
Cuando planeo actividades, viajes, etc. ¿Integro medidas de prevención?

CUMPLIMIENTO DE NORMAS
¿Entiendo y cumplo con todas las normas de mi organización?

REACCIONES ANTE INCIDENTES DE SEGURIDAD
¿Platico de los incidentes con mi entorno social, busco conocer su interpretación, comparto mis propuestas de reacción? ¿Tengo la capacidad de involucrar a mi red social en la reacción ante estos incidentes?

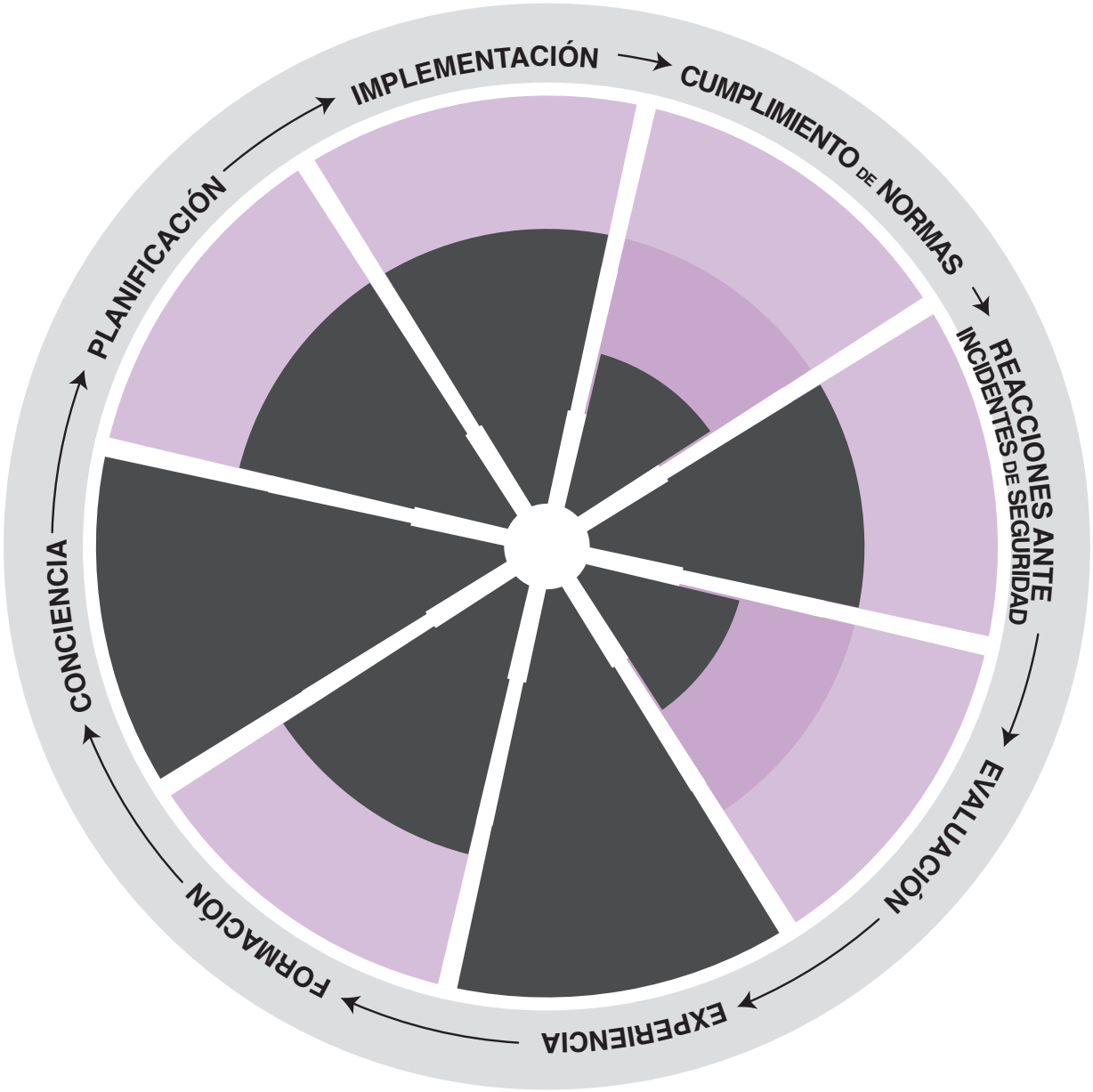
EVALUACIÓN
¿Se contacta automáticamente a la prensa en caso de emergencia o más bien se necesita una decisión dentro de la organización antes de contactarla? ¿Quién decide el mensaje? ¿Quién se comunica con ellos?

---

*Adaptada de Peace Brigades International (Oficina Europea) & Frontlinde Defenders, *Manual de Protección para los Defensores de Derechos Humanos*, cap 7.

Anexo T2 M4 S1c

La rueda de la seguridad (ejemplo de rueda rellenada después de las actividades)



Taller 3
Manejo de Información Sensible

El taller sobre Manejo de Información Sensible se enfoca en los riesgos específicos a los sistemas de comunicaciones y de almacenamiento de la información. El taller condensa y adapta las herramientas y los procesos desarrollados en los talleres 1 y 2 en relación con la problemática particular del manejo y comunicación de información de forma segura. Este taller impulsa la construcción de una política de comunicación y manejo de información adaptada al contexto de las PDDH. Lo anterior se hace a partir de un mapeo de la información y un análisis del riesgo específico del manejo de la información en la organización. El taller plantea impulsar una visión amplia de la seguridad de la información desde la seguridad de las sedes donde se almacena la información hasta las comunicaciones entre los integrantes de la organización.

Objetivos generales del taller y resultados esperados:

- Ofrecer una metodología para realizar un diagnóstico de la seguridad de la información de la organización
- Desarrollar una visión amplia de la seguridad de la información en el ámbito de las sedes, almacenamiento y las comunicaciones de la organización.
- Impulsar la elaboración de una política sobre comunicación y manejo de información sensible, considerando tanto la seguridad física como la protección de la información.

Lo que el taller NO pretende:

- Restringir todos los contenidos a un taller de seguridad digital. El taller contempla el Módulo Opcional B en Seguridad Digital pero abarca más que este tema.
- Ofrecer apoyo técnico profesional o un laboratorio de prácticas de manejo de información.
- Instalar programas o dispositivos de seguridad en las sedes y/o computadoras de las organizaciones.

Duración total

***8 horas** (sin contar pausas ni módulos opcionales adicionales A y B).*

Calendarización

Considerar dar el taller en un día y medio. Contar al menos con 2 horas de pausa en un día repartidas a lo largo del día. Si se decide incluir los módulos adicionales se debe añadir mínimamente un día adicional al taller por cada módulo incluido.

Plan General del Taller:

Módulo 1: Bienvenida e introducción

Sesión 1 Presentación, expectativas, revisión de agenda y acuerdos de convivencia

Módulo 2: Información sensible, amenazas latentes y tecnología

Sesión 1 Seguridad de la información
Sesión 2 Análisis de contexto
Sesión 3 Información sensible
Sesión 4 Análisis de actores e IdS
Sesión 5 Amenazas prioritarias y análisis de riesgo

Módulo 3: Política sobre Manejo de Información sensible

Sesión 1 Preparación de una política de manejo de la información sensible

Módulo 4: Cierre y Evaluación

Sesión 1 Seguimiento, compromisos y cierre

Módulo Opcional A: Buenas prácticas en el manejo de información

Sesión 1 Los pasos de la información
Sesión 2 Seguridad física de la información
Sesión 3 Política de respaldo
Sesión 4 Destrucción de la información sensible
Sesión 5 Control de las comunicaciones
Sesión 6 Reuniones seguras

Módulo Opcional B: Seguridad Digital (*security in a box*)

Sesión 1 Proteger tu computadora de software malicioso y piratas informáticos
Sesión 2 Proteger tu información de amenazas físicas
Sesión 3 Crear y mantener contraseñas seguras
Sesión 4 Proteger los archivos sensibles en tu computadora
Sesión 5 Recuperar información perdida
Sesión 6 Destruir información sensible
Sesión 7 Mantener privada tu comunicación en Internet
Sesión 8 Mantenerse en el anonimato y evadir la censura en Internet
Sesión 9 Protegerte a ti mismo y a tus datos cuando utilizas sitios de redes sociales
Sesión 10 Utilizar los teléfonos móviles de la manera más segura posible
Sesión 11 Utilizar los teléfonos inteligentes de la manera más segura posible

Material y recursos:

- Hojas blancas
- Plumones
- Papelógrafos
- Una manta pegajosa o una superficie amplia y visible para todo el grupo que pueda servir de *Metaplán*
- Cartulinas de colores
- Papelitos adheribles de colores
- Gafetes o etiquetas adhesivas
- Pizarrón
- Hilos de colores
- Papel *foamy* de colores
- Chinches
- Cinta adhesiva
- *Anexos Taller 3*
- *[Anexo T1.M1.S1] Método de gestión de seguridad*
- *[Anexo T1.M1.S2] Tipología de las amenazas latentes para personas defensoras de los DDHH*
- *[Anexo T1.M2.S4a] Definición y análisis básico de los Incidentes de Seguridad*
- *[Anexo T1.M2.S4b] Pasos a seguir para analizar un IdS*
- *[Anexo T1.M2.S4bis a] Análisis de Amenazas Declaradas*
- *[Anexo T1.M2.S4bis b] Pasos para analizar Amenazas Declaradas*
- *[Anexo T1.M2.S6c] Pensar medidas de seguridad para amenazas prioritarias*
- *Anexo T1.M2.S4c] Bitácora de registro de IdS* trabajada y llenada por las personas participantes durante el taller 1
- Fotocopias para llenar del *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b]*
- Computadora y proyector u otro equipo de proyección audiovisual (opcional)
- Equipo de cómputo con conexión a internet y teléfonos móviles para complementar de forma práctica las sesiones (recomendable en caso que se decida impartir el Módulo Opcional B: Seguridad Digital).

Consejos generales para este taller:

Este taller puede adaptarse de acuerdo al nivel de conocimiento de las personas participantes y el tipo de organización que está recibiendo el taller. Algunos contenidos tienen más o menos sentido para las organizaciones dependiendo de cómo manejan su información. Es importante tener claro la forma en que manejan su información antes de empezar el taller para adaptarlo a sus necesidades específicas: *¿Tienen oficina? ¿Comparten la información sobre sus estrategias en asambleas comunitarias? ¿Usan computadoras? ¿Cómo se comunican? ¿Documentan violaciones a los DDHH? ¿Acompañan a víctimas? ¿Producen información física? ¿Consideran que son vigilados o han tenido IdS relacionados con vigilancia?* etc.

Es fundamental que quede claro que la seguridad de la información forma parte de un enfoque integral de la seguridad de la organización. Las amenazas relativas a la seguridad de la información representan una parte de las amenazas latentes que se ven en el Taller 1.

En todo el proceso, es importante usar ejemplos prácticos y sencillos de entender para las personas y tener cuidado para que el grupo no se pierda en discusiones excesivamente técnicas, sobre todo en lo relativo a tecnología.

Evitar culpabilizar a la gente por sus prácticas de uso de tecnologías de la información y la comunicación. También se debe evitar crear fobias al uso de las herramientas y dispositivos que de por sí ya utilizan para su trabajo. Por ejemplo si abordamos los riesgos asociados al uso de teléfonos celulares o la comunicación por correo electrónico, intentar proponer opciones para reforzar la seguridad a través de buenas prácticas adaptadas a su contexto de riesgo. Hacer un balance en que este tipo de herramientas son útiles para nuestro trabajo por lo que es importante saber los riesgos asociados a ciertas formas de uso de las mismas. De esta manera se evita dar la sensación de fatalismo haciendo ver como si fuera un tema excesivamente complejo e imposible de resolver. Incitar a las PDDH a abandonar completamente las herramientas que les funcionan y utilizan dejaría a las PDDH aisladas o incomunicadas, lo que incrementaría sus vulnerabilidades.

Consejos generales para este taller (continuación):

Tener en cuenta durante todo el taller que las organizaciones deben pensar en los diferentes momentos en los cuales la información puede estar en riesgo; al recibir la información (p.e. reuniones, testimonios), al almacenar y procesar la información (p.e. laptops, archiveros), al trasmitir y compartir la información (p.e. reuniones, correos electrónicos, llamadas) y al difundir la información públicamente (p.e. acciones urgentes, informes a donantes, prensa, etc.).

M+ Información sobre los Módulos opcionales adicionales:

Módulo Opcional A: Buenas prácticas en el manejo de información

Este módulo opcional adicional aporta buenas prácticas para retroalimentar la política sobre comunicación y manejo de información de la organización.

El módulo se puede realizar completo o adaptado a las necesidades relativas al manejo de información sin entrar en detalle sobre Seguridad Digital. Si se realiza completo o en su mayoría de sesiones se debe dar después de pasar por el Taller 3 y valorar el nivel de riesgo específico de la organización. Otra opción es incluir solo algunas de sus sesiones en el Taller 3 si durante el sondeo se detectan necesidades específicas.

Este módulo no busca imponer medidas a las organizaciones sino dar ejemplos que se puedan adaptar en función del diagnóstico de seguridad y análisis del riesgo particular de las organizaciones. Por ello las medidas deben ser realistas y apegadas al contexto de la organización. Medidas de protección tomadas sin basarse en un análisis del riesgo pueden crear una falsa sensación de protección y poner a las PDDH en mayor vulnerabilidad. Las buenas prácticas propuestas en el Módulo no son una "solución automática" ni deben menguar la creatividad de la organización para buscar formas alternativas e innovadoras de protegerse.

Es importante que los resultados del debate y ejercicios de este Módulo adicional no se pierdan en las discusiones y se acuerde al final una forma de integrarlos en el *plan de seguridad* de la organización si se valora necesario por parte de las PDDH.

Este módulo debe ser revisado constantemente considerando los nuevos cambios en el contexto de trabajo de las PDDH.

Módulo Opcional B: Seguridad Digital (basado en *security in a box*)

Este módulo opcional adicional brinda recursos para la seguridad digital de PDDH. A diferencia de los demás módulos de los 4 talleres del PASP, sus contenidos no han sido diseñados por PBI-México. Ante las necesidades de las PDDH en materia de seguridad digital, el PASP ha incluido la referencia a la Caja de herramientas de Seguridad protegiendo tu privacidad digital <*https://securityinabox.org/es*> desarrolladas por las organizaciones expertas *Tactical Technology Collective y Front Line Defenders.*

La *Caja de herramientas* se compone de una "Guía Paso a Paso" de 11 sesiones que se complementan con "Guías prácticas" para aprender a utilizar los programas sugeridos. A partir de las 11 sesiones la persona que facilita puede plantear distintas actividades y asesorías prácticas según el perfil y requerimientos de las PDDH participantes. PBI recomienda utilizar la *Caja de Herramientas* para complementar con asesorías prácticas los módulos 1-4 y Opcional A del Taller 3 con base en las necesidades de soluciones digitales específicas de las personas defensoras.

Este módulo debe ser revisado constantemente considerando los nuevos cambios en el contexto de trabajo de las PDDH y las actualizaciones sobre programas y amenazas tecnológicas.

Bienvenida e introducción

Presentación, expectativas, revisión de agenda y acuerdos de convivencia

50min

Objetivos específicos:

- Conocerse entre participantes y facilitadores.
- Recapitular el PASP, sus criterios y marco conceptual básico.
- Conocer qué esperan las personas participantes del taller y consensuar los objetivos del mismo.
- Clarificar el rol de la persona que facilita, sus posibilidades y limitaciones.
- Aclarar la metodología que se usará durante el taller.
- Sondear el conocimiento previo del grupo y ajustar taller si es necesario.
- Revisar la agenda con base en los puntos anteriores. Presentar las diferentes partes del taller y acordar tiempos y pausas.
- Acordar las normas de convivencia que servirán de base para generar un espacio seguro desde la perspectiva psicosocial y garantizar condiciones de equidad durante todas las sesiones subsecuentes.
- Distribuir materiales complementarios y roles de apoyo para la facilitación.

Puntos clave:

- Generar una apertura del taller que facilite la confianza y conocimiento de todas las personas participantes.
- Subrayar que la persona que facilita está para catalizar la participación y que se está construyendo un espacio conjunto de conocimiento. Por ello la participación de todas las personas es crucial para el proceso.
- Recapitular cómo se intersectan las tres dimensiones del análisis del PASP para una visión integral de la seguridad.
- Revisar brevemente las definiciones básicas de seguridad y protección.
- Abordar ideas más allá de lo convencional respecto a la seguridad de la información (normalmente surgen cuestiones materiales de seguridad o ideas asociadas a redes sociales). Poner de relieve también por ejemplo de la responsabilidad de manejar datos sensibles de víctimas de violaciones de DH, etc.)
- Revisar los pasos del método de gestión de la seguridad usados por PBI. Diagnóstico > Planificación > Implementación > Evaluación.
- Consensuar normas de convivencia que promuevan las condiciones necesarias de respeto, diálogo e inclusión durante todo el taller. La persona que facilita debe estar segura que toda la gente se siente cómoda con los acuerdos alcanzados.

Actividades

Actividad 1. Ronda de presentación y expectativas del grupo.

Dinámica de presentación y discusión en plenaria ***10 min***

Abrir con una ronda de presentación. Independientemente de la dinámica de presentación utilizada es importante que las personas participantes comuniquen si ya han recibido talleres previos relacionados con este tema, y qué esperan del taller.

Se pueden apuntar motivaciones y expectativas en papelitos adheribles de colores para agruparlos en un lugar visible durante todo el taller. Estas expectativas se retomaran más adelante y al final del taller se revisarán para evaluar qué hemos cumplido y qué no.

Materiales

- Pizarrón
- Papelógrafo
- Plumones
- Fotocopias con objetivos y agenda del taller
- Papelógrafo o diapositivas con los *Componentes analíticos necesarios para un esquema integral de seguridad y protección [Gráfico 1e, cap. 1]* y con el gráfico del *Método de gestión de seguridad [Anexo T1.M1.S1]*
- Papelitos adheribles de colores
- Gafetes o etiquetas adhesivas
- Computadora y proyector (opcional solo en caso que la actividad 3 no se lleve a cabo con papelógrafo o pizarrón)

Recursos adicionales y lecturas de apoyo:

Para distintas dinámicas de presentación e integración grupal y distención.

- BERISTAIN & SORIANO, *La Alternativa del Juego I. Juegos y Dinámicas de Educación para la Paz*. *[RA1]*

Para comenzar adecuadamente con la construcción de un espacio seguro en un trabajo grupal sobre seguridad con PDDH.

- BARRY & NANIAR. *Integrated Security the Manual*, cap. 1.2, 1.3 y 3.4. *[RA4]*

Para entender los conceptos de seguridad y protección.

- Capítulo 1 de esta Guía.

Para entender el PASP, sus criterios y marco conceptual básico.

- Capítulo 2 de esta Guía

Actividad 2. Lo que entendemos por "Seguridad de la información".

Lluvia de ideas y discusión en plenaria a partir de preguntas detonadoras ***10 min***

Plantear al grupo las siguientes preguntas:

> *¿Al mencionar "seguridad de la información", cuáles son las palabras o ideas que nos vienen en mente?*
>
> *¿De qué se debería hablar dentro de una formación sobre seguridad de la información?*

Apuntar las palabras y conceptos usados por las PDDH en un papelógrafo plenamente visible. Usar y hacer referencia a las palabras y conceptos retomándolos durante las fases subsecuentes del taller.

Actividad 3. Recapitulación del PASP.

Presentación oral con apoyo de elementos visuales (se puede usar papelógrafo, pizarrón o diapositivas en power point) ***10 min***

Presentar de forma concisa en qué consiste el PASP, sus criterios y metodología. Enmarcar este taller dentro del PASP y las estrategias de seguridad y protección más amplias. Bosquejar visualmente las tres dimensiones conceptuales que sustentan el programa de asesorías y los conceptos de seguridad y protección. *[ver definiciones conceptuales y gráficas de cap. 1 sección 1 y gráficos sobre estructura del PASP en cap. 2 sección 3 y 4 de esta guía]*

Explicar que el Taller 3 se basa en el diagnóstico del método de gestión de la seguridad usado por PBI y trabajado durante el Taller 1. *[Anexo T1.M1.S1]*

Actividad 4. Revisión de expectativas y adaptación de agenda y contenidos del taller en caso de ser necesario.

Discusión en plenaria ***10 min***

Presentar los objetivos y contenidos del taller consensuados previamente con la organización. Revisar junto con el grupo las expectativas expresadas en relación con los objetivos y la metodología del taller presentadas.

A partir de una perspectiva realista de las limitaciones en términos de tiempo, objetivos y contenidos del taller así como de las expectativas previamente expresadas por las PDDH, explicar lo que podemos hacer en este taller y lo que no es posible o que puede ser abordado sólo en talleres posteriores.

Realizar ajustes si es necesario.

Pegar la agenda general del taller consensuada en un papelógrafo a la vista de todas las personas participantes.

Actividad 5. Acuerdos de convivencia, distribución de material complementario y roles de apoyo.

Discusión en plenaria y/o dinámica participativa ***10 min***

Acordar en conjunto las normas de convivencia: cómo pedir la palabra, cómo expresar con respeto nuestros desacuerdos, cómo garantizar condiciones de igualdad, confidencialidad de los aspectos tratados durante el taller, uso

de celulares, computadoras y cámaras, entradas y salidas de participantes, puntualidad, etc. *[ver apartado sobre espacios con equidad y espacios seguros desde la perspectiva psicosocial en el apartado 3.2 y recursos de apoyo RA4]* Se puede realizar la "Dinámica de la Estrella" usada previamente u otra distinta.

Después de las normas de convivencia se puede entregar material complementario (por ejemplo. un cuaderno del participante). Pedimos que no se lea inmediatamente ya que este se trabajará a lo largo del taller.

Dejar claro el rol de la persona que facilita y sus posibles limitaciones.

Distribuir roles de apoyo a la facilitación, preguntar a las personas participantes quién quiere ser voluntario/a para tomar actas y apuntar los consensos, para anotar otros pendientes y tareas que surjan durante el taller.

Consejos de facilitación:

- Se pueden utilizar distintas dinámicas de presentación para "despertar" o espabilar al grupo *[ver RA1]*. Si el grupo es numeroso y no se conocían previamente, también se pueden usar gafetes o adhesivos con el nombre de las personas para facilitar dirigirse a las personas por su nombre de pila y recordar los nombres.
- Se puede también pedir a las personas que además de las palabras y conceptos realicen un dibujo sobre su idea de seguridad de la información y luego todo el grupo dice una lluvia de ideas sobre los dibujos de sus demás compañeros.
- En las partes con mayor carga conceptual se recomienda aprovechar al máximo los recursos gráficos propuestos.
- Con base en la actividad 1 y 2, puede ser necesario bajar las expectativas o ajustar la agenda para dedicar más tiempo a algunos temas, quitar otros etc. ¡Hay que ser flexibles y receptivos a la hora de tratar las expectativas del taller e ideas sobre seguridad y protección!
- Se puede consensuar un espacio para dejar los aparatos electrónicos como celulares y computadoras durante el taller (por ejemplo en la esquina de la sala o en una bolsa resguardada). Se puede consensuar cómo retribuirá al grupo alguien que llegue tarde a las sesiones o que pase por alto algún acuerdo de convivencia (por ejemplo puede traer dulces para todas las personas la siguiente sesión, o relevar al relator de acuerdos).
- ¡Atención con el control del tiempo! Este módulo es susceptible a extenderse demasiado.

Información sensible, amenazas latentes y tecnología.

Seguridad de la Información

20min

Objetivos específicos:

- Definir qué es Seguridad de la Información.
- Revisar los conceptos mencionados en la sesión anterior.
- Dar a conocer los componentes del Diagnóstico específico a la Seguridad de la Información.

Materiales

- Papelógrafo
- Plumones
- Papelógrafo o diapositivas con el *Método de gestión de la Seguridad [Anexo T1.M1.S1], Criterios de Seguridad de la Información [Anexo T3.M2.S1]* y *Los pasos del Diagnóstico para la Seguridad de la Información [Anexo T3.M2.S1b]*

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.11. *[RA5]*
- FLORES HINE, *¡Pongámonos las pilas! Reflexiones y acciones concretas para asegurar la información en nuestras organizaciones sociales. [RA10]*

Puntos clave:

- La seguridad de la información es el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. Al mismo tiempo se busca mantener la confidencialidad, disponibilidad, integridad y autenticidad de la misma. El objetivo de esta esfera de la seguridad es la reducción o eliminación de los riesgos asociados al manejo de información:

  a) *Confidencialidad*: solo tiene acceso a la información el personal autorizado para acceder a la misma.

  b) *Disponibilidad*: la información está disponible en cualquier momento para las personas autorizadas.

  c) *Integridad*: la información no puede ser alterada por parte de terceros o personas no autorizadas.

  d) *Autenticidad*: la fuente de información es legítima y de confianza.

- Los pasos del Diagnóstico para la Seguridad de la Información:

  a) *Análisis de Contexto*: analizar el marco legal, la coyuntura e identificar las amenazas latentes.

  b) *Mapa de la información*: identificar la información sensible de la organización: ¿Dónde está? ¿Quién tiene acceso a ella?

  c) *Análisis de actores:* identificar los actores que tienen interés en la información y evaluar sus capacidades para robarla, destruirla, realizar vigilancia, etc.

  d) *Análisis de Incidentes de Seguridad*: análisis de los IdS relacionados a la protección de la información.

  e) *Análisis de Capacidades y Vulnerabilidades*: Identificar nuestras capacidades y vulnerabilidades relacionadas con la seguridad de la información. Priorizar las áreas que deben ser fortalecidas y potenciar las capacidades.

  f) *Análisis del riesgo*: evaluar la probabilidad de que ocurra alguna amenaza ligada y determinar el nivel de daño que podría producir.

Actividades

Actividad 1. Conceptos básicos de Seguridad de la Información.

Presentación 10 min

Retomar los conceptos de la sesión anterior mencionados por las PDDH y detallar los *Criterios de Seguridad de la Información [Anexo T3.M2.S1]:*

a) Confidencialidad

b) Disponibilidad

c) Integridad

d) Autenticidad

Actividad 2. Gestión de la Seguridad y pasos del Diagnóstico para la Seguridad de la Información.

Presentación 10 min

Recordar los componentes del proceso de gestión de la Seguridad. (Diagnóstico > Planificación > Implementación > Evaluación)

Explicar Los pasos del *Diagnóstico para la Seguridad de la Información [Anexo T3.M2.S1b]:*

a) Análisis de Contexto

b) Análisis de Contexto

c) Mapa de la Información

d) Análisis de Actores

e) Análisis de Incidentes de Seguridad

f) Análisis de Capacidades y Vulnerabilidades

g) Análisis del Riesgo Mapa de la Información

Consejos de facilitación:

- El concepto de seguridad de la información no debe de ser confundido con el de seguridad informática/digital. La información puede encontrarse en diferentes medios o formatos. Se debe recalcar que la seguridad digital es sólo un componente de la seguridad de la información.
- Ver también consejos de facilitación *[ver Taller 1, Módulo 1, sesión 3].*

Información sensible, amenazas latentes y tecnología.

Análisis de Contexto

60min

Objetivos específicos:

- "Generar conciencia" sobre los riesgos asociados al manejo de la información de las PDDH por medio de un análisis de su contexto.
- Apoyar la identificación de amenazas latentes sobre la información manejada por la organización.

Materiales

- Papelógrafo
- Plumones
- Papelógrafo o diapositivas con los anexos *Tipología de las amenazas latentes relativas a la seguridad de la información [Anexo T3.M2.S2]* y *Tipología de las amenazas latentes para personas defensoras de los DDHH [Anexo T1.M1.S2]*

Puntos clave:

- Definición de amenaza latente. *"Una fuente de daño potencial o los peligros en nuestro entorno/contexto (causados por actores hostiles u otros factores hostiles)".*
- Las amenazas de origen político son intencionales. Usualmente son causadas por potenciales agresores interesados en la información por motivos políticos, por motivos de fraude (*hackers*), etc. Las amenazas de origen político pueden valerse de medios tecnológicos sofisticados (como software que toma el control de las computadoras) o de métodos más tradicionales (por ejemplo escuchas con infiltrados en asambleas comunitarias).
- Amenazas de origen político:

  a) Uso de informantes infiltrados

  b) Vigilancia con micrófonos y cámaras

  c) Intercepción de comunicaciones

  d) Robos disfrazados de atracos

  e) Allanamiento ilegal de la oficina

  f) Cateo legal de la oficina

  g) Robo de identidad/secuestro de cuenta/contraseñas etc.

  d) Control de las computadoras

  e) Escaneo y recopilación gruesa de metadatos sobre uso de internet
- Las amenazas físicas se refieren a daños o pérdidas fortuitas, causadas por accidentes, deterioro normal o asociado al uso de dispositivos tecnológicos o por mala utilización de los mismos.
- Recordar la interacción que existe entre los gobiernos y las empresas que prestan servicios de teléfonos, internet, etc. Las relaciones y la colaboración, cada vez más estrechas, entre el Estado y proveedores de servicios en internet, como *Facebook, Google, Microsoft (Skype)*, entre otros. Los acuerdos de servicio entre usuarios y proveedores de éstos servicios dejan abierta la posibilidad de que los proveedores pasen las informaciones que almacenan sobre el uso del servicio (mensajes, conversaciones, actualizaciones de estatus, *metadata* etc.) a los gobiernos en el contexto de una investigación. Este ha sido usado en contra PDDH desde los EEUU hasta China. Hay leyes en México que también permiten este tipo de utilización de la información.

Actividades

Actividad 1. Entender las amenazas relativas a la seguridad de la información.

Presentación ***10 min***

Definir qué es una amenaza latente (retomar lo trabajado en el Taller 1)

Presentar la Tipología de las amenazas latentes relativas a la seguridad de la información *[Anexo T3.M2.S2].*

a) Amenazas de origen político

b) Amenazas físicas fortuitas

Brindar ejemplos sobre ambos tipos de amenazas relativas a la seguridad de la información.

Actividad 2. Comprender las amenazas de origen político.

Debate a partir de preguntas detonadoras ***35 min***

Plantear al grupo las siguientes preguntas y debatir:

¿De qué forma podrían robarles la información si ustedes fueran un blanco político?

¿Conocen alguna historia, sea por la prensa o por alguna organización conocida, de robo de información?

Actividad 3. Comprender las amenazas físicas.

Discusión en plenaria a partir de preguntas detonadoras
15 min

Plantear al grupo las siguiente pregunta y debatir:

¿Cuáles son las amenazas físicas a las que está sujeta la información que manejan como PDDH?

Recursos adicionales y lecturas de apoyo:

- Protection International, *Cuadernos de Protección Núm. 2 Vigilancia y contravigilancia para organizaciones defensoras de derechos humanos. [RA12]*
- FLORES HINE, *¡Pongámonos las pilas! Reflexiones y acciones concretas para asegurar la información en nuestras organizaciones sociales.*
- Tactical Technology Collective & Front Line Defenders, *Security in a box. Caja de herramientas de Seguridad protegiendo tu privacidad digital*
- SEDEM Asociación para el Estudio y Promoción de la Seguridad en Democracia, *Guía de Protección para defensores de derechos humanos, periodistas y operadores de justicia. [RA10]*

Consejos de facilitación:

- Esta parte contiene mucho tiempo de presentación y algunas cuestiones técnicas por lo cual es importante promover que las personas participen, guiando con algunas preguntas.
- En la actividad 1, se puede dedicar un poco de tiempo para preguntar a las personas participantes si se acuerdan qué es una amenaza latente.
- Antes del taller, buscar los últimos incidentes públicos y ejemplos de leyes y de vigilancia por parte de gobiernos (por ejemplo el uso de *FinFisher*, que se sabe ha sido utilizado en México contra PDDH).
- Se debe evitar que este módulo sea excesivamente técnico, tratando de explicar con palabras sencillas las cuestiones técnicas o tecnológicas.
- Es importante que la organización conozca las amenazas y las entienda, pero hay que tomar cuidado para que no se vean como algo inaccesible o insalvable para no delinear un panorama excesivamente desesperanzador.
- Se deben analizar las amenazas tanto físicas como políticas en términos contextuales *[ver Taller 1, Módulo 2, Sesión 1]*. Es decir *¿Cuáles son los elementos económicos, sociales y políticos del contexto que tienen un impacto sobre la seguridad en el manejo de la información para las PDDH? ¿Este impacto es diferente para hombres y mujeres?*
- Estar preparados para explicar con mayor detalle qué significan las diferentes amenazas y por qué razón son una amenaza. Por ejemplo el funcionamiento de las redes de teléfonos, al enviar un mail no encriptado, etc. Se pueden hacer cadenas con las personas y que las personas representen los receptores finales, los mensajeros y los puntos de intercepción de la información para que entiendan los flujos y vulnerabilidades de una forma divertida.
- ¡Atención con el control del tiempo! Este módulo es susceptible a extenderse demasiado.

Información sensible, amenazas latentes y tecnología.

Información Sensible

60min

Objetivos específicos:

- Consensuar algunos criterios para identificar la información sensible.
- Compartir y debatir sobre los niveles de "sensibilidad" de la información.
- Realizar un mapa de la información sensible manejada por la organización.

Materiales

- Papelógrafo
- Papelógrafo o fotocopias con los anexos *Niveles de acceso a la información [Anexo T3.M2.S3]* y *Mapa de información [Anexo T3.M2.S3b]*
- Plumones
- *Metaplán*
- Papeles de colores con los niveles de acceso a la información
- Rótulos o tarjetas en blanco

Recursos adicionales y lecturas de apoyo:

- FLORES HINE, *¡Pongámonos las pilas! Reflexiones y acciones concretas para asegurar la información en nuestras organizaciones sociales. [RA10]*
- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.11. *[RA5]*

Puntos clave:

- La definición de información sensible puede variar de organización a organización. Más que una definición se necesita que las personas consensuen criterios para considerar la información como sensible. En general, se puede decir que es *aquella información considerada que las PDDH consideran que debe ser especialmente protegida. Lo anterior debido al impacto negativo que conllevaría su pérdida, destrucción o robo para el trabajo de la organización, la integridad física y/o psicológica de sus integrantes, acompañados o aliados.*
- De acuerdo a qué tan sensible es la información en cuestión, las PDDH pueden plantear distintos niveles de acceso a la misma:

  a) *Confidencial*: de acceso excesivamente restringido (por ejemplo solamente a cierto personal interno autorizado).

  b) *Privada*: de acceso controlado (por ejemplo accesible a todo el personal interno).

  c) *Sensitiva: de acceso* moderadamente controlado (por ejemplo accesible a personal interno y cierto personal externo autorizado).

  d) *Pública*: de libre acceso (no confundir con que debe ser publicada, sino que no tiene restricción de accesos).

Actividades

Actividad 1. Definir la Información Sensible.

Lluvia de ideas y discusión en plenaria a partir de preguntas detonadoras

10 min

Plantear al grupo las siguientes preguntas:

¿Qué consideramos como información sensible?

¿Hay criterios para decir qué es y qué no es información sensible?

¿Tenemos ejemplos de información sensible?

Apuntar las ideas que surjan en el grupo en un papelógrafo con tres columnas para cada una de las preguntas. De ser posible la persona encargada de la relatoría toma acuerdos sobre los criterios y ejemplos respecto a lo que el grupo consideraría como información sensible.

Actividad 2. Definir los niveles de acceso a la información.

Presentación 20 min

Recrear en un *Metaplán* o papelógrafo los *Niveles de acceso a la información [Anexo T3.M2.S3].*

Presentar los 4 Niveles de acceso a la información:

a) Confidencial
b) Privado
c) Sensitivo
d) Público

Pedir a las personas participantes que apunten ejemplos de información que manejan para cada una de las categorías (uno por rótulo o tarjeta).

Requerir que peguen sus tarjetas en el espacio del *Metaplán* sobre una de las 4 categorías, según su opinión.

Revisar en plenaria los ejemplos propuestos por las personas participantes. Intentar llegar a una visión común de los niveles de seguridad. A partir de las conclusiones se pueden rellenar directamente fotocopias del anexo o dejar nota de los consensos en la relatoría.

Actividad 3. Trazar un Mapa de la información.

Ejercicio en grupos 30 min

Recrear en un *Metaplán* o papelógrafo el *Mapa de la información [Anexo T3.M2.S3b].* También se pueden distribuir fotocopias del anexo.

Dividir a las personas en grupos de 3 a 5 personas. Distribuir entre los grupos los ejemplos de información que manejan propuestos previamente. Pedir a las personas participantes que completen las primeras cuatro columnas del *Mapa de la información* para la información que les tocó trabajar.

Requerir que después de llenar las primeras cuatro columnas definan en conjunto los permisos otorgados, si la información tiene copias o respaldos. En caso afirmativo también apuntar los dispositivos, ubicación y formas de acceso.

Revisar en plenaria el *Metaplán* llenado, dejar nota de los consensos en la relatoría o guardar lo escrito en las fotocopias de anexo si éstas fueron utilizadas.

Consejos de facilitación:

- En la actividad 2 en caso de que resulte complicado para las personas entender el nivel sensitivo se puede proponer limitar la división en tres niveles (por ejemplo confidencial, privado y público).
- El objetivo de la actividad 2 es conseguir una visión de la organización sobre qué es información sensible y sus niveles. Algunos criterios que pueden ser útiles son: estrategia interna de la organización, confidencialidad de la información, grado de vulnerabilidad a la que puede exponer la información, etc.
- En algunas ocasiones las PDDH participantes dejan de lado el abordaje de la información relacionada con las comunidades con las cuales trabajan. Se debe hacer énfasis en la importancia de incluir por ejemplo la información relacionada con víctimas acompañadas, expedientes con sus datos personales, documentación de casos de violencia de género, etc.
- En la actividad 3 se recomienda más trabajar con el *Metaplán* ya que facilita la visibilidad para todas las personas. Mantener el *Metaplán* con la información trabajada en sesiones posteriores puede ser de gran utilidad para otras sesiones de este taller.
- Al abordar la información sensible la gente normalmente piensa en discos duros, computadoras, archivos de documentación física. Se debe plantear que los contactos en sus teléfonos, sus cuentas de almacenaje virtual en internet, correo electrónico e incluso cuentas de redes sociales para ocio pueden contener información sensible. Es importante que esta información también quede reflejada en el mapeo.
- En la actividad 3 el acceso es aquél que se da en la realidad, es decir que no se refiere a cómo debería de funcionar idealmente. Es decir, si hay una política relativa a la información que no se cumple en la organización, entonces lo que queremos ver es cómo se da en la práctica y no lo que dice dicha política.
- Al trabajar la parte de acceso a la información al interior de una organización es importante resaltar las asimetrías en el acceso y manejo de la información. Por ejemplo en muchas organizaciones las cuestiones técnicas, tecnológicas o de almacenaje y gestión de información son relegadas a hombres, ingenieros en sistemas, etc. esto conlleva patrones de exclusión para algunas defensoras y su capacidad de acceso a dicha información.

Información sensible, amenazas latentes y tecnología.

Análisis de Actores e Incidentes de Seguridad

60min

Objetivos específicos:

- Identificar los actores que tienen interés en la información y valorar sus capacidades para conseguir esta información.
- Analizar los Incidentes de Seguridad relacionados con el manejo de la información para poder bosquejar más adelante conclusiones sobre las principales vulnerabilidades y las medidas de seguridad necesarias.

Materiales

- Papelógrafo
- Plumones
- *Metaplán*
- Rótulos o tarjetas de colores
- Hojas
- Papelógrafo o diapositivas con los anexos *Definición y análisis básico de los Incidentes de Seguridad [T1.M2.S4a]*, *Pasos a seguir para analizar un IdS [T1.M2.S4b]*, *Análisis de Amenazas Declaradas [T1.M2.S4bis a]*, *Pasos para analizar Amenazas Declaradas [T1. M2.S4bis b]* y *Bitácora de registro de IdS [T1.M2.S4c]*, trabajada y llenada por las personas participantes durante el taller 1.

Puntos clave:

- Enfatizar la importancia de los mapeos de actores y de analizar los recursos y capacidades reales de los posibles agresores.
- Recordar lo que es un Incidente de Seguridad (IdS): *"Cualquier hecho o acontecimiento fuera de lo común que pensamos podría afectar a nuestra seguridad personal o como organización".*
- Retomar la idea de que los IdS son indicadores de nuestra situación de seguridad. Los IdS nos permiten medir el impacto de nuestro trabajo y si hay personas que están recopilando información o planificando algo en contra de nosotros.
- Recordar los diferentes tipos de IdS. Algunos IdS pueden ser provocados por nosotros mismos, otros por actores externos; algunos pueden haber sido provocados intencionalmente, otros pueden ser fortuitos; algunos pueden tener un origen político, es decir ser dirigidos hacia nosotros debido a nuestro trabajo o al revés no tener que ver con nuestro trabajo y deberse a la delincuencia común o bien al contexto de violencia general en el que trabajamos como en el caso de los incidentales.

Actividades

Actividad 1. Identificar actores y capacidades para conseguir nuestra información.

Lluvia de ideas y discusión en plenaria a partir de preguntas detonadoras

30 min

Plantear al grupo las siguientes preguntas y debatir:

> *¿Quién podría estar interesado en la información de la organización?*
>
> *Para cada actor identificado. ¿Con qué recursos cuentan para actuar y conseguir nuestra información?*

Apuntar los actores y recursos mencionados por el grupo y sugerir otros si son necesarios.

Pegar actores y recursos en tarjetas en el *Metaplán*.

Apuntar los tipos de amenazas que podrían ejecutar los actores identificados utilizando una amenaza por tarjeta de color. Se recomienda retomar la lista de amenazas latentes trabajadas previamente *[ver Taller 3, Módulo 2, Sesión 2].*

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.1, 1.3 y 1.4.
- Front Line Defenders, *Manual sobre seguridad. Pasos prácticos para defensores/as de derechos humanos en riesgo*, p. 35 y cap. 6. ***[RA5]***
- *Taller 1, Módulo 2, Sesiones 3 y 4a de esta guía.*

Actividad 2. Incidentes de Seguridad y manejo de información.

Ejercicio en plenaria 30 min

Disponer rótulos o tarjetas de colores:

Tarjeta roja. IdS externos intencionales.

Tarjeta amarilla. IdS no se sabe si fue provocado o fortuito.

Tarjeta azul. IdS interno o fortuito.

Cada participante tiene derecho a tres rótulos de cartón. En cada tarjeta deberán escribir un IdS relacionado con el manejo de información.

Colocar los IdS en el *Metaplán* y se agruparlos según el tipo de amenazas latentes *[ver Taller 3, Módulo 2, Sesión 2].*

Elaborar conclusiones grupales a partir del *Metaplán* construido.

Consejos de facilitación:

- Para la actividad 1 la personas facilitadora puede dar un poco de ejemplos de introducción si es que faltan posibilidades entre las sugerencias de las personas participantes. Por ejemplo, la posibilidad de uso de software malicioso, o de *keyloggers* físicos especialmente si la organización ha sufrido un allanamiento, o la relación entre las compañías de servicios de provisión de internet y el gobierno. Esto implica cierta preparación previa y análisis de coyuntura.
- En la actividad 1 hay que asegurar que la Organización no se pierde con los potenciales agresores y con otros tipos de amenazas que no son relativas a la Seguridad de la Información.
- Para la actividad 2, puede ser necesario retomar el concepto de Incidente de Seguridad y sus clasificaciones (internos/externos, provocados/fortuitos, origen) *[ver anexo T1.M2.S4a].*
- Para la actividad 2, las personas participantes pueden cambiar los colores de las tarjetas si no tienen un ejemplo para cada tipo, pero se debe intentar que cada quien escriba 3 IdS. Otra opción es que escriban en hojas blancas y luego en plenaria se decide qué tipo de incidentes son. Para ello se pueden pegar papelitos adheribles de colores en la hoja del IdS de tal manera que queden clasificados.

Información sensible, amenazas latentes y tecnología.

Amenazas prioritarias y análisis de riesgo *30min*

Objetivos específicos:

- Identificar las amenazas prioritarias relativas a la seguridad de la información.
- Analizar las amenazas latentes según la probabilidad que ocurran y el impacto que representan para la seguridad de la información.

Materiales

- *Metaplán*
- Cartulinas blancas u hojas grandes de papelógrafo
- Papelógrafo o diapositivas con el anexo *Matriz de priorización de amenazas [ver Anexo T1.M2.S6b]*
- Tarjetas de cartón o *foamy* verdes, amarillas y rojas
- Rótulos o tarjetas de cartón con las amenazas relativas a la seguridad de la información que fueron identificadas previamente *[ver Taller 3, Módulo 2, Sesión 3 y 4].*
- Chinches
- Cita adhesiva

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.5.
- Front Line Defenders, *Manual sobre seguridad. Pasos prácticos para defensores/as de derechos humanos en riesgo*, cap. 2. *[RA5]*
- *Taller 1, Módulo 2, Sesión 6 de esta guía.*

Puntos clave:

- Retomar el concepto de Análisis de Riesgo y los conceptos de Probabilidad e Impacto abordados durante el Taller 1.
- Los niveles aceptables de riesgo varían de persona a persona y por eso debemos ponernos de acuerdo sobre qué nivel de riesgo aceptan de forma consensuada las personas integrantes de una organización.Para determinar las amenazas prioritarias en seguridad de la información primero debemos valorar el impacto y la probabilidad de que la amenaza se concrete.
- Para valorar el impacto, analizar para cada amenaza latente:

  a) Qué tanto limita el funcionamiento de la organización.

  b) Posibilidad de recuperación de la información.

  c) El daño que podría causar a integrantes de la organización y a terceros (por ejemplo víctimas acompañadas, aliados, etc.).
- Para valorar la probabilidad:

  a) Valorar el interés que los agresores potenciales podrían tener en la información y su capacidad para materializar las amenazas.

  b) Valorar las vulnerabilidades de la propia organización y sus integrantes en el manejo de información sensible.

  c) Analizar los IdS precedentes y pautas y patrones (repetición, aumento, tipo y origen de IdS, etc.). A partir de este análisis determinar si la posibilidad que se concretice la amenaza es inmediata o remota.

Actividades

Actividad 1. Valorar la probabilidad e impacto de las amenazas relativas a la seguridad de la información.

Ejercicio en plenaria* *15 min

Retomar las amenazas relativas a la seguridad de la información identificadas a través del Mapa de la Información, el mapeo de los agresores y el análisis de IdS *[ver Taller 3, Módulo 2, Sesión 3 y 4].*

Llenar con el grupo una *Matriz de Priorización de Amenazas* sobre el *Metaplán [ver anexo T1.M2.S6b]* adaptándola específicamente a las amenazas relativas a la seguridad de la información.

En la columna izquierda "Amenazas latentes" se adhieren las tarjetas con las amenazas detectadas en la actividad precedente

En la columna central "Probabilidad" cada persona escogerá una sola tarjeta de color (Roja-probabilidad alta; Amarilla-probabilidad media; Verde-probabilidad baja).

En la columna derecha "Impacto" cada persona escogerá una sola tarjeta de color (Roja-impacto alto; Amarilla-impacto medio; Verde-impacto bajo).

Al final cada participante habrá pegado para cada amenaza de la Matriz una tarjeta de probabilidad y una de impacto. Como resultado cada amenaza tendrá varias tarjetas de valoración para probabilidad e impacto. Es normal que haya divergencias sobre las valoraciones de cada amenaza.

Otra forma de hacer la matriz es colocar el listado de amenazas y poner un semáforo con los tres colores en cada espacio de las columnas para probabilidad e impacto. Pedir que cada persona pegue dos chinches (una para probabilidad y otra para impacto) en el color que considere para todas las amenazas.

Actividad 2. Priorizar las amenazas relativas a la seguridad de la información.

Presentación y discusión en plenaria ***15 min***

En plenaria se debate el resultado que se ve en el *Metaplán*. El grupo intenta acordar cuáles son las amenazas que representan mayor probabilidad e impacto a partir de las opiniones reflejadas en el *Metaplán* y el debate (se recomienda seleccionar de 3 a 5 amenazas prioritarias). A partir de la *Matriz de Priorización de Amenazas* rellenada previamente mostramos que puede haber varias percepciones del riesgo pero lo importante es llegar a un consenso sobre cómo valorar las amenazas.

Se intenta consensuar qué amenazas latentes se deben priorizar a través de una política de manejo de información sensible.

De preferencia se deja por escrito el consenso sobre las amenazas prioritarias.

Consejos de facilitación:

- Puede ser difícil valorar la probabilidad y el impacto en la ecuación del riesgo. Dejar claro que no podemos ser 100% exactos. Es importante dejar claro que cada participante debe poner su opinión personal con base al conocimiento que tienen y el análisis que hemos estado realizando durante el taller. Es una valoración subjetiva inicialmente y el objetivo posterior es que todas las PDDH lleguen a un acuerdo sobre cuál es el nivel de riesgo para cada una de las amenazas identificadas. Al momento de valorar la probabilidad e impacto de las amenazas latentes es probable que cada participante piense de forma diferente (ante el robo de información por ejemplo un participante puede poner una tarjeta amarilla mientras otra considerará que debe tener una tarjeta verde). La actividad hace patente la subjetividad del riesgo. La función de la persona que facilita es la de impulsar un consenso para permitir llegar a una visión compartida del riesgo y acordar como lo valora la organización en su conjunto.

- Si se elige la dinámica del semáforo no dar por sentado que todas las personas entienden su funcionamiento. Hay comunidades y grupos más de base que no necesariamente lo tienen tan claro. Es importante decir qué significa cada color para Probabilidad y para Impacto y asegurarse que todas las personas participantes han entendido la actividad.

Política de manejo de la información sensible

Preparación de una política de manejo de la información sensible

120min

Materiales

- Papelógrafo
- Plumones
- Rótulos o tarjetas de cartón
- *Metaplán*
- Papelógrafo, fotocopias y/o diapositivas con el anexo *Vulnerabilidades y Capacidades relativas a la seguridad de la información [Anexo T3.M3.S1]* y *Pensar medidas de seguridad para amenazas prioritarias [Anexo T1.M2.S6c]*

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.7.
- Front Line Defenders, *Manual sobre seguridad. Pasos prácticos para defensores/as de derechos humanos en riesgo*, cap. 7. *[RA5]*
- FLORES HINE, *¡Pongámonos las pilas! Reflexiones y acciones concretas para asegurar la información en nuestras organizaciones sociales.*
- Tactical Technology Collective & Front Line Defenders, *Security in a box. Caja de herramientas de Seguridad protegiendo tu privacidad digital [RA10]*
- *Taller 1, Módulo 2, Sesión 5 y 6 de esta guía.*
- *Taller 2, Módulo 2, Sesión 1 de esta guía.*

Puntos clave:

- Revisar los conceptos de capacidad: *"Los puntos fuertes y recursos a los que puede acceder una PDDH para lograr un nivel mínimo de seguridad. Estas capacidades siempre son mejorables."* y vulnerabilidad. *"El grado en que las PDDH son susceptibles a pérdida, daños, sufrimiento o la muerte en caso de un ataque".*
- Vincular capacidades y vulnerabilidades a componentes específicos relacionados con la seguridad de la información.
- Las vulnerabilidades y capacidades son características nuestras, propias, internas, sobre las cuales podemos trabajar.
- Las capacidades y vulnerabilidades son las dos caras de una misma moneda. Podemos convertir una vulnerabilidad en una capacidad.
- Las medidas de seguridad relativas al manejo de la información deben estar relacionadas con nuestras vulnerabilidades y capacidades específicas.

Objetivos específicos:

- Identificar las capacidades y vulnerabilidades relacionadas a las amenazas prioritarias relativas a la seguridad de la información.
- Revisar los diferentes aspectos de la seguridad de la información.
- Promover el compromiso institucional en favor de la seguridad de la información.

Actividades

Actividad 1. Pensar medidas para la seguridad de la información.

Ejercicio en grupos 60 min

Dividir a las personas en grupos de 3 a 5 personas. Cada grupo trabajará con una amenaza prioritaria de las identificadas en el módulo anterior *[ver Taller 3, Módulo 2, Sesión 5].*

Cada grupo trabajará con base en el formato *Pensar medidas de seguridad para amenazas prioritarias [Anexo T1.M2.S6c]* identificando capacidades y vulnerabilidades relacionadas con la amenaza prioritaria relativa al manejo de la información de su grupo y proponiendo medidas de seguridad específicas.

Para identificar las vulnerabilidades y capacidades se pueden apoyar en el *Anexo Vulnerabilidades y Capacidades relativas a la seguridad de la información [Anexo T3.M3.S1].*

Pedir que apunten las medidas identificadas en rótulos o tarjetas de cartón. Una medida de seguridad por tarjeta.

Actividad 2. Consensuar las medidas necesarias para la seguridad de la información.

Discusión en plenaria ***60 min***

Cada grupo presenta lo que trabajaron haciendo énfasis en las medidas de seguridad propuestas.

Las personas participantes colocan las tarjetas de medidas de seguridad en el *Metaplán*, bajo la amenaza prioritaria y en conjunto debaten las medidas propuestas, su pertinencia y factibilidad.

La persona que facilita intenta promover un consenso sobre las medidas que deberían ser implementadas en una política sobre manejo de la información sensible en la organización.

Revisar en plenaria el *Metaplán* llenado, dejar nota de los consensos en la relatoría o guardar lo escrito en las fotocopias de anexo si éstas fueron utilizadas.

Consejos de facilitación:

- Elaborar una política sobre manejo de la información sensible toma mucho tiempo y es una actividad que la organización debe hacer posteriormente invirtiendo recursos en términos de tiempo, responsabilidades, seguimiento, etc. Por ello no podemos completar esta actividad del todo en un taller. Esta sesión sirve para sentar las bases de un consenso de posibles medidas que deberán retomar y trabajar a profundidad por su cuenta para elaborar una política más completa.
- Pueden haber vulnerabilidades y capacidades que se repiten para diferentes amenazas prioritarias.
- Puede ser complicado para el grupo pasar de las vulnerabilidades/capacidades a medidas de seguridad. En vez de pensar en la amenaza como un simple suceso (por ejemplo robo de información), pensar en ella en términos de *¿qué es lo que quieren evitar?* Quieren evitar la posibilidad que ocurra algo y quieren evitar que en el caso de que ocurra el impacto sobre la organización no sea tan grave (por ejemplo queremos evitar que roben información sensible y que nos quedemos sin archivos para continuar nuestro trabajo). *Queremos que sea más difícil llevar a cabo la amenaza y queremos también que sí se lleva a cabo, las consecuencias negativas para la organización sean menores, ¿qué medidas podemos tomar para esto?*
- Considerar si la amenaza toca todos los espacios del defensor (casa, trabajo, traslados etc.) y verificar si están cubiertos por las medidas propuestas. Al revés, se puede tomar cada medida y ver en qué espacio protegen a las PDDH o reducen la posibilidad de que la amenaza se materialice.
- Las personas suelen elegir medidas generales de seguridad y poco aplicables, es importante hacerlas ver que tienen que ser específicas para que realmente sean medidas. Es fundamental que las capacidades y vulnerabilidades estén directamente relacionadas con la amenaza prioritaria y que las medidas de seguridad sean detalladas. Es común que las organizaciones planteen medidas generales como "tener una política de comunicación en viajes". Hay que alentarlos a que detallen y a pensar cuáles serían los componentes de esta política entonces junto con mecanismos específicos p.e. "llamadas de monitoreo cada 5 horas durante los viajes de trabajo a la persona designada de guardia mediante el teléfono celular de la organización".
- Las personas suelen preguntar sobre medidas generales que sirvan de antemano (preguntan por ejemplo si es bueno "encriptar la información"). En este caso, explicar que no opinamos específicamente sobre este tipo de medidas (ni las recomendamos ni las rechazamos *a priori*, sino que las deben consensuar a la luz de su contexto específico. Una medida apropiada para una organización no necesariamente sirve para otra. Por ejemplo la información encriptada sin las capacidades adecuadas por parte de las PDDH integrantes de la organización o aliadas puede entorpecer la comunicación o excluir a ciertas personas que necesitan acceso a dicha información para su labor de defensa de DH.
- Las medidas deben ser realistas y apegadas al contexto de la organización. Hay organizaciones que han estudiado y observado que en un contexto de defensa de derechos humanos, ciertas medidas han funcionado para la mayoría de organizaciones y son vistas como buenas prácticas. Estas posibles medidas y/o buenas prácticas no deben menguar la creatividad de la organización para buscar formas alternas de protegerse. Es decir, al usar un catálogo de buenas medidas existe el riesgo de caer en una fórmula única que en caso de no poder ser cumplida deja en desprotegida a la organización.
- La Actividad 1 en ocasiones puede tardar mucho tiempo. Es importante acotarla para que el espacio de la Actividad 2 para consensuar y discutir la factibilidad de dichas medidas pueda darse con condiciones de tiempo adecuadas.

Cierre y evaluación

Seguimiento, compromisos y cierre

45min

Objetivos específicos:

- Revisar el contenido y los conocimientos adquiridos.
- Identificar tareas y responsabilidades para darle seguimiento al taller e implementar lo aprendido.
- Acordar el seguimiento.
- Evaluar el taller.

Materiales

- Papelógrafos
- Plumones
- *Metaplán*
- Hojas
- Papelógrafo con un punteo de los *Objetivos generales del taller y resultados esperados*
- Fotocopias con *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b]*
- Urna o caja de cartón con una ranura

Puntos clave:

- Enfatizar que si la organización no le destina los recursos (responsables, espacios, tiempo, etc.) al ámbito de seguridad y protección no se podrán llevar a cabo estrategias ni planes integrales.
- Abordar las expectativas de seguimiento y acordar si se necesita seguimiento, de qué tipo y cómo se podría dar.
- Revisar los acuerdos alcanzados y establecer los compromisos con las personas participantes en cuanto a las estrategias de seguridad y protección que serán desarrolladas a nivel organizativo.
- Revisar las tareas apuntadas e identificar plazos, espacios, recursos y responsables con un nivel aceptable de detalle y claridad.
- Cerciorarnos que no hayan quedado dudas sobre los aspectos fundamentales del taller.
- Evaluar el taller y la facilitación.

Actividades

Actividad 1. Revisión de "Actas y Acuerdos".

Discusión en plenaria* *15 min

La persona que facilita el taller pide a la persona encargada de actas o relatora que haga un pequeño recuento del taller.

Entre todas y todos, vamos apuntando las tareas y pendientes que surgieron del taller.

Mientras las personas participantes van identificando las tareas pendientes, sondear las necesidades y voluntad para una asesoría ulterior (tener en cuenta las posibilidades de los módulos opcionales adicionales del Taller 3 "Buenas Prácticas generales en el manejo de la información" y "Seguridad Digital" y los módulos propuestos por el Taller 4 del PASP).

Plantear al grupo las siguientes preguntas:

¿Cuándo podríamos realizar una entrevista de seguimiento?

¿Sienten que necesitan otras asesorías?

Consejos de facilitación:

- Si el grupo no quiere llegar a acuerdos en términos del seguimiento no hay que forzarlo.
- Si se tiene más tiempo al final se puede optar por la evaluación en fotocopias que permite sistematizar mejor la información y retroalimentaciones. Algunos grupos prefieren rellenar las evaluaciones sin la persona que facilita presente. Se pueden poner cajitas a modo de urnas para que se depositen las evaluaciones individuales dobladas y de forma anónima.

Actividad 2. Evaluación del cumplimiento de los objetivos del taller y expectativas.

Trabajo en plenaria 10 min

Retomar las expectativas de las personas participantes trabajadas al inicio del taller. En un papelógrafo se pegan las expectativas iniciales del grupo del lado izquierdo y a la derecha se hacen tres columnas para evaluar el cumplimiento de las mismas: 1) se cumplió 2) se cumplió parcialmente y 3) no se cumplió. Para cada una de las expectativas se pide que cada persona pegue un papelito adherible en la columna que considere.

En otro papelógrafo se tiene listo un punteo de los *Objetivos generales del taller y resultados esperados*. Enfrente de cada aspecto del punteo se hacen tres columnas al igual que para las expectativas y se pide que las personas peguen un papelito adherible en la columna que consideren. También pueden escribir sobre el papelito que peguen si gustan ahondar en algún objetivo específico si sienten que hubo aspectos del objetivo que se les dificultaron o que no se cumplieron a cabalidad.

La persona que facilita hace un recuento y revisa especialmente aquellos objetivos y expectativas que faltó cumplir a cabalidad. Se contrasta si dichos objetivos y expectativas estaba en las posibilidades planteadas por el taller o si se pueden abordar en talleres subsecuentes.

Actividad 3. Evaluación del taller y la facilitación.

Trabajo individual o plenaria 10 min

Escoger una de las siguientes formas de evaluación.

a) En un papelógrafo se hacen dos columnas: 1) adecuado y 2) puede mejorar. Se reparten papelitos con los distintos criterios adaptados de las 2 tablas del *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b]*.

Se les pide que cada quien tome 3 criterios de evaluación del taller y 3 criterios de evaluación de la facilitación (de preferencia aquellos donde tengan más que aportar o que les llamaron la atención para evaluar) y que escriban sobre los papelitos con sus opiniones, críticas y sugerencias. Luego se les pide que adhieran los papelitos en una de las dos columnas según corresponda a su punto de vista.

b) Se distribuyen individualmente fotocopias del *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b]*. Se pide a las personas que lo llenen y lo depositen doblado y de forma anónima en una caja o urna.

Actividad 4. Conclusión.

Discusión en plenaria 10 min

Se da una oportunidad para dudas y comentarios al grupo, se comentan las apreciaciones y se hace una última ronda de críticas y sugerencias.

Se recuerda la confidencialidad de lo abordado en los talleres.

Se dan los agradecimientos y se clarifica que se deja la posibilidad abierta para futuras colaboraciones.

Buenas prácticas en el manejo de información

Los pasos de la información

15min

Objetivos específicos:

- Favorecer una visión amplia de la seguridad de la información
- Introducir los 5 pasos de la información,
- Introducir los 5 ámbitos de Buenas prácticas relativas al manejo de información.

Materiales

- Papelógrafo
- Plumones
- Papelógrafos o diapositivas con *Los pasos de la información [Anexo T3.MA.S1]* y *Buenas prácticas relativas al manejo de información [Anexo T3.MA.S1b].*

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.8 y 1.11.
- Front Line Defenders, *Manual sobre seguridad. Pasos prácticos para defensores/as de derechos humanos en riesgo,* Apéndices 5, 6, 14 y 15. *[RA5]*

Puntos clave:

- Recordar que las medidas de seguridad de este módulo son una recopilación de buenas prácticas de diferentes organizaciones. No es una receta de cómo actuar.

Actividades

Actividad 1. Los pasos de la información.

Presentación* *8 min

Presentar *Los pasos de la información [Anexo T3.MA.S1]* desde el momento en que llega a nuestras manos hasta que la difundimos.

1) *Contacto con la información/informante (fuente)*
2) *Almacenamiento y procesamiento de la información*
3) *Trasmisión de la información*
4) *Difusión pública de la información*

Actividad 2. Punteo de las buenas prácticas relativas a manejo de la información.

Presentación* *7 min

Presentar las *Buenas prácticas relativas al manejo de información [Anexo T3.MA.S1b].*

1) *Seguridad Física*
2) *Política de Respaldo*
3) *Destrucción de la Información Sensible*
4) *Control de Comunicaciones*
5) *Reuniones Seguras*

Consejos de facilitación:

- No se debe tardar mucho tiempo en la presentación de la Actividad 1 pero sí se debe dejar claro a las personas que a partir de ahora y hasta el final del módulo adicional, cuando estemos pensando en medidas de seguridad, tendremos que pensar en los diferentes pasos o momentos por los que atraviesa la información. Se puede dejar pegado el papelógrafo de los pasos durante toda la sesión, de esta manera en etapas posteriores podemos corroborar que cubrimos todos los pasos.
- La actividad 2 es simplemente una presentación de lo que será desglosado a mayor profundidad en las siguientes sesiones de este módulo opcional adicional.

Buenas prácticas en el manejo de información

Seguridad física de la información

60min

Objetivos específicos:

- Favorecer una visión amplia de la seguridad física de la información considerando los diferentes niveles de acceso a dicha información.
- Dar ejemplos para filtros de acceso.
- Sensibilizar sobre los riesgos de daño físico de los dispositivos en los que se almacena información sensible.
- Presentar buenas prácticas para proteger los aparatos de las amenazas físicas para que las PDDH debatan y adapten dichas medidas a sus propios contextos y riesgo específico.

Materiales

- Papelógrafo
- Plumones
- Papelógrafo o diapositivas con el anexo
- *Filtros de Acceso [Anexo T3.MA.S2].*
- Fotocopias con el anexo *Formato de pendientes sobre seguridad física [Anexo T3.MA.S2b]*.

Puntos clave:

- La información o los dispositivos en los que se almacena son vulnerables a fallas, robos y pérdidas. Lo anterior se puede prevenir tomando medidas de seguridad física.
- Algunos ejemplos de buenas prácticas:

  1) Filtros de acceso: guardar información sensible bajo llave, proteger accesos de puertas y ventanas, tener una política de llaves y duplicados, control de entradas a la oficina, videocámaras, grabadora de llamadas, vigilantes, claves, división de espacios entre visitantes y personal interno, etc.

  2) Daños físicos: sistema de cableado en buenas condiciones para evitar sobrecargas eléctricas, uso de *no-break* y fusibles, no exponer a humedad y polvo, limpieza de los materiales y oficinas, cuidado con líquidos y comida en los espacios de trabajo, respaldo periódico de la información, prevención de incendios, reglas para no fumar en la oficina refuerzo de estanterías para objetos vulnerables a sismos.

Actividades

Actividad 1: Filtros de acceso.

Presentación y discusión en plenaria* *10 min

Presentar y discutir algunas buenas prácticas y sugerencias para la seguridad física de la información en la organización

> Guiar la discusión con las siguientes preguntas: *¿Cómo se accede a la información? ¿Cuáles son las barreras?*

La persona que facilita dibuja en un papelógrafo o pizarrón "círculos concéntricos", es decir círculos desde uno más pequeño hasta los más grandes que lo rodean, ver ejemplo *Filtros de Acceso [Anexo T3.MA.S2]*. Dentro de cada círculo se representa el nivel de acceso a la información física de la oficina de la organización. Por ejemplo: en el primer círculo al centro se representa la mesa con la computadora o el archivero con documentación sensible; en el segundo círculo se representa la oficina; en el tercero, el edificio/casa entera; en el cuarto, la calle, en el quinto, el barrio. Y así en adelante. Representar en cada círculo los filtros de acceso como barreras físicas (poner por ejemplo si hay puertas y ventanas de acceso), barreras tecnológicas (por ejemplo si hay contraseñas o información encriptada en las computadoras) y prácticas de trabajo (por ejemplo si hay cerraduras pero siempre están abiertas durante horas de trabajo representarlas como un filtro abierto).

Preguntar al grupo y discutir en plenaria *¿Cómo podríamos volver estos filtros de acceso más difíciles?*

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.8 y 1.11.
- Front Line Defenders, *Manual sobre seguridad. Pasos prácticos para defensores/as de derechos humanos en riesgo*, Apéndices 5, 6, 14 y 15. *[RA5]*
- Protection International, *Cuadernos de Protección Núm. 2 Vigilancia y contravigilancia para organizaciones defensoras de derechos humanos. [RA12]*
- Tactical Technology Collective & Front Line Defenders, *Security in a box. Caja de herramientas de Seguridad protegiendo tu privacidad digital*, Sesión 2 "Proteger tu información de amenazas físicas". *[RA10]*

Actividad 2: Análisis de sede.

Ejercicio en grupos 40 min

Analizar la seguridad de la sede (oficina y/o casa de la organización). Pedir a las personas participantes que se dividan en grupos y hacer un análisis del lugar donde se encuentran identificando las probables vulnerabilidades y capacidades para cada uno de los siguientes elementos:

a) *Ubicación* (características del barrio)

b) *Vecindario* y relación con este y sus habitantes

c) *Accesibilidad* (cómo se accede físicamente pero también cuáles son los procedimientos de acceso a personas externas)

d) *Susceptibilidad de accidentes o riesgos naturales* (incendios, terremotos, inundaciones etc.)

e) *Solidez y antigüedad de la estructura*

f) *Barreras físicas y técnicas* (puertas, ventanas, rejas, llaves, luces, alarmas, etc.)

Al final uno de los grupos presenta brevemente sus resultados y los demás aportan si hay elementos que faltan.

Actividad 3: Daños físicos y su prevención.

Presentación y discusión en plenaria 10 min

Presentar y discutir algunas buenas prácticas y sugerencias para la seguridad física de la información en la organización.

Guiar la discusión con las siguientes preguntas:

¿Qué daños físicos podrían afectar la información de la organización? (polvo, líquidos, sismos, etc.)

¿Cómo podemos prevenir estos daños?

A partir de la discusión de toda esta sesión se puede llenar el Formato de pendientes sobre seguridad física *[Anexo T3.MA.S2b].*

Consejos de facilitación:

- Promover que las personas participantes den ejemplos de manera activa y que la sesión no se vuelva una simple enunciación de medidas por parte de la persona que facilita.
- Recordar que estas medidas son solamente ejemplos y no soluciones automáticas. Por ende deberían ser balanceadas y valoradas respecto al nivel de riesgo de la organización y su realidad.
- Subrayar que el análisis de sede no es sólo útil desde el punto de vista de la información pero también para prevenir ataques.
- Las personas participantes deberían acordar si consideran necesario y útil retomar más adelante las vulnerabilidades y medidas de seguridad identificadas para valorar si quieren completar la política de acceso a la información de la organización *[ver Taller 3, Módulo 3, Sesión 1].* Se puede comenzar a rellenar el *Formato de política sobre manejo de información sensible [Anexo T3.MA.S4]* para que quede constancia de las conclusiones o acuerdos a los cuales lleguen las personas participantes.

Buenas prácticas en el manejo de información

Política de Respaldo

30min

Objetivos específicos:

- Sensibilizar sobre los riesgos de pérdida o destrucción de la información y la importancia de respaldarla.
- Identificar la información cuya pérdida tendría un impacto alto.
- Presentar buenas prácticas para una política de respaldo para que las PDDH debatan y adapten dichas medidas a sus propios contextos y riesgo específico.

Materiales

- Papelógrafo
- Plumones
- Papelitos adheribles de colores
- *Metaplán*
- Fotocopias con el *Formato de Política de Respaldo [Anexo T3.MA.S3].*
- *Metaplán* o papelógrafo trabajado previamente para el *Mapa de la Información [Anexo T3.M2.S3b]* y los *Niveles de acceso a la información [Anexo T3.M2.S3]*
- Fotocopias con *Formato de política sobre manejo de información sensible [Anexo T3.MA.S4]*

Puntos clave:

- Para abordar la importancia de la política de respaldo, puntualizar los recursos económicos, humanos, materiales, posible daño de imagen pública, daño en relaciones de confianza, tiempo, etc. que podrían ser causados por una pérdida de la información (sea por factores políticos, tecnológicos o físicos).

Actividades

Actividad 1: Importancia de una política de respaldo.

Presentación y discusión en plenaria 10 min

Presentar la importancia de contar con una política de respaldo. Se puede guiar la discusión con algunas preguntas.

¿Cuál sería el costo en caso de pérdida de la información?

¿Cuál es el costo de recuperación?

¿En caso de pérdida, qué información tendría un impacto alto sobre la organización?

Presentar los pasos principales de una política de respaldo efectiva

1) Organizar y seleccionar la información que se tiene que respaldar

(Documentos, fotos que se tiene que digitalizar, archivos electrónicos, bases de datos, directorios de contactos, etc.)

2) Escoger los medios de respaldo

3) Separar el respaldo de los archivos originales

4) Establecer filtros de acceso para los respaldos

5) Establecer una política de seguridad: *¿Quién? ¿Cuándo? ¿Cómo? ¿Dónde?*

Actividad 2: Política de respaldo.

Actividad en grupos 20 min

Dividir a las personas participantes en pequeños grupos y distribuir el *Formato de Política de Respaldo [Anexo T3.MA.S3].*

Pedir a cada grupo que elabore una política de respaldo, trabajando con el formato. Se pueden apoyar en el *Metaplán* o papelógrafo trabajado previamente para el *Mapa de la Información [Anexo T3.M2.S3b]* y los *Niveles de acceso a la información [Anexo T3.M2.S3]* que definieron en su organización.

Organizar un debate en plenaria a partir de lo que aportaron en los formatos de la política de respaldo. La persona que lleva la relatoría toma nota de los acuerdos.

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.8 y 1.11.
- Front Line Defenders, *Manual sobre seguridad. Pasos prácticos para defensores/as de derechos humanos en riesgo*, Apéndices 5, 6, 14 y 15. *[RA5]*
- Tactical Technology Collective & Front Line Defenders, *Security in a box. Caja de herramientas de Seguridad protegiendo tu privacidad digital*, Sesión 2 "Proteger tu información de amenazas físicas", Sesión 4 "Proteger los archivos de tu computadora" y Sesión 5 "Recuperar Información Perdida". *[RA10]*

Consejos de facilitación:

- Evitar entrar mucho en detalles sobre la parte de seguridad digital y recordarles que existe la opción de una sesión especializada para aprender a "Proteger tu información de amenazas físicas", "Proteger los archivos de tu computadora" y "Recuperar Información Perdida" *[ver Taller 3, Módulo B, Sesiones 2, 4 y 5]* de la *Caja de herramientas de Seguridad protegiendo tu privacidad digital*. En estas sesiones se puede ahondar sobre cuestiones técnicas y prácticas para aprender a utilizar programas para proteger y recuperar información.

- Se puede retomar el *Mapa de la Información* *[ver Taller 3, Módulo 2, Sesión 3]* y reorganizar la información del *Metaplán* trabajado en nuevas categorías. Por ejemplo se puede organizar en categorías a partir de los dispositivos o lugares donde se almacenan (discos duros, discos externos, celulares, etc.). Se puede distinguir entre las copias "maestras" y los duplicados (se pueden usar papelitos adheribles). Luego se puede "reproducir" el efecto de una pérdida de datos para clarificar la importancia de los respaldos simplemente tirando los datos pegados en la categoría de "computadora/disco duro" en el suelo. Por ejemplo, decir que hubo un virus, o que el disco de la computadora madre y su información es irrecuperable y arrancar los papeles que representen la información que estuviera en la computadora madre. Es algo visible y lúdico y representa bien lo que queremos mostrar en el taller. Se debe evitar el fatalismo ya que hay que enfatizar que este tipo de escenarios son completamente prevenibles.

- La actividad 2 debe ser sencilla y no tomar mucho tiempo. Por el tiempo no se podrán abocar a realizar una política de respaldo exhaustiva, sólo delinearán un primer bosquejo que si les interesa tendrán que trabajar a profundidad en otro espacio por su cuenta.

- Recordar que estas medidas son solamente ejemplos y no soluciones automáticas. Por ende deberían ser balanceadas y valoradas respecto al nivel de riesgo de la organización y su realidad.

- Las personas participantes deberían acordar si consideran necesario y útil retomar más adelante las vulnerabilidades y medidas de seguridad identificadas para valorar si quieren completar la política de acceso a la información de la organización *[ver Taller 3, Módulo 3, Sesión 1].* Se puede comenzar a rellenar el *Formato de política sobre manejo de información sensible [Anexo T3.MA.S4]* para que quede constancia de las conclusiones o acuerdos a los cuales lleguen las personas participantes.

Buenas prácticas en el manejo de información

Destrucción de la Información Sensible *10min*

Objetivos específicos:

- Sensibilizar sobre los riesgos de vigilancia y de robo de información inherentes a malas prácticas de destrucción de información sensible.
- Presentar buenas prácticas para destruir la información sensible para que las PDDH debatan y adapten dichas medidas a sus propios contextos y riesgo específico.

Materiales

- Papelógrafo
- Plumones
- *Metaplán*
- *Fotocopias con Formato de política sobre manejo de información sensible [Anexo T3.MA.S4]*

Puntos clave:

- Tirar discos duros, CDs o papeles a la basura es una forma de poner en vulnerabilidad a la organización o a la gente que asesoran o acompañan. En muchas ocasiones la forma más fácil y económica de vigilar a una organización es revisar su basura. No hay necesidad de papel cuando se puede guardar de manera electrónica con una adecuada política de respaldo.
- La simple eliminación o envío de archivos electrónicos a la papelera de reciclaje no bastan para destruir información electrónica sensible.

Actividades

Actividad 1: Prácticas de destrucción de información sensible.

Presentación y discusión en plenaria** **10 min

Empezar la discusión con la pregunta: ¿cómo destruyen la información sensible?

Presentar rápidamente las buenas prácticas de destrucción de la información en 3 principales aspectos.

a) *Papeles y archivos físicos:* Destrucción de todos los papeles con información sensible (con una trituradora o incineración)

b) *Dispositivos extraíbles:* Formateo o destrucción física de los dispositivos extraíbles (USB, Disco Duro, DVD, CD, etc)

c) *Archivos electrónicos:* Usar programas de eliminación permanente para los archivos electrónicos eliminados *[ver Taller 3, Módulo B, Sesión 6].*

A partir de la presentación organizar un breve debate para ver evaluar si con base en su nivel de riesgo, vulnerabilidades y capacidades existe alguna medida que consideren factible adaptar a su contexto.

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.8 y 1.11.
- Front Line Defenders, *Manual sobre seguridad. Pasos prácticos para defensores/as de derechos humanos en riesgo*, Apéndices 5, 6, 14 y 15. *[RA5]*
- Tactical Technology Collective & Front Line Defenders, *Security in a box. Caja de herramientas de Seguridad protegiendo tu privacidad digital*, Sesión 6 "Destruir Información Sensible". *[RA10]*

Consejos de facilitación:

- Evitar entrar mucho en detalles sobre la parte de seguridad digital y recordarles que existe la opción de una sesión especializada para aprender a "Destruir Información Sensible" *[ver Taller 3, Módulo B, Sesión 1]* de la *Caja de herramientas de Seguridad protegiendo tu privacidad digital*. En esta sesión se puede ahondar en cuestiones técnicas y prácticas para aprender a utilizar programas eficaces para destruir información (p.e. *Eraser*, *CCleaner*, etc.).
- Recordar que estas medidas son solamente ejemplos y no soluciones automáticas. Por ende deberían ser balanceadas y valoradas respecto al nivel de riesgo de la organización y su realidad.
- Las personas participantes deberían acordar si consideran necesario y útil retomar más adelante las vulnerabilidades y medidas de seguridad identificadas para valorar si quieren completar la política de acceso a la información de la organización *[ver Taller 3, Módulo 3, Sesión 1]*. Se puede comenzar a rellenar el *Formato de política sobre manejo de información sensible [Anexo T3.MA.S4]* para que quede constancia de las conclusiones o acuerdos a los cuales lleguen las personas participantes.

Buenas prácticas en el manejo de información

Control de las comunicaciones

20min

Objetivos específicos:

- Revisar los criterios de un sistema de comunicación adecuado para la seguridad de las PDDH.
- Presentar buenas prácticas con el uso de teléfonos y el uso de códigos para que las PDDH debatan y adapten dichas medidas a sus propios contextos y riesgo específico.

Materiales

- Papelógrafo
- Plumones
- *Metaplán*
- Fotocopias con *Formato de política sobre manejo de información sensible* *[Anexo T3.MA.S4]*

Puntos clave:

- Recalcar la importancia de un sistema de monitoreo entre PDDH como parte del *plan de seguridad* de la organización
- Capacidades y vulnerabilidades del sistema de comunicación:
  - **a)** Contar con un sistema alternativo de comunicación
  - **b)** Capacidad de monitorear a los equipos en el terreno
  - **c)** Cobertura en áreas de riesgos
  - **d)** Siempre disponible para contactos de emergencia
  - **e)** Costo
  - **f)** Disponibilidad de los recursos necesarios: batería, cargador, crédito
  - **g)** Capacidad de los agresores de cortar el sistema
  - **h)** Probabilidad de robo por parte de la delincuencia
  - **i)** Presumir siempre que hay alguien escuchando o espiando nuestra información
- Hacerse siempre las preguntas claves:

  ¿Confías en la persona con la que estás hablando?

  ¿Ésta persona necesita la información que le estás dando o estás dando información adicional innecesaria?

  ¿Te encuentras en un entorno seguro donde hay gente escuchando o leyendo aparentemente?
- Medidas de seguridad con los celulares.
  - **a)** Nadie le puede garantizar que el teléfono celular no sea perdido o robado
  - **b)** No guardar ninguna información sensible en el celular
  - **c)** Borrar y formatear o respaldar fuera del celular (chip externo)
  - **d)** Usar dos chips de memoria para respaldar los contactos
  - **e)** Activar la contraseña de acceso al teléfono
  - **f)** Habilitar la opción de bloqueo automático o borrado de información a distancia
  - **g)** Usar nombres ficticios, apodos, para los contactos
  - **h)** Desactivar la conexión inalámbrica *Bluetooth* cuando no se usa. No conectarse a Internet en redes *Wi-Fi* cuyo nivel de seguridad es desconocido
  - **i)** Borrar y formatear antes de deshacerse del celular
  - **j)** Apagar y quitar la batería durante reuniones, tapar la cámara y/o situar los teléfonos a lado de un radio con música encendida
- Desventajas del uso de códigos:
  - **a)** Llamar la atención de los servicios de seguridad
  - **b)** Mala interpretación por parte de los servicios de seguridad (riesgos de criminalización)
  - **c)** Posible falta de claridad y errores en la transmisión de la información (especialmente en situaciones de emergencia)
- Propuestas para superar las desventajas del uso de códigos:
  - **a)** Establecer un sistema de código de uso fácil y congruente que siga siendo difícil de descifrar
  - **b)** Espacios para capacitar a todas las personas integrantes de la organización y evaluar su eficiencia
  - **c)** Usar metáforas de la vida cotidiana para no llamar la atención
- Monitoreo de los viajes.
  - **a)** Establecer un sistema de monitoreo claro con responsables de guardias y tiempos
  - **b)** Compartir el itinerario y la agenda detallada antes de viajar
  - **c)** Identificar los medios de comunicación alternativos
  - **d)** Establecer códigos o fórmulas claves para reportarse sin tener que dar información sobre el paradero

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.8 y 1.11.
- Front Line Defenders, *Manual sobre seguridad. Pasos prácticos para defensores/as de derechos humanos en riesgo*, Apéndices 5, 6, 14 y 15. *[RA5]*
- Protection International, *Cuadernos de Protección Núm. 2 Vigilancia y contravigilancia para organizaciones defensoras de derechos humanos*. *[RA12]*
- Tactical Technology Collective & Front Line Defenders, *Security in a box. Caja de herramientas de Seguridad protegiendo tu privacidad digital*, Sesión 7 "Mantener privada tu comunicación en Internet", Sesión 10 "Utilizar los teléfonos móviles de la manera más segura posible" y Sesión 11 "Utilizar los teléfonos inteligentes de la manera más segura posible". *[RA10]*

Actividades

Actividad 1: Pensando las reglas para la comunicación.

Presentación y discusión en plenaria ***20 min***

Empezar la discusión con las siguientes preguntas:

¿Hay reglas dentro de la organización que explican cómo comunicar entre ustedes o con personas externas a la organización?

¿Cuáles son?

¿Qué ha funcionado y qué no?

En caso de que no haya reglas:

¿Cuáles podrían ser?

Presentar brevemente algunas buenas prácticas de comunicación y sondear si en la organización practican algunas de éstas:

a) *Capacidades y vulnerabilidades del sistema de comunicación*

b) *Medidas de seguridad con teléfonos fijos y celulares*

c) *Uso de códigos: riesgos y propuestas*

d) *Monitoreo de los viajes*

A partir de la presentación organizar un breve debate para ver evaluar si con base en su nivel de riesgo, vulnerabilidades y capacidades existe alguna medida que consideren factible adaptar a su contexto.

Consejos de facilitación:

- Evitar entrar mucho en detalles sobre la parte de seguridad digital y recordarles que existe la opción de una sesión especializada para aprender a "Mantener privada tu comunicación en Internet", "Utilizar los teléfonos móviles de la manera más segura posible" y "Utilizar los teléfonos inteligentes de la manera más segura posible *[ver Taller 3, Módulo B, Sesión 1]* de la *Caja de herramientas de Seguridad protegiendo tu privacidad digital*. En estas sesiones se puede ahondar sobre cuestiones técnicas y prácticas específicas.
- Es común que surja la pregunta de si vale la pena establecer lenguaje codificado. Nuestro rol facilitando no es aprobarlo o desaprobarlo, pero hacerles pensar en los pros y contras con algunos ejemplos. El uso de códigos puede funcionar bastante bien en organizaciones que se mantienen constantes con su personal y tienen tiempo para memorizarlos y volverlos parte de su rutina (siendo entonces utilizado en general y no solo en caso de emergencia). Por otro lado, hay que tener en cuenta que durante una emergencia las personas olvidan incluso cosas básicas por el nivel de estrés al que son expuestas. En el caso de otras organizaciones, en una emergencia otras reglas de seguridad relativas a los códigos y comunicación son ignoradas porque lo más importante desde su punto de vista es la claridad de la información y la resolución de la emergencia (es decir, usan códigos en su día a día, pero si hay una emergencia prefieren no usarlos).
- Recordar que estas medidas son solamente ejemplos y no soluciones automáticas. Por ende deberían ser balanceadas y valoradas respecto al nivel de riesgo de la organización y su realidad.
- Las personas participantes deberían acordar si consideran necesario y útil retomar más adelante las vulnerabilidades y medidas de seguridad identificadas para valorar si quieren completar la política de acceso a la información de la organización *[ver Taller 3, Módulo 3, Sesión 1]*. Se puede comenzar a rellenar el *Formato de política sobre manejo de información sensible [Anexo T3.MA.S4]* para que quede constancia de las conclusiones o acuerdos a los cuales lleguen las personas participantes.

Buenas prácticas en el manejo de información

Reuniones Seguras

20min

Objetivos específicos:

- Presentar buenas prácticas para realizar reuniones y/o asambleas más seguras para que las PDDH debatan y adapten dichas medidas a sus propios contextos y riesgo específico.
- Discutir los criterios que deberían de tener las medidas de seguridad de la organización para realizar reuniones y/o asambleas más seguras y prevenir la vigilancia.

Materiales

- Papelógrafo
- Plumones
- *Metaplán*
- Fotocopias con *Formato de política sobre manejo de información sensible [Anexo T3.MA.S4]*

Recursos adicionales y lecturas de apoyo:

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, cap. 1.8 y 1.11.
- Front Line Defenders, *Manual sobre seguridad. Pasos prácticos para defensores/as de derechos humanos en riesgo*, Apéndices 5, 6, 14 y 15. *[RA5]*
- Protection International, *Cuadernos de Protección Núm. 2 Vigilancia y contravigilancia para organizaciones defensoras de derechos humanos. [RA12]*
- Tactical Technology Collective & Front Line Defenders, *Security in a box. Caja de herramientas de Seguridad protegiendo tu privacidad digital. [RA10]*

Puntos clave:

- La gran mayoría de PDDH son vigilados de una u otra forma. Esto se debe asumir sin paranoia y pensando que existen medidas que pueden contrarrestar esa vigilancia o que pueden dificultar la obtención de información.
- Elementos que se deben considerar en reuniones y/o asambleas:

  a) Participantes y observadores

  b) El espacio y los objetos donde se pueden esconder dispositivos de espionaje como micrófonos y cámaras

  c) Los objetos que se traen

  d) Las actas y apuntes de la reunión o cualquier otra documentación audiovisual, escrita etc. de las reuniones

- Buenas prácticas en reuniones y/o asambleas:

  a) Para reuniones en las que se trata información sensible o confidencial escoger espacios con las condiciones físicas adecuadas y no usar siempre el mismo lugar de reunión: sin visibilidad desde fuera, no colinda con propiedades vecinas, no tiene conexiones eléctricas ni telefónicas, está pintado de blanco para facilitar la detección visual de cualquier aparato espía, tiene el mobiliario mínimo necesario, tiene un pizarrón para escribir sin tener que mencionar verbalmente nombres o información confidencial, control de acceso adecuado

  b) No llevar equipo electrónico a reuniones privadas ya que podrían tener colocada un sistema de escucha

  c) Apagar y quitar la batería durante reuniones privadas, tapar la cámara del celular y/o situar los teléfonos a lado de un radio con música encendida

  d) Establecer procedimientos para "limpiar" el espacio después de la reunión (papeles, pizarrón, etc.)

  e) Establecer filtros restringidos de acceso para asambleas, llevar un registro minucioso de participantes, pedir que si hay alguien en la asamblea que la gente no conoce se identifique (contravigilancia, tomarle fotos)

  f) Traer solo los medios indispensables y no portar información sensible que nos pueda poner en una posición de vulnerabilidad

  g) Guardar y transmitir las actas de manera segura

Actividades

Actividad 1.

Presentación y discusión en plenaria ***20 min***

Empezar la discusión con las siguientes preguntas:

¿Dónde se llevan a cabo las reuniones y/o asambleas?

¿Hay reglas sobre dónde se puede hacer una reunión, las personas participantes, objetos que se puede o no traer a la reunión y/o asambleas?

¿Han funcionado estas reglas y por qué?

Presentar:

a) Elementos que se deben considerar en reuniones o asambleas

b) Buenas prácticas en reuniones o asambleas

A partir de la presentación organizar un breve debate para ver evaluar si con base en su nivel de riesgo, vulnerabilidades y capacidades existe alguna medida que consideren factible adaptar a su contexto.

Consejos de facilitación:

- Empezar preguntando cuál es la práctica, si hay medidas que regulan esta práctica y si estas medidas les han funcionado. Si no hay reglas establecidas promover que las personas participantes den ejemplos de posibles reglas y que la persona que facilita complete con ejemplos de buenas prácticas.
- Recordar que estas medidas son solamente ejemplos y no soluciones automáticas. Por ende deberían ser balanceadas y valoradas respecto al nivel de riesgo de la organización y su realidad.
- Las personas participantes deberían acordar si consideran necesario y útil retomar más adelante las vulnerabilidades y medidas de seguridad identificadas para valorar si quieren completar la política de acceso a la información de la organización *[ver Taller 3, Módulo 3, Sesión 1]*. Se puede comenzar a rellenar el *Formato de política sobre manejo de información sensible [Anexo T3.MA.S4]* para que quede constancia de las conclusiones o acuerdos a los cuales lleguen las personas participantes.

Seguridad Digital

Seguridad Digital

45min por sesión

Objetivos específicos:

- *La Caja de herramientas* es un esfuerzo colaborativo desarrollado por el *Tactical Technology Collective* y *Front Line Defenders*. Fue creada para satisfacer las necesidades de seguridad digital y de privacidad de activistas y personas defensoras de derechos humanos.
- *La Caja de Herramientas* incluye una "Guía Paso a Paso" que aborda 11 temas de seguridad digital para responder a objetivos específicos (ver sesiones).
- La *Caja de Herramientas* proporciona una colección de "Guías Prácticas" cada una de las cuales incluye herramientas específicas de software gratuito o de código abierto, así como las instrucciones necesarias sobre cómo utilizar dichas herramientas para asegurar las computadoras de las PDDH, proteger su información o mantener la privacidad de sus comunicaciones por internet.

Recursos adicionales y lecturas de apoyo:

- Tactical Technology Collective & Front Line Defenders, *Security in a box. Caja de herramientas de Seguridad protegiendo tu privacidad digital* ***[RA10]***

Sesiones

La Caja de herramientas de Seguridad protegiendo tu privacidad digital se compone de las siguientes Sesiones (45 min por sesión):

1) Proteger tu computadora de software malicioso y piratas informáticos

2) Proteger tu información de amenazas físicas

3) Crear y mantener contraseñas seguras

4) Proteger los archivos sensibles en tu computadora

5) Recuperar información perdida

6) Destruir información sensible

7) Mantener privada tu comunicación en Internet

8) Mantenerse en el anonimato y evadir la censura en Internet

9) Protegerte a ti mismo y a tus datos cuando utilizas sitios de redes sociales

10) Utilizar los teléfonos móviles de la manera más segura posible

11) Utilizar los teléfonos inteligentes de la manera más segura posible

Materiales

- "Guía paso a paso" y "Guías Prácticas" de la *Caja de herramientas de Seguridad protegiendo tu privacidad digital* descargable en https://securityinabox.org/es
- "De preferencia se recomienda contar con computadoras con conexión a internet y teléfonos móviles para complementar prácticamente las sesiones.

Consejos de facilitación:

- A diferencia de los demás módulos en los 4 talleres de PBI, las actividades de la *Caja de herramientas de Seguridad protegiendo tu privacidad digital* fueron desarrolladas por el *Tactical Technology Collective* y *Front Line Defenders*. PBI recomienda utilizar este recurso con personas integrantes de la organización con base en sus necesidades específicas. Más que actividades, la *Caja de herramientas* se compone de una "Guía Paso a Paso" de 11 sesiones que se complementan con "Guías prácticas" para aprender a utilizar los programas sugeridos. A partir de las 11 sesiones la persona que facilita puede plantear distintas actividades según el perfil y necesidades de las PDDH participantes.

- Se pueden plantear incluso asesorías individuales a las personas que así lo requieran aunque es preferible involucrar a la mayor parte de integrantes de la organización pues esto siempre ayudará a consolidar las capacidades. Por ejemplo la mayoría de la gente puede estar interesada en las asesorías para "Utilizar los teléfonos móviles de la manera más segura posible" mientras que el número de personas que quiera aprender a "Recuperar información perdida" puede ser sólo el personal más relacionado con documentación en la organización.

- Las actividades se pueden trabajar a través de sesiones puntuales aisladas, sin embargo los autores del recurso recomiendan que en la medida de lo posible, las sesiones se sigan en orden para asegurar que se tienen cubiertos los aspectos más básicos de seguridad digital antes de pasar a los más avanzados.

- De preferencia se recomienda contar con computadoras con conexión a internet y teléfonos móviles para complementar de forma práctica las sesiones.

- La persona que facilita estas sesiones no tiene necesariamente que ser experta en programación ni cuestiones digitales. Sin embargo sí se requiere cierta familiaridad previa con el uso de las computadoras y con los recursos y programas de la *Caja de herramientas de Seguridad protegiendo tu privacidad digital*.

- No toda la gente tiene la misma destreza y práctica con la tecnología, por lo que la persona que facilita debe ser paciente para que durante las sesiones prácticas las PDDH vayan a su ritmo y utilicen por su cuenta los recursos digitales de tal manera que se vayan empoderando. Por lo anterior no sirve de mucho que la persona que facilita tome el ratón y el teclado para instalar y correr los programas en las computadoras si las PDDH no se apropian del proceso paulatinamente.

Taller 3

Anexos

Anexo T3 M2 S1

Criterios de Seguridad de la Información

Confidencialidad

Solo tiene acceso el personal autorizado.

Disponibilidad

La Información está disponible en cualquier momento.

Integridad

La Información no puede ser alterada
por parte de terceros no autorizados.

Autenticidad

Legitimidad de las fuentes de información.

Anexo T3 M2 S1b

Los pasos del Diagnóstico para la Seguridad de la Información

Análisis de CONTEXTO

Identificar y explicar las tendencias coyunturales que impactan la seguridad de la información. Analizar el marco legal. Identificar las amenazas latentes.

Mapa de la INFORMACION

Identificar la información sensible de la organización.
¿Dónde está? ¿Quién tiene acceso a ella?

Análisis de ACTORES

Identificar los actores que tienen interés en la información.
Evaluar sus capacidades para robarla, destruirla, realizar vigilancia, etc.

Análisis de INCIDENTES

Identificar y analizar los incidentes de seguridad relacionados con la protección de la información.

Análisis de CAPACIDADES y VULNERABILIDADES

Identificar las capacidades y vulnerabilidades de la organización y de sus integrantes relativas a la seguridad de la información. Priorizar las áreas que deberían ser fortalecidas y potenciar las capacidades.

Análisis de RIESGO

Evaluar la probabilidad de que se materialice alguna amenaza ligada a la seguridad de la información y su impacto.

Anexo T3 M2 S2

Tipología de las amenazas latentes relativas a la seguridad de la información

1 Amenazas de origen político

- Uso de informantes infiltrados
- Vigilancia con micrófonos y cámaras
- Intercepción de comunicaciones
- Robos disfrazados de atracos
- Allanamiento ilegal de la oficina
- Cateo legal de la oficina
- Robo de identidad / secuestro de cuenta/ contraseñas etc.
- Control de las computadoras (p.e. FinSpy)
- Escaneo y recopilación gruesa de metadatos sobre uso de internet

2 Amenazas físicas (fortuitas o asociadas al desgaste o daño de los dispositivos)

- Daño de los aparatos o dispositivos de al-macenamiento
- Pérdida de la informació

Anexo T3 M2 S3

Niveles de acceso a la información

ACUERDOS ENTRE LOS/LAS PARTICIPANTES

Niveles de acceso a la información

Confidencial	De acceso excesivamente restringido (por ejemplo solamente a cierto personal interno autorizado)	
Privado	¿De acceso controlado (por ejemplo accesible a todo el personal interno).	
Sensitivo	De acceso moderadamente controlado (por ejemplo accesible a personal interno y cierto personal externo autorizado).	
Público	De libre acceso (no confundir con que debe ser publicada, sino que no tiene restricción de accesos).	

Anexo T3 M2 S3b

Mapa de la información

Tipos de datos					
Dispositivo de almacenamiento ¿Disco duro, folder, archivero, etc?					
Ubicación ¿Dónde están guardadas, física o virtualmente?					
¿Quién puede tener acceso? (en la realidad, más allá de las normas)					
¿Nivel de información? Permisos otorgados	*Confidencial*				
	Privado				
	Sensitivo				
	Público				
Maestra o copia					
Amenazas latentes					

Anexo T3 M3 S1

Vulnerabilidades y Capacidades relativas a la seguridad de la información

Componentes de vulnerabilidades y capacidades para la seguridad de la información: barreras físicas y tecnológicas

Componentes	Información necesaria para la evaluación	¿Vulnerabilidad o Capacidad?
OFICINA ·BARRERAS FÍSICAS	¿Es fácil para alguien de fuera acceder a su oficina sin permiso? ¿Se pueden romper las ventanas o forzar la puerta? ¿Son su oficina, el personal y las pantallas de las computadoras visibles desde el exterior de las ventanas?	V o C
OFICINA BARRERAS TECNOLÓGICAS	¿Hay barreras tecnológicas para proteger la oficina?¿Tiene un sistema de alarma, y confía en las autoridades que responderán a la intrusión?	V o C
ESPACIO DE TRABAJO BARRERAS FÍSICAS	¿Hay alguien que pueda ver la pantalla de su ordenador mientras usted está trabajando en su escritorio? ¿Guarda información confidencial en lugares de acceso fácil en su entorno de trabajo? ¿Está su computadora bien fijado a su área de trabajo o puede moverse fácilmente? ¿Tienes un cable de seguridad para la laptop?	V o C
OFICINA BARRERAS TECNOLOGICAS	¿Hay alguien en la oficina que conozca su contraseña? ¿Restringe el acceso inmediato a su ordenador cuando usted no se encuentra en su escritorio u oficina?	V o C
DATOS	¿Se usan contraseñas para todos los dispositivos de almacenamiento de información sensible? ¿Quién conoce éstas contraseñas? ¿Tiene un almacenamiento seguro (p. ej., caja fuerte) para los documentos?	V o C

Anexo T3 M3 S1 Continuación

Vulnerabilidades y Capacidades relativas a la seguridad de la información

Componentes de vulnerabilidades y capacidades para la seguridad de la información: filtros de acceso y prácticas de trabajo		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
DIVISIÓN DE ESPACIOS	¿Están tus oficinas abiertas al público? ¿Existen áreas reservadas únicamente al personal?	**V o C**
ADMISIÓN DE VISITANTES	¿Debes tratar con desconocidos que acuden a tus oficinas? ¿Tiene una "sala de espera" o área de recepción donde pueda cuestionar al visitante antes de que entre en la oficina principal? ¿Se admiten trabajadores sin presencia del personal de confianza?	**V o C**
MANEJO DE LAS LLAVES	¿Cuántas copias de llaves de su oficina existen y quién las tiene? ¿Existe un registro? ¿Quién puede realizar copias de las llaves? ¿Se cambian las chapas cuando hay llaves perdidas?	**V o C**
SELECCIÓN DEL PERSONAL	¿Existe un proceso de selección del personal que contemple niveles de confianza? ¿Se revisan los antecedentes y se piden recomendaciones antes de emplear el nuevo personal? ¿Hay un monitoreo de las actividades y funciones?	**V o C**
ACCESO A LA FOTOCOPIADORA	¿Dónde está la fotocopiadora? ¿Quién puede sacar copias? ¿Podría un intruso sacar copias de documentos sensibles sin que el personal se dé cuenta?	**V o C**
PERSONAL DE LIMPIEZA	¿Qué nivel de confianza le merece el personal de limpieza y qué nivel de acceso tiene este a los documentos de trabajo? ¿El personal de limpieza tiene las llaves? ¿Tienen acceso a las oficinas cuando no hay personal de confianza?	

Anexo T3 M3 S1 Continuación

Vulnerabilidades y Capacidades relativas a la seguridad de la información

Componentes de vulnerabilidades y capacidades para la seguridad de la información: protección ante los daños físicos		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
EDIFICIO Y RIESGOS NATURALES	Susceptibilidad de accidentes o riesgos naturales: incendios, inundaciones graves, deslizamientos de tierra, huracán, terremoto, etc.	**V o C**
APARATOS RIESGOS NATURALES	¿Los aparatos electrónicos están sometidos a variaciones de corriente? ¿Están expuestos al polvo o a la humedad?	**V o C**
ALTERACIÓN FÍSICA DE LA RED O DE LOS APARATOS	¿Por dónde pasan los cables de red? ¿Los cables del teléfono? ¿Se tiene acceso a los cables fuera de la oficina? ¿Los dispositivos de red como servidores, enrutadores, y módems están en lugares seguros? ¿Los visitantes tienen acceso a éstos dispositivos? ¿Las torres de las computadoras están cerradas o es posible alterar el hardware interno?	**V o C**

Anexo T3 M3 S1 Continuación

Vulnerabilidades y Capacidades relativas a la seguridad de la información

Componentes de vulnerabilidades y capacidades para la seguridad de la información: destrucción de la información sensible y respaldo		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
DESHACERSE DE LOS ARCHIVOS PAPEL	¿Se deshace de la basura de manera que sería imposible que alguien de fuera pudiese buscar o acceder a ella? En este sentido, ¿cómo se deshace de los documentos confidenciales? ¿Tiene un método seguro de destrucción (p. ej., trituradora) de los documentos confidenciales?	**V o C**
POLÍTICA DE RESPALDO	¿Cuál sería el costo en caso de pérdida de la información? ¿Existen respaldos? ¿Están los respaldos guardados en lugares seguros? ¿Hay una política de respaldo con plazos y responsables?	**V o C**

Anexo T3 M3 S1 Continuación

Vulnerabilidades y Capacidades relativas a la seguridad de la información

Componentes de vulnerabilidades y capacidades para la seguridad de la información: control de las comunicaciones		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
SISTEMA DE COMUNICACIÓN	¿Disponen las PDDH de un buen sistema de comunicación? ¿Funciona correctamente en todo momento? ¿Podrían los actores amenazadores cortarlos antes de un posible ataque? ¿El sistema permite monitorear los equipos en el terreno? ¿Cuenta con cobertura en áreas de riesgos? ¿Está siempre disponible para contactos de emergencia? ¿Las PDDH siempre tienen acceso a los recursos necesarios para su funcionamiento (batería, cargador, crédito)?	**V o C**
CELULARES	En caso de pérdida/ robo de celular ¿cuál sería el impacto para la seguridad de la información? ¿Se transmite información sensible por celular? ¿Existen respaldos de los contactos fuera del celular? ¿El celular tiene activo la contraseña y el bloqueo de pantalla?	**V o C**
USO DE CÓDIGOS	¿Los integrantes usan códigos para sus comunicaciones? ¿Este sistema permite transmitir la información necesaria de manera clara? ¿Los códigos usados pueden llamar la atención o son metáforas de la vida cotidiana?	**V o C**
MONITOREO DE LOS VIAJES	¿Las PDDH cuentan con un sistema para reportarse cuando viajan en zonas de riesgo? ¿Existen procedimientos establecidos para reportarse?	**V o C**

Anexo T3 M3 S1 Continuación

Vulnerabilidades y Capacidades relativas a la seguridad de la información

Componentes de vulnerabilidades y capacidades para la seguridad de la información: reuniones seguras		
Componentes	**Información necesaria para la evaluación**	**¿Vulnerabilidad o Capacidad?**
ESPACIOS DE REUNIONES	¿Se cambia el espacio de reuniones? ¿El espacio de reunión es conocido por gente externa a la Organización? ¿Se usan espacios seguros?	**V o C**
PARTICIPANTES	¿Participa únicamente el personal autorizado? ¿Pueden visitantes acceder al lugar de reunión? ¿Pueden observar / escuchar gente ajena?	**V o C**
MATERIAL	¿Se traen celulares en los lugares de reunión? ¿El acceso a los apuntes y documentos que se usan durante las reuniones está restringido? ¿Se limpia el espacio después de la reunión (apuntes en el pizarrón, papeles)?	**V o C**

Anexo T3 MA S1

Los pasos de la información

Paso 1

Contacto con la información/informante (fuente)

Paso 2

Almacenamiento y procesamiento de la información

Paso 3

Transmisión de la información

Paso 4

Difusión pública de la información

Anexo T3 MA S1b

Buenas prácticas relativas al manejo de la información

Anexo T3 MA S2

Filtros de Acceso

Representar:

- Barreras físicas (Candados, rejas, cerraduras y nivel de seguridad de los mismos)
- Barreras tecnológicas (Sistemas de alarmas, contra-señas, etc.)
- Prácticas de trabajo (política de uso de llaves, acceso a personal de confianza, uso de trituradora de papel para documentos, política de tratamiento de papeles de basura)

Anexo T3 MA S2b

Formato de pendientes sobre seguridad física

ACUERDOS ENTRE LOS/LAS PARTICIPANTES			
Ámbito	**Herramientas y Medidas de Seguridad**	**Responsabilidades y espacios**	**Recursos y / o asesoría**
Barreras físicas y tecnológicas	Barreras	Responsable Plazo de implementación:	
Política de acceso y atención al público (incluyendo manejo de las llaves)	Normas	Responsable Plazo de implementación:	
Protección física de los aparatos		Responsable: Plazo de implementación:	

Anexo T3 MA S3

Formato de Política de Respaldo

FORMATO DE POLÍTICA DE RESPALDO

	¿Quién?	¿Cuándo?	¿Qué?	¿Cómo?	¿Dónde?
Ejemplo	Directora de comunicacio-nes	1er día del mes, cada 2 meses	Base de datos y de contactos	Disco externo cifrado TrueCrypt	Caja segura casa
			Comunicados	Servidor seguro	Fuera del país
			Contenido de la página web	Thunderbird GPG	Oficina

Anexo T3 MA S4

Formato de política sobre manejo de información sensible

ACUERDOS ENTRE LOS/LAS PARTICIPANTES			
Ámbito	**Herramientas y Medidas de Seguridad**	**Responsabilidades y espacios**	**Recursos y / o asesoría**
Barreras físicas y tecnológicas		Responsable Plazo de implementación:	
Transmisión y almacenamiento de información sensible **(charlas, celulares, viajar con datos, etc.)**		Responsable Plazo de implementación:	
Monitoreo de los viajes		Responsable: Plazo de implementación:	

Taller 4
Generando estrategias de incidencia que coadyuven a la seguridad de la organización

Este taller surge de las necesidades del acompañamiento internacional a organizaciones locales en México. Inicialmente fue pensado para que PBI y las PDDH acompañadas pudieran coordinar y acordar sus estrategias de incidencia con el fin de maximizar la protección que brinda el acompañamiento de PBI. Sin embargo puede funcionar a otras ONGs que quieran desarrollar estrategias de incidencia. El taller facilita algunas herramientas de análisis basadas en mapeo de actores e identificación de pistas de influencia para diseñar una estrategia de incidencia. El taller plantea que la incidencia política incluya la estrategia de seguridad al intentar influenciar potenciales agresores o responsables de la protección de las personas defensoras. A pesar de lo anterior, las herramientas compartidas en el taller no se restringen exclusivamente al ámbito de seguridad y protección sino que abordan estrategias más amplias del trabajo político de las PDDH.

Objetivos generales del taller y resultados esperados:

- Compartir experiencias e identificar buenas prácticas de incidencia
- Compartir una metodología para desarrollar estrategias de incidencia basada en mapeos de actores e identificación de pistas de influencia
- Proporcionar un espacio en el cual la organización peticionaria sienta las bases para formular su propia estrategia de incidencia
- Identificar los actores más relevantes para el fortalecimiento político, técnico y de seguridad de la organización a nivel nacional e internacional
- Adicionalmente y de manera opcional se puede dar el taller con el objetivo de establecer la base de una incidencia coordinada entre la organización facilitadora y la organización peticionaria

Lo que el taller NO pretende:

- Asesorar o proponer a la organización sus estrategias internas
- Emitir valoraciones sobre las estrategias de las organizaciones
- Evaluar estrategias de incidencia
- Suplantar las estrategias de incidencia de la organización participante

Plan General del Taller:

Módulo 1: Bienvenida e introducción

Sesión 1 Presentación, expectativas, revisión de agenda y acuerdos de convivencia

Sesión 2 ¿Qué es incidencia?

Módulo 2: Intercambio de experiencias generales de incidencia

Sesión 1 Estrategias de incidencia exitosas y no exitosas

Módulo 3: Mapeo de Actores Políticos

Sesión 1 Mapeo de Actores Políticos para la incidencia

Módulo 4: Estrategias de incidencia

Sesión 1 Cómo identificar y trabajar pistas de influencia

Sesión 2 Identificación y priorización de actores para una estrategia de incidencia coordinada (opcional*)

Módulo 5: Discurso y Mensaje

Sesión 1 Reuniones con actores de incidencia

Módulo 6: Conclusión y cierre

Sesión 1 Seguimiento, compromisos y cierre

Duración total

***8 horas** (sin contar pausas).*

Calendarización

Considerar dar el taller en un día y medio si se incluye la sesión opcional del Módulo 4 para desarrollar una estrategia coordinada de incidencia. Contar al menos 2 horas de pausa en un día repartidas a lo largo del día.

*Atención Sesión Opcional: Esta sesión se da exclusivamente si se busca desarrollar una estrategia coordinada de incidencia entre la organización encargada de la facilitación y la organización participante.

Material y recursos:

- Hojas blancas
- Plumones
- Papelógrafos
- Una manta pegajosa o una superficie amplia y visible para todo el grupo que pueda servir de *Metaplán*
- Cartulinas de colores
- Papelitos adheribles de colores
- Gafetes o etiquetas adhesivas
- Pizarrón
- Hilos de colores
- Papel *foamy* de colores
- Chinches
- Cinta adhesiva
- *Anexos Taller 4*
- *Método de gestión de seguridad [Anexo T1.M1.S1].*
- Lista de actores trabajada en el *Taller 2, Módulo 1, Sesión 2, Actividad 3*
- *Metaplán* con *Mapeo de Actores para incidencia [ver Anexo con ejemplo prediseñado T4.M3.S1b]*
- Fotocopias para llenar del *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b]*
- Computadora y proyector (opcional)

Consejos generales para este taller:

Si el taller busca únicamente brindar un espacio para compartir herramientas de protección e incidencia sin desarrollar una estrategia conjunta, el taller será más parecido a los talleres previos. En este caso no se lleva a cabo la Sesión 2 del Módulo 4.

Si se busca desarrollar una estrategia coordinada (ver sesión opcional en Módulo 4) es aún más importante la reunión previa entre la persona que facilita y la organización peticionaria para aclarar las expectativas y compromisos mínimos entre ambas partes. De esta manera se podrá definir mejor el tipo de colaboración que se tendrá (cómo y hasta dónde se coordinará, criterios de comunicación, criterios de trabajo en común, etc.). Es importante poder definir de antemano ejemplos y contactos sobre los cuales las personas participantes quisieran trabajar, de esta manera la sesión opcional adicional tendrá mejores bases.

Para este taller se puede también considerar incluir más contenido relativo al funcionamiento de algunos actores específicos (órganos de derechos humanos de la ONU o del Sistema Interamericano por ejemplo) o la aplicación del derecho internacional de los derechos humanos (convenios, textos no vinculantes como las Directrices de la UE para PDDH o la Declaración sobre PDDH de la ONU, leyes nacionales como la Ley de Protección para Periodistas y Personas de Defensoras de Derechos Humanos en México por ejemplo).

Es importante en este taller que no se salten pasos. Es común que las organizaciones quieran por ejemplo pensar en mensaje antes de terminar el mapeo y empezar a desarrollar inmediatamente las estrategias (una precipitación que debemos evitar a toda costa). La persona que facilita debe tener en todo momento perspectiva sobre los objetivos y secuencia de las sesiones ya que comenzar a hacer una estrategia sin los pasos previos propuestos por el taller no tiene sentido. También es fundamental que cada módulo se haga por separado y entero; es el secreto para que la estrategia quede bien definida y que este taller sea realmente útil para las personas participantes.

Los casos ficticios presentados aquí son para explicar el enfoque y los pasos para las estrategias de incidencia. Lo ideal es que una vez que el grupo tenga esta claridad, trabajen sobre casos reales vinculados a su trabajo en la medida de lo posible; esto le dará mayor utilidad al resultado.

La persona que facilita debe estar preparada para preguntas sobre algunos actores concretos (cuerpo diplomático y actores internacionales por ejemplo) o algunos instrumentos internacionales (Directrices de la UE para PDDH por ejemplo). Suelen surgir esas preguntas durante la construcción de las estrategias a detalle.

Este taller es fácilmente adaptable a grupos de PDDH de distintas organizaciones que quieran desarrollar estrategias de incidencia coordinadas. En este caso, se debe cuidar aún más la confianza en el grupo y los procesos de establecimiento de alianzas durante los ejercicios. Puede servir agrupar a las organizaciones según los temas que estén trabajando o quieran trabajar de forma coordinada.

Bienvenida e introducción

Presentación, expectativas, revisión de agenda y acuerdos de convivencia

50min

Objetivos específicos:

- Conocerse entre participantes y facilitadores.
- Presentar donde se inserta este taller en el marco del PASP.
- Conocer qué esperan las personas participantes del taller y consensuar los objetivos del mismo.
- Clarificar el rol de la persona que facilita, sus posibilidades y limitaciones.
- Aclarar la metodología que se usará durante el taller.
- Sondear el conocimiento previo del grupo y ajustar taller si es necesario.
- Revisar la agenda con base en los puntos anteriores. Presentar las diferentes partes del taller y acordar tiempos y pausas.
- Acordar las normas de convivencia que servirán de base para generar un espacio seguro desde la perspectiva psicosocial y garantizar condiciones de equidad durante todas las sesiones subsecuentes.
- Distribuir materiales complementarios y roles de apoyo para la facilitación.

Puntos clave:

- Generar una apertura del taller que facilite la confianza y conocimiento de todas las personas participantes.
- Subrayar que la persona que facilita está para catalizar la participación y que se está construyendo un espacio conjunto de conocimiento. Por ello la participación de todas las personas es crucial para el proceso.
- Recapitular la metodología y visión integral de la seguridad del PASP *[ver cap. 1 y 2 de esta guía]*
- Clarificar cómo la incidencia se inserta en el proceso de seguridad para ampliar el espacio de actuación.
- Enfatizar el papel de las estrategias de incidencia en el marco de una estrategia más amplia de seguridad y protección de la organización. *[ver cap. 1 sección 1 de esta guía]*
- Si el taller busca desarrollar una estrategia coordinada de incidencia:

  a) Explicar que el Taller de Incidencia tiene como objetivos compartir experiencias de incidencia entre ambas organizaciones, facilitar una herramienta de análisis basada en el mapeo de actores y de pistas de influencia, así como establecer las bases para que se pueda diseñar en conjunto una estrategia con la organización.

  b) Proponer una definición de "Estrategia de Incidencia Coordinada", por ejemplo: *es la base de cómo la organización acompañante y la organización acompañada trabajarán conjuntamente para fortalecer las redes de contactos políticos, técnicos y de seguridad que contribuirán a que la organización acompañada lleve a cabo su trabajo a favor de los derechos humanos con mayor impacto. La estrategia conlleva una priorización de contactos, es flexible y se condiciona por las capacidades de ambas organizaciones*. Esta definición puede ser adaptada y consensuada para reflejar adecuadamente la relación específica con la organización que participa en el taller.
- Consensuar normas de convivencia que promuevan las condiciones necesarias de respeto, diálogo e inclusión durante todo el taller. La persona que facilita debe estar segura que toda la gente se siente cómoda con los acuerdos alcanzados.

Materiales

- Papelógrafo
- Plumones
- Fotocopias con objetivos y agenda del taller
- Papelógrafo o diapositivas con los *Componentes analíticos necesarios para un esquema integral de seguridad y protección [Gráfico 1e, cap. 1], Ampliando el espacio de actuación [Gráfico 1a, cap. 1]* y con el gráfico del *Método de gestión de seguridad [Anexo T1.M1.S1]*
- Papelitos adheribles de colores
- Gafetes o etiquetas adhesivas
- Computadora y proyector (opcional solo en caso que la actividad 3 no se lleve a cabo con papelógrafo o pizarrón)

Recursos adicionales y lecturas de apoyo:

Para distintas dinámicas de presentación e integración grupal y distención.

- BERISTAIN & SORIANO, *La Alternativa del Juego I. Juegos y Dinámicas de Educación para la Paz*. ***[RA1]***

Para comenzar adecuadamente con la construcción de un espacio seguro en un trabajo grupal sobre seguridad con PDDH.

- BARRY & NANIAR. *Integrated Security the Manual*, cap. 1.2, 1.3 y 3.4. ***[RA4]***

Para entender los conceptos de seguridad y protección.

- Capítulo 1 de esta Guía.

Para entender el PASP, sus criterios y marco conceptual básico.

- Capítulo 2 de esta Guía

Actividades

Actividad 1: Ronda de presentación y expectativas del grupo.

Dinámica de presentación y discusión en plenaria 10 min

Abrir con una ronda de presentación. Independientemente de la dinámica de presentación utilizada es importante que las personas participantes comuniquen si ya han recibido talleres previos relacionados con este tema, y qué esperan del taller.

Se pueden apuntar motivaciones y expectativas en papelitos adheribles de colores para agruparlos en un lugar visible durante todo el taller. Estas expectativas se retomaran más adelante y al final del taller se revisarán para evaluar qué hemos cumplido y qué no.

Actividad 2: Recapitulación del PASP.

Presentación oral con apoyo de elementos visuales (se puede usar papelógrafo, pizarrón o diapositivas en power point) 15 min

Presentar de forma concisa en qué consiste el PASP, sus criterios y metodología. Enmarcar este taller dentro del PASP y las estrategias de seguridad y protección más amplias. Bosquejar visualmente las tres dimensiones conceptuales que sustentan el programa de asesorías y los conceptos de seguridad y protección. *[ver definiciones conceptuales y gráficas de cap. 1 sección 1 y gráficos sobre estructura del PASP en cap. 2 sección 3 y 4 de esta guía]*

Explicar que el Taller 4 se basa en el diagnóstico del método de gestión de la seguridad usado por PBI y trabajado durante el Taller 1 y 2. *[Anexo T1.M1.S1]* Especificar que además el Taller 4 complementa las estrategias de seguridad y protección con herramientas y buenas prácticas de incidencia para expandir el espacio de actuación de las PDDH *[ver Gráfico 1a sobre el Espacio de Actuación en cap. 1 sección 1 de esta guía]*

Actividad 3: Revisión de expectativas y adaptación de agenda y contenidos del taller en caso de ser necesario.

Discusión en plenaria 15 min

Presentar los objetivos y contenidos del taller consensuados previamente con la organización. Revisar junto con el grupo las expectativas expresadas en relación con los objetivos y la metodología del taller presentadas.

A partir de una perspectiva realista de las limitaciones en términos de tiempo, objetivos y contenidos del taller así como de las expectativas previamente expresadas por las PDDH, explicar lo que podemos hacer en este taller y lo que no es posible o que puede ser abordado sólo en talleres posteriores.

Realizar ajustes si es necesario.

Pegar la agenda general del taller consensuada en un papelógrafo a la vista de todas las personas participantes.

Actividad 4: Acuerdos de convivencia, distribución de material complementario y roles de apoyo.

Discusión en plenaria y/o dinámica participativa ***10 min***

Acordar en conjunto las normas de convivencia: cómo pedir la palabra, cómo expresar con respeto nuestros desacuerdos, cómo garantizar condiciones de igualdad, confidencialidad de los aspectos tratados durante el taller, uso de celulares, computadoras y cámaras, entradas y salidas de participantes, puntualidad, etc. *[ver apartado sobre espacios con equidad y espacios seguros desde la perspectiva psicosocial en el apartado 3.2 y recursos de apoyo RA4]* Se puede realizar la "Dinámica de la Estrella" usada previamente u otra distinta.

Después de las normas de convivencia se puede entregar material complementario (por ejemplo. un cuaderno del participante). Pedimos que no se lea inmediatamente ya que este se trabajará a lo largo del taller.

Dejar claro el rol de la persona que facilita y sus posibles limitaciones.

Distribuir roles de apoyo a la facilitación, preguntar a las personas participantes quién quiere ser voluntario/a para tomar actas y apuntar los consensos, para anotar otros pendientes y tareas que surjan durante el taller.

Consejos de facilitación:

- Se pueden utilizar distintas dinámicas de presentación para "despertar" o despabilar al grupo *[ver RA1]*. Si el grupo es numeroso y no se conocían previamente, también se pueden usar gafetes o adhesivos con el nombre de las personas para facilitar dirigirse a las personas por su nombre de pila y recordar los nombres.
- En las partes con mayor carga conceptual se recomienda aprovechar al máximo los recursos gráficos propuestos. Se recomienda escribir de antemano las definiciones en papelógrafos o diapositivas a la vista de todo el grupo.
- Con base en la actividad 1 y 3, puede ser necesario bajar las expectativas o ajustar la agenda para dedicar más tiempo a algunos temas, quitar otros etc. ¡Hay que ser flexibles y receptivos a la hora de tratar las expectativas del taller e ideas sobre seguridad y protección!
- Se puede consensuar un espacio para dejar los aparatos electrónicos como celulares y computadoras durante el taller (por ejemplo en la esquina de la sala o en una bolsa resguardada). Se puede consensuar cómo retribuirá al grupo alguien que llegue tarde a las sesiones o que pase por alto algún acuerdo de convivencia (por ejemplo puede traer dulces para todas las personas la siguiente sesión, o relevar al relator de acuerdos).
- ¡Atención con el control del tiempo! Este módulo es susceptible a extenderse demasiado.

Bienvenida e introducción

¿Qué es incidencia?

20min

Objetivos específicos:

- Definir incidencia.
- Llegar a un entendimiento común sobre qué es incidencia.
- Vislumbrar la relación entre el trabajo cotidiano de las organizaciones con las que se trabaja y las actividades de incidencia que ya llevan a cabo.

Materiales

- Pizarrón
- Papelógrafo
- Plumones
- Papelógrafos o diapositivas preparadas de antemano con las definiciones de incidencia (ver puntos clave del taller)

Recursos adicionales y lecturas de apoyo:

- Oficina en Washington para Asuntos Latinoamericanos (WOLA), *Manual básico para la incidencia política*, pp.6-12.
- Centro para el Diálogo Humanitario, *Presencia proactiva Estrategias de terreno campo para la protección de la población civil.* ***[RA13]***

Puntos clave:

- La incidencia es un *proceso llevado a cabo por un individuo o un grupo con el objetivo de influenciar el comportamiento o decisiones de otra persona o grupo de personas.*
- La incidencia política consiste en: un *cúmulo de actividades dirigidas a ganar acceso y generar influencia sobre actores que tienen poder de decisión en asuntos de importancia para un grupo en particular o para la sociedad en general.*
- Remarcar que la incidencia busca un cambio de comportamiento de actores clave.
- La incidencia social y política es un ejercicio de participación democrática y un derecho por parte de la ciudadanía frente a las decisiones del gobierno y sus administraciones. La incidencia necesariamente implica mayor rendición de cuentas
- La incidencia no se refiere únicamente a dialogar con autoridades.
- Recordar que todas las organizaciones de derechos humanos de una manera u otra realizan labores de incidencia.
- Realizar actividades de incidencia implica una transformación de las relaciones de poder para incluir las perspectivas e intereses de actores que podrían estar marginados del poder político formal. Por ello la incidencia puede ser útil para revertir inequidades de género o promover la influencia de grupos que han sido tradicionalmente ignorados por las autoridades políticas u otros actores con poder.
- Las estrategias de incidencia pueden tener diferentes métodos y mensajes. El método es la forma en la cual comunicamos nuestro mensaje. El mensaje es lo que queremos transmitir a nuestro público meta. Por eso, una reunión con una autoridad es un método de transmitir un mensaje, al igual que un comunicado, una rueda de prensa o una manifestación.

Actividades

Actividad 1: Lo que entendemos por "Incidencia".

Lluvia de ideas y discusión en plenaria a partir de preguntas detonadoras

20 min

Plantear al grupo las siguiente pregunta:

¿Qué entendemos por incidencia?

Apuntar las palabras y conceptos usados por las PDDH en un papelógrafo plenamente visible.

Se presenta la definición de Incidencia después de la lluvia de ideas. Se plantea ahora la siguiente pregunta:

¿Cuáles son las actividades de incidencia que lleva a cabo la organización?

Intentar sacar conclusiones, resumiendo las ideas.

Se refleja como la organización ya realiza sus propias estrategias de incidencia y que pueden ser de varios tipos.

Usar y hacer referencia a las palabras y conceptos de las PDDH retomándolos durante las fases subsecuentes del taller.

Consejos de facilitación:

- Aquí lo más importante no es la definición inicial de incidencia, que incluso podría ser otra si así se decidiera en conjunto con la organización. Lo importante es que quede claro que queremos influir en el comportamiento de un actor con capacidad de resolver nuestro problema o afectarnos. Para influir no lo debemos de hacer necesariamente a través de reuniones o de acciones directas sino que podemos usar otras estrategias, algunas indirectas.
- ¡Cuidado! No pretender enseñar a la organización a hacer incidencia (que no se interprete así). Las organizaciones de derechos humanos ya tienen sus estrategias y lo que queremos es proponer algunas herramientas que se pueden utilizar para mejorar la planeación de dichas estrategias e intersectarlas con la dimensión de seguridad.
- Muchas organizaciones tienen reticencias para dialogar con las autoridades. Hay que dejar claro que la incidencia no solo significa dialogar con autoridades sino que va más allá. Puede ser importante diferenciar entre el mensaje y el método dentro de la estrategia de incidencia para mostrar que una reunión con autoridades es simplemente uno de los métodos.
- Se pueden retomar ejemplos del trabajo que ya hace la organización. Se puede preguntar a la organización si ciertos ejemplos son incidencia o no (una manifestación, una carta pública, una rueda de prensa, etc.).

Intercambio de Experiencias Generales de Incidencia

Estrategias de incidencia exitosas y no exitosas

45min

Objetivos específicos:

- Compartir y rescatar experiencias de buenas prácticas de incidencia.
- Analizar si las estrategias de incidencia utilizadas por las PDDH han funcionado y por qué.
- Identificar cuáles son los elementos que permitieron que una estrategia de incidencia fuera exitosa o que hicieron que una estrategia no funcionara.

Materiales

- Papelógrafos
- Plumones
- Papelógrafos o diapositivas con *Ejemplo de estrategia de incidencia para análisis [Anexo T4.M2.S1].*
- Fotocopias con *Experiencias e ideas para redes de apoyo y estrategias de incidencia en DDHH [Anexo T4.M2.S1b]*

Recursos adicionales y lecturas de apoyo:

- CONECTAS Derechos Humanos, *Política Exterior y Derechos Humanos: Estrategias para la acción de la sociedad civil. [RA13]*
- New tactics in Human Rights, "Powerful Persuasion: Combating Traditional Practices that Violate Human Rights".
- New tactics in Human Rights, "8 Powerful Persuasion Tactics". *[RA13]*

Puntos clave:

- Pensar en cómo adaptar estrategias de incidencia que han funcionado al contexto específico de las personas con las que trabajamos.
- Mostrar que estos ejercicios pueden ser útiles para replicar buenas estrategias o repensar aquellas que no lo fueron tanto.

Actividades

Actividad 1: Lo que nos ha funcionado en estrategias de incidencia.

Trabajo en grupos* *30 min

Dividir a las personas en grupos de 3 a 5 personas. Cada grupo tiene que preparar un papelógrafo, identificando una estrategia de incidencia en su experiencia que funcionó y una que no funcionó, respondiendo a las siguientes preguntas:

¿Cuál fue el objetivo de incidencia?

¿Qué cambios buscaron?

¿Quiénes fueron los blancos del incidencia? (Actores)

¿Por qué?

¿Quiénes fueron sus aliados?

¿Cuáles fueron los mensajes?

¿Cómo comunicaron los mensajes?

¿Cuál fue el resultado?

¿Por qué les parece exitoso o fallido el ejemplo?

Actividad 2: Buenas prácticas de incidencia.

Discusión en plenaria* *15 min

En plenaria, cada grupo presenta las buenas y malas prácticas de incidencia que identificaron a través del caso analizado en la actividad anterior.

La persona que facilita puede añadir o completar con otros ejemplos relevantes.

Consejos de facilitación:

- Actividad 1: Para agilizar la actividad y que el ejercicio quede más claro, se pueden brindar ejemplos como el *Ejemplo de estrategia de incidencia para análisis [Anexo T4.M2.S1].* También se pueden recortar fotocopias de antemano del anexo *Experiencias e ideas para redes de apoyo y estrategias de incidencia en DDHH [Anexo T4.M2.S1b]* para hacer "tarjetas" que la gente puede ir intercambiando o pasando. Los recursos de *New tactics in Human Rights [RA13]* También ofrecen ejemplos de tácticas de incidencia para detonar el debate.
- Otra opción para la Actividad 1 es que la persona que facilita proponga un ejemplo negativo y positivo en plenaria antes del trabajo en grupos.
- Actividad 2: Es importante que se guíen por las preguntas indicadas y que no pierdan tiempo debatiendo el caso en sí, sino más bien discutiendo qué hizo que la experiencia fuese exitosa o no. Lo que debe recogerse en el papelógrafo y compartirse en plenaria son las buenas prácticas o los aprendizajes a partir de las malas y no el recuento del caso ni las respuestas detalladas de las preguntas.
- Puede ser que el tiempo no alcance a todos los grupos para hacer la buena y la mala experiencia. Una idea es pedir que unos grupos se dediquen a la buena y otros a la mala experiencia.
- Para la actividad 2, es necesario que previo al taller se preparen algunos ejemplos que pueden estar basados en la experiencia de su propia organización. Lo anterior con el fin de poder detonar algunos debates o mostrar formas en las que algunas organizaciones abordaron sus estrategias de incidencia. Esto se puede hacer de diferentes maneras:

  a) Con mini-estudios de caso, rescatando las principales buenas prácticas de esa estrategia. Para ideas sobre cómo estructurar los ejemplos prácticos de incidencia *[ver CONECTAS Derechos Humanos, Política Exterior y Derechos Humanos: Estrategias para la acción de la sociedad civil. RA13].*

  b) Con consejos, observaciones y ejemplos aplicados para guiar este intercambio. *[ver Anexo T4.M2.S1b]* Experiencias e ideas para redes de apoyo y estrategias de incidencia en DDHH. Esta lista propuesta en el anexo es sólo un detonador de las discusiones, no es exhaustiva y está lejos de ser acabada. Este anexo no pretende "enseñar" buenas prácticas sino "compartir" experiencias e ideas que puedan ser adaptadas a las necesidades de las PDDH y enriquecidas por sus propias experiencias y buenas prácticas.

Mapeo de Actores Políticos

Mapeo de Actores Políticos para la incidencia

60min

Puntos clave:

- Los mapeos deben de responder a un objetivo específico. Es importante distinguir entre la estrategia global y los objetivos específicos.
- El objetivo específico debe buscar cambiar la actuación de un actor en particular; la incidencia será de cierta forma un juego de poder y necesitaremos ejercer presión sobre el actor con poder de cambio.
- Lo que vamos a explicar es solamente una forma de generar estrategias de incidencia basada en mapeo de actores y pistas de influencia. Es decir, compartiremos una metodología que puede ser útil, pero hay otras formas de desarrollar estrategias de incidencia.
- Los actores siempre deben ser relevantes para el objetivo de incidencia en sí.
- Funciona para objetivos específicos y no es muy funcional para estrategias más amplias. Es importante recordar que hay que determinar pasos y objetivos específicos para poder generar estrategias que sean lo más atinadas posibles.
- Recordar que el Mapeo de Actores es una herramienta que puede ser realizada de diferentes maneras. En la forma que proponemos, sólo identificamos los principales actores, aquellos que tienen la capacidad de incidir en la resolución del problema (objetivo específico).
- Los Pasos del Mapeo de actores para una estrategia de incidencia son:

  1) *Elegir el problema sobre el que queremos incidir*: el proceso de planificación para la incidencia política empieza con la identificación y priorización de un problema que afecta a las PDDH en forma concreta.

  2) *Definir el objetivo específico/preciso de incidencia:* A partir de la priorización de un problema se debe pensar en un objetivo específico que brinde una solución a nuestro problema. El problema puede ser resuelto teniendo como objetivo acciones o cambios concretos que queremos lograr a través de acciones de los actores (regularmente gobierno).

  3) *Identificar a los actores clave que tienen influencia sobre o son influenciados por este problema*: En los actores clave se debería incluir actores que tengan alguna responsabilidad directa sobre la amenaza o el problema, también se pueden incluir actores que puedan tener influencia sobre los actores principales (por ejemplo una autoridad con el poder de frenar a los perpetradores o de pedir a los responsables que resuelvan el problema) y por último otros actores que puedan ser aliados de las PDDH directamente afectadas por la problemática que puedan apoyar. No es un mapeo extenso, sino un mapeo específico de los actores clave.

  4) *Analizar a los actores:* Para analizar a los actores se deben anotar las características e intereses más relevantes en la cartulina del actor. En particular: la función de este actor en el conflicto, sus intereses y objetivos y la influencia real o potencial que tiene sobre el problema Para ello se pueden responder las siguientes preguntas:
  ¿Cuál es la función de este actor en el conflicto? ¿Qué queremos que este actor cambie o realice? ¿A quién escucha? ¿Quiénes son sus aliados/partido etc.? ¿A quién le hace caso? ¿Es un agresor? ¿Es un facilitador? ¿Es un obstáculo? ¿Es un aliado potencial? ¿Cuáles son sus intereses y objetivos? ¿Por qué actúa de esa manera? ¿Cuál es su influencia real o potencial sobre el problema? ¿Su influencia es positiva o negativa? ¿Su influencia es fuerte o débil?

  5) *Comprender las relaciones clave entre actores:* Una vez que se hayan hecho varias "cartas de actores", se representan los vínculos entre actores a través de líneas o conexiones. Se debe reflexionar cuáles son las relaciones más importantes que debemos de caracterizar. Se coloca una carta de un color diferente entre dos actores y sobre esta carta se describen las relaciones en términos de su impacto en el problema y la capacidad de la organización a la que pertenecemos para influir en este actor (positivo, negativo, aliados, enemigos, ambiguos, influencia alta/baja, etcétera). Este proceso de caracterizar las relaciones debería provocar debate entre el grupo.

Objetivos específicos:

- Compartir la herramienta del mapeo de actores para identificar blancos potenciales de una estrategia de incidencia.
- Proporcionar un espacio para que la organización participante comience un mapeo de los actores más relevantes para los casos o temas sobre los cuales quisiera incidir.

Materiales

- Papelógrafo
- Plumones
- *Metaplán*
- Rótulos o tarjetas de cartón o *foamy* de varios colores diferentes
- Fotocopias, papelógrafo o diapositivas con los *Pasos del Mapeo de actores para una estrategia de incidencia [ver Anexo T4.M3.S1]*.
- *Metaplán* con *Mapeo de Actores para incidencia [ver Anexo con ejemplo pre-diseñado T4.M3.S1b]*
- Cinta adhesiva
- Chinches

Recursos adicionales y lecturas de apoyo:

- Centro para el Diálogo Humanitario, *Presencia proactiva Estrategias de terreno campo para la protección de la población civil. [RA13]*

5) *Situar a nuestra organización en la representación:* Ubicar relacionalmente a nuestra organización respecto a aliados y otros actores no aliados. Para ello se representan los vínculos más importantes con los otros actores clave a través de líneas o conexiones. Se pueden describir las relaciones en cartas pegadas sobre las líneas o vínculos. Representar las relaciones entre nuestros aliados y sus relaciones con los actores clave: Ubicar a aliados locales, federales e internacionales, ONGs etc. y representar sus relaciones con otros actores clave en relación con la resolución del problema. Deben representarse junto con sus relaciones y esferas de influencia en la medida que puedan coadyuvar para lograr nuestro objetivo influyendo directa o indirectamente en los actores adversarios o aquellos de los cuales no estamos seguros si son aliados o no.

Actividades

Actividad 1: Presentación de Mapeo de actores para la incidencia (ejemplo).

Presentación* *15 min

Usando el *Metaplán* y un ejemplo ficticio la persona que facilita muestra cómo se abordan los *Pasos del Mapeo de actores para una estrategia de incidencia específica [ver Anexo T4.M3.S1]*. Se recomienda mostrar los pasos de forma práctica utilizando el ejemplo de *Metaplán* con *Mapeo de Actores para incidencia [Anexo prediseñado T4.M3.S1b]*. Utilizar rótulos o tarjetas de cartón o *foamy* de colores para los actores y sus características.

Junto con el grupo se elaborará un *Metaplán* que recrea el caso ficticio del "Preso Político Jaime Sierra" del anexo. Plantear que somos el "Comité Civil" con el objetivo de liberar al preso político (rótulo verde que se posicionará hasta el paso 6 descrito más abajo). El mapeo representa los actores y sus características (en tarjetas rosas en el ejemplo del anexo) y las características de las relaciones entre todos estos actores (en tiras de cartulina amarillas en el ejemplo del anexo).

Explicar que un mapeo pasa por los siguientes pasos (ver puntos clave para más detalle):

Paso 1 *Elegir el problema sobre el que queremos incidir* (en este caso Jaime Sierra está preso)

Paso 2 *Definir el objetivo específico/preciso de incidencia* (en este caso la liberación de Jaime Sierra).

Paso 3 *Identificar a los actores clave que tienen influencia sobre o son influenciados por este problema* (en este caso el Juez Miguelón tiene influencia para determinar la libertad de nuestro preso político, pero existen otros poderes formales como el Gobernador y otros fácticos como el "Cacique Benito" que también tienen influencia).

Paso 4 *Analizar a los actores* (analizamos cómo a partir de los intereses del Gobernador o del Juez Miguelón se puede abordar el problema).

Paso 5 *Comprender las relaciones clave entre actores* (en este caso se remarca

que existen relaciones de lealtad, alineación de intereses o de posible influencia entre actores por ejemplo la influencia del Gobernador respecto al juez).

Paso 6 *Situar a nuestra organización en la representación* (en este punto se inserta al "Comité Civil" que representamos y marcar sus principales conexiones con otros actores). Se pueden añadir o citar otros actores (la prensa, alguna empresa privada importante etc.) o reemplazar actores por otros (remplazar PBI por otras ONGs nacionales o internacionales por ejemplo).

Paso 7 *Representar las relaciones entre nuestros aliados y sus relaciones con los actores clave*. Se elaboran también las relaciones con nuestros aliados y actores clave para entender la posible ruta de influencia a través de las conexiones y características de nuestras relaciones con los demás actores (en este caso por ejemplo los actores internacionales podrían influir a través del Gobernador para presionar indirectamente en una aplicación efectiva de la justicia por parte del Juez Miguelón)

El mapeo se acaba aquí. No entramos en la estrategia en sí.

Actividad 2: Mapeo de actores para la incidencia de la organización participante.

Trabajo en grupos ***30 min***

Replicar el mapeo pero esta vez con casos y objetivos concretos de la organización participante. Para ello se seguirán los siguientes pasos:

En plenaria el grupo completo propone de 3 a 5 casos relevantes para la labor de incidencia de la organización. Por ahora sólo se definen las áreas de incidencia sin definir el objetivo específico de cada caso.

Dividir en grupos de 3 a 5 personas. Cada grupo trabajará una problemática con un objetivo concreto de incidencia.

Distribuir un papelógrafo y cartulinas de color a cada grupo (por ejemplo: verde para que representen su organización, rosas para representar a los demás actores y tiras amarillas para representar las relaciones entre los actores).

Pedir a cada grupo que trabaje un mapeo para uno de los casos definidos en plenaria. Para llevar a cabo el mapeo tendrán necesariamente que pasar por los *Pasos del Mapeo de actores para una estrategia de incidencia* *[ver Anexo T4.M3.S1]* se les puede facilitar la fotocopia de dicho anexo o dejar los pasos visibles en un papelógrafo o diapositiva.

Cada grupo seguirá los mismos 7 pasos que en el ejemplo de la actividad precedente pero ahora aplica los pasos a su caso.

La persona que facilita se pasea por los grupos para guiar los debates y la construcción del *Metaplán*. Se debe enfatizar que la elaboración de las tarjetas de colores y la preparación del mapeo se realizan de manera simultánea al debate. No es cuestión de debatir y luego hacer el mapeo. El mapeo en sí es la metodología para debatir, no el resultado del debate.

Actividad 3: Socialización y discusión del mapeo.

Discusión en plenaria ***15 min***

Pedir que cada grupo exponga muy rápidamente a los demás su mapeo de actores.

Favorecer la discusión y aporte de otras ideas por parte del grupo, especialmente sobre actores que consideran que deben ser agregados a los mapeos originales.

Consejos de facilitación:

- Es muy importante que el objetivo sea realmente concreto. Un objetivo general no funcionará y la estrategia al final será difícil de llevar a cabo y de medir. El mapeo debe elaborarse alrededor de un objetivo de incidencia particular y no del objetivo general de la organización.
- Lo importante en la Actividad 2 es que la organización elija para sus mapeos casos relevantes que están trabajando ahora y que este espacio pueda servir para su misma reflexión.
- Es fundamental que las personas participantes no se salten los pasos. Por el momento sólo buscamos identificar los actores. No buscamos definir aún las estrategias en sí o los mensajes y métodos. Si los grupos de trabajo se pierden hay que reenfocarlos al objetivo inicial de esta sesión.
- Para poder incidir tenemos que entender las características y los intereses de cada actor. Dichas características se pueden escribir bajo el nombre del actor.
- Para posicionar a los actores se sugiere el siguiente orden: a) identificar el actor o los actores que tienen responsabilidad sobre el problema, b) identificar los actores que tienen influencia sobre aquellos identificados (incluso si no son aliados de la organización) y c) identificar otros actores que pueden tener influencia sobre el problema o sobre los actores y que además sean aliados de la organización o compartan sus objetivos e intereses.

Estrategias de Incidencia

Cómo identificar y trabajar pistas de influencia

120min

Puntos clave:

- Los componentes básicos de una estrategia de incidencia son:

  1) *Una lista priorizada de objetivos y resultados deseados.*

  2) *Un plan de actividades* que nos lleva desde donde estamos hasta la consecución de los objetivos planteados teniendo en cuenta los recursos reales disponibles y todas las restricciones del contexto.

  3) *Una lógica clara* que vincula las actividades a objetivos intermediarios y a objetivos finales e identifica los indicadores para poder medir el éxito de nuestra estrategia.

- Para ser efectiva una estrategia de incidencia debe ser realista, tanto con los objetivos que se quieren lograr como con la inversión de recursos necesarios para lograrlos.
- Las pistas de influencia son las relaciones entre actores identificadas en el mapeo. Nos indican formas de influir sobre el actor cuya actuación queremos cambiar.
- El método es la forma que utilizaremos para enviar el mensaje que queremos al actor identificado.
- Los mensajes pueden ser de 3 tipos:

  1) *Mensajes indirectos o implícitos:* comunicaciones que son entendidas sin decirse explícitamente.

  2) *Mensajes directos pero no públicos*: conversaciones privadas pero honestas, generalmente advierten preocupaciones y posibles consecuencias.

  3) *Mensajes públicos*: aquellos que son difundidos ampliamente para toda audiencia.

- Lo importante en el mensaje es el contenido de lo que se quiere hacer llegar al actor objetivo, más allá de lo que se dice en sí (discurso).
- Enfatizar la importancia que de que se hagan evaluaciones de nuestras estrategias de incidencia y que se documente si el resultado se está logrando.
- Los indicadores miden si nuestra estrategia está funcionando y la necesidad o no de reestructurarla, pueden ser de tres tipos:

  1) I*ndicadores de proceso*: Reflejan el avance de las actividades implementadas para la incidencia (por ejemplo número de reuniones con autoridades logradas, cartas enviadas, etc.). Sirven para monitorear la consecución de las actividades que nos hemos fijado en la estrategia.

  2) I*ndicadores de progreso:* Son indicadores de resultados respecto a los cambios intermedios que esperamos antes de lograr el objetivo final. Estos indicadores verifican si algún cambio esperado ocurrió a partir de las actividades de incidencia realizadas (por ejemplo si a partir de las reuniones logradas los actores hicieron un pronunciamiento o presión esperada por nuestra estrategia). A partir de estos indicadores podemos entender mejor los avances y las brechas faltantes para llegar a nuestro objetivo final.

  3) *Indicadores de impacto*: Son indicadores de resultados de mayor plazo que miden el impacto de nuestras acciones respecto al objetivo final (por ejemplo que cambio logramos al final; liberar a Jaime Sierra o no).

- Los indicadores se miden de diversas maneras y una de ellas es ver el impacto de nuestras acciones a través de actos, información oficial y no oficial en distintas fuentes (prensa, declaraciones públicas, acciones legales, cambios en políticas públicas, legislaciones, etc.)
- Reconocer la dificultad de conseguir indicadores en el trabajo de incidencia.

Objetivos específicos:

- Compartir una metodología para elaborar una estrategia de incidencia basada en la identificación de blancos, pistas de influencia, métodos y mensajes.
- Proporcionar un espacio para que la organización trabaje sobre una estrategia concreta que quiera llevar a cabo.
- Subrayar la importancia de los indicadores en una estrategia de incidencia.

Materiales

- Papelógrafo
- *Metaplán*
- Plumones
- *Metaplán* con *Mapeo de Actores para incidencia [Anexo prediseñado T4.M3.S1b]* trabajado en la primera actividad de la sesión anterior.
- Fotocopias, papelógrafo o diapositivas con los *Pasos para una estrategia de incidencia [Anexo prediseñado T4.M4.S1]* y los *Componentes básicos de una estrategia de Incidencia [Anexo T4.M4.S1b].*

Recursos adicionales y lecturas de apoyo:

- Centro para el Diálogo Humanitario, *Presencia proactiva Estrategias de terreno campo para la protección de la población civil.*
- CONECTAS Derechos Humanos, *Política Exterior y Derechos Humanos: Estrategias para la acción de la sociedad civil*.
- New tactics in Human Rights, "Powerful Persuasion: Combating Traditional Practices that Violate Human Rights".
- New tactics in Human Rights, "8 Powerful Persuasion Tactics".
- Federación Internacional de Planificación de la Familia, "Comprensión de los indicadores para un proyecto de Advocacy". *[RA13]*

Actividades

Actividad 1: Los pasos y componentes de una estrategia de incidencia.

Presentación 15 min

La persona que facilita presenta los *Componentes básicos de una estrategia de Incidencia [Anexo T4.M4.S1b]*. Se plantea cómo desarrollar una estrategia de incidencia a través de pistas de influencia, métodos y mensajes (ver puntos clave).

A continuación se presentan los *Pasos para una estrategia de incidencia [Anexo T4.M4.S1]*, se puede ejemplificar retomando los pasos y aplicándolos al ejemplo del "Preso Político Jaime Sierra" trabajado en la primera actividad de la sesión anterior de la siguiente manera:

1) Recordar el objetivo específico de incidencia, el cambio que se busca (en este caso la liberación de Jaime Sierra)

2) Elegir un blanco directo de incidencia (en este caso el Gobernador)

3) Clarificar qué queremos que el blanco haga después de que cabildeemos con él (en este caso que presione al Juez para que no pueda haber impunidad en el caso de Jaime)

4) Identificar pistas de influencia (por ejemplo: un a reunión con la OACNUDH para que presione al Gobernador, la movilización de la sociedad civil a manifestarse fuera de la embajada de España para que la embajada presione a su vez al Gobernador).

5) Decidir los métodos, mensajes (comunicación/persuasión) que serán lo más exitosos con este actor, de acuerdo con las características que identificamos en el mapeo (en este caso primer el método es una serie de reuniones y el mensaje es que si Jaime no es liberado, la OACNUDH podría hacer un reporte negativo sobre el estado y por lo tanto su imagen sería dañada; el segundo método es la manifestación pública y el mensaje es que el Estado español está invirtiendo en un estado dónde se violan los DDHH)

Actividad 2: Generar pistas de influencia para la incidencia.

Trabajo en grupos 40 min

Reagrupar a las personas participantes en los mismos grupos que trabajaron los mapeos de actores en el Módulo 3. Pedir a los grupos que trabajen una estrategia de incidencia para su objetivo concreto haciendo hincapié en las pistas de influencia.

Pedir a una persona de cada grupo que escriba los puntos más importantes de su estrategia para un blanco de incidencia o narre brevemente su estrategia. Para ello deberá identificar:

a) El objetivo específico de incidencia

b) El blanco directo de incidencia

c) Qué quieren que el blanco haga después de que se cabildeé con dicho actor

d) Identificar las pistas de influencia

e) Clarificar método y mensaje a utilizar

Si hay tiempo los grupos pueden trabajar un blanco de incidencia fácil y un

blanco de incidencia más difícil.

Actividad 3: Exposición de la Estrategia para un blanco de incidencia.

Discusión en plenaria* *20 min

Pedir que cada grupo exponga su estrategia.

Debatir brevemente con el grupo las distintas estrategias presentadas.

Actividad 4: Indicadores y estrategias de incidencia.

Presentación* *10 min

La persona facilitadora explica los tipos de indicadores para las estrategias de incidencia (ver ideas clave):

1) *Indicadores de proceso*

2) *Indicadores de progreso*

3) *Indicadores de impacto*

Se presenta cómo identificar indicadores para asegurar el impacto de una acción de incidencia tomando de nuevo el ejemplo del "Preso Político Jaime Sierra". La persona facilitadora presenta ejemplos de indicadores con el mapeo de actores ficticio:

Indicadores de proceso: Relacionados con la consecución inmediata de las actividades que determinamos para la incidencia (por ejemplo la OACNUDH se suma a la estrategia y/o la manifestación se hace).

Indicadores de progreso: Relacionados con las consecuencias intermediarias y derivadas de nuestra estrategia (por ejemplo la OACNUDH expresa preocupación al Gobernador y/o la Embajada busca a otras fuentes de información y además lleva su mensaje al Gobernador).

Indicadores de impacto: Relacionados con el objetivo y balance final de la estrategia (por ejemplo: Jaime Sierra es liberado).

Se presenta cómo medir dichos indicadores: Por ejemplo la OACNUDH nos dice que..., en la prensa o en comunicados relacionados con el impacto de nuestras acciones, a través de sentencias judiciales, etc.

Actividad 5: Pensar en indicadores para las estrategias de las PDDH.

Trabajo en Grupos* *25 min

Reagrupar a las personas participantes en los mismos grupos que trabajaron los mapeos de actores en la Sesión 3.

Pedir a los grupos que piensen en posibles indicadores para sus estrategias.

Actividad 6: Recapitulación.

Presentación* *10 min

Para finalizar la persona que facilita retoma las estrategias trabajadas por las PDDH participantes y clarifica sus razonamientos a partir de los principales conceptos compartidos hasta el momento (ver puntos clave).

Consejos de facilitación:

- Aquí se ve la importancia de que se haya hecho bien el mapeo en el Módulo 3. Será importante que las relaciones y las características hayan sido bien identificadas, ya que a partir de las relaciones se obtienen las pistas de influencia. También se parte de las características de los actores para crear el mensaje/discurso.
- Ojo con los tiempos y que las personas participantes sigan todos los pasos. Es preferible que identifiquen un par de actores objetivo y sigan todos los pasos a que intenten cubrir muchos actores y se pierdan en todas las posibilidades. Lo importante es que los pasos se sigan al menos con un actor para que quede claro cómo funciona la metodología y que se podría replicar con los otros actores más adelante y con más tiempo.
- Cuando explicamos lo que son las pistas de influencia y el método y damos ejemplos para ilustrar estas definiciones es importante que quede claro que no son necesariamente reuniones, los métodos usados pueden ser de diferentes tipos (campañas, cartas, reuniones, manifestaciones, comunicados, llamadas etc.).
- Puede ser complicado para las personas participantes distinguir entre indicadores de proceso, de progreso y de impacto. Dar un ejemplo para clarificar: *Si decidimos mandar una Acción Urgente pidiendo que se exprese preocupación al Gobernador del Estado por el caso de un defensor amenazado, un indicador de proceso podría ser a cuantas personas hemos mandado esta Acción Urgente, un indicador de progreso sería cuantas personas a su vez han contactado el Gobernador y un indicador de impacto si finalmente el Gobernador tomó alguna acción para proteger a la PDDH amenazada.*

Estrategias de Incidencia

Identificación y priorización de actores para una estrategia de incidencia coordinada (opcional*)

1h 30min

Atención Sesión Opcional: Esta sesión se da exclusivamente si se busca desarrollar una estrategia coordinada de incidencia entre la organización encargada de la facilitación y la organización participante.

Objetivos específicos:

- Identificar los actores sobre los cuales se debería enfocar una estrategia coordinada de incidencia.
- Sentar las bases de dicha estrategia.

Materiales

- Papelógrafo
- Papelitos adheribles de colores
- Rótulos o tarjetas de cartón o *foamy* de varios colores diferentes
- Plumones
- Chinches
- Lista de actores trabajada en el *Taller 2, Módulo 1, Sesión 2, Actividad 3*
- *Metaplán* o papelógrafo para recrear el anexo *Matriz de Priorización de actores de Incidencia [Anexo T4.M4.S2]*

Puntos clave:

- La identificación de actores no debe suplantar estrategias propias de la organización sino identificar conjuntamente con la organización actores que se deberían disuadir/persuadir y contactos nacionales e internacionales que les pueden coadyuvar a sus objetivos.
- Identificar a tres tipos de actores diferentes para la estrategia de incidencia:

  a) *Actores políticos:* actores sobre los cuales la organización quiere incidir para lograr la consecución de sus objetivos políticos.

  b) *Actores técnicos:* actores que deberían reforzar las capacidades de la organización en distintos ámbitos.

  c) *Actores de seguridad:* actores que afectan la seguridad de la organización o tienen una responsabilidad de protección.
- Muchas veces los mismos actores que son "políticos" son también "de seguridad". Esto no es un problema.
- La priorización de actores depende de dos factores:

  a) Su grado de influencia

  b) Su grado de apoyo/obstaculización respecto a nuestros objetivos
- Ser conscientes sobre la necesidad de tener un análisis e información más completa sobre los diferentes actores que pueden potenciar nuestro trabajo.
- Acordar quiénes son las personas responsables de dar seguimiento a este proceso para que la estrategia coordinada sea llevada a cabo.

Actividades

Actividad 1: Identificar actores políticos, técnicos y relacionados con la seguridad.

Discusión en plenaria y lluvia de ideas* *30 min

Retomar los actores identificados en los mapeos del Módulo 3.

Recordar el objetivo amplio de la estrategia de incidencia entre ambas organizaciones. En una lluvia de ideas junto con el grupo:

1) Completar la lista de actores políticos necesarios para esta estrategia de incidencia conjunta.

2) Replicar la dinámica con actores técnicos. Preguntar al grupo qué contactos

Recursos adicionales y lecturas de apoyo:

- *Taller 1, Módulo 2, Sesión 3*
- *Taller 2, Módulo 1, Sesión 2*
- Centro para el Diálogo Humanitario, *Presencia proactiva Estrategias de terreno campo para la protección de la población civil.*
- CONECTAS Derechos Humanos, *Política Exterior y Derechos Humanos: Estrategias para la acción de la sociedad civil.*
- New tactics in Human Rights, "Powerful Persuasion: Combating Traditional Practices that Violate Human Rights".
- New tactics in Human Rights, "8 Powerful Persuasion Tactics". *[RA13]*

técnicos o capacidades (por ejemplo: colectivos de abogados/as, investigadores forenses, traductores, psicólogos, etc.) requiere la organización para tener mayor impacto en su trabajo.

3) Repetir la dinámica con actores relacionados con la seguridad de la organización. Para ello se puede retomar la lista de actores desarrollada en conjunto en el Taller 2, Módulo 1, Sesión 2, Actividad 3 y verificar que no falta ningún actor. En dado caso que no se tenga disponible la lista a la mano se puede reelaborar esta lista con las preguntas para actores relacionados con la seguridad en la sección de consejos de facilitación.

Al final de la dinámica tendremos tres listas de actores (actores políticos, actores técnicos y actores relacionados con la seguridad).

Actividad 2: Identificar tipos de relaciones con los actores.

Discusión en plenaria* *30 min

Para cada una de las listas de actores, las PDDH identificarán los actores con los cuáles:

a) Tienen una relación autónoma

b) No tienen relación

c) Tienen una relación a través de otra organización

Mientras el grupo debate, un integrante del grupo identifica el tipo de relación para cada actor. La identificación de cada tipo de relación se puede hacer con papelitos adheribles de color pegados al lado de cada actor o situando los actores en un matriz en un papelógrafo (con tres columnas para cada tipo de relación y marcando con X la columna que le corresponda a cada actor).

Actividad 3: Priorización de actores de incidencia.

Discusión en plenaria* *20 min

Explicar brevemente la importancia de priorizar los actores sobre los cuales queremos incidir.

En discusión plenaria en conjunto con el grupo se priorizarán los actores a partir de la discusión de las siguientes preguntas :

¿Qué influencia tiene este actor?

¿Cuál es su grado de apoyo u oposición hacia nuestra organización u objetivos?

A partir de las respuestas se llenará con el grupo una *Matriz de Priorización de actores de Incidencia [Anexo T4.M4.S2]* en un *Metaplán* colocando una tarjeta para cada actor en la matriz a partir de las respuestas.

Otra opción si no se realiza el *Metaplán* es indicar el nivel de prioridad con un papelito adherible de color o símbolo en las listas de actores escritas en un papelógrafo.

Pedir a la persona relatora que tome notas del ejercicio para que la organización pueda profundizar esta priorización con más tiempo y más adelante en un espacio fuera del taller.

Actividad 4:

Discusión en plenaria* *10 min

La persona que facilita se refiere nuevamente al programa en general y retoma la definición de estrategia de incidencia coordinada *[ver Taller 4, Módulo 1, Sesión 1].*

Reiterar el compromiso de establecer una propuesta de estrategia una vez afinada la priorización de actores y acordar fechas para compartir esta priorización y para elaborar una primera propuesta de estrategia coordinada consensuada entre ambas organizaciones.

Consejos de facilitación:

Actividad 1:

- *Identificación de actores políticos*: la idea es completar los mapeos que se habían hecho en torno a los casos concretos con actores que podrían influir en la estrategia coordinada entre ambas organizaciones. Puede ser que las personas participantes recuerden actores muy importantes que no son parte de los casos que ellos eligieron trabajar en este taller.
- *Identificación de actores técnicos:* Buscar que la organización piense en actores, nacionales o internacionales que podrían apoyar su trabajo (expertos, contactos con ciertas características o especializados en algún tema).
- *Identificación de actores relacionados con la seguridad:* Son los que se trabajaron en los Talleres 1 y 2. Si no se cuenta con los materiales trabajados en dichos talleres se pueden volver a realizar las siguientes preguntas:

  a) *¿Cuáles actores tienen una obligación o un interés en protegernos?*

  a) *¿Cuáles actores tienen el poder de ejercer influencia sobre los perpetradores?*

- Esta actividad se hace con base en la lista de actores identificada en el Taller 2. Si no se han hecho previamente el taller, dejar esta actividad de lado y programar un mapeo de actores enfocado en la seguridad y protección de la organización para otro día (de preferencia antes del Taller 4). No es recomendable hacer el mapeo de actores de seguridad el mismo día que se hicieron los ejercicios anteriores. Es muy pesado y se pueden confundir las herramientas.
- Puede ser que ninguna de las dos organizaciones tenga un contacto preestablecido con los contactos que surgen. Es importante identificar todos los que se puedan, para después del taller y de cara al diseño de la estrategia coordinada, valorar si es factible acceder a los contactos identificados, entrar en contacto o buscar nuevos actores. Hay que dejar claro que la lista de actores deseados deberá luego adaptarse a la realidad.
- En la medida de lo posible hay que poner nombres de individuos y no de instituciones: puede haber diferencias de posturas dentro de las instituciones y una incidencia más efectiva se suele enfocar en individuos.
- Si no se pueden dar nombres con categorías o tipos de contacto es suficiente (por ejemplo: puede ser que necesiten "abogados especialistas en Sistema Interamericano" u "organizaciones que ayudan con asilo político").

Actividad 3:

- En el *Metaplán* elaborado a partir de la *Matriz de Priorización de actores de Incidencia [Anexo T4.M4.S2]* Es una prioridad mantener los contactos del área verde bien presentes en la estrategia de incidencia y pasar los contactos del área roja a la amarilla, que reflejará contactos secundarios respecto al área verde pero también importantes para nuestra estrategia. Los contactos en las cajas grises se pueden excluir temporalmente de la estrategia de incidencia, pero hay que monitorearles por si acaso su estatus cambia. El área azul es un espacio donde se puede mapear los contactos negativos; aquellos que se oponen abiertamente a nuestras metas y las obstaculizan.
- Si aparecen más de treinta actores en la tabla, es probable que los objetivos sean demasiado ambiciosos.
- Es probable que no dé tiempo para priorizar todos los actores de las tres listas. En este caso se puede pedir a la organización que complete o profundice esta priorización en un espacio propio posterior al taller. El resultado de estas priorizaciones debería ser compartido entre ambas organizaciones al ser un elemento importante para definir la base de la estrategia coordinada.

Actividad 4:

- El objetivo no es establecer y detallar la estrategia en sí, sino averiguar si se ha compartido la información principal que ambas organizaciones requieren para proponer una estrategia coordinada y si hay actividades que quedaron pendientes para otro momento.

Discurso y Mensaje

Reuniones con actores de incidencia

1h30min

Materiales

- Pizarrón
- Cuaderno
- Hojas en Blanco
- Papelógrafo
- Plumones
- Fotocopias, papelógrafo o diapositivas con el anexo *Preparar adecuadamente una reunión con actores de incidencia [Anexo T4.M5.S1]* y *Consideraciones y preguntas clave para preparar una reunión de incidencia [Anexo T4.M5.S1b].*
- Fotocopias con *Experiencias e ideas para reuniones de incidencia [Anexo T4.M5.S1c].*

Recursos adicionales y lecturas de apoyo:

- BERISTAIN, *Manual sobre la Perspectiva Psicosocial en la investigación de derechos humanos,* cap. 10 y 11. ***[RA3]***
- Centro para el Diálogo Humanitario, *Presencia proactiva Estrategias de terreno campo para la protección de la población civil.*
- CONECTAS *Derechos Humanos, Política Exterior y Derechos Humanos: Estrategias para la acción de la sociedad civil.*
- New tactics in Human Rights, "Powerful Persuasion: Combating Traditional Practices that Violate Human Rights".
- New tactics in Human Rights, "8 Powerful Persuasion Tactics". ***[RA13]***

Objetivos específicos:

- Brindar elementos para preparar adecuadamente reuniones con actores de incidencia.
- Compartir buenas prácticas de mensaje y discurso, en especial enfocado a reuniones cara a cara.

Puntos clave:

- La preparación y estudio del actor con quien nos reuniremos y sus intereses nos ayuda a prever situaciones complejas y pensar mejor el discurso y el mensaje adecuados.
- No siempre lo que decimos es lo más importante, sino cómo lo decimos para que sea interesante para el actor que nos recibe.
- Es fundamental tener un análisis del actor, del contexto, así como nosotros mismos. Lo anterior nos permite definir el discurso y las tácticas sobre cómo llevar a cabo la reunión. Una vez que tengamos este análisis y estrategia, puede ser importante practicar la reunión en un juego de rol.
- Los juegos de rol nos ayudan a prepararnos para:

  a) Ser flexibles

  b) Presentarnos como gente razonable y sensible a los intereses legítimos de nuestras contrapartes

  c) Superar obstáculos y disminuir el conflicto generando consensos

  d) Insistir en ser tratados con respeto y evitar una actitud de debilidad

  e) Mantener una actitud dialógica asegurando nuestros mensajes sean claros y bien interpretados

Actividades

Actividad 1: Preparar una reunión con actores de incidencia.

Discusión en plenaria 30 min

En plenaria, la persona que facilita elige un actor objetivo de uno de los mapeos de actores del Taller 4, Módulo 3, Actividad 2. Preferiblemente debe ser un actor considerado como contacto difícil.

A partir del anexo *Preparar adecuadamente una reunión con actores de incidencia [Anexo T4.M5.S1]* hacer una sesión de preguntas y respuestas con el grupo. Puntear en un papelógrafo o pizarrón las ideas principales.

Actividad 2: Recrear una reunión con actores de incidencia.

Juegos de Rol* *30 min

Dividir el grupo nuevamente de acuerdo a los mapeos de actores realizados en el Módulo 3. Para cada sub-grupo, dividir a las personas en tres roles: 1) los que tendrán el papel de la organización de DDHH, 2) los que serán el actor objetivo y 3) observadores (sólo se limitarán a observar y sacar conclusiones del juego).

Dar unos minutos de preparación a los equipos. Los que tendrán el papel de la organización pueden preparar la reunión guiándose en el anexo *Consideraciones y preguntas clave para preparar una reunión de incidencia [Anexo T4.M5.S1b]*.

Realizar los juegos de rol sin interrumpir.

Actividad 3: Observaciones y retroalimentaciones de las reuniones.

Discusión en plenaria a partir de preguntas detonadoras
30 min

Pedir a las personas que fungieron como observadores que presenten sus reacciones sobre el juego de rol y lo que observaron. Posteriormente se puede también incorporar las observaciones de las personas participantes que tenían un rol activo en el juego.

Algunas preguntas detonadoras que se pueden hacer:

¿Fue difícil?
¿Quiénes representaron a la organización de DDHH? ¿Cumplieron con todos sus objetivos?
¿La reunión ficticia se desarrolló tal como lo habían planeado?
¿Hay puntos que se podrían mejorar?

Con base en lo anterior se pueden compartir e intercambiar puntos de vista e ideas para desarrollar mejor prepararse ante reuniones, preparar discursos y prevenir situaciones difíciles. Se puede compartir el anexo *Experiencias e ideas para reuniones de incidencia [Anexo T4.M5.S1c]* y enriquecerlo con estrategias y experiencias propias de la PDDH participantes.

Consejos de facilitación:

En la Actividad 2

- Hacer por lo menos un juego de rol por grupo de mapeo de actores, dependiendo del número de participantes del taller. Los juegos de rol se realizan en paralelo, al mismo tiempo, en espacios diferentes del salón. Dos a cuatro personas representan la organización, una a dos personas representan los actores objetivos y el resto observa.
- Es importante que quien facilite prepare a quienes serán los actores objetivos para hacer algunas situaciones incómodas y lo más apegadas a la realidad posible. En este tipo de juego, se intenta desestabilizar muchas veces a la persona "que asiste a la reunión", con la intención de recordar las situaciones difíciles para las cuáles debemos de prepararnos y mostrar los puntos débiles que nos faltan por trabajar. En este caso, tanto la "autoridad" como "la persona que asiste a la reunión" se preparan como si fueran realmente ese personaje. Este tipo de actividad ayuda también a darse cuenta si el mensaje está bien diseñado y preparar momentos complicados que pueden desestabilizarnos durante una reunión.
- Escenarios típicos que pueden suceder durante una reunión: la persona no presta atención, atiende su celular, solo habla con el compañero hombre, difama a PDDH o alguno de los casos que la organización de DDHH acompaña, presenta datos opuestos a la información presentada por las PDDH, habla todo el tiempo y no permite hablar, coloca un arma sobre la mesa en actitud amedrentadora, quiere grabar la reunión, hay presencia de prensa en la sala, la persona está todo el tiempo mirando los apuntes de las PDDH, entre otros. Lo importante es crear un conocimiento colectivo sobre este tipo de situación y brindar elementos que nos preparen para dichas situaciones.
- Las personas que fungen como observadores deben identificar las dificultades que tuvieron las personas participantes. Este rol permite que sean las mismas organizaciones que identifiquen y verbalicen sus dificultades. La persona que facilita debe tener cuidado en no entrometerse. Podemos usar ejemplos propios para mostrar algunas situaciones para las cuales debemos de prepararnos antes de una reunión con un actor nuevo o de gran dificultad para dialogar.
- También se debe recordar a las PDDH participantes que una situación será difícil en ocasiones por el simple hecho de saber que esa persona es una agresora o potencial agresora.
- El anexo Experiencias e ideas para reuniones de incidencia [Anexo T4.M5.S1c] está para guiar el intercambio y detonar el debate. Las ideas listadas parten de las experiencias de la sociedad civil de México y otros países donde PBI lleva a cabo reuniones de incidencia. Esta lista no es exhaustiva y está lejos de ser acabada. Este anexo no pretende "enseñar" buenas prácticas sino "compartir" ideas que puedan ser adaptadas a las necesidades de las PDDH y enriquecidas por sus propias experiencias.

Conclusión y cierre

Seguimiento, compromisos y cierre

45min

Objetivos específicos:

- Revisar el contenido y los conocimientos adquiridos.
- Identificar tareas y responsabilidades para darle seguimiento al taller e implementar lo aprendido.
- Acordar el seguimiento.
- Evaluar el taller.

Materiales

- Papelógrafos
- Plumones
- *Metaplán*
- Hojas
- Papelógrafo con un punteo de los *Objetivos generales del taller y resultados esperados*
- Fotocopias con *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b]*
- Urna o caja de cartón con una ranura

Puntos clave:

- Enfatizar que si la organización no le destina los recursos (responsables, espacios, tiempo, etc.) al ámbito de seguridad y protección no se podrán llevar a cabo estrategias ni planes integrales.
- Abordar las expectativas de seguimiento y acordar si se necesita seguimiento, de qué tipo y cómo se podría dar.
- Revisar los acuerdos alcanzados y establecer los compromisos con las personas participantes en cuanto a las estrategias de seguridad y protección que serán desarrolladas a nivel organizativo.
- Revisar las tareas apuntadas e identificar plazos, espacios, recursos y responsables con un nivel aceptable de detalle y claridad.
- Cerciorarnos que no hayan quedado dudas sobre los aspectos fundamentales del taller.
- Evaluar el taller y la facilitación.

Actividades

Actividad 1: Revisión de "Actas y Acuerdos".

Discusión en plenaria* *15 min

La persona que facilita el taller pide a la persona encargada de actas o relatora que haga un pequeño recuento del taller.

Entre todas y todos, vamos apuntando las tareas y pendientes que surgieron del taller.

Mientras las personas participantes van identificando las tareas pendientes y sólo en caso de que este taller se haya brindado sin haber pasado por el Taller 3 o sus módulos opcionales se pueden plantear las opciones de dichas asesorías.

*En dado caso de haber pasado por todos los talleres previos, se puede simplemente proponer un seguimiento de apoyo puntual para las tareas pendientes, incluyendo las de incidencia coordinada si se dio la sesión opcional del Módulo 4 de este taller.

Actividad 2: Evaluación del cumplimiento de los objetivos del taller y expectativas.

Trabajo en plenaria* *10 min

Retomar las expectativas de las personas participantes trabajadas al inicio del taller. En un papelógrafo se pegan las expectativas iniciales del grupo del lado izquierdo y a la derecha se hacen tres columnas para evaluar el cumplimiento de las mismas:

Consejos de facilitación:

- Si el grupo no quiere llegar a acuerdos en términos del seguimiento no hay que forzarlo.
- Si se tiene más tiempo al final se puede optar por la evaluación en fotocopias que permite sistematizar mejor la información y retroalimentaciones. Algunos grupos prefieren rellenar las evaluaciones sin la persona que facilita presente. Se pueden poner cajitas a modo de urnas para que se depositen las evaluaciones individuales dobladas y de forma anónima.

1) se cumplió 2) se cumplió parcialmente y 3) no se cumplió. Para cada una de las expectativas se pide que cada persona pegue un papelito adherible en la columna que considere.

En otro papelógrafo se tiene listo un punteo de los *Objetivos generales del taller y resultados esperados.* Enfrente de cada aspecto del punteo se hacen tres columnas al igual que para las expectativas y se pide que las personas peguen un papelito adherible en la columna que consideren. También pueden escribir sobre el papelito que peguen si gustan ahondar en algún objetivo específico si sienten que hubo aspectos del objetivo que se les dificultaron o que no se cumplieron a cabalidad.

La persona que facilita hace un recuento y revisa especialmente aquellos objetivos y expectativas que faltó cumplir a cabalidad. Se contrasta si dichos objetivos y expectativas estaba en las posibilidades planteadas por el taller o si se pueden abordar en talleres subsecuentes.

Actividad 3: Evaluación del taller y la facilitación.

Trabajo individual o plenaria ***10 min***

Escoger una de las siguientes formas de evaluación.

a) En un papelógrafo se hacen dos columnas: 1) adecuado y 2) puede mejorar. Se reparten papelitos con los distintos criterios adaptados de las 2 tablas del *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b]*

Se les pide que cada quien tome 3 criterios de evaluación del taller y 3 criterios de evaluación de la facilitación (de preferencia aquellos donde tengan más que aportar o que les llamaron la atención para evaluar) y que escriban sobre los papelitos con sus opiniones, críticas y sugerencias. Luego se les pide que adhieran los papelitos en una de las dos columnas según corresponda a su punto de vista.

b) Se distribuyen individualmente fotocopias del *Formato de evaluación individual de taller y la facilitación [Anexo T1.M3.S1b].* Se pide a las personas que lo llenen y lo depositen doblado y de forma anónima en una caja o urna.

Actividad 4: Conclusión.

Discusión en plenaria ***10 min***

Se da una oportunidad para dudas y comentarios al grupo, se comentan las apreciaciones y se hace una última ronda de críticas y sugerencias.

Se recuerda la confidencialidad de lo abordado en los talleres.

Se dan los agradecimientos y se clarifica que se deja la posibilidad abierta para futuras colaboraciones.

Taller 4

Anexos

Anexo T4 M2 S1

Ejemplo de estrategia de incidencia para análisis

Ejemplo:

Creación de un Mecanismo de Protección Gubernamental para la Protección de Personas Defensoras de Derechos Humanos y Periodistas en México.

Objetivo:

Aprobar una Ley de Protección para Personas Defensoras de Derechos Humanos y Periodistas. Cambio buscado: que existiera una Ley específica.

Blancos:

Los legisladores. Porque son los que tienen el poder de aprobar leyes.

Aliados:

Sociedad civil amplia, embajadas, OACNUDH, organizaciones internacionales.

Buenas prácticas:

1) Estar dispuestos a dialogar y llevar a cabo un proceso largo

2) División de tareas

3) Formación de coaliciones / superar diferencias por objetivo común

4) Utilizar actores internos y externos

5) No bajar la presión / tener paciencia

6) Mesas de trabajo con legisladores

7) Mantener reuniones periódicas

8) Utilizar fechas simbólicas

9) Usar alianzas en varios niveles (local, federal, internacional)

Mensajes:

Las autoridades mexicanas no están haciendo lo suficiente para proteger a personas defensoras de derechos humanos y periodistas que enfrentan un riesgo creciente y necesitan un mecanismo que responda a esta problemática

Resultado:

Se aprobó la ley.

Anexo T4 M2 S1b

Experiencias e ideas para redes de apoyo y estrategias de incidencia en DDHH*

VENTANAS DE OPORTUNIDAD

- Se pueden ubicar a través de un análisis de coyuntura.
- Se pueden aprovechar a través de nuestras acciones.
- Pueden ser predecibles, impredecibles, o creadas.

Ejemplos: un gobierno saliente con deseo de dejar un legado positivo, un funcionario o gobierno recién llegado y buscando una imagen de frescura y apertura, hechos emblemáticos (desastres o violaciones impactantes que demandan un cambio, o hechos positivos que podrían desencadenar otros cambios positivos), la llegada de nuevos actores, un cambio en la coyuntura social o política.

Coaliciones

- El trabajo en coalición puede aumentar nuestra legitimidad y posicionarnos como "un actor a tener en cuenta".
- "Fuerza en números". El trabajo en coalición con otros actores puede aumentar de forma exponencial nuestra capacidad y por lo tanto nuestro potencial de generar cambios.
- El trabajo previo de encontrar puntos de coincidencia y metas en común es fundamental para asegurar que el frente común no se quiebre bajo el estrés de actores obstaculizadores.
- Este trabajo previo también nos permite ubicar las capacidades y vulnerabilidades de cada organización y definir una división de tareas relevante.
- Una coalición nos permite dividir las tareas. Cada miembro de la coalición puede enfocarse en distintos actores que son considerados estratégicos y así cubrimos más actores con potencial de cambio.
- Al contrario, una coalición puede garantizar múltiples acciones dirigidas hacia el mismo actor que tiene gran potencial de cambio pero que requiere recibir mucha presión para atender nuestras demandas.
- Una coalición de organizaciones o individuos con distintos mandatos y trayectorias, y quienes normalmente no cooperan puede tener un gran impacto al dar la imagen de que el asunto es muy importante y que la coalición es muy fuerte (frente común).
- Dependiendo de las pistas de influencia identificadas, se pueden formar coaliciones de distintos tipos: con aliados en el gobierno, con personajes públicos, entre organizaciones locales, nacionales e internacionales.

* Las ideas listadas parten de las experiencias de la sociedad civil de México y otros países donde PBI lleva a cabo acompañamiento. Esta lista también se ha nutrido del aprendizaje con especialistas, personal de gobierno, cuerpos diplomáticos y redes de apoyo internacionales. Esta lista no es exhaustiva y está lejos de ser acabada. Este anexo no pretende "enseñar" buenas prácticas sino "compartir" experiencias e ideas que puedan ser adaptadas a las necesidades de las PDDH y enriquecidas por sus propias experiencias.

Anexo **T4 M2 S1b Continuación**

Experiencias e ideas para redes de apoyo y estrategias de incidencia en DDHH

AUTO-LEGITIMAR COMO ACTOR

- Puede ser útil mantener un perfil público alto ante los actores que queremos que nos respeten. Esto puede significar asistir a eventos, salir en los medios o participar en otras iniciativas en las que nuestro objetivo inmediato es aumentar el perfil y respeto para nosotros mismos.
- En reuniones y actividades se pueden nombrar otros contactos y experiencias de la organización o individuo que impresionarán a la diana (p.e. contactos de alto nivel del gobierno, participación en foros convocados por entidades internacionales de gran importancia, premios ganados etc.)
- En comunicaciones escritas, se pueden poner en copia visible a estos "contactos importantes".

LEGITIMAR DESDE OTROS ACTORES

- Los medios tienen gran potencial para colocar un asunto en la agenda pública, o de aumentar el costo político sobre el actor señalado como responsable. También pueden servir para legitimarnos como actores.
- Los periodistas están bajo presiones económicas ya que se les demanda escribir "historias" de interés para su audiencia, o de beneficio político-económico de su dueño o inversionistas. Hay que proporcionar información que pueda reproducir para estos fines sin gran inversión de energía/tiempo.
- Debemos tener un mensaje claro y conciso. No siempre se puede prever o controlar el resultado de lo que se publica en los medios. Hay que preparar bien nuestro discurso para que en caso de que se descontextualice, el sentido del mensaje no pueda ser alterado. Es Importante tener claro una estrategia para contrarrestar mensajes contrarios a los que queríamos transmitir en un primer momento.

FECHAS SIMBÓLICAS ¡UTILÍCELAS!

- Aniversarios, el día internacional de..., la visita a México de un personaje, una gira del Presidente a..., fechas límite de compromisos gubernamentales etc.

VISIBILIZAR LOS PROCESOS CON EL ESTADO

- Felicitar una iniciativa puede aumentar el coste de que fracase.

Anexo T4 M2 S1b Continuación

Experiencias e ideas para redes de apoyo y estrategias de incidencia en DDHH

SEA ÚTIL PERO NO SE DEJE UTILIZAR

- No queremos volvernos una mera fuente de información o favores, ni ser explícitamente utilizados con fines políticos. Sin embargo se puede valorar qué es aceptable proporcionar o hacer para un contacto. Así es más probable que vaya a querer ser útil para nosotros, proporcionándonos información y respondiendo positivamente a nuestras peticiones (esta forma de trabajar es mucho menos complicada cuando se tratan de contactos no directamente implicados en el conflicto).

LEGITIMAR DESDE OTROS ACTORES

- Tener claro quiénes son actores que queremos disuadir para prevenir que tomen acciones negativas y quienes son actores que queremos persuadir para que tomen acciones positivas.
- ¿Cómo les haremos saber que habrá un costo político de que tomen o no tomen ciertas acciones?
- Cómo hacerle creer que la gente que él/ella requiere (pe. Votantes, donantes, su partido, los medios) están monitoreando sus acciones y están preocupados porque haya resolución del conflicto.
- ¿Quiénes son los actores no-estatales o con poder informal/escondido? (p.e. Asesores y consejeros, caciques, inversionistas, grupos armados)
- ¿A quiénes podemos convencer de la relevancia de nuestras ideas/análisis y que puedan a su vez presionar al actor con poder/perpetrador? (Hay gente que conocemos que activarán estos contactos con más facilidad con la que nosotros podríamos, y lo harán por interés real, por interés personal, para demostrar que pueden operar...)
- ¡Matizar el mapeo! Con nombre y apellidos. ¿Hay aliados dentro de alguna institución? Hay que ubicarlos y fortalecerlos.

PROBAR LA DEMOCRACIA

- Pedir que ciudadanos presionen a su "representante" para que tome acción sobre un asunto.

Anexo **T4 M2 S1b Continuación**

Experiencias e ideas para redes de apoyo y estrategias de incidencia en DDHH

SER ESTRATÉGICOS CON ROMPER EL DIÁLOGO

- Importancia de ser estratégicos al romper el diálogo con el gobierno u otras partes del conflicto
- En Colombia, una coalición amplia de organizaciones tiene una postura de nunca rehusar una oferta de "diálogo" con un actor, pero de siempre visibilizar su contenido, su calidad, y los compromisos acordados (explicando la naturaleza ante otros actores claves y/o la prensa).

PREVER LA LINEA/ESTRATEGIA DEL ESTADO

- Y comunicar nuestro punto de vista a la gente ante la cual el estado manifestará su versión también (p.e. La opinión pública en general, la comunidad internacional, otras ONGs...)

UTILIZAR EVENTOS PÚBLICOS PARA AUMENTAR CANTIDAD DE ACTORES IMPLICADOS

- Proporcionar información que pueden usar para entender mejor el tema después del evento.
- Siempre tener una acción simple e inmediata que los integrantes de la audiencia ya pueden tomar en el momento, por ejemplo: firmar una petición, rellenar y enviar una postal, firmar para donar o tomar una acción futura etc.

VALORAR ACCIONES MÚLTIPLES Y SIMULTÁNEAS

- En estado de mareo ¡el enemigo pude conceder!
- Asegurar la capacidad de seguimiento antes de tomar acciones.

Anexo T4 M2 S1b Continuación

Experiencias e ideas para redes de apoyo y estrategias de incidencia en DDHH

CONSTRUCCIÓN DE REDES E INCIDENCIA CONSTANTE

- Algunas reuniones no rinden resultados inmediatos, sin embargo ayuda con que establezcamos contactos y tejamos redes que podríamos activar en caso de emergencia o cuando se abra una ventana de oportunidad.

CONOCIMIENTO JURÍDICO Y ANÁLISIS PROPIO DE COYUNTURA

- Para el cabildeo internacional es importante contar con el conocimiento mínimo sobre el marco legal mexicano, local e internacional ¡ya que muchos contactos lo van a preguntar!
- Para el cabildeo internacional es importante saber que está pasando en el país o en la región donde trabajamos y poder ofrecer un análisis propio, conciso y claro de esta coyuntura.

VÍNCULO INCIDENCIA-SEGURIDAD

- Sea consciente que las acciones de incidencia (particularmente si son muy visibles o muy exitosas) pueden provocar represalias. Analice el riesgo implicado y diseñe un protocolo de seguridad alrededor de las acciones de alto riesgo.

LAS DIRECTRICES DE LA UNIÓN EUROPA PARA DEFENSORES/AS DE DERECHOS HUMANOS

- Contienen muchas acciones y buenas prácticas que se pueden y que se deben de tomar desde las embajadas para legitimar y proteger a las PDDH.
- También sirven para conseguir acciones multilaterales y de embajadas que no son de la UE, mostrándoles buenas prácticas que las embajadas de la UE tienen.
- Tener en cuenta también las Directrices para PDDH de Noruega y de Suiza.

Anexo T4 M3 S1

Pasos del Mapeo de Actores para una estrategia de incidencia

Paso 1 Elegir el problema sobre el que queremos incidir

El proceso de planificación para la incidencia política empieza con la identificación y priorización de un problema que afecta a las PDDH en forma concreta.

Paso 2 Definir el objetivo específico/preciso de incidencia

A partir de la priorización de un problema se debe pensar en un objetivo específico que brinde una solución a nuestro problema. El problema puede ser resuelto teniendo como objetivo acciones o cambios concretos que queremos lograr a través de acciones de los actores (regularmente gobierno).

Paso 3 Identificar a los actores clave respecto al problema

En los actores clave se debería incluir actores que tengan alguna responsabilidad sobre esta amenaza (puede ser el perpetrador), también se pueden incluir actores que puedan tener influencia sobre los actores principales (por ejemplo una autoridad con el poder de frenar a los perpetradores o de resolver el problema) y por último otros actores que puedan ser aliados de las PDDH directamente afectadas por la problemática que puedan apoyar. No es un mapeo extenso, sino un mapeo específico de los actores clave.

Paso 4 Analizar a los actores

Para analizar a los actores se deben anotar las características e intereses más relevantes en la cartulina del actor. Para ello se deben responder las siguientes preguntas: *¿Cuál es la función de este actor en el conflicto? ¿Qué queremos acción que este actor cambie o realice? ¿A quién escucha? ¿Quiénes son sus aliados/partido etc.? ¿A quién le hace caso? ¿Es un agresor? ¿Es un facilitador? ¿Es un obstáculo? ¿Es un aliado potencial? ¿Cuáles son sus intereses y objetivos? ¿Por qué actúa de esa manera? ¿Cuál es su influencia real o potencial sobre el problema? ¿Su influencia es positiva o negativa? ¿Su influencia es fuerte o débil?*

Paso 5 Comprender las relaciones clave entre actores

Una vez que se hayan hecho varias "cartas de actores", se representan los vínculos entre actores a través de líneas o conexiones. Se debe reflexionar cuáles son las relaciones más importantes que debemos de caracterizar. Se coloca una carta de un color diferente entre dos actores y sobre esta carta se describen las relaciones en términos de su impacto en el problema y la capacidad de la organización a la que pertenecemos para influir en este actor (positivo, negativo, aliados, enemigos, ambiguos, influencia alta/baja, etcétera). Este proceso de caracterizar las relaciones debería provocar debate entre el grupo.

Paso 6 Situar a nuestra organización en la representación

Ubicar relacionalmente a nuestra organización respecto a aliados y otros actores no aliados. Para ello se representan los vínculos más importantes con los otros actores clave a través de líneas o conexiones. Se pueden describir las relaciones en cartas pegadas sobre las líneas o vínculos.

Paso 7 Representar las relaciones entre nuestros aliados y con actores clave

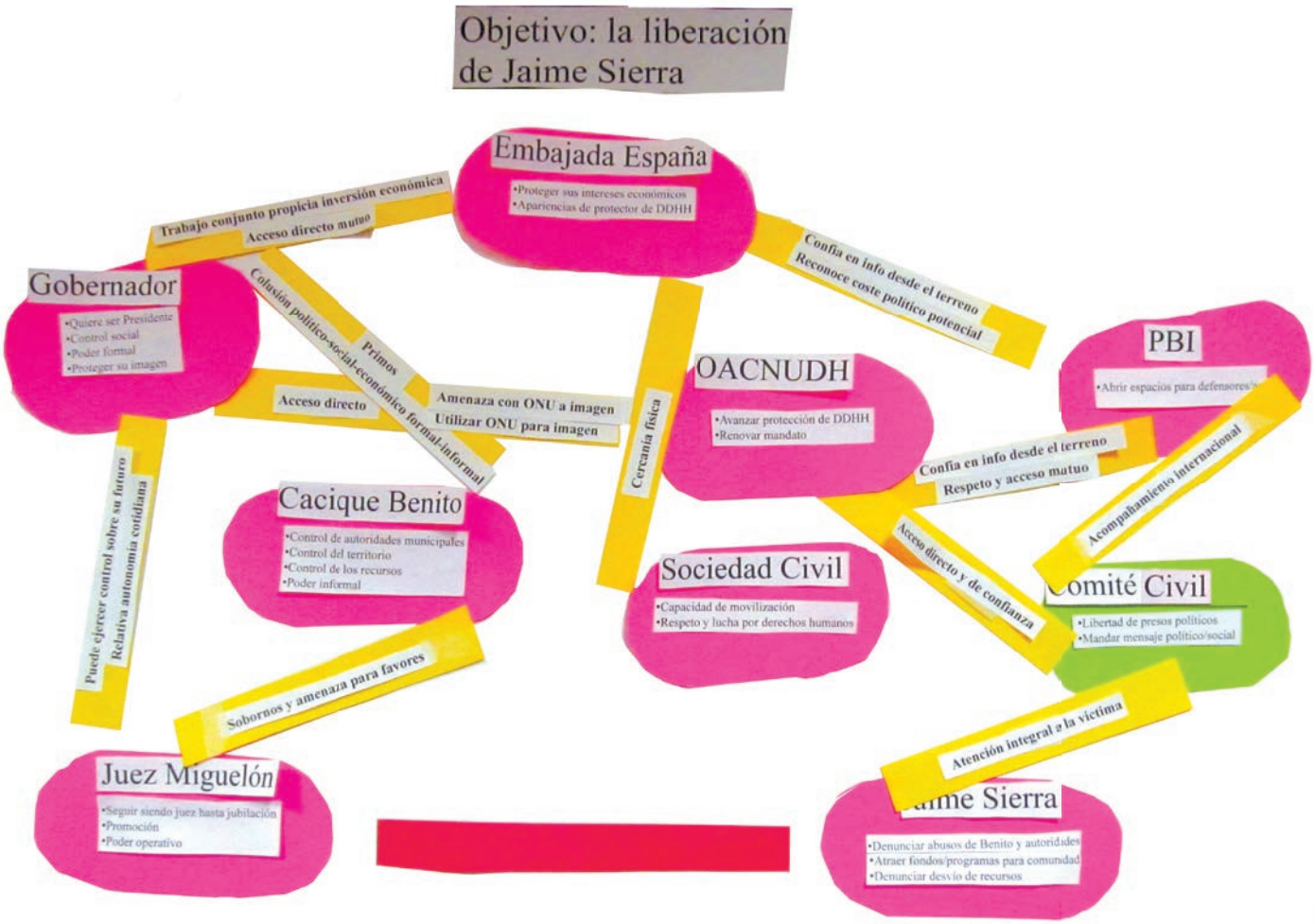
Ubicar a aliados locales, federales e internacionales, ONGs etc. y representar sus relaciones con otros actores clave en relación con la resolución del problema. Deben representarse junto con sus relaciones y esferas de influencia en la medida que puedan coadyuvar para lograr nuestro objetivo influyendo directa o indirectamente en los actores adversarios o aquellos de los cuales no estamos seguros si son aliados o no.

Anexo **T4 M3 S1b**

Mapeo de Actores para incidencia (ejemplo de *Metaplán*)

Uso de herramientas complementarias: *Metaplán para Mapeo de actores*

El Metaplán para Mapeo de actores *es una herramienta para identificar las relaciones entre los actores clave que afectan un problema. Cada actor clave es blanco potencial de las estrategias de cabildeo. El objetivo de esta herramienta no es crear una obra gráfica de arte; tampoco se puede utilizar de manera efectiva para representar todas las relaciones detalladas y complejas entre los actores en un escenario real de conflicto. Es una herramienta visual que ayuda a identificar a los actores más influyentes y a desarrollar una comprensión de sus vínculos. También ayuda a identificar algunos puntos de presión y pistas de influencia. Recuerden arreglar el mapeo mientras van debatiendo ¡El mapeo es la metodología, no el resultado!*



Anexo T4 M4 S1

Pasos para diseñar una estrategia de Incidencia

Paso 1

Definir un objetivo de cabildeo (a partir del cambio que se busca)

Paso 2

Identificar pistas de influencia (aprovechando el mapeo de actores)

Paso 3

Escoger un blanco directo de cabildeo y clarificar qué se quiere que el blanco haga después del cabildeo

Paso 4

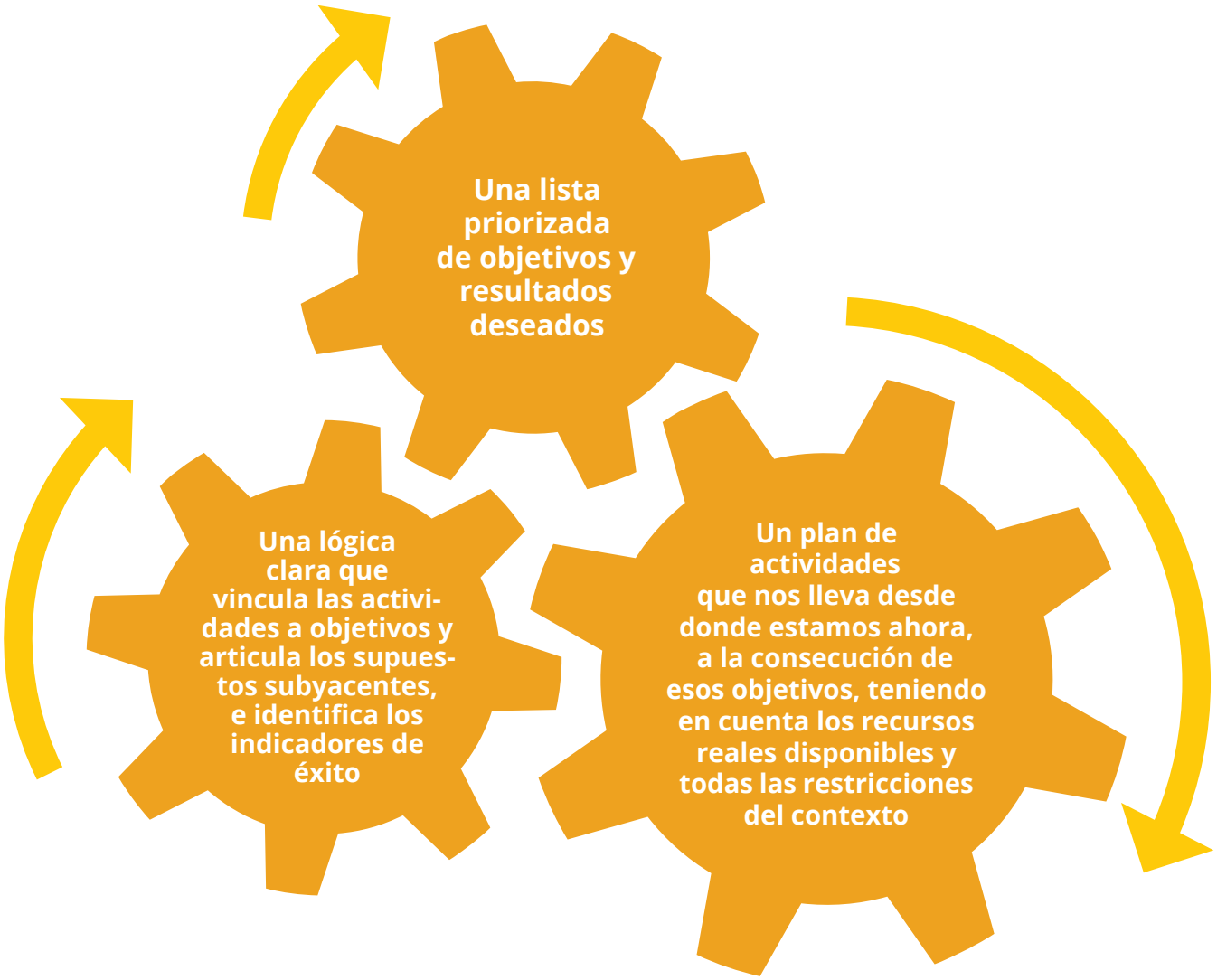
Decidir el/los método(s) y mensaje(s) de comunicación/persuasión que se cree van a ser los más exitosos con este actor

Paso 5

Seguimiento: Identificar indicadores para estar seguros de cuál es el impacto de la acción de cabildeo

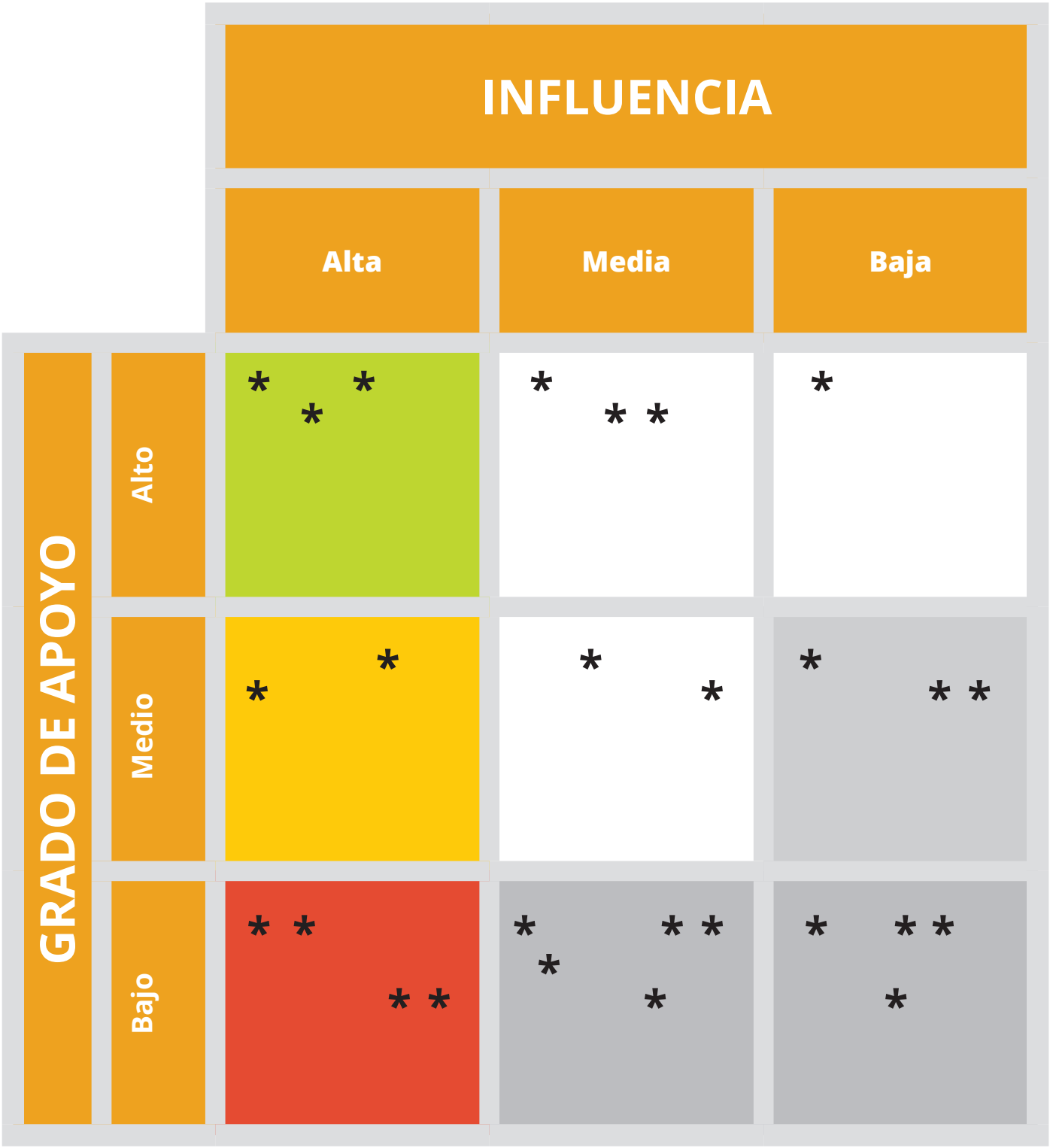
Anexo T4 M4 S1b

Componentes básicos de una estrategia de Incidencia



T4 M4 S2

Matriz de priorización de actores de incidencia (ejemplo para *Metaplán*)



* Los asteriscos representan fichas o rótulos de actores concretos

Anexo T4 M5 S1

Preparar adecuadamente una reunión con actores de incidencia

Supongamos que [ACTOR] ha aceptado nuestra petición de reunión...

- ¿Por qué nos recibe? (pe. Comparte nuestros valores, mostramos compatibilidad con sus intereses, le importa lo que hacemos o pensamos...)
- ¿Qué piensa de nosotros? (compatibles, poderosos, con contactos, serios, útiles...)
- ¿Qué tipo de relación quiere?
- ¿Cómo es?
- ¿Por qué reaccionaría a nuestras peticiones?
- ¿Cuál es el contexto en el cual la reunión se da?
- ¿Cuáles temas son delicados y podrían provocar innecesariamente un conflicto?
- ¿Cuáles obstáculos, respuestas difíciles y tensiones podemos prever?
- ¿Cuáles son nuestros objetivos?
- ¿Cómo aseguramos su respeto y prevenimos la intimidación?
- ¿Cómo mostramos compatibilidad con sus intereses/mostramos que nuestra labor es relevante?
- ¿Cómo podemos influir en sus percepciones?
- ¿Cuáles son nuestras limitaciones?
- ¿Qué tipo de relación queremos? (alianza cooperativa, dependencia mutua, firme y crítica, espacio de confianza...)
- ¿Qué tipo de mensaje mandamos?
- Indirectos/implícitos (cosas que son entendidas sin decirlas)
- Directos pero no publicados (privada pero honesta, advertencias)
- Públicos (prensa, eventos públicos, actos conjuntos)
- ¿Quiénes asistiremos y como dividimos los papeles?

Anexo T4 M5 S1b

Consideraciones y preguntas clave para preparar una reunión de incidencia

Factores a tomar en cuenta en la preparación de interlocución con autoridades:

Cada reunión es diferente y por lo tanto requiere de una preparación meticulosa y estratégica. Una reunión mal preparada puede resultar en la sensación de falta de profesionalidad, malentendidos que pueden dañar nuestra relación con el actor en cuestión, y una pérdida de tiempo, tanto el suyo como el nuestro.

- ¿Cómo presentaremos quiénes somos, cuál es nuestro trabajo y a quiénes representamos?
- ¿Qué estrategia tenemos para maximizar la incidencia con esta persona?
- ¿Cuáles son los instrumentos locales e internacionales que podemos citar para respaldar nuestro discurso
- ¿Cuáles son las preguntas que le vamos a plantear para promover un diálogo y entender mejor su trabajo, su postura sobre ciertas temáticas y su visión de nuestro trabajo y el de nuestros acompañados.
- ¿Cuáles son las peticiones concretas que le vamos a plantear para que ambos salgamos de la reunión con la sensación de haber logrado algo.
- ¿Cuáles son los hechos públicos coyunturales relacionados con la competencia de esta persona para citarlas y entrar en un diálogo sobre los mismos.
- ¿Cuál será nuestro discurso y las temáticas que queremos visibilizas? (A veces no hace falta todo el discurso para cada actor ni presentar todos los acompañamientos)
- ¿Quién va a decir qué en la reunión?
- ¿Qué le vamos a entregar? (Tarjetas de presentación, publicaciones, etc.)
- ¿Qué escenarios deberíamos prevenir para la reunión? (Estrategias alternativas para lograr nuestros objetivos, peticiones adicionales si todo va bien, alternativas si algo sale mal).

¿Quién es nuestro interlocutor, y porqué hemos pedido la reunión con esta persona?

Si es nuevo en su puesto o no tenemos información previa:

- ¿Qué es su competencia y descripción de responsabilidades?
- ¿Cuánto tiempo lleva en el puesto?
- ¿Dónde trabajaba antes?
- ¿Cómo fue nuestra relación con su predecesor?
- ¿Quién es su superior y cuánto contacto hemos tenido con él/ella?
- ¿Hay que pedirle que sea contacto de emergencia? ¿Qué reciba nuestras publicaciones?

Si ya hemos tenido reuniones previas:

- ¿Cuántas veces ya le hemos visto?
- ¿Cuándo fue la última vez que tuvimos una reunión?
- ¿Quién asistió a la reunión?
- ¿Qué se dijo en la reunión?
- ¿Cuáles fueron los compromisos? ¿Los hemos cumplido? (en caso negativo: ¿Por qué?
- ¿Cuándo fue la última vez que nos comunicamos y para qué?

Anexo T4 M5 S1c

Experiencias e ideas para reuniones de incidencia*

IDEAS PARA CONSEGUIR CITAS CON ACTORES CLAVE

- Llamadas persistentes: dejar clara la importancia y el prestigio de su organización y la urgencia del tema, conseguir nombre de contacto y si es posible del secretario particular
- Enviar una carta formal solicitando la cita, para respaldar la petición telefónica
- Pedir la reunión para una cita particular con argumentación sobre el porqué de la fecha. Es decir, apurar la respuesta con una petición explícita de fecha.
- Gran parte del análisis de actor que usamos para el discurso para la reunión misma, nos puede sirve de forma resumida para persuadir por teléfono a que nos den la cita.
- Buscar a contactos y aliados que pueden arreglarnos citas que para nosotros mismos son difíciles de conseguir (pe. Contactos del mismo partido, contactos de la sociedad civil que ya tienen acceso etc.)
- Mantener sin embargo en mente que nuestros interlocutores han sido más disponibles por una razón (pe. épocas electorales).

PARA PREPARAR LAS REUNIONES

- Es importante recabar información previa sobre la naturaleza del carácter con quien nos vamos a reunir.
- ¿Es emocional? ¿serio? ¿comprometido? ¿egoísta? ¿de mucho discurso y poca acción? ¿perezoso? Etc.
- ¿Está convertido a nuestra causa ya? ¿No está decidido? ¿Es hostil? ¿Está harto?
- Este tipo de información nos ayudará a apelar a sus instintos positivos y no provocar los negativos.
- Hacer una investigación previa sobre la diana
- ¿Quién es?
- ¿Con quién está vinculado?
- ¿Cuáles son sus responsabilidades formales?
- ¿Cuáles son sus intereses reales?
- ¿Qué sabe ya? (y por lo tanto cuánto contexto le doy)
- ¿Qué pueden hacer? (cuál es su poder)

La información que tenemos sobre la diana debe ayudarnos a adaptar nuestra presentación, ilustración, narrativo, ejemplos, data, lenguaje, tono, lenguaje corporal etc.

Pensar en cómo hacer que la reunión sea interactiva.

Buscar puntos de posible vinculación o encuentro. ¿De dónde es? ¿Qué hizo antes? ¿Cuáles son sus intereses personales etc?

Estar preparado/a para recortar o alargar el discurso acorde al tiempo/atención/actitud que presentan.

* Las ideas listadas parten de las experiencias de la sociedad civil de México y otros países donde PBI lleva a cabo reuniones de incidencia. Esta lista no es exhaustiva y está lejos de ser acabada. Este anexo no pretende "enseñar" buenas prácticas sino "compartir" ideas que puedan ser adaptadas a las necesidades de las PDDH y enriquecidas por sus propias experiencias.

Anexo T4 M5 S1c Continuación

Experiencias e ideas para reuniones de incidencia

PARA PREPARAR LAS REUNIONES (continuación)

Prever traducción si es necesario

- Hacer una reunión previa con el traductor/a para explicar tu discurso, asegurar que entienda tu concepto, aclarar jerga, definir ritmo e intercambio de palabra, y asegurar que las peticiones se traducirán con fuerza.

Prever las preguntas que harán y las cosas que nos retarán

- Y tener las respuestas y argumentos listos.

¿Cuáles son los incentivos implícitos que ofrecemos para sus acciones?

- Su nombre sobre una iniciativa positiva/publicidad positiva.
- Una experiencia interesante para ellos (pe. Interactuación con actores de base, viaje, comida, interacción con sus supuestos clientes/ beneficiarios)
- Una sensación de agradecimiento/'*feel-good factor*' (en este caso hay que asegurar que su acción recibe dicho agradecimiento, preferencialmente público, para que tomen acciones futuras). La sensación de gratificación emocional puede ser poderosa.

DOCUMENTOS

- Los documentos impresos son útiles a la hora de asistir a reuniones.
- Es importante preparar documentos adecuados y útiles según el receptor. Si es congresista, por ejemplo, proporcionar información sobre los cambios legislativos necesarios. Si es de la UE es bueno ligar nuestro discurso con las políticas de la UE y hacer una corta valoración de estas con propuestas para mejorarlas. Si es activista, hay que demostrar cómo puede aportar a un movimiento o una acción conjunta.
- Los actores con potencial de incidencia valoran resúmenes cortos (de entre 1 y 4 páginas) y condensados con información que les permite entender la problemática y las soluciones requeridas, aunque empiecen su lectura con un "entendimiento cero".
- Documentos más testimoniales, especialmente con fotos, y que demuestran el lado "humano" de la historia, pueden servir para enganchar a actores que ya tienen una apertura, que son de naturaleza más emocionales o que tienen el tiempo e interés o empatía por este lado de la historia.
- Ante actores que queremos tomen acciones, hay que proporcionar información que requiere poca modificación antes de reproducirse. Periodistas a veces publican textualmente comunicados de calidad, y se han dado varios ejemplos de cartas enviadas desde dianas importantes que son casi un copia y pega del *briefing* proporcionado ¡Hay que hacer la vida del actor con potencial de incidencia más fácil! (y por lo tanto más factible que nos apoye).
- Tarjetas de presentación son parte fundamental del protocolo de muchos actores y hacen más fácil que nos recuerden y que se comuniquen con nosotros.

Anexo T4 M5 S1c Continuación

Experiencias e ideas para reuniones de incidencia

DISCURSO

El inicio de la reunión

- Tener una apertura clara y fuerte: ¡las primeras impresiones cuentan mucho!
- Explicar nuestros objetivos de la reunión y recordar los temas de los cuales vamos a hablar. Hacer referencia nuestra petición, y preguntar de cuánto tiempo disponen.
- Tener un órden estructurado del discurso.
- Por ejemplo: *¿Qué pasa? ¿Porqué? ¿Qué debería pasar? ¿Qué pueden hacer?*

Peticiones o llamadas a la acción

- Es fundamental tener peticiones claras y realistas, basadas en un conocimiento de qué puede hacer ese actor (y por lo tanto claridad de sus competencias).
- A veces se puede adoptar una estrategia de pedir algo con el propósito de conseguir una acción menos ambiciosa. Es una estrategia de regateo político.

Fundamento

- Es vital dar fundamento a nuestros argumentos. A muchos contactos les importan estadísticas y datos duros y siempre debemos contar con unos en nuestro discurso, y poder demostrar que la fuente es fiable. Si es imposible recabar cifras, hay que poder explicar porqué de una forma convincente.
- Estudios de casos y experiencia personal son otras formas eficaces de fundamentar nuestro discurso. Una mezcla de cifras y narrativa más personalizada suele ser una forma impactante de ilustrar una problemática.
- Los actores suelen estar más dispuestos a tomar acciones si saben que hay ejemplos del pasado dónde esas acciones han funcionado o dónde sus homólogos han tomado el "riesgo" que les pedimos tomar. Por ejemplo, si vamos a cabildear la publicación en idiomas locales y distribución de las directrices de la UE, se puede señalar el hecho que en Nepal ya se publicaron en Nepali y se distribuyeron entre defensores aislados.
- Asegurar la fiabilidad de la información que manejas antes de pedir acciones. Si un contacto toma una acción respecto a nuestra petición, y luego resulta que la información que proporcionamos fue errónea, es poco probable que respondan en futuras ocasiones. Lo mismo se aplica a la información que proporcionamos a la prensa esperando cobertura.

Apelando a la empatía de nuestro interlocutor

- Las historias personales y testimonios pueden ser impactantes para la audiencia/diana y pueden servir para enganchar a gente emocionalmente en el lado humano de la problemática.
- Las historias personales y testimonios muestran el lado humano del problema y apelan a la empatía del interlocutor. Siempre hay que tener en cuenta la voluntad de la persona que da su testimonio, los riesgos de revictimización y la posible necesidad de un acompañamiento psico-social.

Evitar lo abstracto

- Ir por lo concreto siempre.
- ¡Nunca mentir!

Anexo T4 M5 S1c Continuación

Experiencias e ideas para reuniones de incidencia

DISCURSO (continuación)

No caigamos en la provocación, pero tampoco permitamos la difamación

- En caso de que un actor desee provocar una discusión a través de una difamación a un individuo/movimiento/propuesta, contrarrestemos la difamación, dejemos claro nuestro mensaje, y sigamos adelante con el discurso, sin permitir que la reunión se enfrasque en una discusión inútil.

Incluir herramientas audiovisuales en la medida de lo posible

- Hacer la interacción más interesante, apelar a sus distintos sentidos y gustos de comunicación. Este tipo de recursos facilitan la difusión con otros contactos.

Utilizar la diplomacia

- ¡Reconocer lo positivo... antes de destacar lo negativo!

Preguntas a las cuáles no sabemos contestar

- Se puede contestar que encontraremos la información y se la proporcionaremos después y acordar cómo; se puede entonces regresar a nuestro mensaje.

Sea apasionado/a por su mensaje/sujeto y el impacto que puede crear

- Y sea memorable.

Tener metas/objetivos para nuetras presentaciones

- Y que sean específicos, medibles, alcanzables, realistas y definidos en el tiempo.

En presentaciones públicas, utilizar la voz

- Cuidar las pausas, el ritmo, el tono, el impacto, los patrones, la pasión...
- Articular adecuadamente.

DESPUÉS DE LA REUNIÓN

Publicidad

- Si nuestra valoración es que sería estratégico que el público y otros actores supieran de la reunión o actividad, hay que pedir de forma explícita que el actor publique algo en su sitio web/revista/blog y pedir permiso para hacer lo mismo.

Respetar el acuerdo explícito o tácito

- Si la reunión fue privada, no divulgar su contenido públicamente. Hacerlo es una forma fácil de perder a potenciales aliados.
- Si no sabemos si podemos difundir alguna información ¡preguntar!

Seguimiento

- Un buen nivel de seguimiento es igual de importante que la preparación y la reunión misma.
- Saliendo de la reunión, es bueno apuntar los puntos claves, compromisos, puntos de seguimiento y pendientes.
- Mandar un correo de seguimiento lo más pronto posible con los pendientes más sencillos ya cubiertos.

Monitoreo

- Monitorear acciones e impacto es fundamental para poder redefinir, adaptar y mejorar las estrategias.
- Es importante poder demostrar el vínculo entre las acciones de las dianas que identificamos y el impacto que buscábamos para los beneficiarios. Hay que dar retroalimentación tanto a las dianas como los beneficiarios cuando es posible.

Reflexión

- Hay que tomar el tiempo para analizar los resultados y el impacto de reuniones y eventos, recopilando insumos de nuestra audiencia.
- En base en lo anterior, adaptar nuestros discursos para la próxima reunión.

Recursos adicionales y lecturas de apoyo

RA1) Recursos especializados para facilitación (dinámicas de presentación, juegos deconfianza, comunicación, cooperación, resolución de conflictos y distensión):

- BERISTAIN & CASCÓN, *La Alternativa del Juego I: Juegos y Dinámicas de Educación para la Paz*, Ed. Los Libros de la Catarata, Madrid, 1999.
- Caja de Herramientas Comunitarias "Desarrollar destrezas de facilitación".

  http://ctb.ku.edu/es/tabla-de-contenidos/liderazgo/facilitacion-al-grupo/desarrollar-habilidades-y-destrezas-de-facilitacion/principal

RA2) Facilitación enfocada en seguridad y protección de PDDH basada en metodologías de educación popular y atención en las distintos tipos de audiencias:

- Protection International, *Guía de facilitación para el nuevo manual de protección para los defensores de derechos humanos*, 2014.

  http://protectioninternational.org/wp-content/uploads/2014/08/140818_FACILITATORSGUIDE_ES_LT.pdf

RA3) Perspectiva psicosocial para el trabajo en derechos humanos y habilidades para la sensibilidad cultural y la comunicación con personas defensoras:

- BERISTAIN, *Manual sobre la Perspectiva Psicosocial en la investigación de derechos humanos*, Fundar-SERAPAZ-HEGOPA-CDHDF, 2011.

  http://www.contralatortura.org/uploads/1cf6ab_161345.pdf

RA4) Espacio seguro desde la perspectiva psicosocial, bienestar, salud mental, autocuidado emocional y dinámicas de distención:

- BARRY & NANIAR. *Integrated Security the Manual*, Urgent Action Fund for Women's Human Rights, The Kvinna till Kvinna Foundation, 2011.

  http://www.integratedsecuritymanual.org/sites/default/files/integratedsecurity_themanual_1.pdf
- CAPACITAR, *Herramientas de Capacitar que nos pueden ayudar en casos de emergencia*, 2005.

  http://www.capacitar.org/kits/SpanCapEmergKit%20.doc
- CONSTANZA & AGILAR, *Introducción a la Salud Mental*, Chiapas, CIEPAC, 2005.
- Inter-Agency Standing Committee, *Guía del IASC sobre Salud Mental y Apoyo Psicosocial en Emergencias Humanitarias y Catástrofes*, 2007.

  www.who.int/mental_health/emergencies/iasc_guidelines_spanish.pdf
- IM-Defensoras & JASS, *¿Qué signfica el autocuidado para las defensoras de derechos humanos?* - Diálogos entre nosotras, 2013.

  http://www.scribd.com/doc/204540151/Que-signfica-el-autocuidado-para-las-defensoras-de-derechos-humanos-Dialogos-entre-nosotras
- Espacio de Frontline sobre estrés en PDDH y herramientas para el bienestar:

  http://www.frontlinedefenders.org/es/node/15184
- Front Line Defenders, "Bienestar y estrés" en *Manual sobre seguridad: Pasos prácticos para defensores/as de derechos humanos en riesgo*, 2011, cap. 4.

  http://www.frontlinedefenders.org/files/workbook_sp.pdf

RA5) Seguridad y Protección para PDDH:

- Centro de Derechos Humanos Fray Francisco de Vitoria & Comité Cerezo, *Manual de Introducción: Seguridad en las organizaciones civiles y sociales*, 2010.

  http://comitecerezo.org/IMG/pdf/ManualSeguridadWeb.pdf
- EGUREN, *Beyond Security Planning: Towards a model of security Management*, July 2000.

  http://sites.tufts.edu/jha/files/2011/04/a060.pdf
- Front Line Defenders, *Manual sobre seguridad: Pasos prácticos para defensores/as de derechos humanos en riesgo*, 2011.

  http://www.frontlinedefenders.org/files/workbook_sp.pdf
- MAHONY & EGUREN, *En buena compañía: el Acompañamiento Internacional para la Protección de los Derechos Humanos*, Universidad de Cantabria, 2006.
- New tactics in Human Rights, "Staying Safe: Security Resources for Human Rights Defenders", 2010.

  https://www.newtactics.org/conversation/staying-safe-security-resources-human-rights-defenders
- Peace Brigades International (Oficina Europea) & Frontlinde Defenders, *Manual de Protección para los Defensores de Derechos Humanos*, 2005.

  http://www.frontlinedefenders.org/files/en/Protection%20Manual%20for%20Human%20Rights%20Defenders%20Spanish.pdf

- Protection International, *Nuevo Manual de Protección para los Defensores de Derechos Humanos*, 2010.

  http://protectioninternational.org/wp-content/uploads/2012/04/Nuevo_Manual_Proteccion.pdf

RA6) Seguridad y protección para PDDH con perspectiva de género:

- AWID, *Diez ideas para fortalecer las respuestas a mujeres defensoras de los derechos humanos en riesgo*, 2012.

  http://awid.org/esl/Library/Diez-ideas-para-fortalecer-las-respuestas-a-mujeres-defensoras-de-los-derechos-humanos-en-riesgo

- _____, *Lista de Materiales y Recursos para las defensoras de los derechos humanos.*

  http://awid.org/esl/content/download/101561/1220755/file/WHRD_materiales_recursos.pdf

- IM–Defensoras, "A Feminist Alternative for the Protection, Self-Care, and Safety of Women Human Rights Defenders in Mesoamerica", *Journal of Human Rights Practice*, Vol. 5, Núm. 3, 2013.

  http://jhrp.oxfordjournals.org/content/early/2013/10/07/jhuman.hut017.full.pdf+html

- Jane Barry with Vahida Nainar. *Insiste, Persiste, Resiste, Existe*, Urgent Action Fund for Women's Human Rights, The Kvinna till Kvinna Foundation and Front Line International Foundation for the Protection of Human Rights Defenders, 2008.

  http://urgentactionfund.org/wp-content/uploads/downloads/2012/06/Insiste-Resiste-Persiste-Existe-WHRDs-Security-Strategies.pdf

- Protection International & UDEFEGUA, *Cuadernos de Protección* No.. 4 Protegiendo tu vida, mi vida, nuestra vida, 2012.

  http://protectioninternational.org/wp-content/uploads/2013/09/Cuaderno-n.4-Protegiendo-tu-vida-mi-vida-nuestra-vida.pdf

RA7) Sobre las Personas Defensoras de Derechos Humanos:

- OACNUDH Video Campaña "Yo me declaro"

  http://www.youtube.com/watch?v=O9VeYx-svnE&feature=youtu.be

- _____, *Comentario a la Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos*, 2011.

- ONU, *Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones de promover y proteger los derechos humanos y las libertades fundamentales universalmente reconocidos*, 9/12/1998, A/RES/53/144.

  http://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=528e06b04

RA8) PDDH en México y su situación en seguridad y protección:

- Acción Urgente para Defensores de Derechos Humanos, Campaña Nacional Contra la Desaparición Forzada y Comité Cerezo México, *La defensa de los derechos humanos en México: una lucha contra la impunidad, junio de 2013 a mayo de 2014*.

  http://comitecerezo.org/IMG/pdf/informeweb.pdf

- Brigadas Internacionales de Paz – Proyecto México, Panorama de la Defensa de los Derechos Humanos en México: Iniciativas y Riesgos de la Sociedad Civil Mexicana, México 2013.

  http://www.pbi-mexico.org/fileadmin/user_files/projects/mexico/files/PBI_Publications/Panorama_de_la_Def ensa_de_los_Derechos_Humanos_en_Me%CC%81xi.pdf

- OACNUDH México, *Informe sobre la situación de las y los defensores de derechos humanos en México* : actualización 2012 y balance 2013.

  http://hchr.org.mx/files/doctos/Informe_defensoresDH_2013_web.pdf

- Red TDT, *El derecho a defender los derechos humanos en México: Informe sobre la situación de las personas defensoras* 2011-2013.

  https://www.dropbox.com/s/jj1tw0490fslbxt/INFORME%202014%20REDTDT%20Final.pdf

- Ley Federal de Protección para Personas Defensoras y Periodistas,

  http://www.diputados.gob.mx/LeyesBiblio/pdf/LPPDDHP.pdf

- JOLOY, "Mexico's National Protection Mechanism for Human Rights Defenders: Challenges and Good Practices", Journal of Human Rights Practice, Vol. 5, Núm. 3, 2013.

  http://jhrp.oxfordjournals.org/content/5/3/489.full.pdf+html

RA9) Manuales adaptados para grupos específicos de PDDH:

LGBTI :

- Protection International, *Manual de protección para defensores LGBTI.*

  http://protectioninternational.org/wp-content/uploads/2013/02/Manual-de-protecci%C3%B3n-para-defensores-LGBTI-%E2%80%93-Primera-edici%C3%B3n.pdf

Defensores comunitarios:

- Protection International & UDEFEGUA, *Cuidándonos. Guía de protección para defensoras y defensores de derechos humanos en áreas rurales*, 2012.

  http://protectioninternational.org/wp-content/uploads/2013/05/Cuaderno-Cuidandonos-Guia-Proteccion-Rural-Dec-2012.pdf

Periodistas:

- Comité para la Protección de los Periodistas, *Manual de seguridad para periodistas.* Cubriendo las noticias en un mundo peligroso y cambiante, 2012.

  http://cpj.org/security/guide_es.pdf

RA10) Seguridad digital:

- FLORES HINE, *¡Pongámonos las pilas! Reflexiones y acciones concretas para asegurar la información en nuestras organizaciones sociales*, México 2009.

  http://protectionline.org/files/2012/10/Manual-de-Sedem-sobre-seguridad-inform%C3%A1tica-%C2%ABPong%C3%A1monos-las-pilas%C2%BB.pdf

- SEDEM Asociación para el Estudio y Promoción de la Seguridad en Democracia, *Guía de Protección para defensores de derechos humanos, periodistas y operadores de justicia*, Guatemala, 2005.

  http://www.libertad-expresion.org.mx/wp-content/uploads/2009/01/Gu%C3%ADa-Proteccion-Sedem-Guatemala-2005.pdf

- System of Solidarity of Support, *Digital Security.*

  http://sos.escr-net.org/resources/digital-security

- Tactical Technology Collective & Front Line Defenders, *Security in a box. Caja de herramientas de Seguridad protegiendo tu privacidad digital* ,

  https://securityinabox.org/es

RA 11) Documentos especializados sobre análisis de contexto:

- Consejo de Educación Popular de América Latina y el Caribe, *Guía para hacer análisis de coyuntura*,

  http://www.ceaal.org/sitefiles/texteditor/imagenes/Guia%20Coyuntura.doc

RA 12) Vigilancia y criminalización de PDDH:

- Protection International, *Cuadernos de Protección Núm. 2 Vigilancia y contravigilancia para organizaciones defensoras de derechos humanos*, Guatemala, 2011.

  http://protectioninternational.org/wp-content/uploads/2012/05/cuaderno_no_2_vigilancia_y_contravigilancia.pdf

- Protection International & UDEFEGUA, *Guía para defensoras y defensores de derechos humanos ante la criminalización*, Guatemala, 2009.

  http://protectioninternational.org/wp-content/uploads/2012/05/folleto_guia_criminalizacion.pdf

RA 13) Incidencia Política:

- Centro para el Diálogo Humanitario, *Presencia proactiva Estrategias de terreno campo para la protección de la población civil,* Suiza, 2006.

  http://www.fieldviewsolutions.org/fv-publications/PP_resumen_esp.pdf

- CONECTAS *Derechos Humanos, Política Exterior y Derechos Humanos: Estrategias para la acción de la sociedad civil*, Brasil, 2009.

  http://www.conectas.org/arquivos/editor/files/CONECTAS%20Esp_hyper.pdf

- Federación Internacional de Planificación de la Familia, "Comprensión de los indicadores para un proyecto de Advocacy", *Manual de planeación en advocacy*, México, 2009.

  https://www.ippfwhr.org/sites/default/files/ManualPlaneacionAdvocacy.pdf

- *New tactics in Human Rights, " Powerful Persuasion: Combating Traditional Practices that Violate Human Rights", 2013.*

  https://www.newtactics.org/conversation/powerful-persuasion-combating-traditional-practices-violate-human-rights

- _____, "8 Powerful Persuasion Tactics".

  https://www.newtactics.org/resource/8-powerful-persuasion-tactics

- Oficina en Washington para Asuntos Latinoamericanos (WOLA), *Manual básico para la incidencia política*, Washington, 2005.

  http://www.wola.org/sites/default/files/downloadable/Advocacy%20Training/past/atp_manualbasi co.pdf

- Tactical Technology Collective, *Visualising Information for Advocacy*, 2014.

  https://www.tacticaltech.org/visualising-information-advocacy

Responsabilidades

Los contenidos de esta guía no representan necesariamente la posición de Brigadas de Paz Internacionales. Ni las personas que han escrito esta obra ni quien la publica garantizan que la información contenida en la misma esté totalmente completa y exenta de errores.

Esta guía y sus contenidos no pueden tomarse como garantía de seguridad absoluta para las personas defensoras de derechos humanos. Las personas u organizaciones que decidan aplicar sus contenidos lo deberán de hacer bajo su propia responsabilidad, complementando las estrategias propuestas con sus propios análisis de riesgo.

Programa de Asesorías en Seguridad y Protección
para Personas Defensoras de Derechos Humanos

Brigadas Internacionales de Paz (PBI) es una organización no gubernamental con 30 años de experiencia en el acompañamiento internacional y con presencia permanente en México desde 1999. PBI tiene como objetivo la protección del espacio de actuación de las personas y organizaciones que promueven los derechos humanos de manera no violenta y que sufren represión por su trabajo.

Actuando a petición de las organizaciones locales, PBI no pretende suplantar en ningún momento las iniciativas mexicanas que promueven el respeto a los derechos humanos sino que se limita a apoyarlas con su presencia.

PBI realiza visitas periódicas a zonas en conflicto, distribuye información y realiza tareas de interlocución con autoridades civiles y militares, así como con organizaciones de derechos humanos y otros actores de la sociedad civil mexicana. Para promover cobertura internacional, PBI mantiene diálogo con el cuerpo diplomático y órganos intergubernamentales, divulga información y solicita apoyo exterior para garantizar la seguridad de las y los defensores mexicanos. PBI busca contribuir a crear las condiciones necesarias para que las personas defensoras puedan continuar su labor.

Puede obtener más información sobre el trabajo de PBI en México en nuestra página web: *www.pbi-mexico.org*

BRIGADAS INTERNACIONALES DE PAZ
PROMOVIENDO LA NO VIOLENCIA Y
PROTEGIENDO LOS DERECHOS HUMANOS DESDE 1981
www.peacebrigades.org

pbi abriendo espacios para la paz

Guía de facilitación