PROTECTION international

Nuevo Manual de Protección para los Defensores de Derechos Humanos

Investigación y Texto de Enrique Eguren y Marie Caraj

Nuevo Manual de Protección

para

Los Defensores de Derechos Humanos

Investigación y Texto de Enrique Eguren y Marie Caraj

Protection International (PI)

Publicado por Protection Internacional en 2010

Publicado por Protection International en diciembre de 2010
Rue de la Linière, 11
1060 Bruselas - Bélgica.
Primera edición en español (basada en la tercera edición en inglés).

Puede pedir copias del Nuevo Manual a:

Protection International
Rue de la Linière, 11. 1060 Bruselas (Bélgica)
Tel: +32(0)2 609 44 09 Fax: +32(0)2 609 44 06
pi@protectioninternational.org

Se puede descarga de manera gratuita en: **www.protectionline.org**
Precio de la copia impresa:

Distribución gratuita

El Nuevo Manual existe en inglés, francés, español, portugués y árabe (Protection International lo está traduciendo también a otros idiomas).

ISBN: 978-2-930539-04-1

EAN 9782930539041

Impreso por:
Impresora Aco
Simón Bolivar No. 132
Col. Juárez Pantitlán
Cd. Nezahualcoyótl
Edo. de México. C.P. 57460
Tel. (01) 5793-5196
e-mail: impresora_aco@yahoo.com.mx

Prefacio de Hina Jilani (Primera edición)

En mi trabajo como Representante Especial de Defensores de Derechos Humanos del Secretario General he notado con mucha preocupación un aumento en el número de informes sobre abusos serios de derechos humanos contra los defensores de derechos humanos, y un notable cambio en estos abusos, pasando de acciones de nivel bajo, como intimidación y hostigamiento, a violaciones más serias, como amenazas y ataques contra la integridad física de los defensores. En el 2004 hemos trabajado en informes de al menos 47 defensores que han sido asesinados debido a su trabajo.

Está claro que la responsabilidad principal de la protección de los defensores recae en los gobiernos, tal y como está establecido en la Declaración sobre Defensores de Derechos Humanos de las Naciones Unidas.[1] *Debemos continuar trabajando para que todos los gobiernos tomen seriamente en consideración sus obligaciones con respecto a esto y para que tomen medidas efectivas para asegurar la protección de los defensores.*

Sin embargo la gravedad de los riesgos que los defensores asumen a diario es tal que es también importante buscar otros medios para reforzar su protección. En este sentido, espero que este Manual de Protección sirva para apoyar a los defensores en el desarrollo de sus propios planes de seguridad y mecanismos de protección. Muchos defensores están tan comprometidos en su trabajo para proteger a otros que a veces no prestan la suficiente atención a su propia seguridad. Es importante que todos los que estamos involucrados en el trabajo de derechos humanos entendamos que debemos preocuparnos tanto por nuestra propia seguridad como por la de las personas con las que y por las que trabajamos.

Hina Jilani

Representante Especial para Defensores de Derechos Humanos del Secretario General de las Naciones Unidas (2000-2008)

[1] 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.

Protection International -PI-

Las personas que trabajan en PI tienen más de 25 años de experiencia en la protección de defensoras y defensores de derechos humanos y otros grupos vulnerables.[2]

En PI trabajamos para ayudar a que se haga realidad la obligación que existe a nivel nacional e internacional de ofrecer protección a las personas que defienden los derechos humanos. Numerosas ONGs y organismos trabajan el tema de los derechos humanos y su defensora, y el trabajo de PI se inscribe en este marco.

La estrategia global de PI para ofrecer protección ofrece:

Formación

- Valoración de los riesgos, gestión de los temas de seguridad y protección.
- Transmisión del conocimiento y las herramientas necesarios.
- Publicación de manuales, como el presente Nuevo Manual (y su anterior edición).[3]
- Formación: entre 2004-2008 más de 1.700 defensores y defensoras/es han participado en los talleres de PI de seguridad y protección, lo que les ha ayudado a mejorar la gestión de su propia seguridad así como el servicio de protección que le ofrecen a otras personas.

Investigación

- Estudio y elaboración de herramientas útiles para temas de protección /seguridad.
- Publicación de información basada en lo aprendido en el terreno y lo que ha funcionado mejor en la práctica.

Protección

- Distribución de información sobre protección entre DDH, IDP (Desplazados internos), organismos de la UE y Estados Miembros de la UE: recomendaciones, informes, comunicados de prensa y documentales.

[2] A partir del 25 de octubre de 2007 y por decreto del Servicio Público Federal d Justicia, la Oficina Europea de Brigadas Internacionales de Paz, mediante la enmienda de sus estatutos publicados en el Boletín Oficial Belga, se constituyó en "Protection International", una asociación internacional sin ánimo de lucro.

[3] Publicada en 2005 con el apoyo económico de Front Line y la Cooperación al Desarrollo de Irlanda.

- Recordatorio a las autoridades nacionales e internacionales de sus obligaciones internacionales en materia de protección a DDH, IDP, poblaciones refugiadas y otros actores sociales.
- Promoción de debates y de actuación a favor de la protección de las y los defensores; contactos con parlamentos, sindicatos y medios de comunicación.
- Lucha contra la impunidad mediante cabildeo y observación de juicios.

Lucha contra la impunidad mediante cabildeo y observación de juicios

Vídeo-advocacy (protección a través del medio audiovisual)

- Retratos de defensoras y defensores de derechos humanos.

Oficinas

- En colaboración con redes locales de DDH, establecimiento de oficinas de protección que funcionen como centros nacionales y regionales para la protección y la gestión de la seguridad.
- Traspaso progresivo a las Oficinas de Protección de todo el proceso de gestión de la seguridad/protección (asumir toda la gestión es parte de dicho proceso).

Protectionline

- www.protectionline.org es un sitio web realizado por, con y para las defensoras y los defensores de derechos humanos (DDH) y quienes desean trabajar en la protección de DDH.
- Actualización diaria de información, documentos, publicaciones, testimonios, acciones urgentes y herramientas diseñadas para impulsar la protección de DDH.

Marco legal:

PI se rige por el derecho humanitario internacional y los derechos humanos. Más concretamente, utiliza las directrices que proporcionan la Declaración de las Naciones Unidas sobre Defensoras/es de Derechos Humanos (1998), las Directrices de la Unión Europea para DDH (2004), así como las resoluciones sobre defensoras/es impulsadas por PI y adoptadas por estados miembros de la UE en España, Bélgica y Alemania.

Talleres de protección y seguridad de PI

De 2004 a 2007, 1.747 defensoras y defensores de derechos humanos (DDH) han participado en los talleres de protección y seguridad de PI.

- En Sudámerica y Centroamérica: 558 DDH
  (Bolivia, Brasil, Colombia, Guatemala, Honduras, México, Perú)
- En Asia: 650 DDH
  (Birmania, Indonesia, Nepal, Tailandia)
- En África: 441 DDH
  (Kenia, Uganda, República Democrática del Congo)
- En Europa: 98 DDH
  (Alemania, Bélgica, Irlanda, Serbia, República de Ingushetia)

Los defensores trabajan para proteger a otras personas, pero a menudo sin prestar suficiente atención a su propia seguridad. Esto sucede por diferentes razones; la formación en seguridad que PI ofrece aborda estas razones y ofrece un espacio para reflexionar sobre los riesgos y las amenazas que afrontan los defensores. La formación de PI ofrece el conocimiento y la lógica que se necesitan para incorporar la debida seguridad a los planes de trabajo de los defensores; durante la formación se analizan los distintos componentes de la seguridad, se reflexiona sobre los escenarios y opciones posibles, y se elige el curso de acción que sea más manejable para los defensores, siempre sabiendo que ninguna opción ofrecerá plena garantía de seguridad.

En cualquier caso, no se va a encontrar una solución mágica que funcione siempre; la formación en seguridad intenta ofrecer a los defensores las herramientas necesarias para analizar, gestionar y actualizar las opciones en seguridad. Y es necesario hacer esto a nivel individual, a nivel de la organización, y a nivel inter-organizacional, teniendo siempre en cuenta la exposición física, psicosocial y política a los riesgos.

Prefacio

Tras más de una década de formación, investigación y reuniones con defensoras y defensores de derechos humanos y los agentes sociales responsables de la protección de los mismos, quienes trabajamos en Protection International hemos decidido renovar nuestro tributo a las y los defensores incluyendo una vez más sus aportaciones en este Nuevo manual, escrito con, por y para las y los defensores de derechos humanos.

En los últimos tres años, Protection International ha seguido desarrollando sus sesiones de formación y sus investigaciones partiendo de sus experiencias en el campo y su comunicación con las defensoras y los defensores de derechos humanos.

En el Nuevo manual, Protection International presenta un enfoque que puede adoptarse en diferentes tipos de contextos y estructuras para lograr un mismo resultado: la incorporación de un plan de seguridad al plan de trabajo. No existen soluciones mágicas, tan sólo opciones y consecuencias que hay que gestionar. Esto puede hacerse a través de lluvias de ideas, la formulación de las preguntas adecuadas, la valoración de riesgos y de cuestiones de seguridad en la organización, el diseño de planes y procesos inclusivos...

Este Nuevo manual pretende, por tanto, que las y los defensores de derechos humanos puedan asumir y llevar a la práctica la lógica y los procesos de seguridad y protección que les afectan, pues desarrollar esta capacidad es parte integral del proceso de mejora en cuestiones de seguridad. Así pues, el Nuevo manual es una herramienta para el desarrollo de la independencia y la sostenibilidad de los procesos de seguridad y protección que afectan a sus protagonistas.

Aunque no existe un plan de seguridad aplicable a toda situación, el Nuevo manual transciende las diferencias generadas por los diferentes contextos y estructuras culturales, sociales, religiosas y de organización: puede usarse fácilmente con la información del conocimiento y la experiencia que las y los defensores desarrollan en sus lugares de trabajo.

Protection International diferencia entre la seguridad de los defensores de derechos humanos (hacia sí mismos) y la necesaria protección de los defensores de derechos humanos por parte de las autoridades responsables de la misma.

Agradecimientos:

♦ Para la elaboración de esta nueva versión del manual hemos incluido aportaciones de:

• Todas y todos los defensores de derechos humanos que han asistido hasta la fecha a los talleres de formación en gestión de seguridad y protección impartidos por Protection International. No podemos nombrarles a todos. Mencionar al menos su procedencia: Bolivia, Brasil, Burma, Colombia, República Democrática del Congo, Guatemala, Honduras, Indonesia, Ingushetia, Kenia, México, Nepal, Perú, Serbia, Sri Lanka, Tailandia, Uganda.

• Las personas que actualmente trabajan y que trabajaron antes para PI: Pascale Boosten, Soledad Briones, Shaun Kirven, Christoph Klotz, Rainer Mueller, Michael Schools.

• Las y los colaboradores, de ahora y del pasado: Ana Cornide, Jérôme Hieber, Eric Juzen, María Martín, Thomas Noirfalisse, Sheila Pais, Flora Petrucci, Sophie Roudil, Catherine Wielant, Javier Zabala…

• Carmen Díez Rozas y Montserrat Muñoz, quienes trabajaron con el máximo mimo y cuidado en el diseño y maquetación del anterior manual así como del presente. Thomas Noirfalisse, que diseñó el logo de PI y aportó ideas para el diseño de la cubierta del manual.

Un cariñoso recuerdo para Brigitte Scherer.

Quisiéramos agradecer el apoyo al Bundeministerium für Wirtschaftliche Zusammenarbeit und Entwicklung (Ministerio alemán para la Cooperación y el Desarrollo) y al Service public fédéral Affaires Etrangères Belgique (Servicio Público de Asuntos Exteriores belga).

El Nuevo Manual de Protección para Defensoras/es de Derechos Humanos revisa y amplía el primer Manual de Protección para Defensoras/es de Derechos Humanos (autor: Luis Enrique Eguren © 2005 PI), que fue publicado con el apoyo económico de Front Line y la Cooperación al Desarrollo de Irlanda.

El borrador de este manual fue leído y comentado por Arnold Tsunga (Zimbawe, Abogados a favor de los Derechos Humanos), Sihem Bensedrine (Túnez, Conseil National pour les Libertés en Tunisie), Padre Bendan Forde (Colombia, Franciscanos Itinerantes), Indai Sajor (Filipinas, antiguo Director del Centro Asiático para los Derechos Humanos), James Cavallaro (Brasil, Director asociado del Programa para los Derechos Humanos del Harvard Law School), y Nadejda Marques (Brasil, Asesora e Investigadora de Global Justice).

Asimismo, han aportado su trabajo: José Cruz e Iduvina de SEDEM (Guatemala), Jaime Prieto (Colombia), Emma Eastwood (Reino Unido) y Cintia Lavandera del Programa para Defensoras/es de Derechos Humanos de Amnistía Internacional en Londres.

El Programa para Defensoras/es de Derechos Humanos de Amnistía Internacional en Londres y el Proyecto Indonesia de PBI proporcionaron los fondos necesarios para la traducción de la primera edición del manual al portugués y al indonesio,

respectivamente. La Comisión Internacional de Juristas lo tradujo al tailandés, y PBI al nepalí. Otras instituciones van a colaborar en sucesivas traducciones de este Nuevo Manual.

El capítulo 1.11 está basado en el trabajo de Robert Guerra, Katitza Rodríguez y Caryn Madden de Privaterra (Canadá).

Agradecimientos del autor: Luis Enrique Eguren

Existen más personas que han contribuido a que podamos reunir el conocimiento necesario para escribir este manual, y ciertamente es imposible mencionarlas a todas. Quisiera al menos mencionar a las personas de PBI, en especial, a las que fueron mis compañeras y compañeros en el proyecto de Colombia: Marga, Elena, Francesc, Emma, Tomás, Juan, Mikel, Solveig, Mirjam, Jacobo y tantas otras…

A Danilo, Clemencia y Abilio y sus compañeros de la Comisión Intereclesial de Justicia y Paz de Colombia, que me enseñaron a vivir con el corazón de la gente.

A la gente de Santa Marta, en El Salvador, y de Cacarica, Jiguamiando y San José de Apartadó en Colombia, que, entre otras cosas, me mostraron la dignidad con que vive la gente del campo.

A Irma Ortiz, co-formadora en muchos talleres, y a todos los otros compañeros de Pensamiento y Acción Social (PAS) de Colombia.

Por sus consejos y el conocimiento inicial que me proporcionaron, a REDR (Londres) y Koenraad van Brabant (Bélgica).

Y a las muchas personas defensoras de derechos humanos que conocí en El Salvador, Guatemala, Colombia, México, Perú, Bolivia, Burma, Sri Lanka, Croatia, Serbia, Kosovo, Ruanda, República Democrática del Congo, Ingushetia, etc. Un mar de conversaciones, lágrimas, sonrisas, aprendizaje y compromiso…

Por último, nada de esto me habría sido posible sin el amor y la dedicación y el apoyo de Grisela e Iker y de mis padres. Todo mi amor para ellos.

Agradecimientos de la coautora: Marie Caraj

Siento admiración, respeto, solidaridad, empatía y agradecimiento hacia todas/todos y cada uno/una de los defensores que he conocido, conoceré o nunca conoceré: han cambiado mi vida. Los días compartidos, de manera imperceptible, nos han unido.

Me siento dividida entre la rabia hacia los violadores de derechos humanos y la esperanza de que un día éstos puedan darse cuenta de que los/las defensores de derechos humanos no les discriminan, sino que pueden unirse a este movimiento hacia el día en que todos los derechos humanos sean respetados y quienes los defienden puedan disfrutar de una vida normal.

A Leze Gegaj, mi madre, la primera defensora de derechos humanos que conocí.

A todas mis amigas, amigos y compañeros por su apoyo tácito o explícito. Casi todos han compartido las historias que me traje conmigo y me han ayudado a recargar las pilas.

Por todo lo que nos han dado, le damos las gracias a todas las personas mencionadas y a muchas otras con las que hemos trabajado y de las que hemos aprendido. Cualquier error de este Nuevo manual será porque no lo detectamos al revisarlo (¡aunque nos hemos empeñado en intentar eliminarlos todos!). Esperamos que este trabajo pueda ser una herramienta útil para mejorar la protección y la seguridad de las y los defensores, aunque entendemos que no proporciona ninguna garantía de resultados y que en estos temas cada cual debe asumir su parte de responsabilidad. No dudéis en enviarnos vuestros comentarios.

Protection International

April 2009

Cláusula de exención de responsabilidad

Los contenidos de este manual no representan necesariamente la posición de Protection International.

Ni las personas que han escrito esta obra ni quien la publica garantizan que la información contenida en la misma esté completa y exenta de errores, por lo que no son responsables de ningún daño que se pudiera asociar al haberla utilizado. Ninguna parte de este manual puede tomarse como norma o como garantía de nada, y tampoco puede usarse sin los criterios necesarios para valorar los riesgos y los problemas de seguridad a los que se enfrentan las defensoras y los defensores.

INTRODUCCIÓN

Nuevo manual de protección para defensoras y defensores de derechos humanos

Defensores y defensoras de derechos humanos en riesgo

El derecho internacional garantiza el respeto a los derechos humanos; sin embargo, trabajar para que esto sea así y con casos de personas que han sido objeto de violaciones de derechos humanos puede ser peligroso en muchos países del mundo. Las y los defensores de derechos humanos son a menudo la única defensa que tienen las personas objeto de actuaciones abusivas por parte de un Estado. Por lo tanto, su trabajo es vital para desarrollar las instituciones y los procesos democráticos, para poner fin a la impunidad y para impulsar y proteger los derechos humanos.

Es frecuente que las y los defensores se enfrenten a situaciones de acoso, arresto, tortura, difamación, suspensión de empleo, negación de libertad de movimiento, y dificultad para obtener el reconocimiento legal que precisan sus organizaciones. En algunos países, además, estas personas son asesinadas, secuestradas o desaparecidas.

En los últimos años se ha tomado más conciencia sobre el riesgo que enfrentan quienes trabajan en derechos humanos. Es fácil identificar este riesgo cuando las y los defensores desarrollan su trabajo en situaciones hostiles, como por ejemplo, en lugares donde se penalizan ciertos tipos de actividades relacionadas con la defensa de los derechos humanos. Sin embargo, también corren peligro allí donde a pesar de la existencia de leyes que protegen los derechos humanos, éstas no se aplican cuando se producen amenazas o ataques. En situaciones de conflicto armado, el riesgo es incluso mayor.

Aunque puedan darse situaciones caóticas en las que, por ejemplo, la vida de una defensora esté en manos de lo que puedan hacer determinados soldados en un puesto de control, la violencia ejercida contra las y los defensores no es aleatoria. En la mayoría de los casos los ataques que sufren son una respuesta premeditada y cuidadosamente calculada contra su trabajo, respuesta que suele inscribirse además en el marco más amplio de un proyecto político o militar.

Lo grave de la situación hace que sea necesario que quienes se dedican a la defensa de los derechos humanos desarrollen estrategias de seguridad integrales y adaptables en su trabajo cotidiano. Los consejos bien intencionados o recordarles que deben cuidarse no sirve de mucho. Lo fundamental es pensar cómo puede gestionarse el tema de la seguridad.

Este manual no puede ofrecer una serie de fórmulas fijas aplicables a cualquier escenario posible; pero sí pretendemos ofrecer un conjunto de estrategias que ayuden a mejorar la protección y la seguridad de las y los defensores de derechos humanos.

Las mejores lecciones de seguridad proceden de las y los propios defensores: aprendemos de su experiencia cotidiana y de las tácticas y estrategias que desarrollan a lo largo del tiempo para proteger tanto a las personas con las que trabajan como a su propio equipo. Consecuentemente, este manual será revisado y actualizado conforme nos llegue su información. Otra fuente valiosa son las ONGs humanitarias internacionales que han empezado a elaborar reglas y medidas de seguridad para proteger a quienes trabajan en ellas.

Es importante que comprendamos que el principal riesgo que corren las y los defensores es que las amenazas suelen acabar materializándose en ataques. Los agresores disponen de la voluntad, los medios y la impunidad necesarios como para consumarlas. Así pues, la mejor herramienta de protección es una acción política dirigida a abordar el gran tema pendiente: la necesidad de que los gobiernos y la sociedad civil presionen y actúen con objeto de impedir que quienes día a día amenazan, acosan y asesinan a quienes defienden los derechos humanos puedan seguir haciéndolo. Lo que aconsejamos aquí no sustituye en modo alguno la responsabilidad que todos y cada uno de los gobiernos tienen de proteger a quienes defienden los derechos humanos.

Una vez aclarado esto, las y los defensores de derechos humanos pueden mejorar significativamente su seguridad siguiendo una serie de reglas y procedimientos que han sido concebidos y puestos en práctica en el terreno.

Este manual es una pequeña aportación a un objetivo que compartimos muchas organizaciones diferentes: el de preservar el valiosísimo trabajo que están haciendo quienes se dedican a la defensa de los derechos humanos. Son estas personas las principales partes interesadas en este manual además de sus protagonistas indiscutibles.

El Manual

El propósito de este manual es ofrecer a las y los defensores de derechos humanos una serie de nociones y herramientas útiles que les ayuden a mejorar su comprensión de los temas de protección y seguridad. Pensado como herramienta para los cursos de formación en el tema de seguridad y protección, se espera que les ayude a evaluar los riesgos que corren y a establecer reglas y medidas de seguridad adecuadas a las situaciones concretas que les toca vivir.

Esta publicación es el producto de más de 25 años de experiencia de las personas que colaboramos con Protection International (PI), tanto en el área de los

derechos humanos y el derecho humanitario como en la protección de las y los defensores y otros grupos vulnerables. Esta experiencia arrancó con nuestro trabajo en la estructura y los proyectos de Brigadas de Paz Internacionales (Peace Brigades International, PBI). Además, hemos disfrutado de la oportunidad de aprender de, y de compartir experiencias y conocimientos con cientos de defensoras y defensores en los lugares donde trabajaban, en talleres, en reuniones y foros sobre seguridad. Casi todo el contenido del manual ha sido puesto en práctica, ya sea aplicándolo en la protección de personas que se dedican a la defensa de los derechos humanos o bien usándolo en cursos de formación. Este manual es el fruto de todos estos intercambios, por lo que queremos dar nuestro más cariñoso agradecimiento a todas estas personas, por todo lo que nos han aportado.

La seguridad y la protección son campos complejos. Parten de un conocimiento estructurado, pero también se ven influidas por actitudes individuales y por las rutinas del día a día que se generan en las organizaciones. Uno de los mensajes clave del manual es que hay que dedicarle al tema de la seguridad el tiempo, el espacio y el esfuerzo necesarios, a pesar de la presión que ejerce en las personas y organizaciones el volumen de trabajo existente, y a pesar del estrés y el miedo por los que se pasa. Esto implica ir más allá de lo que cada persona sabemos sobre seguridad para poder construir una cultura de organización en la que los temas de seguridad sean algo inherente.

Otras claves para gestionar adecuadamente el tema de la seguridad son conocer bien el escenario del conflicto y comprender la lógica política que opera en el lugar donde trabajemos. Este manual contiene un marco general y unos pasos concretos útiles para el diseño de un plan de seguridad (un producto) y también para su gestión (el proceso). Se incluyen reflexiones sobre conceptos básicos como riesgo, vulnerabilidad y amenaza, además de algunas sugerencias sobre cómo mejorar y aumentar la seguridad de las y los defensores en su trabajo diario. Esperamos que los temas cubiertos permitan a las ONGs y a las y los defensores prever y abordar los crecientes problemas de seguridad que enfrenta el trabajo de derechos humanos.

Quisiéramos recordar que las personas que defienden los derechos humanos ponen en juego su bienestar y sus vidas, y que esto es una cuestión muy seria. A veces la única manera de salvar una vida es pasar a la clandestinidad y después huir. Las técnicas y sugerencias recogidas en este manual no son la única forma de abordar el tema de su seguridad; desearíamos dejar esto muy claro. Hemos escrito este trabajo con toda nuestra buena voluntad, pero (y lo decimos con tristeza) no está en nuestra mano ofrecer ningún tipo de garantía.

Mejoremos el manual...

Los riesgos cambian, por lo que será preciso revisar este manual periódicamente. Si eres defensor o defensora de derechos humanos, todo lo que puedas comentarnos tendrá un valor inmenso para que podamos mejorarlo.

Podéis enviarnos todas vuestras ideas y comentarios, en especial las relativas al uso del manual en vuestro contexto. Con vuestra ayuda, mejoraremos una herramienta diseñada especialmente para personas que defienden los derechos humanos en todo el mundo.

Nuestro correo electrónico es:

pi@protectioninternational.org

Otros datos de contacto:

Protection International. Rue de la Linière, 11 - 1060 Bruselas (Bélgica)
Tel: + 32 (0) 2 609 44 05, +32 (0) 2 609 44 07
Fax: +32 (0) 2 609 44 06

www.protectioninternational.org
www.protectionline.org

Breve introducción sobre las defensoras y los defensores de derechos humanos

'Defensora o defensor de derechos humanos' es un término empleado para describir a personas que, individualmente o con otras, actúan para impulsar o proteger los derechos humanos. Se identifica a estas personas sobre todo por las actividades que realizan, por lo que el término se explica mejor describiendo sus acciones y algunos de los contextos donde trabajan. Las actividades que realizan las y los defensores de derechos humanos son legales y están legitimadas por la sociedad civil, a la que representan. Todos los días, en todo el mundo, cientos de defensoras y defensores de derechos humanos se ven expuestos a la violencia política debido a su defensa de los derechos de otras personas. Arriesgando su propia integridad física y mental, luchan por poner fin a la impunidad de las violaciones de derechos humanos y por impulsar la paz y la justicia social.

En 1998 la Asamblea General de las Naciones Unidas (ONU) aprobó 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" (conocida como la "Declaración sobre los Defensores de Derechos Humanos" de la ONU). En otras palabras, 50 años después de la "Declaración universal de derechos humanos" y tras 20 años negociando el borrador de una declaración sobre defensoras y defensores de derechos humanos, las Naciones Unidas reconocen al fin la realidad: que miles de personas luchan por la protección de los derechos humanos en todo el mundo. Esta declaración reconoce, por tanto, la cantidad y la diversidad de personas que trabajan por impulsar y proteger los derechos humanos.

Inicialmente se creó el puesto de Representante Especial del Secretario General de las Naciones Unidas sobre Defensores de Derechos Humanos, con la misión de "buscar, recibir, estudiar y responder a información sobre la situación y los derechos de cualquier persona que, actuando individualmente o en asociación con otras, se dedique a fomentar y proteger los derechos humanos y las libertades fundamentales".[1] En 2008 este puesto ha sido reemplazado por el de Relator/a Especial sobre Defensores y Defensoras de Derechos Humanos.

[1] "Los defensores de los derechos humanos: protección del derecho a defender los derechos humanos". Folleto informativo nº 29. http://www2.ohchr.org/spanish/about/publications/docs/fs29_sp.pdf

En la "Guía sobre los defensores de derechos humanos" (2004) de la Unión Europea (UE) no sólo se ha integrado la totalidad de la "Declaración sobre los Defensores de Derechos Humanos" de la ONU, sino que además se hace una serie de recomendaciones concretas a los Estados miembros.

Las personas dedicadas a la defensa de los derechos humanos desarrollan una actividad legal y legitimada por las comunidades nacionales y la comunidad internacional. PI suscribe la definición de defensor, defensora de derechos humanos proporcionada por la "Declaración sobre defensores de derechos humanos" de la ONU y recogida también en la "Guía sobre defensores de derechos humanos" de la UE:

> "Se usa la expresión 'defensor de los derechos humanos' para describir a la persona que, individualmente o junto con otras, se esfuerza en promover o proteger esos derechos. Se les conoce sobre todo por lo que hacen, y la mejor forma de explicar lo que son consiste en describir sus actividades y algunos de los contextos en que actúan".[2]

(Ver apéndice al final del Nuevo Manual para más información sobre las citadas declaraciones de la ONU y guía de la UE).

¿A quién corresponde proteger a las defensoras y los defensores de derechos humanos?

La "Declaración sobre defensores de derechos humano" señala que el Estado es el principal responsable de su protección. Asimismo, reconoce la "valiosa labor que llevan a cabo los individuos, los grupos y las instituciones al contribuir a la eliminación efectiva de todas las violaciones de los derechos humanos y las libertades fundamentales de los pueblos y los individuos" y "la relación entre la paz y la seguridad internacionales y el disfrute de los derechos humanos y las libertades fundamentales".[3]

Sin embargo, según Hina Jilani,[4] anterior Representante Especial del Secretario General de las Naciones Unidas sobre Defensores y Defensoras de Derechos Humanos, "la manifestación de las violaciones de los derechos humanos y la búsqueda de compensación de éstas depende en gran medida del grado de seguridad de que disfruten los defensores de los derechos humanos".[5] Si consultamos cualquier informe sobre defensores de cualquier lugar del mundo nos encontraremos con historias de tortura, desapariciones, asesinatos, amenazas, robos, allanamientos en oficinas, acoso, detenciones ilegales, persecuciones, espionaje, etc. Por desgracia, para estas personas, estas situaciones son la norma y no la excepción.

---

2 Op. cit.

3 Declaración sobre los defensores de derechos humanos" adoptada por la Asamblea General de Naciones Unidas el 9 de diciembre de 1998.

4 Margaret Sekaggya (Uganda) ha sucedido a Hina Jilani en el 2008, como Relator especial sobre la situación de los defensores de los derechos humanos, nombrada por el Consejo de Derechos Humanos de ONU.

5 Informe sobre Defensores de Derechos Humanos, 10 Sept 2001 (A/56/341).

Para más información...

Sobre defensoras y defensores de derechos humanos:

- www.unhchr.ch/defender/about1.htm (El Alto Comisionado sobre Derechos Humanos de las Naciones Unidas).
- www.protectionline.org (Protection International).
- El Observatorio para la Protección de Defensores de Derechos Humanos, creado por la Federación Internacional de Derechos Humanos (FIDH; www.fidh.org) y la Organización Mundial contra la Tortura (OMCT; www.omct.org).
- Amnistía Internacional: www.amnesty.org y http://www.amnesty.org/es/human-rights-defenders
- www.ishr.ch, ver bajo "HRDO" (La Oficina de DDH del Servicio Internacional para los Derechos Humanos de Ginebra).
- www.frontlinedefenders.org (Front Line, La Fundación Internacional para Defensores de Derechos Humanos).

Sobre instrumentos legales existentes y la Declaración sobre defensores de derechos humanos de la ONU:

- www.unhchr.ch: web del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.
- www.protectionline.org (Protection International).
- www.ishr.ch (International Service for Human Rights, Ginebra), colección de instrumentos regionales e internacionales para la protección de las y los defensores de derechos humanos.

PRIMERA PARTE

RIESGO, ANÁLISIS DE AMENAZAS Y OTRAS HERRAMIENTAS

INTRODUCCIÓN:

En la primera parte de este manual vamos a tratar los conceptos básicos de seguridad, algunas herramientas prácticas y cómo abordar ciertos casos desde el punto de vista de la seguridad.

Todo ello será integrado en el plan de seguridad y en el manual de seguridad de la organización.

CONTENIDOS DE LA PRIMERA PARTE:

CAPÍTULO 1.1

La Toma de decisiones sobre seguridad y protección

Objetivo

Concienciarnos de la importancia de analizar nuestro entorno de trabajo con vistas a los temas de seguridad

Aprender diferentes métodos para analizar el contexto y a los actores o partes interesadas

Los entornos de trabajo

Las personas que trabajan en la defensa de los derechos humanos suelen hacerlo en entornos complejos, donde hay una gran variedad de actores y donde se toman decisiones de carácter marcadamente político. Ocurren muchas cosas diferentes casi al mismo tiempo y todos los acontecimientos tienen repercusiones en otros. En este escenario, la dinámica de cada actor o parte interesada desempeña un papel significativo en las relaciones de ese actor con otros. Por lo tanto, será necesario que las y los defensores dispongamos de información no sólo sobre los temas directamente relacionados con nuestro trabajo, sino también sobre las posiciones de los principales actores.

Como primer ejercicio podríamos hacer una lluvia de ideas para identificar del modo más completo posible todos los actores sociales, políticos y económicos que pudieran desempeñar algún papel en temas de seguridad del grupo en este momento determinado. Después podemos recoger esa información en una lista a limpio.

Análisis del entorno de trabajo

Es fundamental conocer y comprender lo mejor posible el contexto en que estamos trabajando. Un buen análisis de ese contexto permite la toma consciente de decisiones sobre qué reglas y medidas de seguridad conviene aplicar. Asimismo, es importante que imaginemos escenarios posibles futuros, para así tomar medidas preventivas allí donde nos sea posible.

Sin embargo, analizar el entorno de trabajo no basta en sí mismo. Hay que considerar también cuál va a ser el impacto de las medidas que se tomen y cómo

podrían reaccionar los diferentes actores, además de la dimensión del espacio de trabajo, porque aunque hagamos el análisis a nivel de un país o región, tenemos que ver también cómo opera esa macrodinámica en la zona concreta donde estamos trabajando; esto es, hay que considerar la microdinámica que genera la macrodinámica. Por ejemplo, los paramilitares de determinado pueblo podrían actuar de manera muy distinta a cómo esperaríamos que actuasen desde una perspectiva nacional o regional. Tenemos que conocer las características del lugar concreto. Asimismo, es crucial que evitemos tener ideas fijas sobre nuestro escenario de trabajo, porque las situaciones cambian y evolucionan; por esto es tan importante revisarlas con regularidad.

Vamos a considerar tres métodos útiles para analizar el entorno donde trabajamos: la técnica de las preguntas, el análisis de campo de las fuerzas y el análisis de los actores o partes interesadas.

La técnica de las preguntas

Supongamos, por ejemplo, que tenemos el problema de que las autoridades del lugar nos están acosando. Si nuestra pregunta es "¿Qué podemos hacer para reducir el acoso?", puede que al final nos encontremos buscando remedios para los síntomas, en este caso, el acoso. Pero si buscamos una pregunta que apunte a una solución, puede que entonces demos con la solución. Por ejemplo, si preguntamos: "¿Es nuestro entorno sociopolítico lo bastante seguro como para que continuemos con nuestro trabajo?", ahí sólo caben dos respuestas: sí o no. Si la respuesta es sí, tendremos que formular otra pregunta que nos ayude a identificar de manera muy concreta, y a comprender muy bien, cuáles son los temas fundamentales que afectan a nuestra seguridad. Si, tras considerar seriamente todas las actividades, planes y recursos disponibles, así como las leyes, negociaciones, análisis comparativos con otros defensores de la zona, etc., la respuesta fuera no, esto, en sí mismo, sería la solución a nuestro problema de seguridad.

Pasos de la técnica de las preguntas:

- Buscar preguntas que nos ayuden a identificar de manera muy concreta y con claridad cuáles son los temas fundamentales que afectan a nuestra seguridad;
- Formular las preguntas anticipando las soluciones;
- Repetir este procedimiento tantas veces como sea necesario (a modo de debate).

Ideas sobre preguntas que pueden hacerse:

- ¿Cuáles son los temas fundamentales que operan en el terreno sociopolítico y económico?
- ¿Quiénes son las principales partes interesadas en conexión con estos temas fundamentales?
- ¿Cómo puede afectar (positiva y negativamente) nuestra labor a los intereses de esos actores?
- ¿Cómo podríamos reaccionar si pasáramos a ser blanco de cualquiera de estos actores debido al trabajo que estuviéramos realizando?

- ¿Es nuestro entorno sociopolítico lo bastante seguro como para que continuemos con nuestro trabajo?
- ¿Cómo reaccionaron las autoridades locales/nacionales en el pasado ante la labor de otras defensoras y defensores en relación con este tema?
- ¿Cómo han reaccionado las principales partes interesadas ante un trabajo similar o anterior de defensa de los derechos humanos, u otros relacionados?
- ¿Cómo han respondido los medios de comunicación y la comunidad en circunstancias similares?
- Etc.

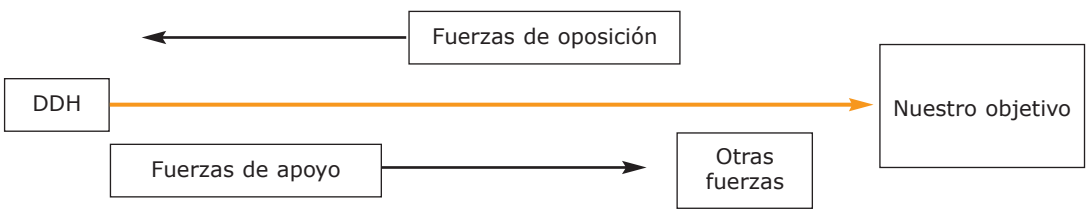
Análisis de campo de las fuerzas

Esta técnica[1] puede ayudarnos a visualizar cómo las diferentes fuerzas nos ayudan o se oponen a la consecución de nuestros objetivos: existen unas fuerzas a favor y otras en contra, y se asume que los problemas de seguridad podrían surgir de las fuerzas en contra, mientras que se podrían aprovechar las fuerzas a favor para mejorar nuestra seguridad.

La técnica puede usarla una persona sola, pero es más eficaz cuando lo hace un grupo heterogéneo con un objetivo de trabajo muy concreto siguiendo metodología clara para lograrlo.

Dibujamos una flecha horizontal que apunte a una caja (nosotros o nosotras hacia nuestro objetivo). En la caja resumimos nuestro objetivo de trabajo (esto nos ayudará a identificar más fácilmente las fuerzas de apoyo y de oposición). Dibujamos otra caja por encima de la flecha. Anotamos en ella la lista de todas las fuerzas que potencialmente podrían intentar evitar que logremos nuestro objetivo. Dibujamos otra caja igual por debajo de la flecha, y ahora anotamos todas las fuerzas que podrían apoyar nuestro trabajo. Dibujamos una última caja para anotar en ella las fuerzas que no sabemos o no podemos identificar aún qué apoyarán.

Tabla 1: Análisis de campo de fuerzas para valorar los entornos de trabajo



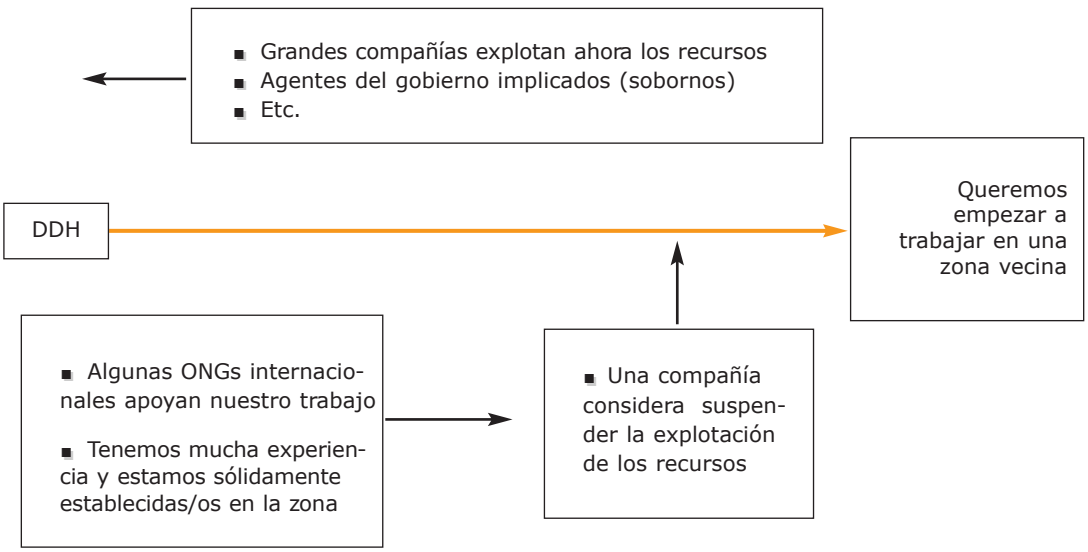
[1] Nota: ésta es una técnica original de Kurt Lewin e inspirada en el mundo de la física; aplicada al análisis de los problemas sociales, "la técnica consiste en descubrir y cuantificar esas fuerzas en un sentido y en otro. Hecha esta descripción y cuantificación se tendrán elementos de juicio para cambiar la situación". Ver en IEPALA/GLOOBAL,

http://www.gloobal.net/iepala/gloobal/fichas/ficha.php?entidad=Herramientas&id=65.

Después de completar la tabla evaluamos los resultados. Este tipo de análisis nos ayuda a ver gráficamente también con qué fuerzas estamos lidiando. El objetivo es encontrar maneras de reducir o de eliminar el riesgo generado por las fuerzas de oposición, contando en parte con la ayuda potencial de las fuerzas de apoyo. Respecto a las otras fuerzas, tendremos que decidir si considerarlas de apoyo o bien si estar pendientes de ellas hasta detectar si van a ser de apoyo o de oposición.

Por ejemplo:

Imaginemos que pertenecemos a una organización que trabaja por los derechos de los pueblos indígenas a los recursos naturales que hay en sus tierras. Hay conflictos entre una serie de actores sobre la explotación de estos recursos. Por nuestra parte, lo que nos interesa ahora es ampliar nuestro trabajo a una zona vecina donde hay problemas parecidos.



Análisis de los actores o partes interesadas

Analizar la cuestión de los actores es una manera sustancial de aumentar la información disponible para poder tomar decisiones informadas sobre protección. Implica ser capaz de identificar y describir a los diferentes actores o partes interesadas y sus relaciones, partiendo de sus características e intereses, y relacionándolo todo con el tema dado de protección.

Un actor o parte interesada en protección es una persona, grupo o institución con un interés o un papel en un plan de acción que afecta a temas de protección.[2]

2 Adaptado de *Sustainable Livelihoods Guidance Sheets* nº 5.4 (2000).

Las partes interesadas en protección pueden ser de varios tipos:

Los actores principales. En el contexto de la protección son las y los defensores y las personas con y para las que trabajan, pues todas tienen un interés primordial en su propia protección.

Los actores responsables de proteger a las y los defensores:

- Las instituciones del gobierno y del Estado (incluidas las fuerzas de seguridad, los jueces, los legisladores, etc.);
- Los organismos internacionales con un mandato de protección, tales como los organismos de las Naciones Unidas, las organizaciones regionales, las fuerzas de mantenimiento de la paz, etc.;
- Para el caso de actores de la oposición armada, se les puede recordar su obligación de no atacar a las y los defensores, pues éstos son civiles, en especial cuando controlan el territorio.

Los actores clave, con capacidad de influir significativamente en la protección de las y los defensores debido a su peso político o a su capacidad de presionar a los actores responsables que no estén asumiendo sus responsabilidades (otros gobiernos, organismos de la ONU, etc.) y, de manera parecida, que puedan estar directa o indirectamente implicadas en ataques y presiones a las defensoras y los defensores (como empresas privadas, medios de comunicación de masas u otros gobiernos). Los intereses y las estrategias de cada una de estas partes interesadas dependerán del contexto. Una lista no exhaustiva podría incluir:

- Organismos de la ONU (distintos a los que tienen un mandato de protección).
- El Comité Internacional de la Cruz Roja.
- Otros gobiernos e instituciones multilaterales (tanto en calidad de donantes de fondos para proyectos como en calidad de responsables políticos, capaces de diseñar políticas).
- Otros actores armados.
- Las ONGs (sean nacionales o internacionales).
- Las iglesias e instituciones religiosas.
- Las compañías privadas.
- Los medios de comunicación de masas.

A la hora de entender qué estrategias tiene cada actor, una dificultad es que las relaciones entre ellos pueden no estar bien definidas, o incluso puede que algunos de los distintos actores no se relacionen entre sí. Muchas veces son los actores responsables de proteger (como gobiernos, fuerzas de seguridad y grupos armados de oposición) los que violan los derechos humanos y causan la desprotección de los defensores. Y en ocasiones otros actores en protección (como terceros gobiernos, o la ONU) tienen intereses que entran en conflicto con su disposición a proteger. Estos factores, junto con otros factores inherentes a los escenarios de conflicto, contribuyen a la gran complejidad de los entornos de trabajo de los defensores.

ANÁLISIS DE ACTORES Y DE PROCESOS Y ESTRUCTURAS EN TRANSFORMACIÓN

Los actores sociales **no** tienen papeles fijos. Se relacionan entre sí a muchos niveles, creando así una densa red de relaciones. Es importante prestar atención a las relaciones que moldean y transforman las necesidades de protección de la gente

Las estructuras son partes interrelacionadas del sector público, la sociedad civil y las entidades privadas. Las consideraremos desde el punto de vista de la protección. Dentro del sector público, podríamos considerar un gobierno como un conjunto de actores con una estrategia unificada o bien con una serie de estrategias internas que se contraponen. Por ejemplo, podríamos encontrar fuertes discrepancias entre el ministerio de Defensa y el ministerio de Asuntos Exteriores a la hora de tratar las políticas relacionadas con las y los defensores de derechos humanos, o entre la oficina del Defensor/a del Pueblo y el ejército. Las estructuras pueden tener una composición variada, por ejemplo, podría crearse una comisión intersectorial (miembros del gobierno, ONGs, la ONU y el cuerpo diplomático) para supervisar la situación de seguridad de una organización dada de defensa de los derechos humanos.

Los procesos, en el mundo de la protección, son las cadenas de decisiones y acciones emprendidas por una o más estructuras con el objetivo de mejorar la situación de seguridad de un grupo dado. Puede tratarse de procesos legislativos, culturales y políticos. No todos los procesos consiguen que mejore la situación de protección: a menudo los procesos de protección están en conflicto entre ellos, incluso pueden neutralizarse unos a otros, como cuando personas que tendrían que estar recibiendo protección no quieren aceptarla si viene del gobierno, por considerar que el ofrecimiento tiene el objetivo implícito de desplazar a la gente de la zona (las Naciones Unidas y las ONGs podrían entonces apoyar a la gente en este proceso).

El análisis de los actores es fundamental para entender:

- Quién es parte interesada y en qué circunstancias entra en juego su interés.
- Las relaciones entre las partes interesadas en la protección, sus características e intereses.
- Cómo se verán afectadas todas por las medidas de protección.
- La disposición de cada actor a ser parte de las medidas de protección.

El análisis de los actores puede hacerse de varias maneras. La siguiente emplea una metodología sencilla, algo fundamental para obtener buenos resultados.

Cuando valoremos los procesos de protección es importante que los contemplemos con cierta distancia en el tiempo y que siempre tengamos en cuenta los intereses y objetivos de todas las partes interesadas.

Un análisis de los actores en cuatro pasos:

1. Considerar el tema de la protección desde una perspectiva amplia y concreta, esto es, identificar la situación de seguridad de las y los defensores en la región X del país Y.

2. ¿Quiénes son los actores? (Principalmente, ¿cuáles son las instituciones, grupos y personas con una responsabilidad o un interés en la protección?) A través de la lluvia de ideas y la discusión, identificar todas las partes interesadas en el tema de la protección. Pasar a limpio en forma de lista.

3. Analizar las características y los atributos particulares de los actores, tales como sus responsabilidades en la protección, su capacidad para influir en la situación de protección, sus objetivos, estrategias, legitimidad e intereses (incluida su disposición a participar en la protección).

4. Investigar y analizar las relaciones entre los actores.

Después de este análisis, podríamos usar una tabla como la que sigue:

Copiar el nombre de cada actor de nuestra lista en el eje horizontal (primera línea) y hacer lo mismo a lo largo del eje vertical (primera columna) de la tabla. (Ver tabla 2).

A continuación:

- Analizar los rasgos de cada actor (objetivos e intereses, estrategias, legitimidad y poder) y anotarlos en la casilla donde cada parte coincide con ella misma. Se irá formando una línea diagonal de casillas rellenadas.

Ejemplo:

Anotar los objetivos, intereses y estrategias de grupos de oposición armada en las casillas "A".

- Analizar las relaciones entre los actores: rellenar las casillas que definan las relaciones más importantes en relación a la protección, por ejemplo, la que es intersección entre el ejército y el Alto Comisionado de las Naciones Unidas para los Refugiados (ACNUR), sería casilla "B", y así sucesivamente.

Cuando hayamos rellenado las casillas más relevantes, tendremos una tabla de los objetivos, estrategias e interacción de las principales partes interesadas en relación a un tema de protección dado.

Tabla 2: matriz para el análisis de los actores

	Gobierno	Ejército	Policía	Grupo de oposición armada	ONGs de DDHH nacionales	Iglesias	Otros gobiernos	Organismos de la ONU	ONGs internacionales
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)	
ONGs internacionales									(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)

Resumen

- Todas las personas que defienden los derechos humanos corren riesgos.

- No todas estas personas reaccionan igual ante el riesgo.

- Los riesgos dependen del contexto político.

- El contexto político cambia, es dinámico. Consecuentemente, los riesgos cambian, son dinámicos.

Ésta es la hipótesis que fundamenta lo importante que es encontrar información clave planteándose las preguntas adecuadas.

Después, tendremos que identificar y analizar las partes interesadas considerando todas sus muchos componentes y hasta sus más profundos sustratos.

Determinaremos cómo interactúan en relación con el tema de la protección, y cómo se relacionan los temas de protección con los temas estratégicos de los actores o partes interesadas.

Buscaremos intereses convergentes y divergentes, alianzas, métodos de operaciones, etc.

Veremos cuáles son las estructuras y procesos subyacentes.

Podremos identificar con precisión las diferentes fuerzas implicadas (las de oposición, las de apoyo y las que no sabemos qué rumbo tomarán).

La primera vez que sigamos estos pasos puede resultarnos difícil o llevarnos mucho tiempo, pero después, si actualizamos el análisis regularmente, nos será mucho más fácil y tardaremos mucho menos.

Todo esto nos permitirá llevar a cabo una toma consciente de decisiones sobre seguridad y protección.

CAPÍTULO 1.2

cómo Valorar el riesgo: amenazas, vulnerabilidad y capacidad

Objetivo:

Comprender los conceptos de amenazas, vulnerabilidad y capacidad aplicados al tema de la seguridad

Aprender a hacer una valoración de los riesgos

Análisis de los riesgos y necesidad de protección

El trabajo en derechos humanos puede tener repercusiones negativas en los intereses de algunos de los actores, lo que podría poner a las y los defensores en una situación de peligro. Es importante señalar que en determinados países el riesgo que corren es parte de su día a día y surge o aumenta precisamente a raíz del trabajo que realizan.

Podemos abordar el tema del riesgo estudiándolo de la siguiente manera:

> Análisis de los intereses y estrategias de los principales actores ⇨ Evaluación de la repercusión del trabajo de las y los defensores en esos intereses y estrategias ⇨ Evaluación de las amenazas recibidas por las y los defensores ⇨ Evaluación de los puntos vulnerables y la capacidad de las y los defensores ⇨ Lista de riesgos.

En otras palabras,

- Lo **que** hacemos puede traer consigo que recibamos amenazas.
- **Cómo, dónde y cuándo** trabajamos suscita temas relacionados con nuestra vulnerabilidad y nuestra capacidad.

No existe una definición consensuada sobre lo que es el riesgo. Aquí diremos que 'riesgo' hace referencia a "acontecimientos posibles, sean lo inciertos que sean, que causan daño".

En cualquier situación dada, todas las personas que trabajan en derechos humanos pueden encontrarse ante un mismo nivel de peligro, pero no todo el mundo es vulnerable a ese riesgo general de la misma manera por estar en un mismo lugar. La **vulnerabilidad**, la posibilidad de que un defensor o una defensora o su grupo sufra un ataque o un daño, varía de acuerdo a diversos factores, como veremos a continuación.

Un ejemplo:

Pongamos que existe un país donde el gobierno es en sí una amenaza general para cualquier tipo de trabajo de derechos humanos, lo que significa que cualquiera que defienda los derechos humanos está en peligro. Sin embargo, algunas defensoras o defensores estarán corriendo más peligro que otros: una ONG grande sólidamente establecida en la capital no será tan vulnerable como una ONG pequeña que esté en un pueblo. Es lógico, pero es interesante analizar por qué esto es así, porque eso nos ayudará a comprender y a abordar mejor las cuestiones de seguridad que afectan a quienes defienden los derechos humanos.

El nivel de riesgo al que se enfrenta un grupo de defensoras o defensores de derechos humanos aumenta en relación a las amenazas recibidas y a la vulnerabilidad y la capacidad del grupo antes esas amenazas, como representamos en la siguiente ecuación:[1]

$$\text{RIESGO} = \frac{\text{AMENAZAS} \times \text{VULNERABILIDAD}}{\text{CAPACIDAD}}$$

Las amenazas representan 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.[2] La valoración de las amenazas nos será útil para saber qué probabilidad hay de que éstas se lleven a cabo (como veremos en el siguiente capítulo).

En un escenario de conflicto, las y los defensores pueden enfrentarse a muchos tipos de amenazas: si va dirigida a alguien se la conoce como **targeting** y si emana del contexto es una amenaza **incidental**. Desde otro punto de vista, puede haber amenazas **declaradas**, cuando son directas o explícitas, o declaradas hacia otras personas, próximas a ti, las amenazas **indirectas**.

El targeting es el tipo más común de amenaza para las y los defensores de derechos humanos. Tiene el objetivo de frenar o variar el trabajo del grupo o de influir en el comportamiento de sus miembros. Se suele producir directamente por el trabajo que éstos realizan y también por los intereses y necesidades de quienes se oponen a este trabajo.

Resumen de los tipos de amenazas:

- Targeting: amenazas que surgen por el trabajo que hacemos (pueden ser amenazas directas, contra alguien, e indirectas, contra personas relacionadas).
- Amenazas incidentales: emanan del contexto en que trabajamos (amenazas por delincuencia común, o por enfrentamientos armados en zonas de conflicto).

1 Adaptado de *Van Brabant* (2000) y REDR.
2 Dworken (1999).

Las **amenazas incidentales** surgen al menos por:

- Encontrarse en **zonas de enfrentamientos armados** ("estar donde no tienes que estar en el peor momento posible").
- Ataques **por delincuencia común**, en especial si el trabajo de derechos humanos se hace en zonas especialmente peligrosas. Hay que señalar, no obstante, que muchos casos de delincuencia común encubren casos de targeting.

El targeting (amenazas con un propósito concreto) puede hacerse a través de amenazas **directas** (declaradas), por ejemplo cuando las y los defensores reciben una amenaza de muerte (ver capítulo 1.3 para cómo evaluar las amenazas declaradas), y a través de amenazas **indirectas**, cuando por ejemplo un defensor próximo a tu trabajo recibe una amenaza y existen razones para pensar que a ti puede tocarte después.

Vulnerabilidad

La vulnerabilidad hace referencia al grado en que la gente es sensible a la pérdida, el daño, el sufrimiento y la muerte al ser objeto de un ataque. Varía de persona a persona y de grupo a grupo; y también, para la misma persona o grupo, varía en el tiempo. La vulnerabilidad siempre es relativa, porque todas las personas y todos los grupos son de alguna manera vulnerables. No obstante, todo el mundo tiene su propio nivel y tipo de vulnerabilidad, dependiendo de sus circunstancias. Veamos algunos ejemplos:

- Vulnerabilidad y lugar físico: una defensora puede ser más vulnerable cuando está de viaje haciendo una visita de campo que cuando está en una oficina conocida por todos, pues es probable que en la oficina siempre haya testigos si se produce un ataque.
- La vulnerabilidad puede relacionarse con no tener acceso a un teléfono, con poder usar transporte terrestre seguro o con tener buenos cerrojos en las puertas de una casa. Pero también está relacionada con la falta de redes de contactos y de acción conjunta de las y los propios defensores.
- Vulnerabilidad, trabajo en equipo y miedo: si un defensor recibe una amenaza, tendrá miedo, y su trabajo se verá afectado por ese miedo. Si no sabe controlar su miedo (si no encuentra con quién hablarlo, buenos compañeros, etc.), es posible que cometa errores o que no tome la mejor decisión posible, lo que puede aumentar los problemas de seguridad.

(Al final de este capítulo ofrecemos un listado sobre posibles puntos vulnerables y capacidades de respuesta).

Capacidad

La capacidad (de respuesta) en protección alude a los puntos fuertes y a los recursos que tiene un grupo o una persona para conseguir un grado razonable de seguridad. Algunos ejemplos son los cursos de formación dedicados a temas de seguridad o en temas legales, el trabajo en equipo, la posibilidad de usar un teléfono o un medio de transporte seguro, una buena red de contactos, una buena estrategia para controlar el miedo, etc.

En la mayoría de los casos, la vulnerabilidad y la capacidad son dos lados de una misma moneda.

Por ejemplo:

No saber lo suficiente sobre nuestro entorno de trabajo nos hace más vulnerables, y saber lo suficiente aumenta nuestra capacidad de respuesta. Lo mismo puede decirse de tener o no tener acceso a transporte seguro o a buenas redes de contactos.

En cualquier caso, cómo actuamos es un factor determinante.

Por ejemplo:

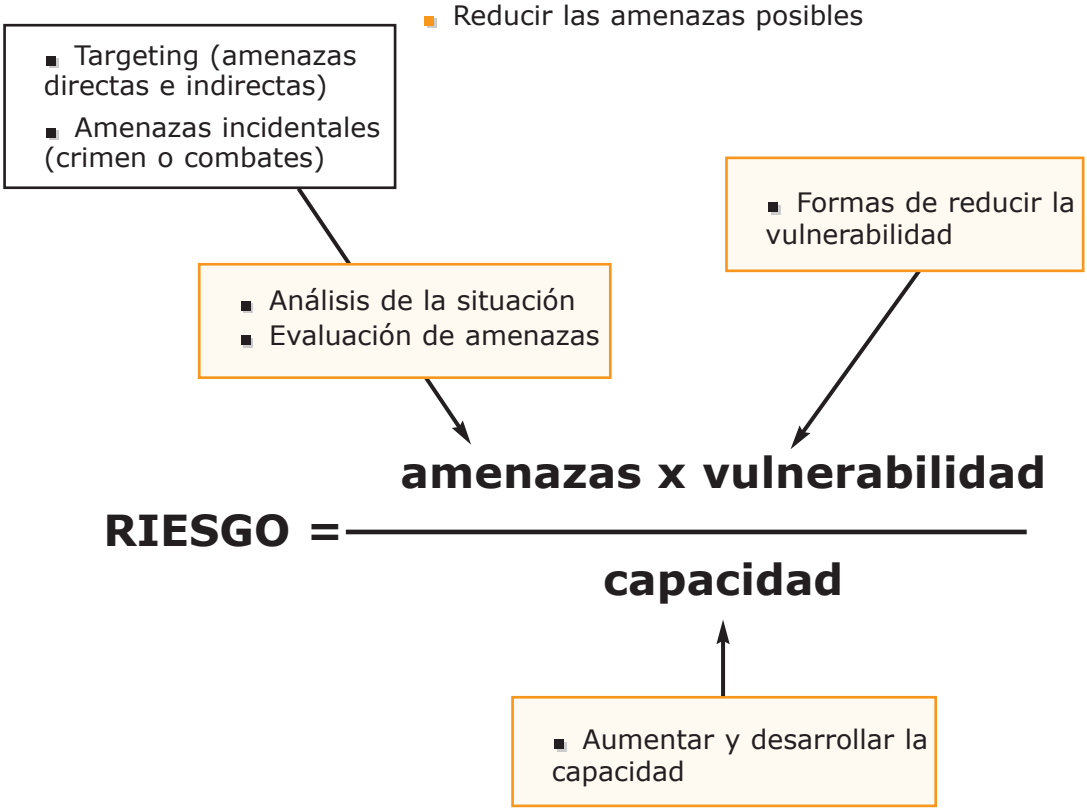
Tener teléfono puede hacernos vulnerables o aumentar nuestra capacidad dependiendo de cómo lo usemos. Si lo usamos sin cuidado, para transmitir información confidencial, tenerlo nos hace más vulnerables. Si lo usamos con discreción y la información confidencial la transmitimos de modo reservado, entonces es una capacidad.

(Al final de este capítulo ofrecemos un listado de posibles puntos vulnerables y capacidades).

En resumen,

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



El riesgo es un concepto dinámico, pues cambia a lo largo del tiempo y en función de las variaciones producidas en la naturaleza de las amenazas, la vulnerabilidad y la capacidad. Esto implica que los riesgos deben ser evaluados periódicamente, en especial si se trabaja en un entorno de trabajo variable, o si nuestros puntos vulnerables o nuestras capacidades para responder cambian. Por ejemplo, la vulnerabilidad puede aumentar con un cambio de líderes que deje al grupo en una posición más débil que antes.

El riesgo aumenta dramáticamente cuando se produce una amenaza clara y palpable. En tales casos, puede que lo mejor no sea intentar reducir los riesgos trabajando la capacidad porque eso va a llevar tiempo. Las medidas de seguridad, tales como hacer un curso de formación en temas legales o poner barreras protectoras, reducen los riesgos sólo en el sentido de que reducen los factores que nos hacen vulnerables. Sin embargo, no sirven para neutralizar una amenaza, el riesgo principal aquí, ni la voluntad de llevar esa amenaza a cabo, en especial allí donde los perpetradores saben que sus actos no van a ser castigados. Toda medida de protección eficaz deberá, por tanto, aspirar a reducir las amenazas, además de la vulnerabilidad, y a aumentar la capacidad.

Un ejemplo:

Un pequeño grupo de defensores de derechos humanos está trabajando el tema de la propiedad de la tierra en un pueblo. Cuando su trabajo empieza a repercutir en los intereses del terrateniente del lugar, el grupo recibe una clara amenaza de muerte. Al aplicar la ecuación del riesgo a su situación de seguridad, vemos que el riesgo que enfrenta el grupo es muy alto, por la amenaza de muerte. Para reducirlo, probablemente no sea el mejor momento de cambiar los cerrojos en la oficina (porque el riesgo no es de robo), ni de comprar un celular para cada miembro del grupo (aunque la comunicación sea importante para la seguridad, si vienen a matarte probablemente esto no baste). En este caso, una estrategia mejor sería trabajar la red de contactos para generar respuestas políticas que luchen contra esa amenaza (y si eso no va a servir de nada en poco tiempo, la única manera de reducir el riesgo significativamente podría ser reducir la exposición de los miembros del grupo, por ejemplo, marchándose una temporada. Tener lugares seguros donde realojarse es también una capacidad).

Tomar esa decisión y llevarla a cabo implica también una capacidad psicológica del defensor o defensora: la de ser capaz de ver que retirarse no es sinónimo de cobardía o de derrota. Retirarse puede proporcionar tiempo para poder analizar la situación adecuadamente y el que se retome el trabajo estando mejor preparados.

La vulnerabilidad y la capacidad (de respuesta), así como algunas amenazas, pueden variar según sexo y edad. Son factores a tener en cuenta al proceder al análisis.

Cómo valorar la vulnerabilidad y la capacidad

Para hacer una valoración de la vulnerabilidad y la capacidad de un grupo (o persona) dado. tendremos que empezar por definir al grupo mismo (comunidad, colectivo, ONG, personas, etc.), el lugar físico donde se encuentra y el factor tiempo (el perfil de la vulnerabilidad cambia y evoluciona a lo largo del tiempo). Después podremos valorar la vulnerabilidad y la capacidad usando la tabla 3 que aparece al final de este capítulo como modelo.

Por favor, atención: Este tipo de evaluación debe plantearse como una actividad abierta que se va nutriendo de información a lo largo del tiempo para que así siempre se pueda disponer de una tabla precisa de cómo evoluciona la situación. Cuando evaluemos la vulnerabilidad y la capacidad, es importante hacer primero la descripción de cuál es la situación de éstas en ese momento y sólo después proceder a hacer una lista de las descripciones posibles o deseables. Posteriormente, tendremos que determinar el procedimiento que nos permitirá llegar a estas últimas.

Tabla 3:

Información necesaria para valorar la vulnerabilidad y la capacidad de un grupo. (Nota: la información de la columna derecha muestra los puntos vulnerables o las capacidades de respuesta para cada componente en términos generales).

Vulnerabilidad y capacidad	Información necesaria para valorar nuestra vulnerabilidad o capacidad como defensores de derechos humanos en relación con los componentes
COMPONENTES RELATIVOS A LAS CARACTERÍSTICAS GEOGRÁFICAS, FÍSICAS Y TÉCNICAS	
Exposición	La necesidad de estar en o pasar por zonas peligrosas para realizar las tareas cotidianas u otras ocasionales, habiendo en ellas actores que suponen una amenaza a la seguridad.
Estructuras físicas	Las características de los edificios (oficinas, casas, refugios); los materiales de construcción, puertas, ventanas, armarios. Barreras protectoras. Iluminación nocturna.
Oficinas y lugares abiertos al público	¿Están las oficinas abiertas al público? ¿Hay zonas reservadas sólo para el personal? ¿Hay que tratar con gente desconocida que viene a visitarnos?
Lugares para ocultarse, rutas para escapar	¿Disponemos de lugares para ocultarnos? ¿Son de fácil acceso (a qué distancia física están) y quién puede usarlos (son para personas concretas o para todo el grupo)? En caso de necesidad, ¿podríamos abandonar la zona durante algún tiempo?
Acceso a la zona donde estamos	¿Cómo de difícil le es acceder a la zona a quienes nos visitan (agentes del gobierno, ONGs, etc.)? (p.e., si es un barrio peligroso). ¿Cómo de fácil le es acceder a quienes pueden ser una amenaza a nuestra seguridad?
Transporte y alojamiento	¿Podemos usar transporte seguro (público o privado)? ¿Qué ventajas y desventajas tiene? ¿Podemos disponer de a alojamiento seguro cuando estamos de viaje?
Comunicación	¿Existen sistemas de telecomunicaciones (radio, teléfono)? ¿Se pueden usar fácilmente? ¿Funcionan siempre? ¿Pueden ser cortados antes de un ataque por quienes nos amenazan?

COMPONENTES RELATIVOS AL CONFLICTO	
Vínculos con las partes implicadas en el conflicto	¿Tenemos algún tipo de vínculo con alguna de las partes implicadas en el conflicto (familiares, gente de nuestra misma procedencia, con nuestros mismos intereses) que podría usarse contra nosotras/os?
Actividades de defensa de DDHH que afectan a las partes del conflicto	Nuestro trabajo, ¿afecta directamente a los intereses de algún actor implicado? (p.e. cuando protegemos recursos naturales valiosos, el derecho a la tierra u objetivos potenciales similares de los actores con poder) ¿Trabajamos algún tema especialmente sensible para los poderosos? (p.e. la propiedad de la tierra).
Transporte de objetos, bienes e información escrita	¿Tenemos objetos, bienes o información que podría ser valiosa para los grupos armados, y que por tanto, haría peligrar para nuestra seguridad? (gasolina, ayuda humanitaria, pilas, manuales de derechos humanos, manuales de asistencia médica, etc.)
Conocimiento de los enfrentamientos armados y las zonas minadas	¿Tenemos información sobre zonas de enfrentamiento armado que pudiera ponernos en peligro? ¿Y sobre zonas seguras donde refugiarnos? ¿Disponemos de información fiable sobre las zonas de minas?
COMPONENTES RELATIVOS AL SISTEMA JUDICIAL Y POLÍTICO	
Acceso a las autoridades y a un sistema judicial para reclamar los propios derechos	¿Podemos iniciar procesos judiciales para reclamar derechos? (Acceso a representación legal, presencia física en los juicios o en las reuniones, etc.) ¿Podemos pedir ayuda para nuestro trabajo y protección a las autoridades que correspondan?
Poder obtener resultados del sistema judicial y de las autoridades	¿Podemos luchar por nuestros derechos usando el sistema judicial que existe? ¿O se nos puede reprimir haciendo uso de las leyes del lugar? ¿Podemos desarrollar suficiente peso político como para que las autoridades no puedan ignorar nuestras peticiones?
Estatus legal, contabilidad y requisitos legales	¿Se le niega el estatus legal al grupo, o se nos somete a largas demoras? ¿Tenemos los libros de contabilidad al día y cumplimos con todos los requisitos legales del país? ¿Usamos software pirata?
COMPONENTES RELATIVOS A LA GESTIÓN DE LA INFORMACIÓN	
Fuentes y fiabilidad de la información	¿Tenemos fuentes fiables de información que puedan fundamentar las acusaciones que hagamos? ¿Tenemos un buen método para contrastar y presentar la información, y para difundirla?
Guardar, enviar y recibir información	¿Podemos guardar la información en un lugar seguro y fiable? ¿Podría ser robada? ¿Puede protegerse de virus y hackers/crackers? ¿Podemos enviar y recibir información usando métodos seguros? ¿Sabemos cuál es la diferencia entre información de alto secreto e información confidencial? ¿Nos llevamos la información fuera del lugar de trabajo?

Ser testigos o disponer de información vital	¿Somos testigos clave para llevar al banquillo a algún poderoso? ¿Tenemos información relevante y única para un caso o un proceso dado?
Saber explicar de manera coherente y aceptable el trabajo y los objetivos	¿Sabemos explicar con claridad y coherencia nuestro trabajo y objetivos? ¿Es esta explicación aceptable, al menos tolerable, para todas las partes implicadas (en especial, las armadas)? ¿Podemos todas/os dar esta explicación cuando se nos pregunte (p.e., en un puesto de control)?
COMPONENTES RELATIVOS A LAS CARACTERÍSTICAS SOCIALES Y ORGANIZATIVAS	
Existencia de una estructura en el grupo	¿Está el grupo estructurado u organizado de alguna manera? ¿Proporciona esta estructura un nivel aceptable de cohesión?
Toma conjunta de decisiones	¿Refleja la estructura del grupo intereses particulares o representa a todo el grupo (tipo de participación de sus miembros) ¿Quién realiza las principales funciones y asume la toma de decisiones, una persona o un conjunto de personas? ¿Existen planes de contingencia para la toma de decisiones y las responsabilidades? ¿Hasta qué punto se hace la toma conjunta de decisiones? ¿Permite la estructura del grupo: a) la toma conjunta de decisiones y su ejecución colectiva de las mismas, b) discusiones conjuntas, c) reuniones esporádicas y poco útiles d) nada de esto?
Planes y medidas de seguridad	¿Tenemos un sistema de reglas y de medidas de seguridad? ¿Lo entiende y asume cada individuo? ¿Se respeta en la práctica? (Para más información, ver capítulo 2.2)
Gestión de la seguridad fuera del trabajo (familia, relaciones personales, tiempo libre)	¿Cómo organizamos nuestro tiempo fuera del trabajo (familia, relaciones personales, tiempo libre)? El consumo de drogas (incluido el abuso del alcohol) representa un importante punto débil. Las relaciones también pueden ser puntos débiles (y puntos fuertes). ¿Qué relación tienen nuestros familiares y amistades con nuestra actividad como defensores de ddhh?
Condiciones laborales	¿Son adecuados los contratos de trabajo de todo el mundo? ¿Podemos acceder a los fondos de emergencia? ¿Tenemos seguros?
Incorporando a gente	¿Son adecuados los procedimientos para incorporar al personal, a colaboradores u otros miembros? ¿Se toma alguna medida de seguridad especial con las/los voluntarios ocasionales (p.e., estudiantes) o las visitas?
Trabajar directamente con la gente o con organizaciones puente	¿Trabajamos directamente con la gente? ¿Conocemos bien a estas personas? ¿O trabajamos con una organización puente (esto es, que nos ayuda a presentar nuestro trabajo a la gente)? ¿Conocemos bien a esas personas?
Protección de testigos o víctimas con quienes trabajamos	¿Valoramos el riesgo que corren las víctimas y los testigos, etc. cuando trabajamos con ellas/os? ¿Usamos medidas de seguridad concretas cuando quedamos con estas personas o cuando vienen a nuestra oficina? Si reciben amenazas, ¿cómo reaccionamos?
Barrio y entorno social	¿Estamos bien integradas/os en la comunidad? ¿Hay grupos sociales que puedan considerar nuestra labor positiva o negativa? ¿Estamos rodeadas/os de gente potencialmente hostil (p.e., vecinos que puedan ser informadores)? ¿Son las y los vecinos simpatizantes parte de nuestro sistema de alarma?
Capacidad de convocatoria	¿Tenemos la capacidad de convocar a la gente a actividades públicas?

COMPONENTES RELATIVOS AL IMPACTO PSICOSOCIAL (GRUPO/INDIVIDUOS)	
CONTROL DEL ESTRÉS Y EL MIEDO	La gente clave de nuestro grupo, o como grupo, ¿confiamos en lo que hacemos? Las personas del grupo/comunidad, ¿expresamos sin ambigüedad (con palabras y hechos) sentimientos de apoyo mutuo y de saber que tenemos un propósito común? Los niveles de estrés, ¿están afectando a la buena comunicación y las relaciones interpersonales? ¿Podemos recibir apoyo psicológico exterior y/o hemos desarrollado nuestros propios recursos psicosociales?
DESÁNIMO Y AGOBIO	¿Se están expresando (con palabras y hechos) sentimientos de depresión y pérdida de esperanza?
COMPONENTES RELATIVOS A LA SOCIEDAD, LA CULTURA Y LA RELIGIÓN	
DISCRIMINACIÓN	¿Sufre alguien discriminación (tanto dentro como fuera de la organización) por razones de sexo, identidad cultural, religión, u orientación o identidad sexual? ¿Se sabe bien (o se confunden) qué son los derechos humanos, sociales, económicos, de identidad, culturales y religiosos?
COMPONENTES RELATIVOS A LOS RECURSOS EN EL TRABAJO	
COMPRENDER EL CONTEXTO DEL TRABAJO Y LOS RIESGOS	¿Tenemos acceso a información precisa sobre el contexto donde trabajamos, las partes implicadas y sus intereses? ¿Podemos procesar esa información para comprender los temas de amenazas, vulnerabilidad y capacidad de reacción?
CONCEBIR PLANES DE ACCIÓN	¿Podemos diseñar y llevar a cabo un plan de acción? ¿Existen ejemplos anteriores?
RECIBIR ASESORAMIENTO DE FUENTES BIEN INFORMADAS	¿Podemos obtener consejos fiables? ¿De fuentes pertinentes? ¿Podemos decidir libremente a qué fuentes consultar?
GENTE Y VOLUMEN DE TRABAJO	¿Hay suficiente gente para el volumen de trabajo? ¿Podemos planear visitas de campo en grupo (de al menos dos personas)?
RECURSOS ECONÓMICOS	¿Tenemos suficiente dinero para temas de seguridad? ¿Podemos manejar dinero líquido (cash) de forma segura?
CONOCIMIENTO DE IDIOMAS Y LUGARES	¿Hablamos los idiomas que hay que usar en esta zona? ¿Conocemos bien el lugar? (carreteras, pueblos, teléfonos públicos, centros de salud, etc.)
COMPONENTES RELATIVOS A CONTACTOS Y MEDIOS DE COMUNICACIÓN NACIONALES E INTERNACIONALES	
ACCESO A REDES DE CONTACTOS NACIONALES E INTERNACIONALES	¿Tenemos contactos nacionales e internacionales? ¿Y con delegaciones visitantes, embajadas, otros gobiernos, etc? ¿Con líderes de la comunidad, religiosos, u otras personas con influencia? ¿Podemos lanzar acciones urgentes a través de otros grupos? Nuestro acceso o afiliación a determinadas organizaciones, ¿podría servirnos para mejorar nuestra capacidad de protegernos?
ACCESO A LOS MEDIOS DE COMUNICACIÓN Y CAPACIDAD PARA OBTENER RESULTADOS CON ELLOS	¿Tenemos acceso a los medios de comunicación (nacionales, internacionales)? ¿Y a los medios de comunicación independientes? ¿Sabemos tratar con los medios de comunicación?

Una balanza de riesgo: otra forma de entender el riesgo

Una balanza es un instrumento que podemos usar para entender el concepto de riesgo. Es lo que podríamos denominar un "riscómetro". Si ponemos en uno de los platos dos cajas, una con nuestras amenazas y la otra con nuestras vulnerabilidades, y en el otro plato una caja con nuestra capacidad (de respuesta), veremos como el riesgo que corremos aumenta o disminuye:

Fig. 1

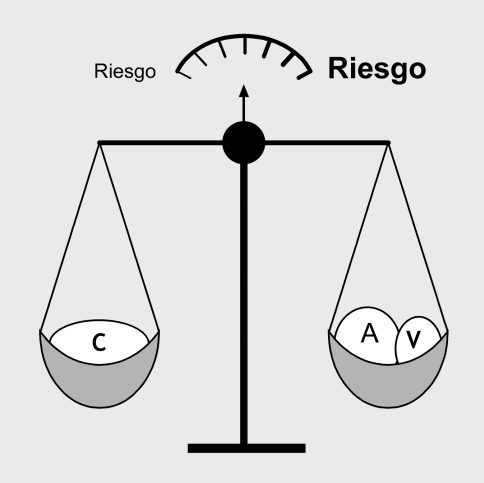
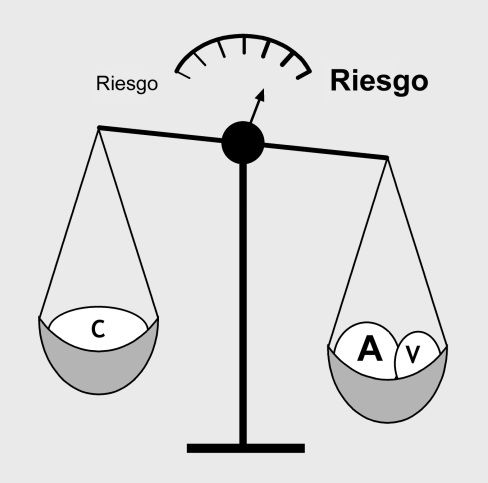
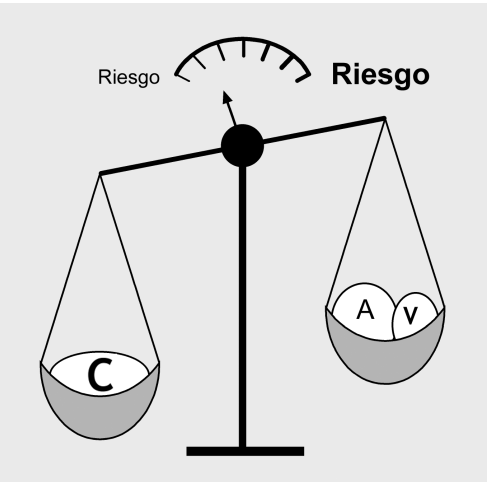


Fig. 2



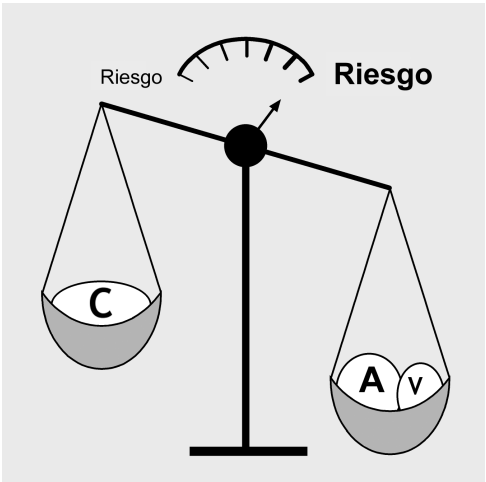
Cuantas más amenazas y vulnerabilidades tenemos, mas riesgo corremos.

Fig. 3



Cuanta más capacidad tenemos, menos riesgo corremos. Para reducir el riesgo podemos reducir nuestras amenazas y vulnerabilidades y aumentar nuestra capacidad.

Fig. 4



Pero… miren lo que pasa cuando las amenazas son muy grandes: aunque intentemos aumentar nuestra capacidad en ese momento, la balanza muestra de toda manera un nivel de riesgo muy elevado.

Resumen

$$\text{RIESGO} = \frac{\text{Amenazas x Vulnerabilidad}}{\text{Capacidad}}$$

La vulnerabilidad y la capacidad son componentes internos (porque podemos trabajarlas).

Las amenazas son componentes externos (porque son hechas por actores externos y siempre pueden darse).

1 • Trabajar la vulnerabilidad y la capacidad reducirá la viabilidad de las amenazas. Hacer una lista de todos nuestros puntos vulnerables y de nuestras capacidades. La técnica de la lluvia de ideas puede ayudar inicialmente.

2 • Agrupar los componentes primero por grandes bloques y luego desarrollar cada punto.

3 • Determinar qué capacidades queremos desarrollar: empezar a trabajarlas considerando cómo hacerlo.

Casi siempre un mismo conjunto de acciones puede resolver varios temas de una misma variable.

4 • El resultado de los pasos anteriores reducirá la viabilidad de la amenaza y, consecuentemente, los riesgos.

Aunque alguna variable pudiera estar vinculada al entorno, los componentes pueden considerarse internos, es decir, susceptibles de ser modificados por las y los defensores. Por ejemplo, una zona peligrosa es, evidentemente, una variable "externa". Sin embargo, podemos convertirla en una variable interna si nos entrenamos para saber lidiar con ella.

Una amenaza es externa y, al margen de lo que se haga, quien amenaza puede seguir haciéndolo. Como defensores y defensoras "sólo" podemos intentar reducir la probabilidad de que se lleve a cabo la amenaza, no siempre podemos eliminarla, a no ser que el contexto político cambie.

CAPÍTULO 1.3

cómo Comprender y evaluar las amenazas

Objetivo:

Comprender a fondo lo que son las amenazas y cómo responder a ellas

Valoración de las amenazas: comprender las amenazas en profundidad

La represión de las y los defensores de derechos humanos es un asunto estrechamente vinculado a la psicología. Las amenazas son un recurso común para provocarles sentimientos de vulnerabilidad, nerviosismo, confusión e indefensión. La represión también pretende destruir las organizaciones, sembrando la desconfianza en las y los líderes y compañeros. Así pues, como defensoras y defensores de derechos humanos tenemos que encontrar un equilibrio entre, por un lado, abordar el tema de las amenazas, con cuidado y eficacia, y por otro, poder trabajar sintiéndonos mínimamente seguros. Éste es el objetivo del presente capítulo también.

En el capítulo 1.2, se definieron las amenazas como "la posibilidad de que alguien dañe la integridad física o moral de otra persona, o su propiedad, mediante una acción intencionada a menudo violenta". Asimismo, tratamos el tema de las **probables** amenazas **(indirectas)**, es decir, cuando amenazan a una defensora próxima a ti y crees que tú podrías ser la siguiente persona; y las amenazas **declaradas** o **directas** (cuando te amenazan de muerte). Consideraremos ahora cómo lidiar con las amenazas declaradas.

Una amenaza declarada **es una declaración o indicación de que pretenden causarnos daño o sufrimiento, o "castigarnos", normalmente para conseguir algo**. Las y los defensores solemos recibir amenazas por el impacto que tiene nuestro trabajo, y la mayoría de las mismas tienen el objetivo claro de interrumpir lo que estamos haciendo o bien de forzarnos a hacer algo.

Una amenaza siempre tiene un **origen**: la persona o grupo que se ve afectado por el trabajo de las y los defensores y que proyecta la amenaza; también tiene un **objetivo**, que está vinculado al impacto de ese trabajo; y un medio de expresión, es decir, una forma de llegar al conocimiento de las y los defensores amenazados.

Las amenazas son un tema difícil. Podríamos decir, con cierta distancia irónica, que son muy "ecológicas" porque pretenden conseguir grandes resultados con

una inversión mínima de energía. ¿Por qué? Hay diferentes razones, mencionemos las siguientes:

- Quien amenaza tiene la capacidad de actuar pero le preocupa en cierta medida el precio político que pueda tener actuar abiertamente contra una defensora o un defensor. Por eso también se hacen amenazas anónimas.
- Quien amenaza tiene una capacidad limitada para actuar y pretende conseguir el mismo objetivo ocultando su incapacidad con una amenaza. La limitación podría ser temporal (p.e., debida a que se tengan otras prioridades en ese momento) o permanente, pero en ambos casos, la situación podría cambiar y desembocar en una agresión.

Un defensor dijo una vez: "Las amenazas siempre consiguen algo, aunque sólo sea porque estamos aquí hablando de ellas". Una amenaza es una experiencia personal porque siempre afecta a las personas de alguna manera. De hecho, toda amenaza tiene un impacto doble: en lo emocional y en temas de seguridad. Aquí nos vamos a centrar en el tema de la seguridad, pero no hay que olvidar el aspecto emocional que conlleva toda amenaza, o el impacto de las emociones en el tema de la seguridad.

Sabemos que las amenazas están normalmente relacionadas con el impacto que tiene nuestro trabajo. Consecuentemente, si nos amenazan estamos recibiendo información sobre cómo está afectando nuestro trabajo a un actor. Visto así, una amenaza se convierte en una valiosa fuente de información, por lo que hay que analizarla cuidadosamente.

La diferencia entre amenazar y constituir una amenaza real

Se amenaza a las defensoras y los defensores por muchas razones, pero sólo algunas de las personas que amenazan tienen de hecho la intención o la capacidad de cometer un acto violento. Por otro lado, algunos individuos pueden representar un grave peligro aunque no formulen ninguna amenaza. La distinción entre amenazar y ser una amenaza real es importante:

- Algunas personas que **amenazan acaban constituyendo una amenaza real.**
- Muchas de las personas que **amenazan nunca son una amenaza real.**
- Algunas de las personas que **nunca amenazan son de hecho una amenaza real.**

Una amenaza solo es creíble si indica que el actor que hay detrás tiene la capacidad de actuar en nuestra contra; debe mostrar un nivel mínimo de fuerza o incluir algún elemento que provoque miedo. Quien amenaza puede demostrar su capacidad de actuación fácilmente, como por ejemplo, dejando una nota en un coche que está cerrado, aunque sólo lo habíamos dejado aparcado allí unos minutos, o llamándonos por teléfono justo cuando entramos en casa, para hacernos saber que nos están vigilando. Para que sintamos miedo, pueden añadir elementos simbólicos, como cuando nos envían una invitación a nuestro propio funeral o nos dejan un animal muerto a la entrada de casa o en nuestra cama. Muchas amenazas combinan todas estas características. Es importante distinguirlas todas, porque algunas de las personas que amenazan usan elementos

simbólicos o que dan miedo para convencernos de que van a actuar, sin ser eso necesariamente cierto.

Cualquiera puede amenazar, pero no todo el mundo puede consumar una amenaza.

Al fin y al cabo, tenemos que saber si nos estamos enfrentando a una amenaza real, que puede ser consumada. Si tenemos una certeza relativa de que no es probable, estaremos en una posición muy distinta a si pensamos que es factible que se produzca.

Los tres objetivos principales a la hora de valorar una amenaza son:

- Conseguir toda la información posible sobre el objetivo y la fuente de la amenaza (ambos estarán ligados al impacto de nuestro trabajo).
- Llegar a una conclusión razonada y razonable sobre si se va a consumar la amenaza.
- Decidir qué hacer.

Cinco pasos para valorar una amenaza

1 • **Determinar los hechos relacionados con la(s) amenaza(s).** Es importante saber exactamente lo que ha ocurrido. Podemos hacerlo a través de entrevistas, o haciéndole preguntas a gente clave, y ocasionalmente a través de informes relevantes.

2 • **Determinar si se ha dado un patrón de amenazas a lo largo del tiempo.** Si se producen varias amenazas seguidas (como ocurre a menudo) es importante buscar patrones, como por ejemplo el medio usado para amenazar, los momentos en que se dan, los símbolos, si la información se pasa por escrito o verbalmente, etc. No siempre puede establecerse un patrón, pero éstos son muy útiles para valorar las amenazas.

3 • **Determinar el objetivo de la amenaza.** Como una amenaza suele tener un objetivo claro relacionado con la repercusión de nuestro trabajo, seguirle la pista a este tema podría ayudarnos a determinar cuál es su objetivo concreto.

4 • **Determinar la fuente de la amenaza.** (Esto sólo puede hacerse si se ha hecho lo anterior.) Hay que intentar concretar lo más posible para distinguir entre la persona que decide hacer una amenaza y quien la lleva a cabo: por ejemplo, podríamos decir que "el gobierno" nos está amenazando, pero como los gobiernos son actores complejos, es más útil averiguar qué parte del gobierno puede estar tras las amenazas. Otros actores complejos son las fuerzas de seguridad y los grupos guerrilleros. También hay que recordar que incluso aunque la amenaza no sea anónima, el dato de autoría podría ser falso: podrían estar mintiendo para evi-

tar pagar un precio político y conseguir, de todos modos, provocar miedo e interrumpir nuestro trabajo.

5 • **Llegar a una conclusión razonada y razonable sobre si van a consumar la amenaza o no.** La violencia es contingente. Nunca estamos completamente seguras o seguros de que una amenaza vaya a consumarse o no. Cuando hablamos de predecir si se va a dar esta violencia, nos estamos refiriendo a que seamos capaces de decir que, dadas determinadas circunstancias, existe un riesgo concreto de que determinada persona o grupo actúe violentamente contra un objetivo determinado.

No podemos saber lo que va a ocurrir, pero esto no implica que no podamos llegar a una conclusión razonable sobre la probabilidad de que una amenaza dada se consume. No obstante, puede ocurrir que tras seguir los pasos anteriores no consigamos la información necesaria para llegar a ningún tipo de conclusión. Y también que en el grupo existan diferentes opiniones sobre cómo de "real" es la amenaza. En cualquier caso, conviene actuar siempre considerando el peor escenario posible.

Por ejemplo:

Una defensora ha recibido amenazas de muerte. El grupo analiza las amenazas y llega a dos conclusiones diferentes, ambas bien fundamentadas. Parte del equipo dice que la amenaza es un farol; otra parte cree que hay razón para preocuparse. Al final de la reunión, el grupo decide asumir el peor de los escenarios posibles (que hay razón para preocuparse) y en consecuencia, procede a tomar medidas de seguridad.

Este método para valorar las amenazas parte de hechos concretos (paso 1) y pasa a un razonamiento cada vez más especulativo. En el paso 2 se empiezan a interpretar los hechos. Existen razones para que se siga el orden propuesto. Si empezamos por el paso 2 o por el 4, por ejemplo, no dispondremos de la información más sólida que proporcionan los pasos anteriores.

Duración y cierre del caso de amenazas

Un incidente de seguridad o una amenaza puede sembrar la alarma en un grupo de defensores o defensoras pero es difícil mantener ese sentimiento durante todo el tiempo de duración de la amenaza. Debido a la presión constante inherente al trabajo de derechos humanos, si se abusa de las alertas, el grupo podría acostumbrarse a ellas y bajar la guardia.

Sólo se debe dar la voz de alarma en el grupo si existe información relevante y podemos centrarnos en anticipar un acontecimiento concreto. Esa alerta tiene que motivar a las y los miembros del grupo a actuar y tiene que estar asociada a unas medidas concretas. Una alerta es eficaz cuando estimula moderadamente: si la estimulación es baja, la gente no actúa, y si es alta, genera una sobrecarga emocional.

Si una amenaza persiste en el tiempo, es esencial entrevistarse con los miembros del equipo para hacer un seguimiento de la situación, corrigiendo la información que ya no sirva, modificando las recomendaciones caducas y reforzando la confianza del grupo en las medidas adoptadas.

Por último, si la amenaza no se materializa, es preciso conocer las razones y que seamos conscientes de que la amenaza ya no es tan grande o que ya ha desaparecido.

Se puede cerrar un caso de amenazas cuando pensamos que el atacante potencial ya no consumaría la amenaza. Para tener la certeza de que puede cerrarse, lo ideal es poder explicar por qué puede hacerse. Asimismo, también habrá que plantearse qué circunstancias tendrían que cambiar para que quien amenaza pueda pasar a mayores.

Reacciones a las amenazas desde la seguridad

- Una amenaza puede considerarse un incidente de seguridad. Para saber más sobre los incidentes de seguridad, ver capítulo 1.4.
- Una valoración de amenazas declaradas puede conducirnos a pensar que podríamos ser objeto de un ataque. En el capítulo 1.5, tratamos cómo prevenir un ataque.

Resumen

Las amenazas (que nos hacen) pueden directas (declaradas) e indirectas (no declaradas).

Una amenaza declarada es una indicación de la intención de actuar contra alguien para conseguir algo.

Cinco pasos para determinar la viabilidad de una amenaza y poder así saber qué hay que hacer:

1 • Determinar los hechos

2 • Determinar el patrón a lo largo del tiempo

3 • Determinar el objetivo

4 • Determinar la fuente

5 • Llegar a una conclusión razonada y razonable sobre la viabilidad de la amenaza.

Es importante evitar conclusiones del tipo "esto es evidente" y esforzarnos por formular los temas de la manera más concreta posible, lo que podemos conseguir imaginando todos los escenarios que nos sugieran los hechos y los patrones que se den, y buscando cómo explicarnos esos escenarios.

CAPÍTULO 1.4

Incidentes de seguridad: definición y análisis

Objetivo:

Aprender a reconocer y a responder a incidentes de seguridad

¿Qué es un incidente de seguridad?

De manera sencilla, un incidente de seguridad puede definirse como cualquier hecho o acontecimiento que pensamos podría afectar a nuestra seguridad personal o como organización.

Un incidente de seguridad puede ser incidental, intencionado o no intencionado.

Ejemplos de incidentes de seguridad podrían ser: ver al mismo vehículo sospechoso aparcado fuera de nuestra oficina o casa varios días seguidos; que suene el teléfono por la noche y que cuando contestemos no responda nadie; que alguien pregunte por alguna o alguno de nosotros en un pueblo vecino; que entren a robar en nuestra casa, etc.

Pero no todo lo que notamos es un incidente de seguridad. Deberíamos **registrarlos** siempre, describirlos por escrito, y luego **analizarlos**, preferiblemente con las y los compañeros, para así averiguar si nos enfrentamos a algo que pudiera estar amenazando nuestra seguridad. Entonces estaremos en condiciones de **reaccionar** al incidente. La secuencia de acontecimiento sería la siguiente:

> Notamos algo ⇨ pensamos que podría ser un incidente de seguridad ⇨ lo registramos / lo hablamos con alguien ⇨ lo analizamos ⇨ determinamos si es un incidente de seguridad ⇨ reaccionamos en consecuencia.

Aunque en la situación dada el tiempo apremie, conviene seguir estos pasos, o al menos la versión abreviada que detallaremos en tres pasos concretos después (ver bajo "Cómo abordar los incidentes de seguridad").

Cómo distinguir entre incidentes de seguridad y amenazas:

Si estás esperando al autobús y alguien que está a tu lado te amenaza por el trabajo que haces, esto, además de ser una amenaza, es un incidente de seguridad. Pero si descubres que un coche patrulla está vigilando tu oficina al otro lado de la calle, o que te han robado el celular, esto son incidentes de seguridad pero no necesariamente amenazas. No obstante, aunque podemos distinguir con claridad una amenaza de un incidente de seguridad no intencionado (como encon-

trarte entre la muchedumbre o perder tus llaves, por ejemplo), los incidentes de seguridad provocados intencionadamente no tienen necesariamente el mismo objetivo que las amenazas (ver capítulo 1.2): el objetivo mínimo de un incidente provocado intencionadamente es reunir información sobre las y los defensores, vaya o no vaya a ser utilizada ésta contra ellos.

Hacer esta distinción es importante al menos para la salud mental de las y los defensores.

Todas las amenazas son incidentes de seguridad, pero no todos los incidentes de seguridad son amenazas.

¿Por qué son tan importantes los incidentes de seguridad?

Los incidentes de seguridad son fundamentales para hacernos cargo de nuestra seguridad porque nos proporcionan información vital sobre el impacto de nuestro trabajo y también sobre posibles actuaciones que se planeen en nuestra contra. Asimismo, tales incidentes nos permiten cambiar nuestro comportamiento o actividades para evitar sitios que podrían ser peligrosos, o más peligrosos de lo normal. Así pues, los incidentes de seguridad pueden verse como indicadores de la situación de seguridad concreta en que nos encontramos. Si no pudiéramos detectar tales cambios, nos sería difícil actuar a tiempo y eficazmente para mantenernos a salvo. Por ejemplo, después de notar varios incidentes de seguridad, nos damos cuenta de que nos están vigilando: ahora podemos hacer algo al respecto.

Los incidentes de seguridad son "la unidad mínima" de las medidas de seguridad y son indicativos de la magnitud de la oposición a nuestro trabajo, o de la presión que soportamos. Hay que fijarse bien en ellos.

¿Cuándo y cómo se notan los incidentes de seguridad?

Esto depende de cómo de obvio sea el incidente. Si éste pudiera pasar desapercibido, reconocerlo dependerá de nuestro entrenamiento en seguridad y de nuestra experiencia y nivel de alerta.

Cuanto más conscientes seamos del entorno y cuanto mejor entrenadas y entrenados estemos, menos incidentes escaparán a nuestra atención.

A menudo los incidentes de seguridad no se perciben, o sí, aunque brevemente, y se olvidan; también ocurre que se puede reaccionar exageradamente ante lo que creemos que es un incidente de seguridad.

¿Por qué puede pasar desapercibido un incidente de seguridad?

Un ejemplo:

Un defensor vive un incidente de seguridad pero la organización para la que trabaja no reacciona. Esto podría deberse a que…

- esa persona no es consciente de que se ha producido un incidente de seguridad;

- esa persona es consciente de ello, pero lo descarta porque decide que no tiene importancia;
- esa persona no ha informado a su organización (se le olvidó, no lo cree necesario, o no dice nada porque cree que fue por un fallo que cometió);
- la organización, habiendo analizado en el equipo el incidente una vez leída la narración de quien lo vivió, no juzga necesario tomar ninguna medida.

¿Por qué a veces se reacciona exageradamente ante los incidentes de seguridad?

Por ejemplo:

Puede que un compañero esté siempre contando historias sobre incidentes de seguridad, pero cuando éstos se analizan, se ve que no lo son. El verdadero incidente de seguridad en este caso es que nuestro compañero tiene un problema: ve incidentes de seguridad donde no los hay. Habría que ofrecerle ayuda para resolverlo, porque puede que esté tenga mucho miedo o estrés.

De todos modos, hay que tener cuidado con obviar o descartar incidentes de seguridad, porque esto se hace en demasiadas ocasiones...

Cómo abordar los incidentes de seguridad

Hay muchas maneras de reaccionar rápidamente ante un incidente de seguridad. Los pasos que se muestran a continuación toman en cuenta la reacción desde el momento en que sucede el incidente (o ha sido reportado), durante el mismo, o después de que haya pasado.

Al menos, habría que plantearse dar los siguientes pasos:

1 • **Registro.** Debemos registrar todos los incidentes de seguridad que notemos, ya sea en una libreta personal o en un cuaderno que use todo el grupo.

2 • **Análisis.** Todos los incidentes de seguridad que registremos deberán ser analizados de inmediato o regularmente. Es mejor analizarlos en equipo porque esto minimiza el riesgo de que se nos escape algo. Alguien debería ser responsable de asegurarse de que esto se hace.

También debemos decidir si ciertos tipos de incidentes (como las amenazas) los clasificaremos como confidenciales. ¿Es ético o realista ocultarle a la gente con la que trabajamos que se ha producido una amenaza? No existe ninguna regla aplicarse a todas las situaciones, pero en general es siempre mejor compartir la información y tratar conjuntamente los temas de logística y los miedos.

3 • **Reacción.** Dado que los incidentes de seguridad dan información sobre el impacto de nuestro trabajo, podemos usarlos para lo siguiente:

- Reaccionar al propio incidente;
- **Recabar información** útil para temas de seguridad sobre nuestro trabajo, nuestros **planes de trabajo** y nuestra **estrategia**. Por ejemplo:

Ejemplo de un incidente
que nos lleva a mejorar nuestra seguridad

Por tercera vez alguien de nuestra organización ha tenido problemas al pasar por un puesto de control de la policía porque a menudo se nos olvida llevar los documentos que necesitamos enseñar allí. Así pues, decidimos hacer una lista de los mismos, y que todos los miembros del equipo tengan que consultarla antes de abandonar la ciudad. Es posible que también optemos por cambiar la ruta para este tipo de salidas.

Ejemplo de un incidente
que nos lleva a replantearnos temas de seguridad

En el mismo puesto de control de la policía, retienen a alguien del equipo durante media hora y se le dice a esta persona que el trabajo que hacemos no vale nada. Se producen amenazas veladas. Cuando esa persona pide una explicación en comisaría, se repite la escena. Nos reunimos para revisar nuestros planes de trabajo, porque parece claro que para seguir trabajando allí habrá que cambiar algunas cosas. Planeamos, pues, una serie de reuniones con funcionarios del ministerio del Interior para que la policía de los puestos de control reciba la orden de no acosarnos; cambiamos algunos de los puntos de nuestro plan de trabajo y decidimos reuniros una vez a la semana para hacer un seguimiento de esta situación.

Ejemplo de un incidente
que nos ayuda a mejorar nuestra estrategia de seguridad

Al empezar a trabajar en una nueva zona, empezamos a recibir de inmediato amenazas de muerte. Además, atacan físicamente a una persona del equipo. No habíamos previsto una oposición tan fuerte a nuestro trabajo, por lo que en nuestra estrategia de seguridad no contábamos con ningún plan de contingencia para ese caso. Así pues, tenemos que modificarla: habrá que trabajar para que aumente la tolerancia a nuestro trabajo en la zona y para disuadir de que se produzcan más ataques y amenazas. Para ello, es posible que tengamos que suspender nuestras actividades durante algún tiempo, retirarnos de la zona y reconsiderar todo el proyecto.

Cómo reaccionar con urgencia a un incidente de seguridad

Hay varias formas de responder con prontitud ante un incidente de seguridad. Los siguientes pasos han sido formulados para establecer cuándo y cómo reaccionar desde el momento en que se informa de un incidente de seguridad, mientras se está dando y una vez ha terminado.

Paso 1: Informar del incidente

- ¿Qué está pasando/ha pasado? (hay que centrarse en los hechos)
- ¿Dónde y cuándo ocurrió?
- ¿Quién(es) estaba(n) allí? (si puede determinarse)
- ¿Se produjo algún daño a las personas o a la propiedad?

Paso 2. Decidir cuándo reaccionar. Existen tres posibilidades:

- Es necesario reaccionar de inmediato para asistir a la gente herida o para detener un ataque.
- Es necesario reaccionar rápidamente (en las próximas horas o días) para evitar que se produzcan nuevos incidentes de seguridad posibles (el incidente ya pasó).
- Es necesario sólo una acción de seguimiento (dentro de varios días, semanas o incluso meses): si la situación se ha estabilizado, puede que ya no sea necesaria una reacción inmediata o rápida. No obstante, cualquier incidente de seguridad que requiera una reacción inmediata o rápida debe recibir un seguimiento para que podamos restablecer o revisar el entorno donde trabajamos.

Paso 3. Decidir cómo reaccionar y cuáles son los objetivos

- Si la reacción tiene que ser inmediata, los objetivos son claros: asistir a las personas heridas y/o impedir otro ataque.
- Si la reacción tiene que ser rápida, los objetivos serán determinados por la persona a cargo o el equipo de crisis (o similares) y se centrarán en restablecer la seguridad necesaria de quienes han vivido el incidente.

Las acciones/reacciones que vengan después seguirán los canales normales de toma de decisiones de la organización, y tendrán el objetivo de restaurar externamente un entorno de trabajo seguro, y también de restablecer los procedimientos internos de la organización y mejorar posteriores reacciones a los incidentes de seguridad.

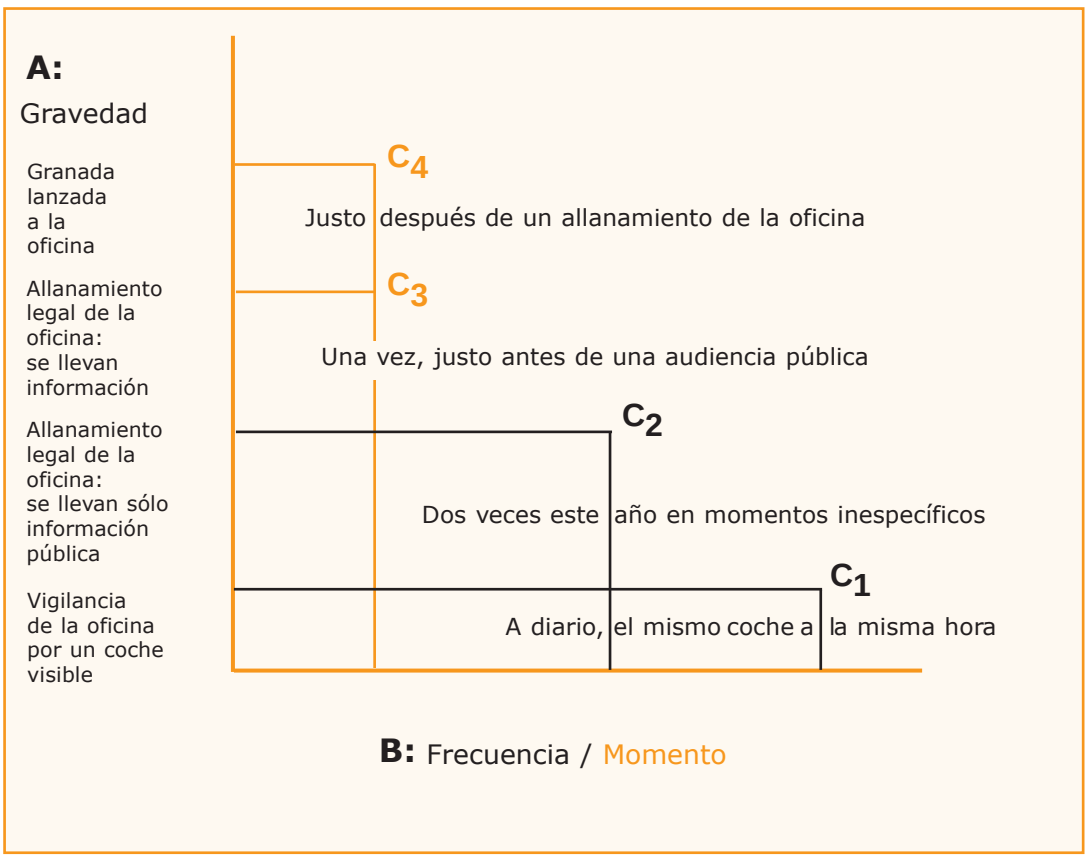
Cualquier reacción deberá tener en cuenta también la seguridad y la protección de otras personas u organizaciones o instituciones con las que mantenemos una relación de trabajo.

Hay que determinar los objetivos antes de actuar. Actuar con prontitud es importante, pero saber por qué se está actuando es más importante. Si se determina primero lo que se desea conseguir (los objetivos), entonces se comprenderá mejor cómo conseguirlo (curso de acción).

Por ejemplo:

Si un grupo de defensoras recibe noticias de que una compañera no ha llegado a su destino en un pueblo, podrían reaccionar llamando a un hospital, a sus contactos de otras ONGs, a una oficina de la ONU cercana y a la policía. Antes de empezar a llamar sería fundamental determinar qué queremos conseguir y lo que vamos a decir. Si no lo hacemos, podríamos generar una alarma innecesaria (imaginemos que la defensora sencillamente llegó tarde porque perdió el autobús y olvidó llamar a la oficina para informar de ello) o una reacción opuesta a la pretendida.

Registrar los incidentes de seguridad (incluyendo, claro, amenazas y ataques), nos puede ayudar a analizarlos con la perspectiva de anticiparse a ellos en ciertos momentos. Por ejemplo, si el registro refleja un aumento de incidentes en períodos pre-electorales, es más probable que sucedan de nuevo en el siguiente período pre-electoral. El registro puede ayudar también a valorar la probabilidad de un ataque contra un defensor por un potencial agresor, o en caso de incidentes de seguridad debidos a descuidos de los defensores, puede contribuir a valorar cómo se maneja la seguridad por los defensores mismos.



C: Probabilidad de una acción inminente más grave contra defensores por un potencial agresor

C1: MUY BAJA (A1: vigilancia de la oficina por un coche visible + B1: a diario el mismo coche a la misma hora)

C2: BAJA: (A2: allanamiento legal de la oficina: sólo se llevan información pública + B2: este año, dos veces en momentos no especialmente críticos)

C3: ALTA: (A3: allanamiento legal de la oficina, se llevan información secreta -por ejemplo nombres de testigos-) + B3: Una vez, justo antes de una audiencia pública)

C4: MUY ALTA: (A4: Granada lanzada a la oficina + B4: Justo después de un allanamiento de la oficina, C3)

Resumen

Un incidente de seguridad es cualquier hecho o acontecimiento que creemos que podría afectar a nuestra seguridad personal o la de nuestra organización.

Los incidentes de seguridad miden la seguridad y el impacto del trabajo en derechos humanos sobre los intereses de otros.

Todas las personas que trabajamos en la defensa de los derechos humanos vivimos incidentes de seguridad. Lo contrario implicaría que...

- El impacto de nuestro trabajo es insignificante, ya sea porque no lo estamos haciendo bien y/o porque no está teniendo repercusión en los intereses de nadie. (En otras palabras, nadie se fija en nosotras o nosotros).

- El agresor potencial ya tiene toda la información nuestra que necesita y no tiene por qué preocuparse: como defensoras y defensores no llegamos a identificar en su día los incidentes de seguridad que provocó.

Un incidente de seguridad no es una amenaza, sin embargo, requiere que le prestemos atención.

Tres pasos para abordar los incidentes de seguridad:

1 • Registrarlos.

2 • Analizarlos.

3 • Reaccionar.

CAPÍTULO 1.5

Cómo Evitar las agresiones y cómo reaccionar ante ellas

Objetivo:

Valorar la probabilidad de que se den diferentes tipos de agresión

Evitar posibles agresiones directas a las defensoras y defensores de derechos humanos

Organizar la contravigilancia

Agresiones a Defensores de Derechos Humanos

La violencia constituye un proceso, además de poder manifestarse en un acto. Un ataque violento a un defensor no ocurre en el vacío. Cuando se analizan las agresiones en profundidad, a menudo se ve que son el punto álgido en un conflicto, disputa, amenaza, incidente de seguridad o error cuyo desarrollo se puede rastrear a lo largo del tiempo.

Las agresiones a las y los defensores son producto de al menos tres factores que interactúan:

1 • **La parte que ejerce la acción violenta y recursos.** Los ataques a las y los defensores son a menudo el producto de procesos de reflexión y de actuaciones que podemos analizar y de las que podemos aprender mucho aunque sean injustificables. La parte tendrá que invertir recursos por lo menos para recoger información (incidentes de seguridad) sobre el defensor en su punto de mira.

2 • **Situaciones pasadas y presentes que llevan al agresor a considerar el uso de la violencia como una opción deseable.** La mayor parte de quienes atacan a las y los defensores considera su acción una forma "útil" para alcanzar su objetivo de "resolver el problema", bien porque perciben impunidad, o bien porque están dispuestos a pagar el coste político puesto que "merece la pena".

3 • **Un escenario** favorable para la violencia, que posibilita que se dé o que no contribuye a evitarla.

¿Quién entonces es un peligro para las y los defensores?

Por regla general, un agresor potencial es quien piensa que atacar a un defensor es una forma posible, deseable, aceptable o potencialmente eficaz para con-

seguir un objetivo. La amenaza es mayor si ese individuo tiene, o puede desarrollar, la capacidad necesaria para hacerlo.

El peligro de amenaza de agresión puede reducirse si se producen cambios en la capacidad del agresor potencial para orquestar esa acción, en su actitud hacia cómo de aceptable es agredir, o bien en cómo de probable es que el individuo vaya a ser identificado como agresor y castigado.

Algunas agresiones vienen precedidas de amenazas; otras no. En cualquier caso, el comportamiento de quienes las planean a menudo ofrece pistas sobre lo que se está haciendo, pues los agresores potenciales tienen que reunir información sobre cuál es el mejor momento para atacar, además de planear cómo llegar a su objetivo y cómo escapar.

Por tanto, es vital detectar y analizar cualquier indicio que pueda apuntar a que se está planeando una agresión. Esto implica:

- determinar la probabilidad de que se materialice una amenaza (ver capítulo 1.3);
- identificar y analizar los incidentes de seguridad.

Los incidentes de seguridad relacionados con que las y los defensores, o su lugar de trabajo, estén siendo vigilados tienen el objetivo de recoger información. Esta información no siempre se usa para planear un ataque físico, pero es importante intentar determinar si es así o no (ver capítulo 1.4). La vigilancia se utiliza para diferentes propósitos:

- Determinar qué actividades realiza quién, cuándo y con quién.
- Usar esa información para planear un ataque a personas u organizaciones.
- Reunir la información necesaria para poder llevar a cabo un ataque.
- Reunir la información necesaria para poder emprender acciones legales u otro tipo de acoso (sin violencia directa).
- Intimidarnos, intimidar a quienes nos apoyan o a las otras personas con quienes trabajamos.

Aunque para diseñar un ataque es necesario vigilar a la víctima potencial, la vigilancia en sí misma no es el ataque físico. Es importante recordar que el hecho de que nos estén vigilando no siempre implica que vayamos a ser objeto de un ataque; y que aunque a veces la violencia hacia una persona concreta se produzca de pronto, cuando un agresor aprovecha lo que es un buen momento para actuar, incluso en ese caso ha habido preparación previa.

A pesar del número tan importante de agresiones a defensores de derechos humanos, existe poca información que nos ayude a saber cuándo se está planeando una agresión. En cualquier caso, los pocos estudios de que disponemos ofrecen reflexiones interesantes.[1]

[1] Claudia Samayoa y José Cruz (Guatemala) y Jaime Prieto (Colombia) han elaborado interesantes estudios sobre las agresiones a defensores/as de derechos humanos. Mahony y Eguren (1997) también analizaron dichas agresiones.

- **Agredir a una persona que trabaja en la defensa de los derechos humanos no es fácil y requiere que se disponga de ciertos recursos.** Es necesario vigilar a la persona que se quiere atacar para averiguar cuáles son sus movimientos y elegir el mejor lugar para la agresión. Asimismo, es vital saber cómo llegar al objetivo y cómo conseguir escapar rápidamente. (En cualquier caso, un entorno físico desfavorable puede facilitarle las cosas al agresor).

- **Quienes atacan a las y los defensores suelen mostrar un mínimo de coherencia en sus actuaciones.** La mayor parte de los ataques se producen contra defensoras o defensores que están muy involucrados en temas que afectan directamente a sus agresores. En otras palabras, las agresiones no suelen ser aleatorias, casuales, sino que responden a los intereses de quienes ejercen la violencia.

- **Los factores geográficos importan.** Por ejemplo, las agresiones a defensoras y defensores de las zonas rurales reciben menos atención pública, y por tanto generan menos reacción legal o política, que las agresiones hechas en zonas urbanas. Los ataques a sedes de ONGs u organizaciones muy conocidas en las zonas urbanas generan mayor reacción.

- **Antes del ataque, los agresores tienen que analizar sus opciones y tomar ciertas decisiones.** Tienen que decidir si atacar a líderes o a activistas de base, y también si hacerlo en una única acción (contra una persona clave, posiblemente muy conocida, lo que podría aumentar el coste político de la actuación) o en una serie de agresiones (contra otras personas de la organización). Los pocos estudios que existen apuntan a que se suelen emplear ambas estrategias.

Cómo establecer la viabilidad de una agresión

Con objeto de saber qué probabilidad existe de que se produzca una agresión, tenemos que considerar todos los factores que entran en juego. Para determinar cuáles son, es útil analizar por separado los diferentes tipos de agresión: la delincuencia común, las agresiones incidentales (estar en el peor momento en el peor lugar) y las agresiones directas (el targeting). Consideremos las siguientes tablas:[2]

[2] Esta clasificación de las agresiones hace uso de las mismas categorías que utilizamos al analizar las amenazas, por lo que se puede consultar ese capítulo también para aclarar dudas.

Tabla 1: Cómo establecer la probabilidad de que se produzcan agresiones directas (targeting)

(**AP** significa Agresor Potencial)

Probabilidad de agresiones directas (targeting)			
Factores	Probabilidad baja	Probabilidad mediana	Probabilidad alta
Capacidad de agredir	AP con poca capacidad para actuar en zonas donde trabajamos	AP podría actuar en zonas próximas a donde trabajamos	AP con control absoluto en zonas donde trabajamos
Móvil económico	AP no necesita nuestro equipamiento ni nuestro dinero	AP interesado en nuestro equipamiento, dinero en efectivo u otro tipo de ingresos (p.e. secuestros)	AP necesita desesperadamente equipamiento o dinero en efectivo
Móvil político y militar	Ninguno. Nuestro trabajo no obstaculiza sus objetivos	Parcial - nuestro trabajo pone coto a sus objetivos políticos y militares	Nuestro trabajo daña claramente sus objetivos, beneficia a sus oponentes, etc.
Agresiones previas	Ningún caso, o excepcionalmente	Algunos casos	Muchos casos anteriores
Actitudes o intenciones	Simpatizan o son indiferentes	Indiferentes Amenazas ocasionales Advertencias frecuentes	Agresividad - claras amenazas en el presente
Capacidad de las fuerzas de seguridad para evitar que se den las agresiones	Existe	Baja	Nula, o las fuerzas de seguridad colaboran con (o pasan a ser) AP
Nuestro nivel de influencia política para neutralizar al AP	Bueno	De medio a bajo	Limitado (dependiendo de las circunstancias) o nulo

Ejemplo

de la probabilidad de agresiones directas (targeting):

El agresor potencial controla las zonas donde trabajamos pero no tiene motivos económicos para agredirnos. Nuestro trabajo limita sólo en parte sus objetivos políticos y militares, y no existen precedentes de agresiones similares en la zona. Su actitud es indiferente, y está claro que no le compensa pagar el precio de atraer la atención o la presión nacional o internacional por atacarnos.

La probabilidad de agresiones directas en este escenario se considera de baja a media.

Tabla 2: Cómo establecer la probabilidad de una agresión por delincuencia común

(**DC** significa Delincuencia Común)

Probabilidad de agresiones por delincuentes comunes			
Factores	Probabilidad baja	Probabilidad mediana	Probabilidad alta
Capacidad de movimiento y localización de DC	DC permanece en sus zonas, no entran en las nuestras	DC suele ir a otras zonas de noche, u operan cerca de las zonas donde trabajamos	DC coopera en cualquier zona, de día o de noche
Agresividad de DC	DC evita el enfrentamiento (cometen crímenes donde no suele haber gente)	DC comete crímenes en la calle (pero no en oficinas con gente)	DC roba abiertamente, en la calle o en lugares cerrados
Posesión y uso de armas	Ninguno, o usa armas no letales	Armas rudimentarias, como machetes	Armas de fuego, a veces muy potentes
Tamaño y organización	Actúan individualmente o en parejas	Actúan en grupos de 2 a 4 personas	Actúan en grupo
Disuasión y reacción policial	Reacción rápida, capaz de ser disuasiva	Reacción lenta, poca eficacia para detener a DC en la comisión del crimen	La policía no suele responder siquiera con un nivel mínimo de eficacia
Entrenamiento y profesionalidad de las fuerzas de seguridad	Bien entrenadas, buenos profesionales (podrían no tener los recursos necesarios)	Entrenan regularmente, salarios bajos, recursos limitados	La policía no existe o es corrupta (trabaja con DC)
Situación general de seguridad	No se aplica la ley, pero la situación es relativamente segura	No es una situación segura	Impunidad absoluta, no se respetan los derechos

Ejemplo

de una valoración de la probabilidad de una agresión por delincuencia común:

En esta ciudad, los delinuentes comunes suelen operar en diferentes zonas, en parejas o grupos pequeños, a veces de día. A menudo son violentos y usan armas de fuego. La policía reacciona despacio y de forma ineficaz: los oficiales no son buenos profesionales y no disponen de los recursos necesarios; los altos cargos de la policía, sin embargo, son disciplinados. A todas luces, la situación no es segura, y si se aplica a los barrios marginales de la ciudad, la probabilidad de agresión por delincuencia común es máxima, pues todos los indicadores están en el máximo nivel.

La probabilidad de agresión por delincuencia común en el centro de una ciudad así es de alta a media.

Tabla 3: Cómo establecer la probabilidad de agresiones incidentales

(**AP** significa Agresor Potencial)

Probabilidad de agresiones incidentales			
Factores	Probabilidad baja	Probabilidad mediana	Probabilidad alta
Nuestro conocimiento de las zonas de conflicto	Bueno	General	Escaso - sabemos muy poco de dónde están las zonas de combate
Distancia de las zonas de conflicto	Trabajamos lejos de estas zonas	Trabajamos cerca de estas zonas y a veces tenemos que entrar en ellas	Trabajamos en la(s) zona(s) de conflicto(s)
Naturaleza de las zonas de conflicto	Son estáticas o cambian despacio, los cambios son verificables	Cambian con relativa frecuencia	Cambian continuamente, de manera impredecible
Nuestro conocimiento de dónde están las zonas con minas	Bueno, o no hay zonas con minas	General	No sabemos nada
Distancia entre nuestro lugar de trabajo y las zonas minadas	Trabajamos lejos de estas zonas, o no hay zonas minadas	Trabajamos cerca de estas zonas	Donde trabajamos hay zonas con minas
Armas de combate y tácticas bélicas	Uso discriminado - no se ataca a la población civil	Uso discriminado, con uso ocasional de artillería, emboscadas y francotiradores	Indiscriminadas: bombardeos, artillería pesada, ataques terroristas o con bombas

Ejemplo

de una valoración de la probabilidad de agresiones incidentales:

En esta zona, conocemos bien dónde se producen los combates, y sabemos que cambian poco y que podemos comprobar qué cambios se han producido. Trabajamos cerca de las zonas de combate, y en ocasiones tenemos que pasar por o quedarnos en ellas. No hay zonas minadas cerca de aquí. Las tácticas de combate no son indiscriminadas, y por tanto no suelen afectar a la población civil.

El trabajo en esta zona conlleva un nivel de riesgo de agresión incidental bajo.

Cómo evitar las posibles agresiones directas/indirectas

Aunque las y los defensores son el objetivo en ambos casos, vamos a distinguir entre:

- Agresión directa a un defensor o una defensora
- Agresión indirecta (ataques a personas próximas a defensoras/es)

En ambos casos, las medidas de prevención seguirán la misma lógica.

Hemos mencionado que el riesgo de amenaza puede reducirse cuando se dan ciertos cambios en la capacidad del agresor potencial para llevar a cabo la agresión, en su actitud respecto a cómo de conveniente es llevar a cabo una agresión, o cómo de probable es que le capturen por cometerla.

Para evitar una agresión es, por tanto, necesario:

- Persuadir al agresor potencial o persona que amenaza de que una agresión traerá consigo costes y consecuencias que le serán inaceptables.

- Hacer que las agresiones sean menos factibles.

Este tipo de prevención de agresiones es análogo al análisis presentado en el capítulo 1.2, donde explicábamos que el riesgo depende de la vulnerabilidad y las capacidades de las y los defensores. Para protegernos y reducir los riesgos que corremos como defensoras o defensores, tenemos que actuar ante las amenazas, reducir nuestros puntos vulnerables y reforzar nuestras capacidades.

Cuando nos amenazan y queremos reducir el riesgo que esto trae asociado, es importante que actuemos, pero no sólo respecto a la amenaza en sí; tenemos que actuar también respecto a la **vulnerabilidad y capacidades** que tengamos y que estén directamente relacionados con esa amenaza. En épocas de mucha presión, cuando hay que reaccionar lo más rápidamente posible, a menudo actuamos sobre los puntos vulnerables que más fácilmente podemos abordar, o que tenemos más a mano, en lugar de sobre aquellos que son más relevantes para el caso de amenazas que nos ocupa.

Atención: Si el riesgo de agresión es alto (esto es, si la amenaza es clara y palpable, y existen unos pocos puntos vulnerables y menos puntos fuertes o capacidades aún), tiene poco sentido empezar a intentar reducir los riesgos abordando problemas de vulnerabilidad o reforzando capacidades, porque eso lleva tiempo. Si el riesgo es muy alto (es inminente una agresión directa y grave) sólo podemos hacer tres cosas para evitarlo:

a Enfrentarnos a la amenaza de manera inmediata y con eficacia, sabiendo que podemos lograr un resultado concreto e inmediato que evitará la agresión. (Sin olvidar que normalmente es muy difícil saber a ciencia cierta que se va a lograr lo que se prende de manera inmediata, porque las reacciones llevan su tiempo; el tiempo es oro en esta situación).

b Pasar a la clandestinidad o abandonar la zona, reduciendo a cero nuestra exposición.[3]

[3] No obstante, habrá ocasiones en que viajar podría ser más peligroso aún.

c ◆ ¡Buscar una protección eficaz! Ver dos ejemplos de lo que podría ser eficaz (dependiendo del contexto):

• Protección de la comunidad: si nos escondemos o buscamos refugio en una comunidad, el ojo público y el hecho de que siempre haya testigos podrían tener el efecto de disuadir al agresor potencial de sus acciones.

• Protección de las armas: podría ser útil de alguna manera y en algún caso, suponiendo que el arma esté a mano, que pueda servir para disuadir al agresor potencial de su acción, y que no incremente el peligro que ya corre el defensor o la defensora ni a medio ni a largo plazo. Siendo realistas, los requisitos para usar las armas como protección ison muy difíciles de cumplir! Algunos gobiernos ofrecen guardaespaldas, o escolta armada, a las y los defensores, tras presiones nacionales o internacionales. En tales casos, que se acepte o rechace este servicio podría relacionarse con si pensamos que el Estado va a asumir de hecho la responsabilidad de velar por la seguridad de las y los defensores. En cualquier caso, si esta escolta es rechazada, el gobierno sigue siendo responsable de su seguridad. El servicio ofrecido por las compañías privadas de seguridad podría aumentar el peligro que se corre porque éstas pueden tener conexión con los agresores.[4] Que las y los defensores lleven armas normalmente no sirve de nada cuando se ha orquestado un ataque en su contra; es más, puede hacerles más vulnerables, porque un gobierno podría usarlo como pretexto para atacarles con la excusa de estar combatiendo el terrorismo o la insurgencia. Por último, que una persona dedicada a la defensa de los derechos humanos lleve armas contraviene la "Declaración sobre defensores y defensoras de derechos humanos de la ONU".

Cuando nos enfrentamos a una situación de amenazas que podría consumarse, es más fácil manejarla bien si se involucra a otros actores o partes implicadas que tengan un papel en esa situación y se trabaja conjuntamente. Por ejemplo, se podría involucrar al sistema judicial siempre y cuando éste funcione bien, así como a redes de apoyo (nacionales e internacionales) que puedan presionar políticamente a los actores responsables de la seguridad de las personas, a redes de activistas sociales (en el propio grupo y entre organizaciones), a redes de familiares y amistades, al personal internacional o de la ONU para el mantenimiento de la paz, etc.

Vigilancia y contravigilancia

Para saber si nos están vigilando debemos organizar tareas de **contravigilancia**. Es difícil saber si nos están interceptando nuestras comunicaciones, y por esta razón siempre debemos partir de la base de que así es.[5] No obstante, es posible determinar si vigilan nuestros movimientos u oficinas.

[4] Para más información puede consultarse el capítulo "Cómo mejorar nuestra seguridad en el trabajo y en casa".

[5] Para más información ver el capítulo de este manual sobre seguridad y comunicaciones.

¿Quién podría estar vigilándonos?

La gente del barrio, como porteras y porteros, las y los vendedores ambulantes, gente que espera en vehículos, gente que nos visita, etc. nos vigila o bien por dinero, porque les están presionando para hacerlo (por miedo), porque lo ven necesario o lo apoyan (por ideología), o por una combinación de estos factores. Quienes ordenan que nos vigilen pueden también recurrir a enviar colaboradores o miembros de su organización a las zonas donde estemos.

También podrían estar siguiéndonos a distancia. En este caso, lo harán normalmente miembros de una institución o grupo organizado y usarán la táctica de seguirnos intentando que no nos demos cuenta. Por eso mantienen una distancia prudencial, se turnan, y van cambiando de ubicación, de vehículo, etc.

Cómo saber si nos están vigilando

Podemos saber si nos están vigilando observando a quienes nos observan y siguiendo las siguientes reglas (sin caer en la paranoia):

- Si tenemos motivos para pensar que alguien podría querer vigilarnos, tendremos que prestar atención a los movimientos de la gente del barrio o la zona, y a sus cambios de actitud; por ejemplo, si empiezan a preguntarnos por lo que hacemos. Debemos recordar que las tareas de vigilancia las pueden hacer mujeres, hombres, jóvenes y viejos.

- Si sospechamos que nos están siguiendo, es posible tomar medidas de contravigilancia implicando a una tercera parte en la que confiemos y que no conozcan quienes nos vigilan. Esta tercera parte puede observar a distancia los movimientos que se produzcan cuando llegamos, nos marchamos o vamos a algún sitio. Quien nos esté vigilando probablemente lo hará desde un lugar donde se nos pueda ver fácilmente, cerca de la casa, de la oficina y en los lugares donde solemos ir a trabajar.

Por ejemplo:

Antes de volver a casa, podríamos pedirle a un familiar o a una vecina de confianza que se coloque en determinado lugar (p.e. que se ponga a cambiar una rueda del coche) para comprobar si alguien nos está esperando. Podemos hacer lo mismo para cuando salgamos de la oficina a pie. Si tenemos que usar un vehículo privado, le pediremos que espere un poco antes de seguirnos en su coche, para que quien nos esté vigilando pueda empezar a seguirnos.

El beneficio de la contravigilancia es que, al menos inicialmente, la persona que te observa no se da cuenta de que sabemos que están ahí. Así, deberíamos dejarle claro a quien esté haciendo la contravigilancia que, en principio, no es aconsejable abordar la persona que nos observa. Se darían cuenta de que sabemos lo que están haciendo y esto podría desencadenar una reacción violenta. Es importante tener el máximo cuidado y mantenerse a distancia si nos damos cuenta de que alguien nos está vigilando. Cuando sepamos a ciencia cierta que nos están siguiendo, podemos proceder a seguir los pasos que sugerimos en este manual.[6]

[6] Ver el capítulo titulado "Cómo mejorar la seguridad en casa y en el trabajo".

La mayor parte de nuestros consejos sobre contravigilancia son sólo aplicables a las zonas urbanas y semiurbanas, pues en las zonas rurales la situación es muy diferente: las y los defensores y quienes allí viven están mucho más acostumbrados a fijarse en la presencia de extraños. Por eso es mucho más difícil para quien nos quiere vigilar conseguir instrumentalizar a quienes viven en las zonas rurales, a no ser que la población esté en contra de nuestro trabajo.

Nota: desarrollar algún contacto con las fuerzas de seguridad que supervisan nuestro trabajo podría ser muy positivo en ciertas circunstancias. En ocasiones, quienes nos están siguiendo desean que nos demos cuenta, porque lo que quieren es justamente que nos demos cuenta de que nos siguen para así intimidarnos. En algunas situaciones las y los defensores cuidan su relación con un contacto en las fuerzas de seguridad que pueda avisarles de que se les va a seguir o de que se planea un ataque en su contra.

Cuándo comprobar si nos están vigilando

La lógica nos dice que es sabio comprobar si nos están siguiendo cuando tenemos razones para creer que así es, por ejemplo, cuando hemos identificado varios incidentes de seguridad relacionados con el tema de que nos están siguiendo. Si nuestro trabajo de derechos humanos conlleva cierto riesgo, es buena idea hacer regularmente un ejercicio de contravigilancia, por si acaso.

No podemos olvidarnos del tema del riesgo en que podemos estar poniendo a otras personas si nos están vigilando. Por ejemplo, si hemos quedado con un testigo o con una familiar de una víctima, es posible que esa persona corra más peligro que nosotros. Tenemos que pensar siempre en sitios lo más seguros posibles para quienes quedan con nosotros. Asimismo, puede que sea necesario avisarles de antemano de que nos están siguiendo.

Cómo reaccionar a las agresiones

No podemos aplicar la misma fórmula en todos los casos de agresiones a las y los defensores. Como estos ataques son también incidentes de seguridad, en el capítulo 1.4 podemos encontrar información útil sobre cómo reaccionar en algunos de estos casos.

Frente a cualquier agresión, hay que recordar dos cuestiones fundamentales:

- ¡La seguridad es lo primero!, tanto durante como **después** del ataque. (Si estamos siendo objeto de un ataque y podemos elegir entre dos reacciones, ¡elijamos la que menos peligro entrañe!).

- Después de una agresión, es preciso recuperarse física y psicológicamente, tomar medidas para resolver la situación, y restaurar un entorno seguro en el trabajo tanto para quien ha sufrido el ataque como para la organización. Es crucial recopilar el máximo de información sobre la agresión: lo que ocurrió, quién y cuántas personas se vieron implicadas, las matrículas de coche, descripciones varias, etc. Esto podrá usarse para documentar el caso, y debería tenerse listo cuando antes. Hay que guardar siempre una copia de cualquier información sobre el caso que se le entregue a las autoridades.

Resumen

Una agresión es la culminación de un proceso que incluye incidentes de seguridad y quizá amenazas.

Así pues, una agresión no es un acontecimiento "inesperado".

Las agresiones pueden ser incidentales o intencionadas y con un objetivo concreto.

No es fácil atacar físicamente a las y los defensores de derechos humanos porque son figuras públicas que disfrutan de sus apoyos.

Una agresión es el resultado de tres factores que interactúan:

- La parte que ejecuta la acción violenta y recursos
- Las situaciones pasadas y presentes que llevan al agresor a ver la violencia como una opción deseable
- Un entorno que la facilita

Orquestar una agresión requiere unas condiciones y una preparación previa: disponerse de ciertos recursos y capacidades, tener acceso al individuo, poder escapar rápidamente y disfrutar de cierto nivel de impunidad, o haber tomado la decisión de que este acto compensa el coste político.

Así pues, para intentar evitar que nos ataquen, es preciso hacer que el coste político sea tan alto como nos sea posible conseguir (o reducir el nivel de impunidad al máximo) y también reducir al máximo nuestra exposición física al peligro, intentando incluso no correr ningún riesgo.

CAPÍTULO 1.6

cómo Diseñar una estrategia global de seguridad

Objetivo:

Identificar las tácticas y estrategias existentes

Analizarlas

Definir una estrategia global que cubra el espacio de trabajo

Tácticas y estrategia de disuasión ad hoc

Las y los defensores de derechos humanos y los grupos que reciben amenazas utilizan diferentes estrategias de disuasión ad hoc para lidiar con los riesgos que detectan. Estas estrategias varían mucho dependiendo del contexto (rural, urbano), del tipo de amenaza, de los recursos sociales, económicos y legales disponibles, etc.

La mayor parte de las estrategias empleadas son de aplicación inmediata y para objetivos a corto plazo, lo que significa que funcionan más como tácticas que como estrategias de respuesta global. Además, responden a las percepciones de amenaza de personas concretas, es decir, son subjetivas y podrían llegar a causar algún tipo de daño al grupo, en especial si no se pueden rectificar.

Las estrategias ad hoc están estrechamente relacionadas con el tipo de amenaza y los daños que ésta puede causar, y también con la vulnerabilidad y la capacidad del grupo.

Cuando reflexionemos sobre seguridad y protección tendremos que tener en cuenta nuestras propias estrategias ad hoc y también las de otras personas. Hay que reforzar las que son eficaces, intentar limitar el impacto de las que hacen daño e intentar respetar las restantes (en especial, las vinculadas a creencias culturales o religiosas).

Algunas estrategias ad hoc utilizadas por los defensores:

- Reforzar las barreras protectoras, ocultar los objetos de valor.
- Evitar comportamientos que pudieran ser malintrepretados por otros actores, en especial si el control del territorio donde trabajamos es objeto de disputas militares.

- Pasar a la clandestinidad cuando se produzcan situaciones de riesgo, usando lugares de difícil acceso, como la sierra o la selva, cambiando de residencia, etc. Unas veces pasarán a la clandestinidad familias completas y otras sólo las y los defensores. Esta acción podría realizarse de noche, o a lo largo de varias semanas, y puede implicar que no se pueda establecer contacto con el exterior.

- Buscar protección armada o política proveniente de uno de los actores armados.

- Suspender las actividades, cerrando la oficina y evacuando al personal. Migración forzosa (desplazamiento interno o como refugiadas y refugiados) o exilio.

- Confiar en la suerte, o recurrir a creencias espirituales.

- Encerrarse en sí misma o sí mismo, romper la comunicación con las y los compañeros; entrar en la fase de negación a la hora de tratar el tema de las amenazas; abuso del alcohol, trabajar compulsivamente, empezar a comportarse de manera imprevisible.

Las y los defensores utilizan también estrategias de respuesta: emitir informes para darle publicidad a un tema concreto, presentar alegaciones, organizar manifestaciones, etc. A menudo dichas estrategias sólo cubren las necesidades a corto plazo y en ocasiones pueden incluso provocar más problemas de seguridad que los que pretenden resolver.

Cómo analizar una estrategia de disuasión

Tanto si la estrategia empleada es global o ad hoc, habrá que considerar lo siguiente:

- **Capacidad de respuesta:** ¿pueden las estrategias que usamos responder con prontitud a las necesidades de seguridad de las personas o del grupo?

- **Versatilidad:** ¿se pueden adaptar nuestras estrategias a las nuevas circunstancias, una vez superado el riesgo de ser objeto de un ataque? Podemos tener varias opciones, por ejemplo, la de escondernos o mudarnos a otra casa temporalmente. Estrategias así pueden parecer poco sólidas, pero son muy versátiles, por lo que resisten bien a lo largo del tiempo.

- **Sostenibilidad:** ¿soportan nuestras estrategias la prueba del tiempo, a pesar de las amenazas o de ataques no letales?

- **Eficacia:** ¿protegen nuestras estrategias a las personas o grupos para las que han sido diseñadas?

- **Capacidad de rectificación:** si las estrategias no funcionan o la situación cambia, ¿podemos rectificar o adoptar otras medidas?

Cómo lidiar con los riesgos después de haberlos valorado

Tenemos que considerar los resultados de nuestra valoración de los riesgos. Como es imposible medir la "cantidad" de riesgo a la que nos enfrentamos, tenemos que acordar cómo vamos a medir el **nivel** del riesgo.

Tanto individual como colectivamente podríamos no coincidir a la hora de identificar ese nivel, porque lo que para unas personas es inaceptable, para otras no lo es, incluso dentro de una misma organización. Por lo tanto, en lugar de discutir sobre posibles reglas o actuaciones, es mejor averiguar cuál es la medición del riesgo que hace cada cual, para así acordar cómo vamos a medir el nivel de riesgo como grupo.

Dicho esto, podemos lidiar con el tema del riesgo de diferentes maneras:

- **Aceptar** la situación porque somos capaces de convivir con ese nivel de riesgo.
- **Reducir** el nivel, para lo que trabajaremos el tema de las amenazas, de nuestra vulnerabilidad y capacidad.
- **Compartir** el problema, emprendiendo acciones conjuntas (con otras organizaciones de defensoras o defensores).
- **Posponer** el problema, pasando a desarrollar otra actividad o enfoque que reduzca las amenazas potenciales.
- **Escapar** del riesgo, reduciendo o deteniendo nuestras actividades (podría implicar el exilio).
- **Ignorar** el riesgo, haciendo oídos sordos. Evidentemente, ésta no es la mejor opción.

No olvidemos que el nivel de riesgo es normalmente diferente para cada una de las organizaciones y personas que trabajan en un caso de derechos humanos, y que quienes desean atacarnos suelen elegir nuestro punto más débil.

Por ejemplo:

Consideremos el caso de un campesino asesinado por el ejército privado de un terrateniente. Es posible que existan varias organizaciones e individuos involucrados en el caso, tales como un grupo de abogados de una ciudad cercana, un comité de campesinos y tres testigos (campesinos de un pueblo cercano). Es crucial valorar el nivel de riesgo que corre cada uno de los actores para poder diseñar bien qué medidas de seguridad hay que adoptar para proteger a cada cual.

Resumen

En temas de seguridad, las organizaciones de defensa de los derechos humanos no parten nunca de cero. Todas han diseñado formas de actuar frente a los riesgos y las amenazas. Lo contrario podría indicar que han desaparecido y/o que han abandonado su trabajo.

Todas y todos los defensores utilizan algún tipo de estrategias o tácticas de disuasión ad hoc y algunos pueden incluso haber diseñado una estrategia de disuasión global.

Sean las que sean esas estrategias, deben responder a los siguientes puntos: capacidad (de respuesta), versatilidad, sostenibilidad, eficacia y posibilidad de ser rectificadas.

Es preciso hacer una valoración del tema de los riesgos para poder establecer si el nivel al que nos enfrentamos es "aceptable". Si no lo es, tendremos que hacer algo para reducir ese riesgo, compartirlo, posponerlo, o escapar de él.

Las defensoras y los defensores de derechos humanos que trabajan en lugares hostiles

Demasiado a menudo, las y los defensores trabajan en lugares hostiles. Existen muchas razones que lo explican, y la mayoría se relacionan con el hecho de que su trabajo implica enfrentarse a actores con mucho poder que están violando el derecho internacional de los derechos humanos (ya sean representantes del gobierno o del Estado, fuerzas de seguridad, grupos de la oposición armada o ejércitos privados). Estos actores podrían reaccionar intentando impedir que se desarrolle este trabajo, y para ello podrían hacer uso de cualquier medio, desde reprimir sutilmente los intentos de ejercer la libertad de expresión, a amenazar o atacar abiertamente. El nivel de tolerancia que muestre tener cada uno de los actores está relacionado con el trabajo de las defensoras y los defensores: a veces considerarán que es aceptable y otras que no; generar incertidumbre es a menudo un objetivo deliberado.

Es preciso hacer dos consideraciones importantes aquí: en muchos casos, sólo ciertos individuos del grupo de los actores complejos (como los mencionados antes) son hostiles a las y los defensores. Por ejemplo, unos miembros del gobierno pueden tener la intención más o menos seria de proteger a las y los defensores, mientras que otros desearán atacarles. Las reacciones hostiles pueden aumentar en tiempos de agitación política, durante elecciones u otros acontecimientos políticos.

El espacio sociopolítico de las defensoras y defensores de derechos humanos

Este manual está centrado en el tema de protección y seguridad para defensores de derechos humanos que trabajan en entornos hostiles. Indudablemente, podremos emprender acciones al nivel sociopolítico: las campañas que desarrollamos se encuentran a menudo destinadas a ampliar el respeto a los derechos humanos en determinada sociedad, o a que las acciones políticas puedan tener mayor peso. No se suele relacionar estas actividades con el tema de la seguridad pero cuando salen bien, suelen tener un impacto muy positivo en la protección de nuestro **espacio sociopolítico**.

El espacio de trabajo sociopolítico podría definirse como la **variedad de actuaciones posibles que una defensora o un defensor puede realizar corriendo un riesgo personal aceptable.** En otras palabras, esta persona observa "una amplia gama de actuaciones políticas posibles y asocia a cada una de ellas un cierto coste o conjunto de consecuencias" para luego decidir cuáles de esas consecuencias son aceptables y cuáles son inaceptables, "definiendo así un espacio político claramente delimitado".[1]

Por ejemplo:

> *Pongamos que un grupo de defensores está trabajando en un caso y de pronto una persona del equipo recibe una amenaza. Si el grupo considera que tienen suficiente espacio sociopolítico para continuar con sus actividades, podrían decidir hacer público que han recibido amenazas y seguir trabajando en el caso. Sin embargo, si ven que su espacio político es limitado, hacer públicas las amenazas podría tener un coste inaceptable, por lo que es posible que cierren el caso por el momento y se centren en mejorar su seguridad.*

La noción de riesgo "inaceptable" puede ir cambiando a lo largo del tiempo y varía mucho de persona a persona, o de organización a organización. Para algunas personas, la tortura y la muerte de un familiar constituyen el riesgo más difícil de asumir. Hay defensoras y defensores que creen que la cárcel es un riesgo aceptable si esto les permite conseguir sus objetivos y saben que no se les va a torturar mientras estén allí. Otras personas consideran que la frontera está cuando reciben amenazas.

Este espacio político para la acción, además de estar definido subjetivamente por quienes se mueven en él, es muy sensible a los cambios que se puedan producir en el contexto político nacional, de ahí que tengamos que contemplarlo como un espacio relativo y susceptible de cambio.

La seguridad y el espacio de trabajo de las y los defensores de derechos humanos

Todas las estrategias de seguridad pueden resumirse en unas pocas palabras: deseamos ampliar nuestro espacio de trabajo y mantenerlo así. Hablando estric-

[1] Esta definición y otras partes clave de este concepto se han tomado de Mahony y Eguren (1997), p. 93, quienes también han desarrollado un modelo de espacio político que integra el espacio de trabajo de las y los defensores con las medidas de protección del acompañamiento.

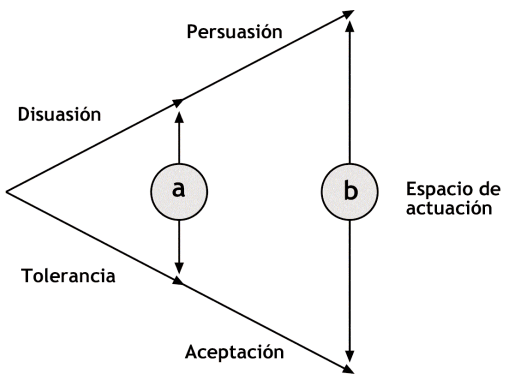
tamente en términos de seguridad, es necesario que nuestro espacio de trabajo sea, al menos, mínimamente tolerado por los principales actores de la zona, en especial por las autoridades políticas y militares y los grupos armados que pudieran verse afectados y decidir, por tanto, actuar en contra nuestra.

Este consentimiento a nuestro trabajo podría ser **explícito**, como cuando las autoridades emiten un permiso, o **implícito**, para el caso de los grupos armados. Será más sólido si el actor ve que puede sacar algún beneficio de nuestra labor, y más frágil si percibe un coste asociado. Para este último caso, su nivel de consentimiento dependerá del coste político que pueda el tener atacarnos. Estos temas son especialmente relevantes en conflictos armados donde las y los defensores nos enfrentamos a más de un actor armado. Determinado actor armado podría considerar que nuestro trabajo está beneficiándole a uno de sus oponentes. Esto significa que la aceptación abierta por parte de un actor del trabajo de las y los defensores podría conducir a que su oponente nos sea hostil.

Nuestro espacio de trabajo puede representarse con dos ejes:

- Uno que representa el nivel de aceptación o tolerancia del trabajo que hacemos por parte de un actor, nivel que dependerá de cómo repercuta este trabajo en los objetivos o intereses estratégicos de dicho actor (el continuo tolerancia-aceptación).

- Otro que representa el grado en que podemos disuadir un ataque, por el alto coste político que tendría hacerlo, pasando por porque nuestra argumentación o presión moral resulta convincente, hasta incluso porque les



convencemos de que existen beneficios políticos en no atacarnos o en dejar de violar los derechos humanos (el continuo disuasión-persuasión).

Podemos ampliar nuestro espacio de trabajo a lo largo del tiempo. Una estrategia de persuasión para conseguir que se acepte el trabajo de defensa de derechos humanos debe tener en cuenta las necesidades de la población, la imagen de las y los defensores, los procedimientos, la integración, etc., todo lo que representa el espacio "b". En zonas de conflicto armado, sin embargo, el espacio disponible suele quedar reducido a lo que consienten los grupos armados, quienes pueden tener en cuenta los costes que de atacarnos (disuasión); es el espacio "a".

En general, en el espacio "b" no se ubican las y los defensores que realizan un trabajo más abiertamente de denuncia, a no ser que hayan conseguido convertir moralmente al agresor potencial, llevándole a aceptarlo por haberle convencido del bien que encierra ese trabajo de derechos humanos.

Estrategia global de seguridad

- Expandir nuestro espacio de trabajo aumentando la tolerancia y la aceptación.
- Expandir nuestro espacio de trabajo aumentando la disuasión y la persuasión.

Definir y llevar a cabo una estrategia global de seguridad ayudará a elevar el precio político de las actuaciones contra las y los defensores porque se estará reduciendo el nivel de impunidad del agresor potencial y ampliando nuestro espacio de trabajo. Como vemos, una estrategia global de seguridad se basa mucho en la defensa.

Cómo ampliar nuestro espacio de trabajo aumentando la tolerancia y la aceptación

Puede que nuestro trabajo esté afectando a los objetivos o intereses estratégicos de alguien a quien no le preocupa mucho el respeto a los derechos humanos, lo que nos sitúa en un entorno de trabajo hostil. Para lograr que se acepte o, siquiera, que se consienta nuestro trabajo es importante limitar el desacuerdo al estricto mínimo. Para ello, podríamos hacer lo siguiente:

- **Proporcionar información y formación sobre la naturaleza y legitimidad del trabajo que realizamos como defensoras/es.** Las y los representantes del gobierno y demás actores podrían sentir más inclinación a cooperar si saben y entienden cuál es nuestro trabajo y por qué lo realizamos. No basta con que los altos cargos de la Administración tengan noticia de lo que hacemos, porque nuestro trabajo diario normalmente afecta a personal funcionario de diferentes niveles de la Administración (u organismos gubernamentales). Por lo tanto, es fundamental mantener siempre formado e informado al funcionariado de todos los niveles.

- **Dejar muy claros nuestros objetivos.** En todos los conflictos es útil aclarar y limitar el alcance y objetivos de nuestro trabajo. Esto reducirá la posibilidad a que se produzcan malentendidos o enfrentamientos innecesarios que podrían impedir que logremos nuestros objetivos como defensoras/es.

- **Proponernos objetivos que puedan encajar en el espacio sociopolítico que tenemos para nuestro trabajo.** Cuando nuestro trabajo afecta intereses estratégicos específicos de un actor armado, éste podría reaccionar violentamente y con poca preocupación por su imagen. Unos tipos de trabajo hacen más vulnerables a unas o unos defensores que a otros, así que tenemos que asegurarnos de que nuestros objetivos son compatibles con la situación de riesgo a que nos enfrentamos y con nuestra capacidad de protegernos.

- **Dejar siempre la posibilidad de una salida digna a nuestros oponentes.** Si tenemos que enfrentarnos a un actor que no está respetando los derechos humanos, nuestra estrategia global de seguridad debe prever que a éste se le pueda reconocer su parte en la resolución del caso.

- **Establecer alianzas con tantos sectores como nos sea posible.**

- **Hallar un equilibrio** entre la transparencia de nuestro trabajo, para mostrar que no tenemos nada que ocultar, y la necesidad de evitar exponer información que pudiera poner en peligro nuestro trabajo o nuestra seguridad, o la de quienes defendemos.

- **Por último,** recordar que la legitimidad y la calidad de nuestro trabajo son condiciones necesarias para mantener abierto nuestro espacio de trabajo, pero que eso podría no ser suficiente. Quizá también tengamos que emplear la disuasión para evitar posibles agresiones (ver abajo).

Cómo ampliar nuestro espacio de trabajo: aumentando la disuasión y la persuasión

Como defensores y defensoras de derechos humanos que trabajan en entornos hostiles debemos de tener la capacidad de generar suficientes costes políticos como para que a un agresor potencial desista de atacarnos: ésta es la idea de la **disuasión.**

Es útil distinguir entre disuasión general y disuasión inmediata. La disuasión general se refiere al efecto de todos los intentos nacionales e internacionales combinados por proteger a las y los defensores, como por ejemplo, cualquier acción que contribuya a que se comprenda que si se les ataca las consecuencias serán negativas. Esto puede hacerse con campañas de información que aborden temas generales, o informando y ofreciendo formación sobre el tema de la protección a las y los defensores. Por otro lado, **la disuasión inmediata** envía un mensaje concreto a un agresor determinado para evitar que ataque a un objetivo específico. La disuasión inmediata es necesaria cuando fracasa la general o cuando se ve que ésta no ha sido suficiente, así como cuando el trabajo de protección se centra en casos específicos.

La persuasión es un concepto más inclusivo. Puede definirse como el resultado de actuaciones que inducen a un oponente a no llevar a cabo una acción hostil que hubiera pensado. Argumentar racionalmente, hacer un llamamiento moral, aumentar la cooperación, mejorar la comprensión humana, distraer, adoptar una política no ofensiva y disuadir pueden usarse en la persuasión. Empleamos cada una de estas tácticas a nivel nacional e internacional en diferentes momentos. Como defensores, no podemos utilizar las "amenazas" directas muy a menudo: la estrategia trata más bien de recordarle a otros que, según la decisión que adopten, se **podría** desencadenar una serie de consecuencias.

Cómo usar la disuasión

Para medir si nos ha funcionado la disuasión, necesitamos que se den una serie de condiciones:

1 ◆ **Las y los defensores tenemos que comunicarle al agresor de manera muy concreta y clara el tipo de actuaciones que nos parecen inaceptables.** La disuasión no funcionará si el agresor no sabe qué acciones provocan una reacción.

2 ◆ **La organización de defensa de los derechos humanos tiene que hacerle saber al agresor de su determinación a disuadirle de sus actos.** Asimismo, debe contar con una estrategia de disuasión lista para ser aplicada.

3 ◆ **La organización de defensa de los derechos humanos tiene que ser capaz de llevar a cabo su estrategia de disuasión y de convencer al agresor de que es capaz de hacer lo que dice que va a hacer.** Si la amenaza de movilizar una reacción nacional o internacional no es creíble, no podemos pensar que va a tener el efecto deseado.

4 ◆ **Las y los defensores tenemos que saber quién es el agresor.** Los escuadrones de ataque a menudo trabajan de noche y rara vez se atribuyen los ataques. Así pues, para averiguar quién lo es, habrá que plantearse a quién beneficia ese ataque. Para que la reacción nacional o internacional sea buena, no basta con que presupongamos "la responsabilidad del Estado", aunque el Estado sea el responsable; hay que ofrecer información más específica, como qué parte del aparato del Estado se encuentra detrás.

5 ◆ **El agresor tiene que haber considerado seriamente atacarnos y después tiene que haber decidido no hacerlo** porque los costes (debido a nuestro trabajo de disuasión) serían mayores que los beneficios.

Es difícil que disuadamos a un agresor de algo si éste no es sensible a lo que decimos: este caso se da cuando los gobiernos pueden ser castigados por la comunidad internacional pero ellos, a su vez, no pueden castigar al que de hecho ha violado los derechos humanos; así ocurre con los ejércitos privados, que suelen estar lejos del control del gobierno, o que no comparten intereses con él. En esos casos, el agresor puede incluso beneficiarse por atacarnos porque esos ataques pondrían al gobierno en una posición difícil y dañarían su imagen.

Como defensores y defensoras no podemos saber de antemano si nuestra "determinación disuasoria" es lo bastante poderosa como para evitar un posible ataque. El agresor podría haber calculado tener unos beneficios en los que no hemos pensado. Valorar la situación lo más cuidadosamente que podamos es un desafío permanente y podría incluso ser imposible debido a la falta de información relevante. Así pues, nuestras organizaciones tienen que haber desarrollado planes alternativos extremadamente flexibles, además de la habilidad de responder rápidamente a acontecimientos inesperados.

Tabla 1: Cómo evitar una agresión directa - diferentes desenlaces de la protección

CÓMO EVITAR UNA AGRESIÓN DIRECTA: DIFFERENTES DESENLACES DE LA PROTECCIÓN	
1 **Generar cambios en el comportamiento del perpetrador:** los agresores desisten de atacar porque han aumentado los costes potenciales de la agresión. → 2 **Generar cambios en la relación de las partes responsables respecto a su cumplimiento con la Declaración sobre defensores de ddhh de la ONU:** los agresores desisten de atacar porque aumenta la probabilidad de que esas partes responsables actúen para proteger a las y los defensores o para castigarles. [2] →	**Enfrentar** y **reducir las amenazas** (actuando directamente contra la fuente, o contra cualquier actuación de la fuente)
3 **Reducir la viabilidad de la agresión:** Reducir la exposición de las y los defensores, mejorar nuestro entorno de trabajo, lidiar bien con el miedo y la ansiedad, desarrollar planes de seguridad, etc. →	Reducir la **vulnerabilidad**, fortalecer **la capacidad (**de respuesta)

[2] Ver capítulo 1.1. Por ejemplo, cuando un defensor denuncia amenazas, el fiscal, la policía o algún otro organismo investiga lo ocurrido y esta investigación lleva a actuaciones contra quienes están amenazando al defensor. Pues bien, al menos esto podría ser el objetivo de una reacción para evitar una agresión.

CAPÍTULO 1.7

cómo Preparar un plan de seguridad

Objetivo:

Aprender a diseñar un plan de seguridad

Primeros pasos para preparar un plan de seguridad

Ahora que disponemos de un esquema de los actores o partes implicadas en el tema de protección, que hemos determinado cuáles son las fuerzas de campo, valorado nuestros riesgos, comprobado que nuestras estrategias están a punto, y establecido nuestra estrategia global de seguridad, no debería sernos difícil preparar nuestro plan de seguridad.

La seguridad es un tema complejo en el que entran en juego diversos factores. Unos tienen que estar presentes siempre; otros, cuando se necesiten. Juntos, constituyen el plan de seguridad, un plan que tendrán que llevarse a cabo a nivel individual, en toda la organización y en colaboración con otras organizaciones.

¿Cómo proceder? Resumamos el proceso en unos cuantos pasos:

1 ◆ **Componentes del plan.** Un plan de seguridad tiene el objetivo de reducir los riesgos. Así pues, partiendo de nuestra valoración de los riesgos, estableceremos al menos tres objetivos:

- Reducir el nivel de amenazas que estamos experimentando.
- Reducir nuestros puntos débiles o vulnerabilidad.
- Mejorar nuestra capacidad.

Un plan de seguridad debe incluir políticas y medidas que se aplican cada día y protocolos para situaciones específicas.

Políticas y medidas del día a día:

- Política de defensa permanente, redes de contactos, código ético, cultura de seguridad, gestión de la seguridad, etc.
- Medidas permanentes para comprobar que el trabajo diario respeta los principios de seguridad.

Protocolos para situaciones específicas:

- Protocolos de prevención: por ejemplo, sobre cómo preparar una conferencia de prensa, o una visita a una zona remota.
- Protocolos de emergencia para reaccionar a problemas concretos, tales como una detención o una desaparición.

Cuantas más políticas y medidas se utilicen cotidianamente, mejor funcionarán los protocolos diseñados para las situaciones concretas.

Unos ejemplos:

- Si empleamos una serie de políticas y medidas permanentes en la gestión de la información y la oficina sufre un ataque (emergencia), los efectos serán menos graves que si no lo hubiéramos hecho;

- Si desarrollamos unas políticas y medidas permanentes con nuestra red de contactos, cuando una defensora o un defensor sea atacado y activemos la red de inmediato, la probabilidad de que las partes interesadas clave reaccionen será mayor, consiguiéndose así el objetivo de protegernos si nos atacan.

  Para conseguir esto último, el plan de seguridad debe incluir la defensa permanente ante las partes interesadas responsables y las partes interesadas clave. Precisará de una política permanente de comportamiento ético que opere en todos los aspectos del trabajo de la organización, y también a nivel individual/ de organización/ entre organizaciones.

- Ante una detención, si hemos estado siguiendo un plan permanente que incluía una política sobre comportamiento ético de cada persona del equipo, sabremos que no se habrán producido infracciones personales, y podremos activar el protocolo de emergencia. Sin duda alguna, las infracciones podrían estar usándose como pretexto, pero el abogado o la abogada de la organización sabrá lo que se debe hacer. Además, la defensora o el defensor detenido sabrá que la organización estará dando determinados pasos, que podrá repasar mentalmente y así "relajarse" (impacto psicológico) porque sabe que fuera se está haciendo algo. No hay que desafiar a las autoridades y exponerse a más riesgos de los que ya se están corriendo si te han detenido.

- Para el caso de misiones de campo a zonas peligrosas, tendremos que haber informado previamente a las partes interesadas clave y estaremos alerta hasta que el equipo esté de vuelta y a salvo.

2 ◆ **Responsabilidades y recursos para materializar el plan.** Para asegurarnos de que el plan de seguridad es operativo, las rutinas de seguridad tienen que estar integradas en las actividades diarias:

- Incluir la valoración del contexto y los temas de seguridad en nuestras rutinas diarias.
- Registrar y analizar los incidentes de seguridad.
- Asignar las responsabilidades.
- Asignar recursos (tiempo y fondos) al tema de seguridad.

3 ◆ **Borrador del plan. ¿Cómo empezar?** Si hemos hecho la valoración de los riesgos para una defensora o defensor o una organización, tendremos una lista con numerosos puntos vulnerables, diferentes tipos de amenazas posibles y una serie de capacidades de respuesta nuestras. Si somos realistas, no vamos a poder cubrirlo todo, así pues, ¿dónde empezar? Es muy fácil:

- **Seleccionar una cuantas amenazas.** Para establecer la lista de prioridades con las amenazas (reales o potenciales) utilizaremos **uno** de estos criterios: la amenaza más grave (por ejemplo, claras amenazas de muerte); la amenaza más probable y grave (si organizaciones parecidas a la nuestra han recibido ataques, esto constituye una amenaza potencial muy clara contra nosotros); **o** bien la amenaza que se relacione más directamente con nuestros puntos vulnerables (porque corremos más riesgos en nuestros puntos débiles).
- **Hacer una lista con nuestros puntos débiles más importantes.** Tendríamos que abordar estas vulnerabilidades primero, recordando que no todos los puntos débiles se corresponden con toda amenaza (ver ejemplo abajo).
- **Hacer una lista con nuestras capacidades de respuesta más importantes.**

Ejemplo

de proceso de selección que lleva a preparar un plan de seguridad:

El líder de una organización de defensa de los derechos humanos (esté en una zona rural o urbana) ha recibido serias amenazas de muerte. La organización hace la valoración de los riesgos y elabora una lista con sus puntos débiles y sus capacidades de respuesta.

Al final, la organización decide utilizar las siguientes medidas de seguridad: poner cerrojos en todos los armarios, poner rejas en las ventanas de la oficina, comprar celulares nuevos para las y los miembros que estén más en peligro, y denunciar públicamente las amenazas de muerte.

En general, lo que tenemos que hacer es preguntarnos y demostrar cómo cada medida va a contribuir a reducir el riesgo concreto; en otras palabras, ¿cómo va a aumentar la seguridad cada una de las medidas respecto a ese riesgo concreto?

Para este caso, ¿cómo van a reducir cada una de estas medidas la amenaza de muerte que se le ha hecho al líder? (Más bien, parecen abordar la seguridad global de la organización, pero quizá no sea ahora el mejor momento para eso).

Hay que preguntarse: ¿Qué probabilidad hay de que la amenaza de muerte se consume en la oficina, cuando siempre hay gente en ella? Además, ¿es que al líder sólo se le puede asesinar en la oficina? No siempre estará allí. Por lo que hay que considerar otros puntos débiles, tales como cuando se sale de la oficina solo de noche, cuando se viaja a zonas aisladas, o se ignoran las medidas de seguridad en casa...

Aunque ponerle cerrojos a los armarios sea importante, esto no va a reducir la amenaza y los puntos débiles del líder. Lo mismo ocurre con las rejas de las ventanas. ¿De qué sirven frente un francotirador o frente una granada?

¿Cómo va a reducir ese riesgo un celular? (¿cómo puede evitar un celular que maten a un líder?).

Probablemente será mucho más útil reducir la exposición del líder en el trayecto de casa a la oficina, o los fines de semana. Éstos son los puntos vulnerables que hay que abordar prioritariamente para intentar evitar que se consume esa amenaza.

Si hacemos bien la selección del proceso y vemos que somos capaces de usar nuestro plan de seguridad con esas amenazas, puntos débiles y capacidades de respuesta que hayamos seleccionado, muy probablemente lograremos reducir los riesgos porque habremos partido de un lugar correcto.

Por favor, nótese que acabamos de describir una manera ad hoc para preparar un plan de seguridad. Hay maneras más "formales" de hacerlo. En cualquier caso, este método es muy directo y nos permite identificar los temas de seguridad más urgentes (siempre y cuando nuestra valoración de los riesgos haya sido la correcta) y diseñar un plan "realista" y "vivo", lo que es lo más importante para nuestra seguridad. (Ver al final de este capítulo la lista de posibles componentes en un plan de seguridad, lista que también podemos usar para valorar los riesgos).

Factores que podríamos incluir en un plan de seguridad

El siguiente "menú" nos ofrece una lista de factores que podríamos incluir en un plan de seguridad. Después de llevar a cabo una valoración de los riesgos, podemos elegir y mezclar todas esas ideas para completar nuestro plan de seguridad.

Un plan de seguridad incluye elementos que serán procedimientos políticos (como reunirse con las autoridades y representantes de los organismos internacionales para reclamar la protección que nos debe el Estado) y procedimientos operativos (tales como los preparativos de siempre antes de salir a una misión de campo).

Elementos de las políticas y medidas permanentes para el trabajo cotidiano:

- El mandato, la misión y los objetivos generales de la organización (conocerlos y respetarlos).
- Una declaración de la organización sobre política de seguridad.
- La seguridad en todos los aspectos de nuestro trabajo cotidiano: valoración del contexto, análisis de los riesgos y de los incidentes, y evaluación de la seguridad.
- Cómo asegurarnos de que todas y todos los miembros de la organización tienen una formación adecuada en temas de seguridad y de que cuando se produzcan relevos en el equipo las responsabilidades conectadas a los temas de seguridad serán asumidas por quienes permanezcan.

- Reparto de responsabilidades: ¿quién tiene que hacer qué en qué situación?

- Cómo manejar una crisis de seguridad: montar un grupo de trabajo o un comité de crisis, designar portavoz para tratar con los medios de comunicación para tratar con los medios de comunicación, comunicarse con las y los familiares, etc.

- Responsabilidades en temas de seguridad por parte de la organización: planes, seguimiento, seguros, responsabilidad civil, etc.

- Responsabilidades individuales en temas de seguridad: seguir reduciendo los riesgos, cómo manejar el tiempo libre o las actividades de ocio, informar de y registrar los incidentes de seguridad, sanciones (algunos de estos puntos podría estar incluidos en los contratos de trabajo, allí donde proceda).

- Políticas de la organización relativas a:
  - descanso, tiempo libre y control del estrés
  - seguridad de las victimas y los testigos
  - salud y prevención de accidentes
  - contactos con autoridades, fuerzas de seguridad y grupos armados
  - gestión y almacenamiento de la información, manejo de documentos e información confidencial
  - la propia imagen en relación con valores religiosos, sociales y culturales
  - gestión de la seguridad en oficinas y casas (incluido el tema de las visitas)
  - manejo del dinero y objetos de valor
  - medios usados para la comunicación y
  - mantenimiento de vehículos
  - seguridad de las defensoras
  - seguridad de los defensores LGBTI (lesbianas, gays, bisexuales, transgéneros, inter-sex)
  - ...

Elementos de medidas específicas para situaciones y tareas no ordinarias:

- Protocolos de prevención para:
  - preparación de viajes de campo
  - minas
  - reducción del riesgo de vernos implicadas o implicados en episodios por delincuencia común, incidentes armados o ataques sexuales
  - reducción del riesgo de accidentes a la hora de viajar o en zonas peligrosas
  - protocolos de respuesta en: emergencias médicas y psicológicas (también en campo)
  - daños personales como resultado de accidentes, ataques, agresiones sexuales
  - robo

- cuando no se sabe dónde está alguien que debería haber llegado a algún lugar
- detención o retención
- secuestro, desaparición
- incendios y demás accidentes
- evacuación
- desastres naturales
- búsquedas legales o ilegales, allanamiento de oficinas o de morada
- si una persona se ve envuelta en un tiroteo
- si matan a alguien
- si se produce un golpe de Estado
- ...

Cómo llevar a cabo el plan de seguridad

Tener un plan de seguridad es importante, pero estos planes no son fáciles de llevar a la práctica. Llevarlos a cabo conlleva algo más que un proceso técnico: implican al conjunto de la organización. Esto supone la necesidad de considerar los cuáles son los puntos de arranque para el plan (que de ahora en adelante llamaremos "puntos de entrada"), y las oportunidades, los problemas y los obstáculos.

Un plan de seguridad debe ejecutarse en al menos tres niveles:

1 ◆ Nivel **individual**. Cada persona debe seguir el plan para que éste funcione.

2 ◆ Nivel de **organización**. La organización en su conjunto tiene que respetar el plan.

3 ◆ Nivel **entre organizaciones**. La seguridad suele implicar algún nivel de cooperación entre diferentes organizaciones.

Ejemplos de puntos de entrada y oportunidades

a la hora de llevar a cabo un plan de seguridad:

- Han ocurrido varios incidentes de seguridad menores en nuestra organización o en otra, y algunas o algunos miembros del equipo están preocupados.
- Existe una preocupación general por la seguridad debido a la situación que se vive en el país.
- Llegan nuevos miembros del equipo y se les puede entrenar para que se acostumbren desde el principio a desarrollar las tareas de seguridad.
- Una organización nos ofrece un taller de formación en seguridad.

Ejemplos de **problemas** y **obstáculos**

a la hora de llevar a la práctica el plan de seguridad:

- Algunas personas piensan que añadir medidas de seguridad supondrá tener mucho más trabajo.
- Otras personas piensan que la organización ya tiene suficientes medidas de seguridad.
- "¡Ahora no podemos ocuparnos de esto, no hay tiempo!"
- "¡Vale, saquemos tiempo para discutir el tema de la seguridad este sábado, y con eso ya cerramos el tema!"
- "Tenemos que dedicarnos a proteger a la gente a la que intentamos ayudar, no a nosotras/os mismas/os."

Maneras de mejorar la puesta en práctica de un plan de seguridad

- **Aprovechar los puntos de entrada y las oportunidades** de que dispongamos para enfrentarnos a los problemas y superar los obstáculos.
- **Proceder paso a paso.** No tiene sentido pretender que todo puede hacerse de golpe.
- **Hacer hincapié en la importancia del tema de la seguridad en el trabajo que realizamos con las víctimas.** Insistir en que la seguridad de las y los testigos y miembros de las familias es crucial para ser eficaces; y en que esto se gestiona mejor integrando buenas prácticas de seguridad en todas las áreas de nuestro trabajo. Utilizar ejemplos en nuestras discusiones o cursos de formación que demuestren el impacto potencialmente negativo de medidas de seguridad laxas con las y los testigos y víctimas.
- Un plan diseñado por dos "expertos" y presentado a la organización en su conjunto fracasará porque en temas de seguridad **la participación es crucial**.
- **Un plan tiene que ser realista y factible.** No sirve tener una larga lista de cosas que hacer antes de un viaje de campo. Para cuidar la seguridad nos basta con un mínimo justo necesario. He aquí otra razón por la que es fundamental implicar a quienes hacen el trabajo, por ejemplo, a quienes hacen los viajes de campo.
- **El plan no es un documento que se hace de una sentada y no se vuelve a modificar:** debe ser revisado y actualizado continuamente.
- **El plan no debe verse como "más trabajo", sino como "una forma de mejorar nuestro trabajo".** La gente tiene que comprender sus beneficios, por ejemplo, asegurándonos de que no vamos a duplicar el trabajo de informar. Es preciso asegurarnos de que los informes de los viajes de campo se elaboran teniendo en cuenta el tema de la seguridad, de que los temas de seguridad son parte normal de las reuniones del equipo, de que los aspectos de la seguridad están integrados en cualquier tipo de formación, etc.

- **Hacer hincapié en que el tema de seguridad no se resuelve con iniciativas individuales.** Las decisiones, actitudes y comportamientos individuales que repercuten en el tema de la seguridad pueden afectar a las y los testigos, familiares de las víctimas o a nuestras compañeras y compañeros. Es fundamental que exista un compromiso de todos y todas con las prácticas establecidas para mejorar la seguridad.

- **Asignar el tiempo y los recursos necesarios** para llevar el plan a la práctica, pues el tema de la seguridad no puede mejorarse usando el tiempo libre del equipo. Para que se comprenda que es un tema "importante", tenemos que integrarlo en nuestra agenda junto a los otros temas "importantes".

- **Es importante que se vea a todo el mundo respetando el plan,** en especial a las y los directores o personas responsables del trabajo de otros. Debemos saber qué medidas tomar si existen individuos que se niegan a respetar el plan.

Resumen

Un plan de seguridad tiene que reducir el número de puntos vulnerables y que aumentar nuestra capacidad para que así las amenazas queden a su vez reducidas o sean menos factibles, y consecuentemente se reduzcan los riesgos.

Un plan de seguridad tiene que ajustarse bien a nuestras necesidades y espacio de trabajo.

No se trata de cubrir un gran espacio sociopolítico. Se trata más bien de ocupar el espacio adecuado y de cubrir el máximo posible del entorno de trabajo haciendo uso de nuestra red de contactos y en coordinación con otras organizaciones. Los procedimientos de seguridad que establezcamos deben trascender las posibles diferencias ideológicas entre las organizaciones.

El tema de seguridad es un tema que concierne a todo el mundo, a nivel individual, de organización y entre organizaciones.

El tema de la seguridad es complejo y resulta de varios factores. Unos deben estar siempre presentes, otros se añadirán en momentos concretos. Juntos constituirán el plan de seguridad.

Nuestro plan de seguridad debe incluir políticas y medidas en el día a día, y protocolos para situaciones concretas.

Ambos tendrán que incluir procedimientos políticos y procedimientos operativos.

CAPÍTULO 1.8

Cómo Mejorar la seguridad en el trabajo y en casa

Objetivo:

Hacer una valoración del tema de la seguridad en el trabajo y en casa

Planear, mejorar y comprobar todo lo relativo a la seguridad en el trabajo y en casa

La seguridad en el trabajo y en casa

La seguridad en la sede de una organización o en sus oficinas, así como en los domicilios de las y los miembros del equipo, es un tema fundamental del trabajo de las y los defensores. Así pues, trataremos en profundidad cómo se puede analizar y mejorar la seguridad de las oficinas o las casas. (Para simplificar, de ahora en adelante hablaremos solo de las oficinas, aunque todo lo explicado se puede aplicar también a la seguridad en las casas).

Aspectos generales de la seguridad en la oficina

Nuestro objetivo para mejorar la seguridad se puede resumir en la siguiente idea: **evitar el acceso no autorizado**, tanto en las zonas rurales como urbanas. En algunos casos, habrá que proteger la oficina también de posibles ataques (p.e. bombas).

Así, llegamos a nuestro primer tema general, los puntos vulnerables de la oficina, pues estos aumentan los riesgos de que se den diferentes tipos de amenazas, según los puntos vulnerables. Por ejemplo, si el riesgo que corremos es que puedan robarnos los equipos o una información, tendremos que abordar el tema de la vulnerabilidad desde ahí. Las alarmas nocturnas (eléctrica, si disponemos de electricidad, un vigilante o una perra guardiana) no sirven de nada si nadie las atiende. Por otro lado, cuando se producen robos con allanamiento de morada y uso de violencia durante el día, de poco sirven los cerrojos y las alarmas. En pocas palabras, las medidas que adoptemos tienen que estar en consonancia con las amenazas a que nos enfrentamos y el contexto en el que trabajamos.

Los puntos vulnerables de una oficina deben determinarse en función de las amenazas a que nos enfrentamos.

Es importante hallar un equilibrio entre preparar medidas de seguridad adecuadas y dar la impresión de que estamos "ocultando" o "protegiendo" algo, porque esto último podría ser muy peligroso. En temas de seguridad, a menudo nos vemos en la disyuntiva de tener que elegir entre no llamar la atención y llamarla porque es inevitable, porque necesitamos tomar esas medidas. En cualquier caso, un agresor potencial sabe que nuestra oficina contiene objetos de valor e información sensible y que "necesitamos" protegerla.

El nivel de seguridad de una oficina no es mayor que el nivel de seguridad de su punto más débil.

Si alguien quiere entrar sin que lo sepamos, no elegirá el punto de entrada más difícil. Recordemos que a veces la forma más fácil de entrar en una oficina para ver lo que pasa en ella es, sencillamente, llamando a la puerta.

El emplazamiento de la oficina

Tanto en el campo como en la ciudad, a la hora de elegir dónde ubicamos nuestra oficina consideraremos: el barrio; si se asocia el edificio a algún grupo de personas o a determinadas actividades del pasado; el transporte público y privado a la zona; el riesgo de accidentes; si las características del edificio nos van a permitir desarrollar nuestras medidas de seguridad, etc. (Ver también abajo Evaluación de riesgos del emplazamiento).

Es útil fijarse en qué medidas de seguridad ha adoptado las personas que viven en el barrio; si son muchas, eso podría indicar que la zona es peligrosa (por ejemplo, porque hay mucha delincuencia común). Asimismo, es importante hablar con estas personas de la seguridad en la zona. En cualquier caso, debemos intentar no llamar la atención con las medidas que adoptemos y ser conscientes de que tener relaciones en el barrio nos puede proporcionar información sobre posibles movimientos sospechosos en el barrio.

Otro factor a tener en cuenta es quién es el dueño o la dueña del edificio. ¿Qué reputación tienen? ¿Podrían ser objeto de presiones por parte de las autoridades? ¿Se sentirán cómodos con nuestras medidas de seguridad?

No podemos elegir una oficina sin tener en cuenta quién va a usarla. Una oficina a la que van víctimas buscando asesoramiento legal no va a necesitar lo mismo que una oficina para nuestro uso como miembros de una organización.

Es importante considerar el tema del acceso a la zona: si se puede llegar en transporte público, si los trayectos desde el domicilio de los miembros del equipo a la oficina son mínimamente seguros, o los que nos llevan a los lugares donde solemos desarrollar actividades, etc. Tenemos que analizar las proximidades, en especial para averiguar si son zonas peligrosas que nos conviene evitar. En algunos casos, la oficina será la propia casa de la defensora o el defensor (ver más adelante, zonas rurales). Aun así, lo anterior es aplicable.

Cuando hayamos elegido la ubicación de la oficina, es importante evaluar periódicamente cualquier cambio, como por ejemplo, si un "cualquier potencial agresor" se instala en el barrio.

ELEMENTOS A CONSIDERAR PARA ELEGIR UN BUEN EMPLAZAMIENTO PARA LA OFICINA EN ZONAS BIEN ABASTECIDAS:	
BARRIO:	Estadísticas del crimen; cercanía a objetivos potenciales de ataques armados, tales como instalaciones militares o edificios del gobierno; lugares seguros utilizables como refugio; otras organizaciones nacionales e internacionales con las que mantengamos contacto.
RELACIONES:	Tipo de gente en el barrio; dueños, anteriores inquilinos; anteriores usos del edificio.
ACCESO:	Una o varias buenas rutas de acceso (cuantas más, mejor, aunque es bueno recordar que el cualquier potencial agresor también tendría más donde elegir); acceso en transporte público y privado.
SERVICIOS BÁSICOS:	Agua y electricidad, teléfono.
ALUMBRADO PÚBLICO:	En la zona.
PROPENSIÓN A ACCIDENTES HUMANOS O NATURALES:	Incendios, inundaciones importantes, deslizamientos de terreno, vertido de materiales peligrosos, fábricas con procesos industriales perjudiciales para la salud, etc.
ESTRUCTURA:	Solidez de las estructuras, posibilidad de instalar nuestro equipo de seguridad, puertas y ventanas, vallas y rejas, puntos de acceso (ver abajo).
PARA LOS VEHÍCULOS:	Un garaje o al menos un patio o espacio cerrado con una barrera de paso.

Para el caso de que la oficina se encuentre en una zona remota, aislada y mal abastecida, habrá puntos de esta lista que no se puedan considerar. Tendremos que compensar estos puntos débiles desarrollando capacidades correspondientes. Por ejemplo, si no hay otras organizaciones en nuestra zona, podríamos plantearnos el recurrir a la comunidad del barrio; si no hubiera agua corriente o extintores, tendríamos que tener siempre lleno algún contenedor de agua.

Acceso no autorizado a la oficina: barreras físicas y cómo proceder con las visitas

Sabemos que el principal objetivo de la seguridad en la oficina es impedir el acceso no autorizado. Una o varias personas podrían entrar para robar, amenazarnos, conseguir información, dejar algo que después pudiera usarse en nuestra contra (como drogas o armas), etc. Todos los casos son diferentes pero nuestro propósito es el mismo: evitarlo.

El acceso al edificio se controla con **barreras físicas** (vallas, puertas, rejas), con **medidas técnicas** (como alarmas con luz) y con un **procedimiento de admisión** de las visitas. Cada barrera y cada procedimiento es un **filtro** por el que tiene que pasar quien desee entrar en la oficina. Lo ideal es que estos filtros se combinen para formar varias capas de protección, capaz de evitar distintos tipos de entradas no autorizadas.

Barreras físicas

Las barreras sirven para bloquear la entrada **físicamente** a las visitas no autorizadas. Su utilidad dependerá de su **solidez** y de su capacidad para cubrir todos **los huecos de entrada**.

Nuestra oficina puede tener barreras físicas en tres zonas:

1 ◆ El perímetro **exterior**: vallas, muros y similares, que acotan el jardín o el patio. Si no existen, tendremos que definir la extensión del perímetro exterior que queremos tener controlada.

2 ◆ El perímetro del **edificio** o de las **instalaciones**.

3 ◆ El perímetro **interior**: barreras que pueden crearse dentro de la oficina para proteger una o varias habitaciones. Esto es especialmente útil en oficinas con mucho tránsito de visitas, pues permite que exista una zona pública y otra privada, protegida.

El perímetro exterior

La oficina debería estar rodeada por un perímetro exterior claro, por ejemplo, una valla, preferiblemente sólida y alta para dificultar el acceso. Las barandillas o alambradas hacen el trabajo más visible porque se puede ver a través de ellas, por lo que es mejor tener muros de ladrillo o similares. Si no hay un perímetro exterior, tenemos que decidir cuánta extensión podemos controlar visualmente para ver si se acerca cualquier potencial agresor. Una posibilidad sería instalar espejos convexos.

El perímetro del edificio o de las instalaciones

Esto incluye las paredes, puertas y ventanas, techo y tejado. Si los muros son sólidos, todos los vanos y el tejado serán también sólidos. Las puertas y ventanas deben tener cerrojos que funcionen bien y un refuerzo de rejas, preferiblemente con barras horizontales y verticales. El tejado, es importante que no que sea sólo una lámina de cinc o una fila de tejas, sino que sirva de protección: si no se puede reforzar, habrá que asegurarse de bloquear todo acceso posible al tejado desde el suelo o desde los edificios colindantes.

Si las ventanas de la oficina dan a la calle o a un espacio público, tendremos que poner las mesas de manera que podamos ver el exterior sin ser vistos desde el exterior. Si dan a vegetación, tomaremos medidas para que nadie pueda esconderse detrás sin que podamos verle.

Algunas oficinas tienen varias puertas, por lo que podríamos decidir cuál va a ser la "salida de emergencia". No hay que olvidar, no obstante, que una salida de emergencia puede convertirse también en un punto de entrada para cualquier potencial agresor.

En un lugar donde exista el riesgo de ser objetivo de un ataque armado es importante establecer zonas seguras en la oficina (ver, en este Manual, el capítulo sobre seguridad en las zonas de conflicto armado).

El perímetro interior

Lo anterior es aplicable para el caso del edificio o las instalaciones. Es muy útil tener una zona segura dentro de la oficina, y normalmente es muy fácil decidir cuál. Hasta una caja fuerte puede ser considerada un perímetro interior de seguridad.

Es posible que nuestra oficina sólo tenga un espacio, por lo que si queremos crear otros espacios privados, fuera de la vista de las visitas, podríamos dividirlo usando paneles de separación.

Sobre las llaves

- Las llaves tienen que estar fuera de la vista de las visitas. Hay que guardarlas en un armario o cajón con un candado y cuya combinación sólo sepan unas pocas personas del equipo. Para mayor seguridad, habrá que cambiar ese código periódicamente.

- Si las llaves tienen su identificación individual, ésta no debe ser una descripción del cuarto, cajón o armario que abran, ya que eso pondría muy fáciles las cosas para un robo. Es mejor usar códigos de números, letras o colores.

Medidas técnicas: iluminación y alarmas

(suponiendo que nuestra oficina tenga electricidad o un generador).

Las medidas técnicas refuerzan las barreras físicas o los procedimientos de admisión de las visitas (mirillas, telefonillos, videocámaras; ver abajo). Esto se debe a que, si funcionan bien, **son sólo útiles para evitar que entren los intrusos**. Para que así sea, tienen que provocar una reacción determinada, por ejemplo, la de atraer la atención de las y los vecinos, la policía o la compañía de seguridad. Si no la provocan, o si el intruso sabe que no la van a provocar, no sirven de mucho, si acaso para evitar pequeños robos o grabar a la gente que entra.

- **La iluminación** alrededor del edificio (patios, jardines, aceras) y en las entradas es fundamental.

- Las **alarmas** tienen varios objetivos, como el de detectar a intrusas o intrusos y evitar que entren o que sigan intentando entrar.

Una alarma puede activar un sonido de emergencia dentro la oficina, una luz, un ruido general fuerte, o bien enviar una señal a las oficinas de una compañía de

seguridad. Una alarma acústica es útil para atraer la atención pero puede ser contraproducente en situaciones de conflicto o si no esperas que alguien de la zona reaccione al oírla. Hay que meditar cuidadosamente si se va a instalar una alarma acústica o luminosa (una luz potente y fija, o bien, una luz roja intermitente). Esta última sí puede disuadir al intruso porque da a entender que va a ocurrir algo más tras esa primera señal.

Las alarmas deben instalarse en los puntos de acceso (patios, puertas y ventanas, lugares vulnerables como habitaciones donde se guarda información sensible). Las alarmas más inmediatas son los sensores de **movimiento**, que activan una luz, emiten un sonido o activan una cámara cuando detectan movimiento.

- Las alarmas deberían:
  - Tener **pilas**, para que puedan funcionar cuando se va la luz.
  - Tener un sistema de **activación retardada** para que las y los miembros del equipo puedan quitarla si la han hecho saltar por accidente.
  - Tener la opción de activación **manual** para el caso de que las y los miembros del equipo tengan que activarla.
  - Que sea fácil de **instalar** y **mantener**.
  - Que se distinga bien de la alarma de incendios.

Cámaras de vídeo

Las cámaras de vídeo pueden ayudar a mejorar los procedimientos de admisión (ver abajo) o grabar a la gente que entre en la oficina. Hay que asegurarse de que la grabación se hace desde un lugar al que no puede acceder el intruso porque si no, podría abrir la cámara y destruir la cinta.

Tendremos que considerar el tema de si las cámaras van a intimidar a personas que queremos que nos visiten, como víctimas o testigos; o si van a ser vistas como material valioso por quien quiere robar. Cuando usamos cámaras, hay que avisarlo porque el derecho a la privacidad es también un derecho humano.

La iluminación y las alarmas cuando la oficina no tiene ni electricidad ni un generador

Sencillamente, debemos evitar quedarnos en la oficina cuando se haga de noche.

La alarma eléctrica puede sustituirse por otro sistema: un o una vigilante, gente vecina, la familia, la comunidad, perros: tendremos que conseguir su apoyo y estudiar cómo pueden incorporarse a un sistema de alarma.

Compañías privadas de seguridad

Es un tema que requiere especial atención. En muchos países, los servicios privados de seguridad los dan antiguos miembros de las fuerzas de seguridad, y existen casos documentados en los que estas personas han vigilado y atacado a defensores y defensoras de derechos humanos. Por eso tiene sentido no confiar en las compañías privadas de seguridad cuando tenemos razones para temer que puedan estar vigilándonos o planeando un ataque en contra nuestra: un servicio de seguridad tiene acceso a nuestras oficinas y podrían instalar micrófonos o permitir el acceso a otras personas.

Si decidimos contratar sus servicios, tendremos que dejar muy claro qué es lo que su personal puede y no puede hacer y a qué zonas del edificio pueden o no puede entrar. Evidentemente, tendremos que poder controlar que estos acuerdos se cumplen.

Por ejemplo:

Si hemos contratado un servicio de seguridad que envía a un guardia cuando salta una alarma, tendremos que saber que ese guardia podría entrar en partes sensibles de la oficina para instalar micrófonos en nuestra sala de reuniones.

Lo mejor es poder decidir con qué personas queremos trabajar, pero esto no suele ser posible.

Si las o los guardias de seguridad van armados es importante que las organizaciones de derechos humanos conozcamos todos los detalles de qué reglas tienen respecto a cuándo usarlas. Incluso más importante puede ser sopesar los beneficios potenciales de que se estén usando armas. Las pistolas no suelen servir de nada frente a atacantes que tienen mejores armas de fuego (que es lo que suele ocurrir, las tienen). Es más, si un potencial atacante sabe que hay personas armadas en el edificio, es probable que fuerce su entrada listo para abrir fuego, a modo de protección en su ataque. En otras palabras, las armas de fuego pequeñas suelen llevar a los atacantes a usar armas de fuego de mayor potencia, por lo que merece la pena hacerse este planteamiento: si nos hacen falta guardias con ametralladoras, ¿estamos teniendo el espacio sociopolítico mínimo necesario como para llevar a cabo nuestro trabajo?

Filtros del procedimiento de admisión

Las barreras físicas tienen que venir acompañadas de un "filtro" que actúe a modo de **procedimiento de admisión**. Dichos procedimientos determinan cuándo, cómo y quién puede entrar en la oficina. El acceso a zonas sensibles, como lugares para llaves, información y dinero, debe estar restringido.

La forma más fácil para entrar en una oficina donde trabajan defensoras y defensores es llamar a la puerta. Así lo hacen muchas personas todos los días. Para poder reconciliar el carácter abierto de una oficina de derechos humanos con la necesidad de controlar quién nos visita y por qué, necesitamos disponer de unos procedimientos de admisión adecuados.

En general, la gente tiene una razón particular para querer entrar o llamar a nuestra puerta. A menudo quieren preguntar algo, o entregar algo, y muchas veces ni llaman antes de entrar. Examinemos el tema caso a caso:

Alguien llama y pide entrar por una razón particular

Tendríamos que seguir entonces tres pasos sencillos:

1 ◆ **Preguntar tanto la identidad como la razón de la visita.** Si quiere ver a alguien de la oficina, consultar primero con esa persona. Si esa persona no está, hay que pedirle a la visita que vuelva en otra ocasión, o que espere en algún lugar que no sea la zona de acceso restringido de la oficina.

Es importante usar mirillas, cámaras o telefonillos para evitar tener que abrir o que acercarse a la puerta, especialmente si pensamos en no dejar entrar a alguien, o vemos que va a entrar usando la fuerza. Así, es buena idea tener una zona de espera que esté físicamente separada de la entrada a la oficina propiamente dicha. Si es esencial que haya una zona pública de fácil acceso, tenemos que asegurarnos de que existen barreras físicas que impiden el acceso a las zonas restringidas de la oficina.

Alguien podría querer entrar con la excusa de reparar una avería o dar un servicio de mantenimiento. También podrían decir que son de los medios de comunicación, o representantes del gobierno, etc. Antes de dejarlos entrar, tenemos que comprobar su identidad con la compañía u organización a la que dicen pertenecer porque ni los uniformes ni las tarjetas de identidad son garantía de una identificación verdadera, en especial en situaciones de riesgo medio o alto.

2 ◆ **Decidir si permitir la entrada o no.** Cuando sepamos la identidad y por qué quieren entrar, tendremos que decidir si lo vamos a permitir o no, porque el que nos lo digan no es razón suficiente para dejarle entrar. Cuando dudemos de la razón que nos han dado, no debemos dejar entrar a la persona.

3 ◆ **No perder de vista a las visitas hasta que se marchen.** Cuando entren en la oficina, todo el mundo tiene que estar pendiente de dónde está esa persona hasta que se marche. Es útil disponer de una sala para las visitas que esté lo más alejada posible de las zonas de acceso restringido.

Hay que llevar un registro de las visitas, y apuntar el nombre, la organización, el propósito de la visita, con quién se reúne, la hora de llegada y la hora de partida. Esto nos puede ser particularmente útil cuando repasamos qué ocurrió tras un incidente de seguridad.

Alguien que llega o que llama nos está haciendo preguntas

Diga lo que diga la persona que viene a visitarnos, bajo ningún concepto debemos informar de dónde están nuestras compañeras o compañeros, o gente próxima; tampoco debemos dar ningún tipo de información personal sobre nadie. Si insisten, podemos ofrecer tomar nota de su recado, pedirles que llamen o que vuelvan luego, o darles día para una entrevista con la persona por la que preguntan.

Habrá personas que se hayan equivocado, y pregunten si tal o cual personal vive aquí, o si algo está a la venta, etc. O vendedores, gente que pide limosna... Si no dejamos entrar a nadie y no les damos la información que deseen estaremos evitando riesgos en relación con el tema de la seguridad.

Alguien quiere entregar un objeto o un paquete

El riesgo que corremos aceptando un objeto o un paquete es que su contenido podría comprometernos o hacernos daño, como cuando se trata de un paquete o carta bomba. No importa lo inofensivo que parezca: no hay que tocar ni manipular el paquete hasta haber dado tres pasos sencillos:

1 ◆ **Comprobar si la persona a la que se ha enviado el paquete lo espera.** No basta con conocer al remitente, porque es fácil poner cualquier remitente. Si la persona a la que va destinado el paquete no espera nada, tendrá que comprobar que el remitente le ha enviado algo de hecho. Si el paquete va dirigido a la oficina, antes de abrirlo hay que analizar a fondo el tema del remitente.

2 ◆ **Decidir si aceptar o no el paquete o carta.** Si no podemos establecer quién manda el paquete, o si necesitamos tiempo para hacerlo, lo mejor es no aceptarlo, en especial si estamos en un entorno de riesgo medio o alto. Siempre podemos pedir que nos lo traigan luego, o sencillamente ir a buscarlo a correos.

3 ◆ **No perderle la pista al paquete una vez esté en la oficina.** Hay que saber en todo momento dónde está el paquete hasta que lo acepte la persona a la que va dirigido.

En algunos países, avisan de que nos ha llegado un paquete y luego tenemos que ir a por él. Podría ser un truco para llevarnos a un sitio y luego atacarnos. Si el teléfono de origen no sale registrado, es posible que no podamos saber de dónde viene la llamada. Si preguntamos de dónde viene el paquete, podemos ponernos en contacto con quien lo haya enviado para averiguar además por qué medio lo ha enviado. Después decidiremos si es seguro o no ir a buscarlo. También podemos pedirle a quien nos llama que lo traiga a la oficina, y seguir los pasos descritos antes. Si es un pretexto, lo más probable es que quien llama nunca aparezca por la oficina.

Durante funciones y fiestas

En estas circunstancias, la regla es sencilla: no debemos permitirle la entrada a nadie que no conozcamos bien. Sólo dejaremos entrar a gente que conocen las personas en las que confiamos, y sólo cuando esa persona en que confiamos se encuentra presente para identificar al invitado o invitada. Si aparece alguien que dice conocer a alguien del grupo y esta persona no está, no hay que dejarle entrar.

Es posible que nos cueste estar haciéndole preguntas a las visitas y luego decirles que no pueden entrar. Sin embargo, no tenemos que presentarlo como una decisión nuestra personal; basta con decir que no tenemos autorización para dejar entrar a nadie.

Además, y esto es aplicable en todo procedimiento de admisión de visitas, tenemos que recordar que si la persona que nos visita lo hace de verdad, apreciará nuestro celo con cuestiones de seguridad. Si es un intruso o una intrusa, verá que tomamos medidas. Así que sea cual sea el caso, podemos darnos o quitarnos la autoridad para permitir entrar a una persona desconocida. Si nos es útil, podemos usar el "no… no obstante": "no estoy autorizada a dejar entrar a gente desconocida; no obstante, si desea dejarme su tarjeta, nos encantará informarle de otros eventos públicos que celebremos".

Anotar las llamadas y las visitas

También puede ser útil anotar las llamadas, los teléfonos, y el nombre de las visitas (en algunas organizaciones, a quienes visitan la oficina por primera vez se les pide que se identifiquen con un documento de identidad, cuyos datos se copian).

Trabajar horas extra en la oficina

Tenemos que haber decidido los procedimientos a seguir si vamos a hacer horas extra. Las y los miembros de la organización que vayan a trabajar horas extra por la noche tendrían que informar cada cierto tiempo de que están bien a otra persona del equipo, tomar medidas especiales al salir del edificio, etc.

Puntos a considerar: Cómo identificar los puntos débiles de los procedimientos de admisión:
◆ **¿Quién** tiene acceso regular a **qué** zonas y **por qué?** Debemos restringir el acceso a no ser que sea estrictamente necesario no hacerlo en un momento dado.
◆ Distinguir entre diferentes **tipos** de visitas (mensajeras/os, mantenimiento, técnicos informáticos, miembros de ONGs que vienen a reuniones, gente con cargos relevantes, invitadas/os para diferentes funciones, etc.) para **desarrollar los procedimientos de admisión adecuados para cada caso**. Todos los miembros de la organización tendemos que conocer todos los procedimientos para los diferentes tipos de visitas, además de asumir la responsabilidad de respetarlos.
◆ Cuando una visita ya ha entrado en la oficina, ¿podría tener acceso a algún punto débil? Hay que desarrollar estrategias para evitarlo.
Puntos a considerar: Acceso a las llaves
◆ **¿Quién** tiene acceso a **qué** llaves y **en qué momentos?**
◆ ¿Dónde y cómo se guardan las **llaves** y sus **copias?**
◆ ¿Llevamos **un registro de las copias** que se han dado?
◆ ¿Corremos el riesgo de que alguien pueda hacer una **copia no autorizada?**
◆ ¿Qué hacemos si **alguien pierde una llave?** Habrá que cambiar la cerradura correspondiente a no ser que tengamos total certeza de que ha sido un accidente y de que nadie puede identificar el domicilio al que pertenece. Recordemos que si alguien tiene la intención de entrar en nuestra oficina, puede robar las llaves (por ejemplo, en un robo hecho con ese propósito pero simulado como robo por dinero).

Todo el personal de la organización es responsable de tomar alguna medida si alguien no está respetando el procedimiento de admisión. Asimismo, hemos de registrar como incidente de seguridad cualquier movimiento de personas o vehículos sospechosos. Lo mismo es aplicable a cualquier objeto que haya sido abandonado fuera del edificio, para así poder descartar el riesgo potencial de una bomba. Si sospechamos que algo puede ser una bomba, no debemos ignorarlo **ni tocarlo**, y avisaremos a la policía.

Cuando nos mudemos, o si las llaves se han perdido o las han robado, es esencial cambiar todos los cerrojos de la entrada como mínimo.

Puntos a considerar: Procedimientos generales de seguridad en la oficina

- Debe haber extintores de incendios y linternas (con pilas de repuesto). Todo el mundo tiene que saber usar estos materiales.
- Debe haber un generador de electricidad si son comunes los cortes del fluido eléctrico, pues éstos amenazan la seguridad (luces, alarmas, teléfonos, etc.), sobre todo en zonas rurales.
- Hay que tener a mano una lista de números de teléfono para las emergencias: de la policía, el cuerpo de bomberos, ambulancias, hospitales cercanos, etc.
- Si existe un riesgo de conflicto en las proximidades, es bueno tener una reserva de comida y agua.
- Hay que saber dónde están las zonas seguras fuera de la oficina, para caso de emergencia (por ejemplo, las oficinas de otras organizaciones).
- Nadie que no sea de la organización debe quedarse **sola** o **solo** en una zona vulnerable con acceso a llaves, información u objetos valiosos.
- **Llaves:** Nunca hay que dejar las llaves donde las visitas puedan cogerlas. Nunca hay que "esconder" las llaves a la entrada de la oficina (hacerlo no es esconderlas sino dejarlas a mano para que las use cualquiera).
- **Procedimientos de admisión:** Las barreras de seguridad no protegen en absoluto si dejamos entrar a un intruso o intrusa potencial. Lo principal que hay que recordar es:
  - Todas y todos los miembros del equipo son responsables en la misma medida del control de las visitas y de su admisión.
  - Todas las visitas deben estar acompañadas en todo momento mientras estén en la oficina.
- Si encontramos a una visita no autorizada en la oficina:
  - Nunca debemos enfrentarnos a una persona que está dispuesta a usar la violencia para conseguir lo que quiere (por ejemplo, si va armada). En tales casos, debemos avisar al equipo, buscar un sitio seguro para escondernos, e intentar avisar a la policía.
  - Tratar con mucha cautela a la persona o buscar ayuda en la oficina o de la policía.
- En situaciones de mucho riesgo, siempre debemos tener controladas las cosas más sensibles (como la información que almacenemos en el disco duro) para que nadie pueda acceder a ellas, o para eliminarlas o llevárnoslas si tenemos que abandonar el lugar en una emergencia.
- No demos olvidar que en caso de enfrentamiento con un intruso o una intrusa potencial, la gente que trabaja en la oficina está en primera línea de fuego. Por eso hay que asegurarse de que han recibido la formación necesaria para cualquier situación que puedan enfrentar, que disponen de todo el apoyo que necesitan y que no tienen que correr riesgos personales.

Inspecciones regulares de la seguridad en la oficina

Hacer inspecciones regulares de los temas de seguridad en la oficina es muy importante, porque las situaciones y los procedimientos de seguridad varían a lo largo del tiempo (por ejemplo, porque el equipo se nos deteriora o porque de pronto cambian muchos miembros del grupo). Asimismo, es importante desarrollar un sentimiento de que las reglas de seguridad son una parte fundamental de nuestro trabajo cotidiano.

La persona encargada de las inspecciones debe hacer un repaso a la oficina al menos una vez **cada seis meses**. Con la ayuda de la lista que aparece a continuación esto puede llevarnos tan poco como una o dos horas. Antes de redactar el informe final debe entrevistarse con todas y todos los miembros del equipo, para averiguar cómo ven los temas, y luego se presentará el informe de seguridad a la organización para que se tomen las decisiones y medidas necesarias. Este informe se archivará hasta ser reemplazado por el siguiente.

En zonas rurales

Las y los defensores también trabajan en zonas rurales, ya sea en pueblos o en zonas remotas y aisladas. Es posible que no tengan mucho dónde elegir a la hora de dónde establecer la oficina. En todo caso, necesitan proteger su espacio de visitas y objetos no deseados.

Pueblos: si son parecidos a las zonas urbanas pequeñas, casi todas las consideraciones anteriores podrían servir. Podemos completarlas con las que siguen.

Lugares remotos y aislados: hay que asegurarse de que la comunidad de las proximidades, nuestras familias y amistades pueden formar parte de nuestro sistema de alarma. Pueden ayudar regularmente sabiendo dónde estamos y teniendo vigilada la oficina (y/o la casa). Podemos también tener perros, educados para que ladren cuando aparece alguien. Eso sí: no deben atacar a la gente, ni dejarse tocar fácilmente por si quieren envenenarlos.

Hacer con precaución los trayectos a la zona, y evitar la noche.

Podemos también considerar el establecer sistemas ágiles para comunicarnos con personas de nuestra confianza para tener acceso a una reacción de apoyo tan rápida como sea posible en caso de que la necesitemos.

PUNTOS A CONSIDERAR PARA REALIZAR UNA INSPECCIÓN Y REDACTAR UN INFORME SOBRE LA SEGURIDAD EN LA OFICINA

REDACCIÓN DEL INFORME
INSPECCIÓN REALIZADA POR:
FECHA:

1 ◆ **CONTACTOS Y EMERGENCIAS:**

- ¿Hay una lista actualizada y a mano de teléfonos y direcciones de ONGs de la zona, hospitales, policía, bomberos, y ambulancias, ONGs internacionales, embajadas?

2 ◆ **BARRERAS TÉCNICAS Y FÍSICAS (EXTERIORES, INTERIORES E INTERNAS):**

- Comprobar el correcto funcionamiento de las puertas, vallas y muros exteriores, de las puertas y ventanas del edificio, las paredes y el tejado.
- Comprobar el funcionamiento de la iluminación exterior, las alarmas, cámaras o telefonillos.
- Comprobar el tema de las llaves, incluido el lugar **donde se guardan**, el **código** con que se identifican, **quién es responsable** de qué llaves y de qué copias, y que todas las llaves **funcionan** correctamente. Cambiar los **cerrojos** si hay llaves perdidas o robadas, y **registrar** esos incidentes.

3 ◆ **PROCEDIMIENTOS Y "FILTROS" DE ADMISIÓN:**

- ¿Funcionan los procedimientos de admisión con todo tipo de visitas? ¿Conoce todo el equipo esos procedimientos y los aplica?
- Repasar el registro de los incidentes de seguridad relacionados con procedimientos o "filtros" de admisión.
- Preguntar a las personas del equipo que realizan los procedimientos de admisión si creen que éstos sirven o funcionan correctamente y si se pueden mejorar de alguna manera.

4 ◆ **SEGURIDAD Y ACCIDENTES:**

- Comprobar los extintores, las válvulas de gas, las cañerías, los enchufes, los cables, los generadores (cuando sea aplicable).

5 ◆ **RESPONSABILIDAD Y FORMACIÓN:**

- ¿Se han asignado responsabilidades en el tema de la seguridad? ¿Funciona?
- ¿Existe un programa de formación en temas de seguridad? ¿Cubre todos los temas tratados en este informe? ¿Han recibido formación las personas nuevas? ¿Sirve esa formación?

Resumen

El objetivo de las medidas de seguridad en la casa o la oficina es reducir el riesgo de un acceso no deseado.

El nivel de seguridad de una oficina no es mayor que el nivel de seguridad de su punto más débil.

Podemos usar esta ecuación[1] para reducir el riesgo de acceso no deseado tanto si vivimos/trabajamos en una zona rural o urbana.

Las amenazas son asimilables a las consecuencias de los riesgos.

Hacer una lista con todas las amenazas/consecuencias que implica el riesgo de acceso no deseado. Después, y en relación con esas amenazas/consecuencias, hacer la lista de nuestros puntos fuertes y débiles (capacidades y vulnerabilidad) para cada una de ellas.

[1] Ver el capítulo 1.2.

CAPÍTULO 1.9

La Seguridad y las defensoras de derechos humanos

Objetivo:

Considerar el tema de la seguridad desde la perspectiva de las defensoras de derechos humanos

Ofrecer más información y herramientas sobre seguridad y protección a las defensoras y los defensores de derechos humanos

Introducción

Aunque la seguridad de las defensoras de derechos humanos es parte del tema de la seguridad de todas las personas que se dedican a esta actividad, hemos decidido dedicarles un capítulo porque la experiencia en este campo nos muestra que existen asuntos que las afectan por el hecho de ser mujer y que no son tenidos en consideración. Esto ocurre por muchas razones complejas, producto del contexto social, cultural y religioso.[1]

Queremos empezar introduciendo el tema con una breve compilación de los comentarios reunidos en nuestras experiencias. Esto nos ayudará a darnos cuenta de que existen temas comunes (más allá del ser hombre o mujer) y también temas condicionados por la cuestión del género, y que es necesario que las y los defensores los tengan en cuenta.

Las defensoras de derechos humanos

En el trabajo de promoción y protección de los derechos humanos siempre ha habido mujeres, aunque no siempre se haya reconocido su presencia. Sin embargo es así: las mujeres trabajan solas y también junto a los hombres en la protección de los derechos humanos.

Por desgracia, con demasiada frecuencia...

- Las mujeres se enfrentan a la violencia del machismo fuera de sus organizaciones pero también en sus propias organizaciones, donde existen los prejuicios y se da la discriminación de género.

[1] Ética del cuidado: Carole Gilligan (psicóloga de Harvard), en su libro "In a different voice" (1982), mantiene que, así como la moral del hombre se basa en la justicia y los derechos, la moral de la mujer se basa en el cuidado para reconocer la importancia de las relaciones humanas y en la atención que muestran hacia las necesidades de otras personas. Por lo tanto, es legitimo pensar que, si los hombres siguieran la ética del cuidado, habría menos violencia.

- A menudo o "no hay tiempo" para tratar los temas de derechos que afectan a las mujeres y que tendrían que aparecer en la agenda del grupo, o se los trata como temas "especiales", no de derechos humanos (sobre todo en las organizaciones mixtas de defensa de los derechos humanos).

- Los defensores siguen considerando a las defensoras sus ayudantes: hay tareas que ellos se niegan a hacer porque las consideran menos importantes, o piensan que hacerlas pondría en cuestión su masculinidad.

El machismo, el clasismo, el racismo, el sistema de castas, la xenofobia y la homofobia son facetas más o menos evidentes de una misma lógica que subyace a todas las violaciones de derechos humanos, sean éstas contra hombres, mujeres, personas de diferente orientación sexual, niñas y niños, personas mayores, grupos étnicos, personas pobres… Todas estas facetas tienen un impacto en el tema de la seguridad. Un ejemplo: en algunos lugares, las y los parias no son incluidos en los planes de seguridad ni positivamente, como personas que conocen bien su entorno por ejemplo, ni negativamente, como informadores del potencial agresor.

Además, el concepto de la violencia no está siempre bien planteado:

- Se lucha contra "la violencia contra las mujeres" en lugar de contra la violencia de los hombres.

- Se usa el término "violencia doméstica" para no decir "violencia ejercida por los hombres".

Si trabajamos para poner fin a la violencia ejercida por los hombres, la violencia doméstica descenderá. La conexión es clara, no son temas diferentes.

Las mujeres siguen siendo a menudo consideradas seres humanos de segunda clase, a pesar de que la ciencia moderna ha establecido que las diferencias de género no implican ningún orden de capacidades. Parece evidente, pero nuestra experiencia con defensores y defensoras en los proyectos y en los talleres nos ha demostrado que esta idea no es comprendida por todo el mundo aún; de ahí nuestra insistencia aquí. Desde que las mujeres pueden ir a la escuela, se ha visto que tienen la misma inteligencia que los hombres (por mencionar sólo el tipo de inteligencia que se evalúa en el colegio). En general, podemos decir que se confunde lo que es ser inteligente con estar informado.

Se puede decir lo mismo sobre las minorías étnicas y cualquier otro grupo que es objeto de discriminación: el problema no es antropológico sino social. Un grupo concreto que accediera a la educación podría argumentar y con ello cuestionar el estatus quo, lo que explica posiblemente por qué a muchas niñas y mujeres todavía no se las permite estudiar.

Las mujeres perciben la contradicción que existe cuando por un lado se defienden los derechos humanos, pero por otro se las trata de manera discriminatoria. Inevitablemente, habrá momentos en que deseen decirle a sus compañeros que paren ya, que reflexionen sobre tales hechos y que vuelvan cuando sean conscientes de que se dan y estén dispuestos a modificar los comportamientos que los generan. Sin embargo, optan por seguir trabajando a su lado. Es más, el porcentaje de mujeres que se suma a las acciones de derechos humanos que orga-

nizan los grupos mixtos es mayor que el de hombres que se apoyan las que organizan los grupos de mujeres.

La violencia contra la mujer (o contra cualquier otro grupo humano) no es un tema de cultura o religión, sino de poder.

En el caso de Nelson Mandela y Desmond Tutu por ejemplo, se puso fin al apartheid no sólo porque de pronto se reconoció que las personas negras eran seres humanos con dignidad, sino también porque un grupo de personas blancas reconoció que había perdido la suya. Lo mismo puede aplicarse a la discriminación de género, y a todo tipo de discriminación.

Mientras que los compañeros defensores de derechos humanos no entiendan que la discriminación de género nace de la misma lógica perversa que legitimiza todos los otros tipos de discriminación, el movimiento de defensa de los derechos humanos tendrá la mitad de la fuerza que podría tener y seguirá actuando a favor de los propósitos de quienes violan los derechos humanos: divide y vencerás.

Los derechos de las mujeres no son sólo un tema de las mujeres

Este capítulo no pretende cambiar las mentalidades o los valores de nadie, pero sí analizar cómo la discriminación de género (al igual que cualquier otro tipo de discriminación) repercute en el tema de la seguridad y la protección de las mujeres primero y también de los hombres. Aspirar a cambios de mentalidad es un objetivo demasiado ambicioso; no lo es luchar por evitar que se produzcan determinados comportamientos, prejuiciosos hacia las mujeres: al fin y al cabo, si los hombres actúan con solidaridad y asumen también los temas de la seguridad de las mujeres, estarán contribuyendo a la seguridad de todo el mundo en el movimiento de defensa de los derechos humanos.

Para más información, consúltese el material producido en la Campaña Internacional sobre Mujeres Defensoras de Derechos Humanos, en Colombo, Sri Lanka, 2005:[2]

http://defendingwomen-defendingrights.org/pdf/WHRD-Proceedings-Spanish-web.pdf

Los ataques a las defensoras de derechos humanos

En su "Informe anual 2002" para la Comisión de Derechos Humanos de las Naciones Unidas, Hina Jilani, representante especial del Secretario General de las Naciones Unidas para las y los Defensores de Derechos Humanos, declaraba:

> *Las defensoras de los derechos humanos figuran, al igual que sus colegas masculinos, en la vanguardia de la promoción y protección de los derechos humanos. Sin embargo, en cuanto mujeres, corren los riesgos propios de su género, amén de los riesgos a los que se enfrentan los hombres.*

[2] Una guía muy útil sobre defensoras de derechos humanos, de las Naciones Unidas: http://www.unhchr.ch/defenders/tiwomen.htm. Ver también Report: Consultation on Women HRDs with the UN Special Representative of the Secretary General on Human Rights Defenders, April 4-6 2003, publicado por Asia Pacific Forum on Women, Law and Development; y Actores esenciales de nuestro tiempo. Los defensores de los derechos humanos en América, de Amnistía Internacional.

En primer lugar, en cuanto mujeres, ***su presencia es más perceptible****. Es decir, las defensoras de los derechos humanos pueden suscitar mayor hostilidad que sus colegas masculinos porque, en cuanto defensoras de los derechos humanos, pueden desafiar las normas culturales, religiosas o sociales acerca de la feminidad y el papel que desempeña la mujer en un determinado país o una determinada sociedad. A este respecto, no sólo están expuestas a violaciones de los derechos humanos por la labor que realizan como defensoras de tales derechos sino que lo están en mayor medida debido a su género y al hecho de que* ***su labor puede hacer tambalear los estereotipos sociale****s de la sumisión de la mujer o cuestionar las ideas que la sociedad tiene sobre la condición de la mujer. En segundo lugar, no es improbable que la hostilidad, el hostigamiento y la represión que tienen que afrontar las propias defensoras de los derechos humanos asuman una modalidad específicamente relacionada con el género, que vaya, por ejemplo, de la agresión verbal dirigida exclusivamente contra la mujer a causa de su género hasta el acoso sexual y la violación.*

A este respecto, ***la integridad profesional y la posición de la mujer en la sociedad pueden verse amenazadas y desacreditadas*** *de maneras muy particulares como el trillado cuestionamiento pretextual de su probidad cuando, por ejemplo, las mujeres reivindican su derecho a la salud sexual y reproductiva, o a la igualdad con el hombre, incluido el derecho a una vida libre de discriminación y violencia. En este contexto, por ejemplo, se ha juzgado a defensoras de los derechos humanos usando leyes por las que se penalizan conductas que corresponden al goce y ejercicio legítimos de derechos amparados por el derecho internacional mediante acusaciones infundadas debido sencillamente a sus opiniones y a su labor de promoción en defensa de los derechos de la mujer.*

En tercer lugar, los abusos perpetrados contra los derechos humanos de las defensoras de los derechos humanos pueden a su vez tener repercusiones de por sí relacionadas con su condición de mujeres. Por ejemplo, ***el abuso sexual y la violación*** *de una defensora de los derechos humanos encarcelada pueden* ***provocar el embarazo y enfermedades de transmisión sexual, como el VIH/ SIDA.***

Ciertos derechos propios de la mujer son casi exclusivamente promovidos y protegidos por defensoras de los derechos humanos. La promoción y defensa de los derechos de la mujer puede ser un factor de riesgo adicional, puesto que la afirmación de algunos de esos derechos puede interpretarse como una ***amenaza al patriarcado y una alteración de los usos y costumbres culturales, religiosos y sociales.*** *En algunos países la defensa del derecho de la mujer a la vida y a la libertad ha tenido por respuesta violaciones de la vida y la libertad de las propias defensoras. Asimismo, la protesta contra prácticas intimidatorias ha sido motivo de persecución de destacadas defensoras de los derechos humanos, acusadas de apostasía.*[3]

[3] Subrayado nuestro. Fuente: E/CN.4/2002/106, 27 de febrero de 2002, páginas 23 y 24: "Promoción y protección de los derechos humanos: defensores de los derechos humanos", informe de la Sra. Hina Jilani, ex Representante Especial del Secretario General sobre la cuestión de los defensores de los derechos humanos, de conformidad con la resolución 2000/61 de la Comisión de Derechos Humanos.

La edad, la pertenencia étnica, la educación, la orientación sexual o el estado civil pueden ser factores añadidos que condicionarán la adopción de diferentes medidas de seguridad y protección para los diferentes grupos de defensoras.

Valorar las necesidades de protección de las defensoras de derechos humanos sirve para determinar con claridad cuáles son sus particulares puntos vulnerables y qué estrategias pueden emplearse para neutralizarlos. Así, podemos mejorar nuestra respuesta tanto en el día a día como en situaciones de emergencia.

LA "DECLARACIÓN SOBRE LA ELIMINACIÓN DE LA VIOLENCIA CONTRA LA MUJER" (1993) DEFINE LA VIOLENCIA CONTRA LA MUJER DEL SIGUIENTE MODO:

Artículo 1

A los efectos de la presente Declaración, por "violencia contra la mujer" se entiende todo acto de violencia basado en la pertenencia al sexo femenino que tenga o pueda tener como resultado un daño o sufrimiento físico, sexual o sicológico para la mujer, así como las amenazas de tales actos, la coacción o la privación arbitraria de la libertad, tanto si se producen en la vida pública como en la vida privada.

Artículo 2

Se entenderá que la violencia contra la mujer abarca los siguientes actos, aunque sin limitarse a ellos:

a) La violencia física, sexual y sicológica que se produzca en la familia, incluidos los malos tratos, el abuso sexual de las niñas en el hogar, la violencia relacionada con la dote, la violación por el marido, la mutilación genital femenina y otras prácticas tradicionales nocivas para la mujer, los actos de violencia perpetrados por otros miembros de la familia y la violencia relacionada con la explotación;

b) La violencia física, sexual y sicológica perpetrada dentro de la comunidad en general, inclusive la violación, el abuso sexual, el acoso y la intimidación sexuales en el trabajo, en instituciones educacionales y en otros lugares, la trata de mujeres y la prostitución forzada;

c) La violencia física, sexual y sicológica perpetrada o tolerada por el Estado, dondequiera que ocurra.

La seguridad de las defensoras de derechos humanos

Las defensoras de derechos humanos pagan un precio muy alto por el trabajo de proteger y promover los derechos humanos de otras personas. Enfrentan riesgos que se dan concretamente porque son mujeres, por lo que al plantearnos el tema de la seguridad habrá que tener esto en cuenta, así como al diseñar los protocolos y políticas de seguridad de la organización. A continuación presentamos una lista no exhaustiva de las causas mencionadas en el citado informe de Hina Jilani.

- La presencia de las mujeres puede atraer una atención no deseada.
- La presencia de las defensoras suele cuestionar tabúes sociales y leyes del patriarcado.
- Existen formas de agresión específicas hacia las defensoras porque son mujeres.
- Las defensoras podrían verse obligadas a tener que "probar que son decentes".
- Podrían existir compañeros que no comprendan, o que incluso rechacen, el trabajo de las defensoras.
- Las defensoras podrían estar siendo objeto de violencia doméstica.
- Es común que las defensoras tengan obligaciones familiares añadidas.
- Todo lo que implica una carga añadida para las defensoras, por el trabajo y el estrés que todo esto lleva consigo.

Pasos para mejorar la seguridad y la protección de las defensoras de DDHH

Políticas y medidas de seguridad globales de carácter permanente.

Incluir la participación de las mujeres desde la perspectiva de género

Brevemente, esto implica asegurarnos de que las mujeres participen en la toma de decisiones; de que se incluyen en nuestras agendas los temas que las afectan sólo a ellas; y de que también las mujeres adoptan las precauciones de seguridad que hayamos establecido. Es vital que tengamos en cuenta las experiencias y percepciones de las defensoras, y que éstas participen en el diseño de las reglas y medidas de seguridad, en su supervisión y evaluación.

Asegurarnos de que vamos a abordar las necesidades de protección y seguridad que se relacionan con el tema del género

Como ocurre con otras necesidades de seguridad, será muy importante decidir quiénes se encargan de los temas de violencia de género y de los riesgos de seguridad que puedan correr las mujeres del grupo u organización de defensa de los derechos humanos. Lo ideal sería que quien esté a cargo de los temas de seguridad comprenda bien cuáles son las necesidades específicas de las defensoras. A veces, sin embargo, será necesario elegir a una persona más que esté

sensibilizada con el tema y tenga conocimientos específicos. Pongamos que la organización tiene a una persona a cargo de los temas de seguridad. Podría nombrarse a una persona más, con una formación y experiencia específicas, para que se encargara concretamente de los temas de violencia de género. A partir de ese momento, ambas trabajarían juntas para cerciorarnos de que todos los procedimientos de seguridad están funcionando adecuadamente y atendiendo las necesidades de todo el mundo.

Formación

La formación para todas las personas que trabajan en una organización de derechos humanos es fundamental para mejorar la seguridad y la protección, y debería incluir el que seamos conscientes de las necesidades específicas de las defensoras.

Trabajo de sensibilización...

- Para aclarar posibles confusiones entre los valores sociales, culturales y religiosos y los derechos de las mujeres (derechos humanos).
- sobre la violencia doméstica hacia las mujeres (todo daño físico, sexual y psicológico en la familia, como los malos tratos, la violación, la mutilación genital femenina y otras prácticas tradicionales que hacen daño y ponen en peligro las vidas de las mujeres).
- En las familias de las defensoras y sobre la necesidad de que frente a la violencia doméstica actúen también como lo hacen frente a la violencia de fuera de la casa. Las organizaciones tienen que abordar la cuestión si sus miembros toleran situaciones de violencia doméstica. Esto es contradictorio con los objetivos de trabajo y, desde el punto de vista de la seguridad, la organización en su conjunto podría verse desacreditada y a consecuencia de ello, perder apoyos fundamentales.
- Sobre el hecho (relevante desde un punto de vista de la seguridad) de que muchas mujeres tienen la responsabilidad añadida de tener que cuidar a hijos, hijas y otros familiares; sobre cómo los hombres pueden aprender a compartir las tareas domésticas sin sentir amenazada su masculinidad.
- Sobre el hecho de que tanto las defensoras como los defensores son a menudo criticados por dedicarse a cuidar personas que no son sus familias.

En resumen

Las diferentes necesidades de las mujeres respecto al tema de la seguridad tienen relación con los diferentes papeles que éstas desempeñan, con los diferentes tipos de amenazas que sufren y con las diferentes situaciones en que se pueden encontrar (detención, trabajo de campo, etc.). El objetivo es que desarrollemos respuestas a la violencia contra defensoras y defensores que incluyan la perspectiva de género.

Comentario adicional

Por desgracia, el número de **denuncias de los casos de violencia de género es mucho menor** que el número de casos que se producen. Si la organización o el grupo es sensible al tema, esto podría ser fundamental para que quienes lo sufren puedan expresarlo. La buena disposición por parte del equipo puede servir también como "punto de entrada" para que las defensoras y los defensores busquen soluciones a amenazas o a violencia de género que estén sufriendo o que sufran otras personas de su organización o comunidad.

La agresión sexual y la seguridad personal

Según las estadísticas, la violación afecta a más mujeres que hombres. Algunos hombres defensores que la han sufrido la describen como tortura sexual y son conscientes de que esto es lo que las mujeres soportan. La violación es tortura pues pretende causar daños físicos o psicológicos a las persona.

Los crímenes comunes se usan normalmente de tapadera cuando se trata de defensores, de tal manera que, cuando en un caso real de delincuencia común se habla de violación, si se trata de un caso de crimen político habría que hablar de tortura sexual [4] (se usa para reprimir el trabajo del defensor, las víctimas pueden ser tanto seleccionadas con antelación como escogidas aprovechando un descuido).

Es un crimen relacionado con el poder y la violencia. La tortura sexual es una forma más para el agresor de demostrar su poder sobre su víctima.

La tortura sexual es una de las consecuencias de la agresión física. La prevención, por tanto, empieza con las medidas de seguridad descritas anteriormente, pues están diseñadas para reducir el riesgo de sufrir ataques. Es en este sentido en el que decimos que la agresión sexual es similar a otros tipos de agresión.

Es preciso recordar que en muchos casos las mujeres que siguen a un potencial agresor a otro lugar son golpeadas, violadas y asesinadas. Sería lógico pensar que las mujeres deberían negarse a no seguir a ningún agresor potencial a ningún lugar (a no ser que tal negativa ponga en peligro inmediato o grave su vida o la de otras personas).

Todas las defensoras se enfrentan al riesgo de la tortura sexual, pero no todas actúan igual cuando ésta se produce, depende de su contexto político, social, cultural y religioso. Unas mujeres se centran en lidiar con los daños a su salud física y psicológica; otras, añaden a esto las consecuencias sociales y culturales, el trago de denunciarlo y de ser interrogadas en un procedimiento legal.

El tema de la agresión sexual tiene que abordarse desde todas las perspectivas e incluyendo todos sus efectos, lo que implica incluir la dimensión psicosocial.

[4] http://www.unhchr.ch/spanish/html/menu3/b/h_cat39_sp.htm
Declaración contra la tortura de la ONU: " (...) todo acto por el cual se inflija intencionadamente a una persona dolores o sufrimientos graves, ya sean físicos o mentales, con el fin de obtener de ella o de un tercero información o una confesión, de castigarla por un acto que haya cometido, o se sospeche que ha cometido, o de intimidar o coaccionar a esa persona o a otras, o por cualquier razón basada en cualquier tipo de discriminación, cuando dichos dolores o sufrimientos sean infligidos por un funcionario público u otra persona en el ejercicio de funciones públicas, a instigación suya, o con su consentimiento o aquiescencia.

Como ocurre con todas las formas de tortura, la persona torturada sexualmente puede experimentar sentimientos de culpa, "dignidad perdida", desconfianza y, además, en el caso especifico de violación sexual, sentirse sucia... Las organizaciones podrían ayudar analizando el concepto de la dignidad: ¿qué es la dignidad? ¿Quién decide sobre la dignidad de otra persona? ¿Quién ha perdido la dignidad: la persona torturada o la que tortura?

Organizativamente, una política permanente debería incluir la perspectiva de género...

- Para integrar las necesidades específicas de las defensoras.
- Para identificar posibles hechos de discriminación por razón de género en el seno de la organización.
- Para abordar en toda su complejidad el impacto del abuso y la tortura sexual en sus víctimas.
- ...

Protocolos concretos para...

- Defensoras en misiones de campo.
- Relaciones públicas entre los actores o partes implicadas en protección.
- Después del abuso o la tortura sexual (por ejemplo, evitar embarazos no deseados y el HIV/SIDA).

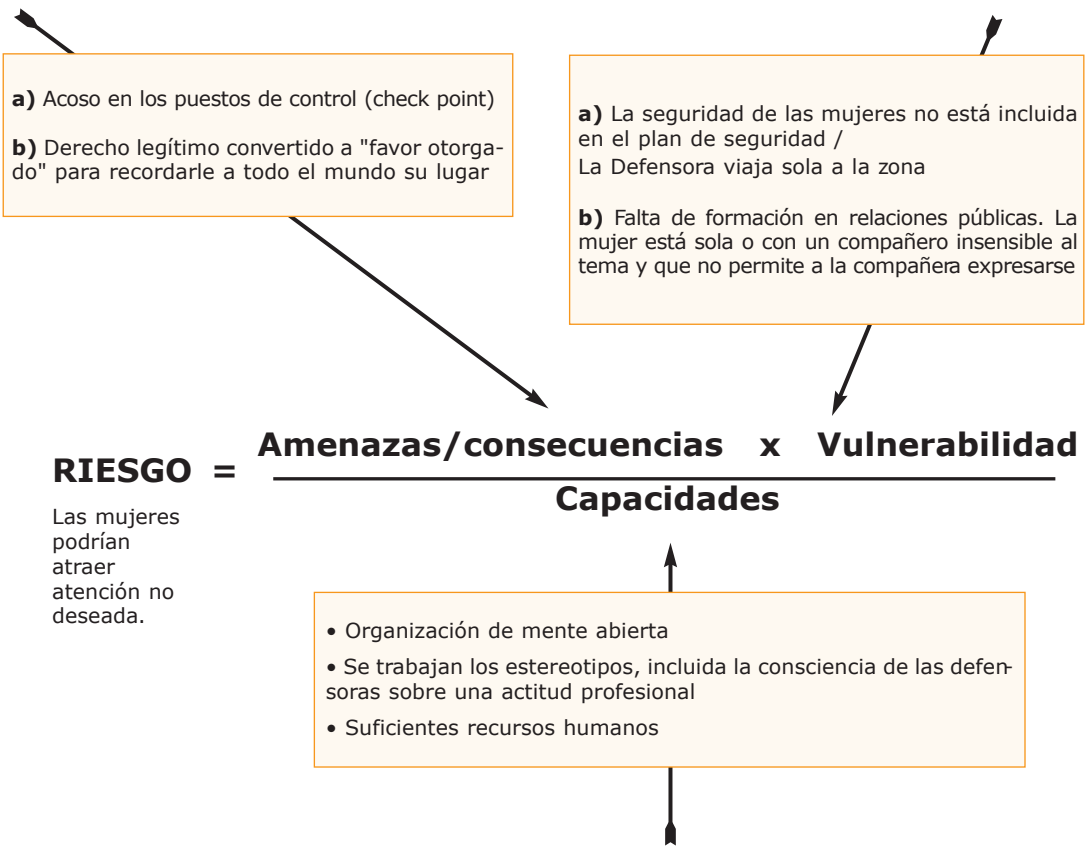
Cuando definamos estos protocolos habrá que recordar que:

- Algunas defensoras no se atreven a mencionar a sus compañeros defensores que han sufrido abusos o tortura sexual por miedo a la estigmatización o a perder el prestigio (recordemos que las víctimas, aun sin motivo alguno que lo justifique, tienen normalmente sentimiento de culpa).
- En algunos países las organizaciones mixtas no lo hablan casi nunca.
- Algunos defensores están en contra del aborto. Por otro lado, no están siempre dispuestos a hacerse cargo de una o un bebé no deseado. En muchos países, donde la ley, la cultura o la religión prohíben el aborto, el infanticidio y el abandono son las opciones de hecho. El abandono desempeña un papel importante en el fenómeno de las niñas brujas y los niños brujos, y en el aumento de las niñas y los niños soldados, además de estigmatizar a sus víctimas. Las mujeres podrían plantearse tomar la píldora del día después para evitar quedarse embarazadas.
- No existe una opción correcta y otra incorrecta; sencillamente, consecuencias que habrá que valorar a nivel interno, en la organización.
- **Se recomienda usar la ecuación del riesgo.**

Ejemplo:

Riesgo: *Las mujeres podrían atraer atención no deseada.*

Vamos a hacer una lista con todas las amenazas/consecuencias posibles relacionadas con el riesgo que nos ocupa. Después, para cada amenaza/consecuencia, anotaremos los puntos vulnerables y las capacidades más relevantes que tengamos en ese momento. A continuación, averiguaremos qué capacidades necesitamos para reducir esos puntos vulnerables y pasamos a trabajarlas. En otras palabras, hay que desentrañar el riesgo lo más posible, como cuando quitamos las capas de una cebolla. Para cada capa (amenaza/consecuencia) determinaremos los puntos vulnerables y las capacidades más relevantes.



(Indicar, en el inventario de capacidades generales de arriba, cuáles podrían encontrarse relacionadas específicamente con nuestros puntos vulnerables "a" y "b". Después, determinar qué otras necesitamos).

Cómo actuar ante una agresión sexual[5]

Las opciones que se tienen ante una agresión sexual son como las que se tienen frente a otro tipo de agresiones físicas y dependen de la víctima. No hay una forma correcta o incorrecta de reaccionar. Sencillamente, cada forma de reaccionar tendrá una serie de consecuencias. En todos los casos, nuestro objetivo sería sobrevivir. Las opciones podrían ser:

[5] La mayor parte de esta información está adaptada del libro de Koen Van Brabant, *Operational Security in Violent Environments*, y de los manuales de seguridad de World Vision y de World Council of Churches.

1 ◆ **No resistirse,** por si eso sirviera para salvar tu vida.

2 ◆ **Resistencia pasiva.** Haz o di cualquier cosa asquerosa que pueda hacer que el agresor abandone su ataque. Di que tienes una enfermedad contagiosa (aunque el agresor podría responder que él también o podría ponerse más violento).

3 ◆ **Resistencia activa:** Lucha con todas tus fuerzas, golpea en las zonas blandas, usa tus puños, tus uñas, tus piernas, tus dientes, grita lo más alto posible... Posiblemente cuanto más luchemos (si podemos), más probabilidades tendremos de escapar.

En todos los casos:

- Tenemos que escapar en cuanto nos sea posible.

- Si es posible, intenta mencionar el uso de un condón. En algunas culturas y religiones esto es considerado como "consentir" aunque no lo sea de hecho, pero si lo ven así es su problema, no el tuyo. Tus problemas son otros: un posible embarazo, consecuencias para tu salud física y psicológica, miedo a los recuerdos y al "¿y qué pasará si...?". Las defensoras podrían plantearse llevar consigo condones o ponerse el condón femenino cuando viajen a zonas peligrosas. Esto implica discutir el tema en la organización, para que ese gasto se incluya también en los presupuestos. Lo mismo es aplicable para la píldora del día después y cualquier atención hospitalaria (ver después: la PPE).

- Intenta fijarte en y acordarte del máximo de información sobre el agresor o los agresores. Esto también puede ayudarte a concentrarte en otra cosa, además, aunque sobre todo será útil para denunciarle(s) y reducir la posibilidad de que quede(n) impune(s).

- Si puedes, intenta concentrarte para distanciar tu yo de lo que le estén haciendo a tu cuerpo.

En todos los casos, haz lo que sea para sobrevivir. Sigue tu intuición o tu instinto. Nadie podemos saber cómo vamos a reaccionar ante esa situación (o ante cualquier otro tipo de tortura) y cómo lo hagamos será lo correcto en ese momento.

En muchos lugares, la tortura sexual va más allá de lo imaginable

Aunque siguiendo la lógica elemental de la seguridad, no podemos salir en una misión de campo donde el riesgo de sufrir tortura sexual a manos de las partes combatientes es extremadamente alto sin haber elaborado antes algún tipo de estrategia disuasoria, algunas organizaciones de defensa de los derechos humanos y algunas defensoras individualmente optan por hacerlo: por poner en peligro su propia seguridad, al pensar en las otras víctimas. Aunque la línea que separa el riesgo aceptable del no aceptable sea personal y de las organizaciones, insistimos en las reglas básicas de seguridad. En los cursos de formación, las lluvias de ideas han aportado las siguientes opciones para los casos de agresión sexual durante misiones de campo: la defensora podría mentar el SIDA (tanto si la tortura se va a aplicar al conjunto de personas como si no) para sembrar la duda de que como nadie sabe quién puede tener el SIDA, todo el mundo podría estar infectado. También podría decirle al agresor que tiene el periodo, lo que

implica que como medida preventiva tendría que llevar puestas compresas manchadas durante toda la misión. Otra opción sería llevar mucha ropa puesta para ganar tiempo en caso de que llegaran a rescatarla.

El HIV/SIDA es una plaga para la sociedad y no tiene fronteras

En algunos países donde la tortura sexual de las mujeres se ha convertido en un arma de guerra, muchas están considerando la posibilidad de ir a explicarles a los agresores que sus acciones afectan en realidad a todo el mundo: que lo que se consigue no es reprimir a las mujeres mediante el uso de la tortura sexual sino la muerte de todo el mundo, que es un tema de vida o muerte para todas las personas, incluidos los propios agresores. Una bomba de relojería para todo el mundo, un genocidio cultural.

Muchos defensores de derechos humanos también trabajan la tortura sexual contra las mujeres y el rechazo cultural asociado. Sin embargo, algunos declaran que repudiarían a sus esposas si eso les pasara a ellas.

Un defensor (que trabajaba en cambiar las actitudes de las familias hacia mujeres que habían sufrido tortura sexual cuestionó una vez a un compañero que lo consideraba adulterio. Sencillamente le dijo a este último: "depende de lo que represente tu esposa para ti".

Éste es el tema subyacente. Demasiado a menudo, una mujer es considerada esencialmente un objeto sexual, una propiedad: una vez "rota", debe ser abandonada o sustituida.

Una mujer es a menudo considerada madre, hija, hermana o esposa de un hombre, no una mujer con su propia identidad. Muchas mujeres son, no obstante, afortunadas por poder contar con compañeros que ofrecen un apoyo verdadero a sus compañeras.

Todas las organizaciones y grupos de defensa de los derechos humanos deberían tener planes de prevención y de reacción operativos para la eventualidad de una agresión sexual.

Allí donde fuera posible, y dependiendo de la localidad y su acceso a laboratorios médicos, debería poderse disponer de lo siguiente:

- visita/atención médica antes de lavarse - (tomar muestra de semen o de cualquier otra sustancia para un análisis del ADN)
- fotos de la víctima
- apoyo psicológico
- posibilidad de informar del caso a las autoridades competentes y de poner una denuncia

En todos los casos, el plan de reacción debería incluir, al menos, proporcionarle a la víctima cuidados médicos adecuados, incluido el psicológico, y después asistencia legal (conviene recordar que una mujer podría preferir ser atendida por otra mujer). Para evitar un embarazo, la víctima debería tener la oportunidad de tomarse la píldora del día después (en las 24 horas que siguen al ataque): se trata de un anticonceptivo de emergencia (no es una píldora abortiva).

Aunque no ofrece garantías pues depende de muchas variables, la PPE, Profilaxis Post-exposición, podría ser otra opción. En algunos hospitales ofrecen un kit para después de una violación, que contiene un tratamiento para detener la transmisión de varias enfermedades para las víctimas que han conseguido recibir atención sanitaria en las 72 horas que siguen a la violación. En cualquier caso, hay que hacerse una revisión cuanto antes y después con regularidad para saber si se tiene alguna enfermedad de transmisión sexual.[6]

Debe existir un equilibrio entre asegurarse de que la víctima recibe atención especializada adecuada y también de que la organización está reaccionando de manera adecuada y solidaria.

Véase también el capítulo 1.5, Cómo evitar y reaccionar a las agresiones.

[6] Para más información, ir a Comité Internacional de la Cruz Roja (ICRC): http://icrc.org/web/eng/siteeng0.nsf/html/congo-kinshasa-feature-201207

Resumen

Las mujeres son objeto de formas específicas de abuso, acoso y tortura por el hecho de ser mujeres en las culturas patriarcales. Con demasiada frecuencia, las organizaciones de defensa de los derechos humanos reproducen esta situación aunque a su micro nivel.

La seguridad de las defensoras es un tema de seguridad para todas las personas que se dediquen a la defensa de los derechos humanos. Tiene que ser incorporada en las políticas y protocolos de seguridad de las organizaciones. Además de realizarse la valoración de los riesgos, es preciso:

- cuestionar los papeles y las actitudes del sistema de sexo-género.
- trabajar las presuposiciones erróneas y cambiar las actitudes sexistas.
- desarrollar políticas de discriminación positiva para facilitar que se den esos cambios.
- incluir en los presupuestos de seguridad los condones, la píldora del día después, la terapia triple...

Una vez más, no podemos garantizar nada, pero la tortura sexual sigue a la agresión física, y reduciendo la exposición a la agresión, la probabilidad de que llegue la tortura será menor.

CAPÍTULO 1.10

La Seguridad en las zonas de conflicto armado

Objetivo:

Reducir los riesgos inherentes en las áreas de conflicto armado

El riesgo en situaciones de conflicto

Trabajar en zonas de conflicto expone a las y los defensores de derechos humanos a riesgos específicos, en especial en situaciones de conflicto armado: muchas de las muertes actuales de civiles se deben a prácticas de guerra indiscriminada, y muchas otras se deben al hecho de que la población civil es objetivo militar; es preciso que reconozcamos. La acción política es siempre necesaria para señalar estos hechos y luchar por ponerles fin.

Aunque no podemos controlar las acciones militares que se estén desarrollando, sí podemos adaptar nuestro comportamiento para así evitar que nos alcance el conflicto o bien para reaccionar adecuadamente.

Si estamos en una zona donde la acción armada es habitual, probablemente ya tendremos muchos de los contactos necesarios para protegernos, para proteger a nuestras familias y a la gente con la que trabajamos.

Sin embargo, si trabajamos en una zona de conflicto armado donde no estamos establecidas o establecidos, **de entrada habrá que recordar tres cuestiones:**

a ◆ ¿Qué nivel de riesgo podemos asumir? Esto también deben considerarlo las personas o a las organizaciones con las que trabajemos.

b ◆ Los beneficios de que estemos en la zona, ¿son mayores que los riesgos? Un trabajo de derechos humanos no puede mantenerse a largo plazo cuando se están corriendo grandes riesgos de manera continua.

c ◆ "Conocer la zona" o "saber mucho de armas" no nos protegerá si nos dispara un francotirador o quedamos atrapadas o atrapados por el fuego de morteros.

El riesgo de estar bajo fuego

Tipos de fuego

Podríamos ser objeto de ataques con rifles, ametralladoras, morteros, cohetes, bombas o misiles de tierra, mar o aire. Esos ataques podrían ir dirigidos a un objetivo concreto o ser de más amplio alcance, y podrían ir desde un francotirador o disparos desde un helicóptero con buena visibilidad a los ataques de morteros dirigidos o el fuego de artillería. También podrían ser del tipo saturación para 'pulverizar' toda una zona.

Cuanto más concreto sea el objetivo del ataque, menos riesgo corremos, suponiendo que no seamos ni nosotras o nosotros ni nuestra zona o una zona vecina el objetivo del ataque. Cuando sea así, retirarse de la zona reduce el riesgo que corremos. **Pase lo que pase, hay que recordar que si somos objeto de un ataque con arma de fuego, será difícil averiguar si es porque somos el objetivo o no. Saberlo, además, no es una prioridad,** como veremos.

Tomar precauciones: cómo reducir la posibilidad de que nos alcance un disparo

1 ◆ **Evitar los sitios peligrosos**

En zonas de guerra o de acción terrorista, hay que evitar tener nuestro centro de operaciones, la oficina, cerca de un objetivo posible, como un cuartel o una instalación de telecomunicaciones; y también hay que evitar pasar mucho tiempo cerca del mismo. Lo mismo es aplicable a zonas estratégicas como los puntos de entrada o salida en áreas urbanas, aeropuertos o lugares que sirven para controlar toda una zona.

2 ◆ **Protegerse bien**

Las ventanas que estallan en los edificios que nos rodean son una de las principales causas de daños físicos. Protegerlas con tablones o con cinta adhesiva puede reducir el riesgo de que esto ocurra. Así, en caso de ataque, hay que alejarse inmediatamente de las ventanas y tirarse al suelo, resguardarse bajo una mesa o preferiblemente en una habitación interior con muros gruesos; lo mejor, un sótano.

A veces es útil usar sacos de arena, pero sólo si otros edificios los tienen también porque de lo contrario podríamos estar llamando la atención.

Si no encontramos nada más, el suelo o cualquier zanja o boquete nos ofrecerá una protección mínima necesaria.

Un muro de ladrillo o la puerta de un coche no protege de los tiros, o de armas más pesadas. Los bombardeos o el lanzamiento de cohetes pueden cobrarse víctimas a varios kilómetros, por lo que cuando estalla un enfrentamiento armado hay que alejarse lo más posible.

Las explosiones pueden reventarnos los oídos: tenemos que tapárnoslos con las dos manos y abrir un poco la boca.

El que nuestra sede, el lugar donde estemos o nuestros vehículos sean fácilmente identificables puede ayudarnos pero sólo **si los agresores respetan nuestro trabajo.** Si no fuera así, estaríamos exponiéndonos innecesariamente. Si necesitamos identificarnos podemos improvisar una bandera o usar colores y señales en los muros o en el tejado (para el caso de ataques aéreos).

3 ◆ Qué hacer si estamos en un vehículo

Si nos encontramos en un vehículo que está siendo blanco de disparos, podríamos intentar evaluar la situación, pero va a ser muy difícil hacerlo bien. En general, **es útil asumir que el vehículo es o será un objetivo, y que lo mejor sería, por tanto, salir de él para buscar refugio de inmediato. Un vehículo es un objetivo muy claro.** Es vulnerable, y además de exponernos a los disparos, nos hace correr el riesgo de que nos hiera el cristal que salta en pedazos o de que explote el tanque de la gasolina. Si oímos tiros no demasiado cerca, podemos intentar seguir en el vehículo un poco más hasta algo que esté cerca y nos pueda servir de refugio.

Minas terrestres y armamento sin detonar (UXO, en inglés)[1]

Las minas terrestres y el armamento sin detonar (los UXOs) son una seria amenaza sobre la población civil de las zonas de conflicto. Pueden ser de los siguientes tipos:

- **Minas:**
  - Las minas antitanque se colocan en carreteras y pistas y, aunque estén diseñadas para destruir un tanque, pueden estallaral paso de un vehículo más ligero.
  - Las minas antipersona son más pequeñas y pueden aparecer en cualquier sitio de tránsito para la gente. La mayoría están enterradas. Hay que recordar que quienes ponen una mina en una carretera, probablemente minen también el campo o los senderos próximos.
- **Bombas trampa:**
  - Las bombas trampa son pequeños explosivos colocados en un objeto que parece normal o atractivo (con colores, por ejemplo) y que estallan cuando lo tocas. El término también se usa con minas vinculadas a un objeto que puede ser trasladado o activado (cualquier cosa desde un cadáver a un vehículo abandonado).
- **Los UXOs:**
  - El acrónimo inglés sirve para aludir a todo tipo de armamento o artillería que está sin explotar.

[1] Gran parte de la información de esta sección la hemos sacado del magnífico manual de Koenraad van Brabant, Operational Security Management in Conflict Areas (ver bibliografía).

En la actualidad hay un resurgir de las municiones de racimo. Hay casi tantas como minas anti-persona. Las municiones de racimo son restos de bombas de racimo sin explotar.[2] Cada bomba de racimo está compuesta de cientos de sub-municiones que se disparan en todas las direcciones. Están diseñadas para cubrir superficies grandes y explotar al chocar con algo. Pero no todas explotan depués de haber sido lanzadas, el porcentaje de fallo es elevado.[3] Además son más inestables que las minas y pueden, por tanto, explotar en cualquier momento. Algunas son de colores, por lo que atraen a los niños.

Cuidados a tener para evitar minas y armamento sin detonar

La única forma de evitar zonas minadas es saber dónde están. Si no vivimos o trabajamos en determinada zona, sólo podemos enterarnos preguntando con asiduidad si se han producido enfrentamientos armados o explosiones en esa zona a la gente que viva allí o a las y los expertos [4] en el tema. Siempre es mejor usar carreteras asfaltadas, carreteras normalmente transitadas y también seguir las pistas dejadas por otros vehículos. **No debemos abandonar la autopista, ni siquiera para ir al arcén, ni con o ni sin el vehículo:** las minas y demás material que no haya explotado puede pasar sin ser detectado muchos años y sin perder su capacidad de estallar.

Puede aparecer armamento sin detonar en cualquier zona donde se hayan producido enfrentamientos armados o se haya abierto fuego, y también puede ser visible. La regla de oro es: **No acercarse, no tocar, dejar una señal cerca e informar de inmediato.**

Suelen encontrarse bombas trampa en zonas que han sido abandonadas por los combatientes. En ellas, es imperativo no tocar ni mover nada, y no acercarse a los edificios abandonados.

[2] Ver Principes de droit de conflicts armés, Eric David (ULB, Brylant, 2002). Ver también las campañas recientes de Handicap International, Amnesty International etc; www.clustermunition.org, www.controlarms.org

[3] Se calcula que el porcentaje de fallo oscila entre el 5-80%, dependiendo del tipo de munición de racimo y del tipo de suelo (duro o blando), lo que las convierte, casi de hecho, en bombas anti-persona.

[4] ONGs especializadas en desactivar y quitar minas o Fuerzas de Paz de la ONU. Otras ONGs internacionales tiene también mapas de zonas con minas y de zonas donde se han desactivado o quitado las minas.

Si una mina explota bajo un vehículo o persona que está cerca

Hay dos reglas de oro:

- Donde hay una mina, habrá más.
- Nunca actuar impulsivamente, aunque haya personas heridas.

Si tenemos que marcharnos de allí, hagámoslo volviendo sobre nuestros pasos si vemos nuestras huellas. Si vamos en un vehículo y sospechamos que hay minas antitanque, debemos abandonar el vehículo y volver sobre nuestros pasos caminando sobre las huellas de los neumáticos.

Si nos vamos a acercar a una víctima o a alejar de una zona minada, la única manera de hacerlo es arrodillándose o tumbándose e ir insertando en la tierra muy cuidadosamente un trozo fino de madera o metal, en un ángulo de 30 grados, para ver si damos con un objeto duro. Si diéramos, debemos apartar con mucho cuidado la tierra de alrededor del mismo para ver qué es. Las minas también pueden estallar porque tropecemos con un alambre. Bajo ningún concepto deben cortarse los alambres.

Todo esto, sin duda, puede llevar mucho tiempo.[5]

[5] Hay manuales y recursos sobre el tema de las minas en la página web de la Campaña internacional para prohibir las minas terrestres (International Campaign to Ban Ladmines): www.icbl.org

CAPÍTULO 1.11

La Seguridad y la tecnología de la información y la comunicación

(Con la colaboración de Privaterra -www.privaterra.org)

Objetivo:

Los increíbles vacíos que existen en la tecnología de la información de todo el mundo también afectan a las defensoras y los defensores de derechos humanos. El presente capítulo se centra sobre todo en la tecnología de la información (ordenadores e Internet).[1] Algunas de sus partes no tendrán interés para quienes no tengan acceso a Internet, y/o no utilicen el ordenador; estas personas necesitarían, más bien, los medios y la formación necesarias para saber usar la tecnología de la información en la defensa de los derechos humanos.

Problemas de seguridad en las comunicación y cómo evitarlos

El conocimiento es poder, y saber qué problemas de seguridad podríamos tener en nuestras comunicaciones nos da más seguridad. Trataremos los temas relacionados con el acceso ilegal a nuestras informaciones y comunicaciones, o su manipulación, para luego plantear maneras de evitarlo.

Hablar con la gente

Acceder ilegalmente a una información no es algo que se haga únicamente por Internet. Cuando tengamos que hablar de temas delicados, habrá que considerar las siguientes cuestiones:

1 ◆ ¿Confiamos en las personas con las que estamos hablando?

2 ◆ ¿Necesitan saber todo lo que les estamos contando?

[1] Capítulo basado en el trabajo de Robert Guerra, Katitza Rodríguez y Caryn Mladen de Privaterra, una ONG que da cursos y asesoramiento a las y los defensores de derechos humanos de todo el mundo sobre temas de seguridad y tecnología de la información (TI). Este texto ha sido ligeramente adaptado en algunas partes por Marie Caraj y Enrique Eguren.

3 ◆ ¿Estamos en un lugar seguro? Los micrófonos y demás transmisores a menudo se instalan en zonas donde la gente cree estar segura, como despachos, calles muy concurridas, dormitorios y vehículos.

Podría ser difícil contestar a la tercera pregunta porque se pueden instalar micrófonos en una habitación para grabar o transmitir todo lo que se diga en ella. Los micrófonos láser, orientados desde grandes distancias a ventanas, pueden permitir también que se escuche lo que se está diciendo en un edificio. Podemos protegernos de ellos usando cortinas gruesas o instalando doble acristalamiento en las ventanas. Algunos edificios seguros tienen dos filas de ventanas para reducir el riesgo de ser alcanzados por esos aparatos de escucha.

¿Qué podemos hacer?

□ **Siempre partir de que nos pueden estar escuchando.** Con una actitud de sana paranoia tendremos más cuidado cuando estemos hablando de temas confidenciales.

□ **Los equipos para detectar aparatos de escucha** funcionan, pero es posible que ese servicio sea caro y difícil de conseguir. Además, a veces quienes lo ofrecen son ¡quienes han instalado antes esos micrófonos! Al ser contratados, o bien encuentran unos pocos micrófonos (baratos) que de hecho han puesto ahí para luego hacer que los encuentran, o, asombrosamente, no encuentran nada y nos comunican que la oficina está "limpia".

□ **El personal de la limpieza puede constituir una amenaza real a nuestra seguridad.** Tienen acceso a nuestras oficinas cuando ya no hay nadie, y se encargan de la basura. Por razones de seguridad, todo el personal debería ser cuidadosamente investigado con asiduidad (pues sus intenciones podrían variar después de haber entrado a trabajar para nuestra organización).

□ **Conviene cambiar a menudo la sala de reuniones.** Cuantas más habitaciones utilicemos para discutir asuntos e intercambiar información, quien nos quiera espiar tendrá que utilizar más recursos humanos y materiales.

□ **Cuidado con los regalos que suelen llevarse encima siempre,** como un bolígrafo caro o un broche, o con los que siempre están en la oficina, como un precioso pisapapeles o un magnífico cuadro. Estos tipos de objetos han sido empleados en el pasado para escuchar conversaciones.

□ **Partamos de que en un momento dado una parte de la información de que disponemos es ya conocida por quien nos espía.** Si cambiamos de planes o de códigos a menudo les estaríamos dando sólo fragmentos de información verdadera. También podemos considerar dar información falsa para comprobar si alguien la está usando o reaccionando a ella.

□ Para minimizar la eficacia de los micrófonos láser, podríamos **discutir los temas delicados en un sótano o en una habitación sin ventanas.** Algunos aparatos de escucha láser son menos eficaces durante las tormentas y similares.

□ **Una grabación de ruido blanco o una canción popular** interferirá la captación del sonido, lo que es útil para el caso de los aparatos de escucha exteriores, que pueden captar una conversación a 50 metros, aproximadamente. En

otras palabras, no es sólo que puedan poner micrófonos allí donde nos reunamos: sólo la tecnología más cara es capaz de limpiar una conversación de los ruidos aleatorios del ambiente.

- **Los espacios amplios y abiertos pueden ser lugares buenos o malos.** Quedar en un sitio apartado nos ayuda a darnos cuenta de si nos están siguiendo pero nos pone difícil el hacerles perder la pista porque no podemos "fundirnos en el paisaje". Los lugares bulliciosos sí nos permiten confundirnos entre la gente, pero también es cierto que se multiplica el número de personas que pueden vernos y oírnos.

- **Si la oficina o lugar de reunión está en una zona rural (abierta),** es bueno comprobar con alguien del grupo si se oye una conversación desde el exterior. Quedarse fuera también conviene para que tengamos vigilados a quienes no queremos que se acerquen a la reunión.

Teléfonos celulares/móviles

Cualquiera con suficiente capacidad tecnológica puede espiar una conversación telefónica, por eso debemos siempre partir de que ninguna llamada es segura. Los celulares/móviles analógicos son mucho menos seguros que los digitales, y ambos son a su vez mucho menos seguros que las líneas terrestres.

La vigilancia celular localiza nuestras llamadas además de escucharlas. Para que la llamada sea localizada, no hace falta que estemos hablando; basta con que tengamos encendido el móvil.

No debemos conservar nombres y números confidenciales en la memoria de nuestros teléfonos. Si nos lo roban, podrían usar esa información para localizar e implicar a personas que, de hecho, deseamos proteger.

Para las emergencias (y allí donde todavía sea posible), podríamos plantearnos tener dos números de teléfono de seguridad no identificados (tarjetas prepago) para establecer comunicación exclusivamente entre ellos y nunca para llamar o recibir llamadas de un número "conocido" (puesto que podría estar en una lista negra y descubrir así el nuestro). Nunca los utilizaríamos en sitios que se puedan relacionar fácilmente con nosotras o nosotros. Debemos acordarnos de sacar las tarjetas de esos móviles cuando no las estuviéramos usando, pues de lo contrario podrían ser rastreadas; además, conviene cambiarlas las dos regularmente. En cuanto a discreción en las conversaciones, hay que tener el mismo cuidado que cuando hablamos desde teléfonos más habituales.

Seguridad física de la información en la oficina

Siempre hay que cerrar la oficina con llave o cerrojo, tanto las puertas como las ventanas. Debemos usar llaves que requieran una autorización específica para hacerse una copia de ellas, y siempre habrá que saber dónde están y quién tiene las copias que se hayan hecho. Bajo ningún concepto debemos darle las llaves a terceras personas, ni siquiera al personal de mantenimiento o de la limpieza. Siempre que haya terceras personas en la oficina, deberá estar presente también alguien de nuestra total confianza. Si esto no fuera posible, tendría que ser

que al menos disponemos de una habitación de acceso restringido para guardar la información más sensible. Podríamos cerrar con llave todas las puertas de dentro de la oficina y dejar la basura fuera, en el pasillo, y sólo con los desperdicios no confidenciales.

Para material confidencial, debemos usar una trituradora que corte el papel en zig zag. Cuando sea especialmente sensible, conviene quemar las tiras de papel, desmenuzar las cenizas y luego tirarlas por el inodoro.

Medidas de seguridad básicas para ordenadores y archivos[2]

Cuando sea posible, cerrar con llave los ordenadores al abandonar la oficina. Las pantallas de los ordenadores nunca deben ser visibles desde las ventanas.

En todas las tomas de corriente eléctrica usaremos protección contra las sobrecargas (las variaciones en la corriente eléctrica pueden estropear los ordenadores).

Debemos guardar las copias de seguridad de la información, incluida la que esté en papel, en un lugar diferente y seguro. Para que estén bien protegidas, las guardaremos en el disco duro de un ordenador protegido con una clave encriptada, o usando cerrojos de máxima seguridad.

Para reducir el riesgo de que alguien entre en nuestro ordenador, debemos proteger el acceso a éste con una clave, y también acordarnos de apagar el ordenador cuando no vayamos a utilizarlo.

En caso de que alguien consiga entrar en nuestro ordenador, conviene tener los archivos encriptados.

Si nos roban el ordenador o queda destruido, podremos recuperar toda la información que contenía si hemos desarrollado la costumbre de hacer una copia de seguridad a diario. Habrá que recordar que las copias de seguridad encriptadas las tenemos que guardar fuera de la oficina en un lugar seguro.

También podemos usar un servidor externo para hacer una copia de la información usando Internet. Esto nos permite recuperarlo todo en caso de que nos quedemos sin el ordenador.

Los archivos que borremos no podrán recuperarse si usamos para destruirlos la utilidad para borrar archivos PGP Wipe o similares, en vez de enviarlos a la papelera de reciclaje del ordenador.

Nuestro ordenador podría estar programado para enviar fuera nuestros archivos, o bien dejarnos sin ellos, haciéndonos más vulnerables. Para evitar esta situación, conviene comprar el ordenador de una fuente segura. A continuación, reformatearemos el disco duro y sólo entonces procederemos a instalar el software que queramos. No debemos dejar que cualquiera manipule nuestro ordenador: sólo técnicos informáticos de nuestra confianza, y siempre estaremos presentes cuando nos lo estén arreglando.

[2] Para información más pormenorizada sobre seguridad informática, escribir a info@frontlinedefenders.org (Front Line) o a info@privaterra.org (Privaterra)

Deberíamos desenchufar el módem o la conexión telefónica del ordenador, o la conexión física a Internet, cuando no estemos usándolo. Así, ningún programa podrá intentar acceder a nuestro ordenador de noche. Siempre tenemos que desenchufar el ordenador cuando nos marchemos. Además, se puede instalar un software que desactiva el acceso al cabo de un tiempo (que determinaremos previamente) sin usarse el ordenador. Esto hace que la máquina no sea vulnerable cuando hacemos un descanso o vamos a hacer unas copias.

En nuestros Favoritos, podemos activar las extensiones de archivo para saber qué tipo de archivo vamos a abrir antes de abrirlo. Si creemos que vamos a abrir un archivo de texto y luego resulta que es un archivo ejecutable podríamos estar activando un virus. En el Explorador de Internet, ir al menú de Herramientas y elegir Opciones de carpeta. Hacer clic en la pestaña Ver y comprobar que NO está marcada la opción Ocultar las extensiones de archivo para tipos de archivo conocidos

Problemas de seguridad con Internet

Nuestros correos electrónicos no van directamente de nuestro ordenador al de quienes escribimos. Pasan por varios nodos y dejan un rastro de información que **puede ser seguido desde cualquier punto del recorrido** (¡no sólo en nuestro país!).

Al escribir un correo, podrían estar espiándonos por encima del hombro, sobre todo en un ciber café. Si nuestro ordenador está en red, cualquier persona que se encuentre en la oficina podría leerlo. La persona a cargo de la administración del sistema también puede acceder a los correos de todo el mundo.

Nuestro proveedor de servicios de Internet (el servidor; ISP en inglés) tiene acceso a todos nuestros correos. Si alguien tiene la capacidad para presionarle, nuestro servidor podría enviarle una copia de todo lo que pidiera, o impedir que correos que hubiéramos enviado lleguen a su destino.

Los correos, al viajar por Internet, pasan por cientos de terceras partes nada seguras. Los hackers pueden acceder a todos los correos cuando éstos se dirigen a su destino. Debemos recordar que el servidor de quienes van a recibir nuestros correos también puede ser vulnerable, así como sus redes u oficinas.

Medidas de seguridad básicas para Internet

Los virus y similares, como los troyanos, pueden venir de cualquier sitio, porque incluso personas amigas pueden estar difundiéndolos sin saberlo. Es fundamental instalar un buen programa antivirus y activar las actualizaciones automáticas que se producen cuando nos conectamos a Internet. Siempre se están creando y descubriendo nuevos virus: en la Virus Information Library (biblioteca de información sobre virus), www.vil.nai.com, podemos encontrar información sobre los últimos parches de protección.

Los virus son programas simples diseñados para reproducirse y pueden ser malignos o no. Los troyanos son programas diseñados para proporcionarle a una tercera parte (¡a cualquiera!) acceso a tu ordenador. Se suelen difundir por correo electrónico, por lo que es importante usar el correo adecuadamente (ver abajo).

Un buen cortafuegos (firewall) nos ayuda a ser invisibles ante los hackers y nos protege de los intrusos que pretenden entrar en nuestro sistema. También nos garantiza que sólo las aplicaciones autorizadas se conecten a Internet desde nuestro ordenador y evita que programas como los troyanos envíen información fuera o abran agujeros por los que cualquier hacker podría entrar.

Un sistema de key logger (registrador de teclas) puede rastrear todas las pulsaciones que hagamos en el teclado. Estos programas se propagan o bien porque alguien los instala en nuestro ordenador cuando no estamos, o bien por un virus o un troyano que haya atacado nuestro sistema desde Internet. Los key loggers averiguan cuáles han sido las teclas que hemos pulsado e informan de nuestras actividades, normalmente a través de Internet. Se combaten usando la protección de una clave, utilizando el correo electrónico de forma segura, instalando un programa antivirus, y usando un programa de teclado virtual para escribir nuestra clave con el ratón (aunque ya existen key loggers que descifran esto también). Se desactivan cuando desconectamos el acceso a Internet de nuestro ordenador físicamente (normalmente, desenchufando la conexión telefónica).

Una dirección de correo electrónico puede ser imitada (spoofing, o suplantación de identidad) o utilizada por alguien que no es quien la tiene de verdad. Esto se hace consiguiendo el acceso al ordenador y contraseña de la víctima, entrando como hacker en el servidor, o utilizando una dirección que se parece a la de esa persona, por ejemplo, cambiando una letra "l" por un número "1". La mayoría de la gente no notará la diferencia. Para combatir el spoofing, debemos titular los correos, para que quede claro que son nuestros, y podemos hacer también alguna pregunta que sólo el auténtico o la auténtica propietaria de ese correo sabría contestar. Ante cualquier petición sospechosa de información, debemos utilizar alguna otra forma de comunicación para comprobar que es fidedigna.

Cuando naveguemos por Internet, si queremos que nuestras visitas sean privadas, tendremos que no aceptar las cookies del sitio visitado o borrar nuestro caché después de usar Internet. En el Explorador de Internet, ir a Herramientas, después a Opciones. En el Navegador de Netscape, ir a Editar, después a Preferencias. En cualquier de estos menús, borraremos entonces toda nuestra historia, las cookies que podamos tener y vaciaremos nuestro caché. Debemos acordarnos de eliminar también nuestros favoritos. Los navegadores también guardan informes de los sitios que visitamos en los archivos caché, por lo que tendremos que averiguar qué archivos hay que borrar en nuestro sistema.

Conviene actualizar a todos los navegadores web a una versión más reciente que les permita funcionar con una encriptación de 128-bits. Esto nos ayudará a salvaguardar cualquier información que queramos transmitir de forma segura a través de la web, incluidas las contraseñas y demás datos confidenciales que usamos para rellenar formularios. Debemos de instalar los últimos parches de seguridad para todo el software que usemos, en especial de Microsoft Office, Microsoft Internet Explorer y Netscape.

No debemos utilizar un ordenador que contenga información sensible para navegar por sitios que no es esencial que visitemos.

Medidas de seguridad básicas con el correo electrónico

A continuación presentamos unas rutinas de seguridad para cuando usemos el correo electrónico y que todos y todas deberíamos asumir, tanto nosotros como nuestras relaciones personales y profesionales. Podríamos decirle a nuestros contactos que hemos decidido no abrir correos que no sigan estas pautas mínimas de seguridad.

1 ◆ NUNCA abrir un correo de alguien que no conozcamos.

2 ◆ NUNCA reenviar un correo de alguien que no conozcamos, incluso si éste nos ha sido a su vez reenviado por alguien que conocemos. También esos correos que circulan con "mensajes positivos" pueden contener virus. Al reenviarlos, podemos estar infectando los ordenadores de todo el mundo. Si alguno nos parece muy bueno y deseamos que más gente lo lea, tendríamos que abrir un nuevo correo y copiar el mensaje, mecanografiándolo. Si no podemos perder el tiempo en eso, no será tan importante...

3 ◆ NUNCA descargar o abrir un documento adjunto a no ser que sepamos lo que contiene y que es seguro. Debemos desactivar la opción del programa de correo electrónico que hace las descargas automáticas. Muchos virus y troyanos se propagan como "gusanos" y los gusanos modernos a menudo resultan haber sido enviados por alguien que conocemos. Los gusanos replicantes escanean nuestro listín de direcciones, en especial si usamos el Microsoft Outlook o el Outlook Express, y luego se envían solos disfrazados de adjuntos normales procedentes de nuestros contactos. Si usamos el programa PGP al firmar nuestros correos, tanto en los que van con adjunto como en los que no, podríamos ayudar a quienes reciben nuestros correos a tener menos dudas respecto a si el adjunto está libre de virus (el PGP es un software que encripta la información. Ver nota a pie de página abajo, en "La encriptación: preguntas y respuestas").

4 ◆ No escribamos los correos con HTML, MIME o texto enriquecido (.rtf; rich text): sólo con el texto, "texto sin formato". Los correos de texto enriquecido pueden contener programas que podrían facilitar el acceso a nuestros archivos del ordenador o que lo estropeen.

5 ◆ Si estamos usando el Outlook o el Outlook Express, conviene desactivar la opción de pantalla Mostrar panel de vista previa que está en el menú Ver - Diseño.

6 ◆ Encriptemos los correos siempre que nos sea posible. Un correo no encriptado es como una postal, puede ser leído por cualquiera. Un correo encriptado es como una carta en un sobre y dentro de una caja fuerte.

7 ◆ Es importante poner títulos con sentido a los mensajes para que quien los reciba sepa que han sido enviados intencionadamente. Podemos comentar con nuestros contactos que debemos usar la línea del asunto del mensaje para así poder reconocer rápidamente que el mensaje procede de tal o cual persona. Cuando no la reconozcamos, es posible que estemos recibiendo un correo del spoofing o que un troyano haya enviado un

programa infectado a toda la lista de correos, incluida nuestra propia dirección. Atención: en los correos encriptados no debemos añadir en el título palabras que desvelen ¡¡información sensible! Recordemos que la línea del asunto del mensaje no va encriptada nunca y que por tanto puede identificar la naturaleza del correo que hayamos encriptado, lo que nos haría más vulnerables a un ataque. Hoy en día existen muchos programas de espionaje que automáticamente escanean y copian mensajes con títulos como "interesante", "informe", "confidencial", "privado" y descriptores similares, que anuncian que el mensaje puede ser interesante.

8 ◆ NUNCA debemos enviar un mensaje a un grupo numeroso usando la línea del "Para" (destinataria/o(s)) o "CC" (con copia a). Cuando deseemos enviar algo a mucha gente, en la línea de "Para" copiaremos nuestra propia dirección y añadiremos las direcciones de los demás en la línea "CCO" (copia oculta a). (Para acceder a CCO es necesario ir a "Herramientas" y luego hacer clic en "Seleccionar destinatarios".) Esto no se hace sólo por cuestión de seguridad: es una cuestión de respeto a la privacidad: darle a otras personas la dirección de correo de alguien que no nos han autorizado a hacer tal cosa se considera una falta de educación, una falta de respeto y algo que nos puede dar un disgusto y poner en peligro.

9 ◆ NUNCA responder al spam, ni siquiera para pedir que nos borren de una lista. Los servidores de spam envían correos a listas interminables de direcciones y nunca saben cuáles están en uso. Cuando respondemos, el servidor nos reconoce como dirección válida y esto suele implicar que a partir de ese momento nos freirán a spam.

10 ◆ Si es posible, conviene tener un ordenador diferente, no conectado a ningún otro, para la recepción de correos y que no contenga archivos con datos.

11 ◆ Asimismo, podemos usar también dos direcciones sólo para nuestras comunicaciones internas (como con los dos números de teléfono para emergencias, y siguiendo las mismas reglas); o bien, una sola dirección que pueden consultar las personas de más confianza de la organización: los correos no tendrán que viajar varias veces (a varias personas) y sin embargo serán leídos por varias personas. Conviene recordar que cuantas más personas usen esa dirección, menos segura será. Es recomendable cambiar la dirección de vez en cuando.

La encriptación: preguntas y respuestas

A continuación respondemos a una lista de preguntas frecuentes. Podéis formular cualquier duda en la ONG Privaterra (www.privaterra.org).

P: ¿Qué es 'encriptar'?

R: Encriptar significa crear un código secreto para unos datos, para que nadie salvo quien deba recibir el mensaje pueda descifrarlo. Con tiempo y capacidad informática, todos los mensajes encriptados pueden descifrarse, pero hace falta

eso mismo: mucho tiempo y muchos recursos. Explicado de manera sencilla, encriptar es una forma de proteger nuestros archivos y correos de ojos que espían. Se traducen nuestros archivos a un código (un montón de números y letras aparentemente combinados al azar) que no tiene sentido para quien lo ve. Para encriptar un archivo, tenemos que "cerrarlo con llave", lo que se hace usando una clave. Para encriptar un mensaje podemos usar la criptografía asimétrica o de clave pública, que es la que usa dos claves, una pública y otra privada. Se cifra el mensaje con la clave pública pero sólo podrá descifrarlo la persona a la que va dirigido, que utilizará su clave privada.

P: ¿Por qué deberían encriptar información los grupos de derechos humanos?

R: Todo el mundo debería encriptar, porque la comunicación digital no es segura. No obstante, las personas que trabajan en derechos humanos corren más peligro que la mayoría de la gente, y sus archivos y comunicaciones contienen de hecho información confidencial; así pues, para protegerse y para proteger a las personas a las que intentan ayudar, es imperativo que encripten sus informaciones.

La tecnología digital es un beneficio para los grupos de derechos humanos, pues les facilita la comunicación, les hace ser más eficaces y les abre más puertas. No obstante, los beneficios no nos libran de los riesgos. Usar un cinturón de seguridad no implica necesariamente que vayamos a tener un accidente; conducir en una situación más peligrosa, como por ejemplo en una carrera, hace que usar un cinturón sea más necesario pues estamos corriendo más riesgos.

Las personas que trabajan en derechos humanos son vigiladas. Como los correos no encriptados pueden ser leídos por casi cualquiera, es casi inevitable que alguien vaya a leer nuestros correos no encriptados en algún momento. De hecho, es posible que nuestros oponentes ya estén leyendo nuestros correos y que no vayamos a enterarnos nunca. Conviene recordar que los oponentes de las personas a las que estamos intentando ayudar son también los nuestros.

P: ¿Es ilegal encriptar información?

R: A veces. En la mayoría de los países es perfectamente legal encriptar información. Sin embargo, existen excepciones. En China, por ejemplo, las organizaciones tienen que pedir un permiso para poder hacerlo, y si tu ordenador portátil dispone de tecnología para encriptar información, tienes que declararlo al entrar en el país. Singapur y Malasia tienen leyes que obligan a quienes encriptan información a desvelar sus claves a las autoridades. En India se están preparando leyes en ese sentido. Existen más excepciones.

En el Electronic Privacy Information Center (EPIC; centro para la privacidad de la información electrónica) podemos encontrar un estudio sobre las políticas de encriptación, el International Survey of Encryption Policy, en http://www2.epic.org/reports/crypto2000/, donde se examinan las leyes de casi todos los países. Actualizaron esta lista en el año 2000. Para solucionar dudas sobre si se puede o no usar la tecnología de encriptación en determinado país, podemos recurrir a Privaterra.

P: ¿Qué necesitamos para la seguridad de nuestros sistemas de tecnología de la información?

R: Depende de nuestro sistema y de nuestras actividades. No obstante, en general, deberíamos disponer de:

- Un cortafuegos (firewall).
- La posibilidad de encriptar nuestros discos.
- Un programa (como PGP - ver nota abajo) para encriptar y firmar digitalmente el correo electrónico.
- Software para la detección de virus.
- Copias de seguridad: podemos enviar por correo electrónico todos los materiales a un sitio seguro, además de hacer copias de seguridad semanales en un CD-RW (CD reescribible) que guardaremos en un lugar distinto y seguro.
- Claves de las que podamos acordarnos pero que no puedan ser adivinadas.
- Un sistema de acceso a nuestra información: no todo el mundo en la organización necesita tener acceso a todo tipo de información en nuestros archivos.
- Coherencia: no podemos usar unos recursos y otros no; ¡si no los usamos todos todo el tiempo, ninguno funcionará!

No obstante, tener el software adecuado no basta. **Normalmente, son las personas y no la tecnología nuestro punto más débil.** Encriptar información no sirve de nada si las personas no usan el recurso como debieran, si le dan sus claves a cualquiera, o las dejan a la vista, por ejemplo, en un post-it pegado a la pantalla del ordenador. El software para hacer copias de seguridad no sirve de nada (p.e., ante la eventualidad de un fuego o un ataque o redada) si no guardamos esas copias en un lugar diferente y seguro. La información confidencial tenemos que darla con cuentagotas (saber lo estrictamente necesario) y no contársela a todo el mundo en la oficina... por eso hay que crear jerarquías y protocolos. En general, es importante tener en cuenta los temas de privacidad y seguridad en cada cosa que hagamos en el día a día. A esto es a lo que llamamos "una sana paranoia".

P: ¿Cómo elijo el software para encriptar?

R: Normalmente, preguntando a las amistades; y podéis confirmarlo con nosotros. Tenemos que hablarlo con ciertas personas y grupos, así, si están usando determinado sistema para encriptar, podríamos elegir el mismo para facilitar nuestra comunicación. No obstante, conviene comprobar las cosas con otra fuente (p.e., nosotros): algunos paquetes de software no sirven para lo que están hechos y otros son "zanahorias". Las zanahorias nos atraen para que usemos un software gratuito y aparentemente excelente que de hecho nos está proporcionando gente que desea espiarnos. ¿Qué puede ser mejor para acceder a nuestras comunicaciones más sensibles que ser quienes están a cargo de super-

visar nuestro software de encriptación? De todos modos, existen muchas marcas buenas tanto de software que se compra como de freeware; lo único es que debemos examinarlo bien antes de usarlo.[3]

P: ¿Encriptar puede incrementar el riesgo de que caigan sobre nosotros/as?

R: Nadie sabrá que estamos usando un programa de encriptación a no ser que ya nos estuvieran vigilando. Si fuera así, ya habrían leído nuestra información privada, por lo que ya sabrían cómo descifrarlo todo; ya estarían sobre nosotros. Si quienes nos vigilan no van a poder leer nuestros correos, quizá deberíamos considerar qué otras medidas podrían adoptar, por lo que cuando empecemos a encriptar debemos conocer bien a nuestras y nuestros compañeros, que llevemos con la máxima cautela el tema de las copias de seguridad y que sigamos todas las medidas de seguridad acordadas en la oficina.

(Nota: No disponemos de información de casos en los que el uso de software para encriptar haya causado problemas a las y los defensores. No obstante, debemos considerar esta posibilidad antes de empezar a encriptar, especialmente si nos encontramos en un país con un conflicto armado (la inteligencia militar podría sospechar que estamos pasando información importante desde el punto de vista militar) o si pocas organizaciones de defensoras o defensores usan la encriptación (podría atraer una atención no buscada).

P: ¿Por qué habría que encriptar documentos y correos todo el tiempo?

R: Si sólo encriptamos materiales sensibles, quienes nos estén vigilando o nuestros clientes sabrán cuándo la actividad es confidencial, y será más probable que caigan sobre nosotros entonces. Aunque la información encriptada no pueden leerla, sí pueden saber qué archivos están encriptados y cuáles no. Si de pronto hay una tanda de documentos encriptados, esto podría provocar un ataque o redada, por eso es mejor empezar a encriptar antes del comienzo de proyectos especiales. De hecho, lo óptimo es que la comunicación sea regular: podemos enviar correos encriptados regularmente aunque no haya nada nuevo que comunicar; de este modo, cuando tengamos que enviar información sensible, no se notará tanto.

P: Si tenemos un cortafuegos (firewall), ¿por qué habría que encriptar los correos?

R: Los cortafuegos evitan que los hackers accedan a nuestro disco duro y a nuestra red; sin embargo, cuando enviamos un correo a Internet, éste queda expuesto al mundo entero. Por tanto, habría que protegerlos.

P: No ha entrado nadie en la oficina, ¿por qué habría de usar software de privacidad?

R: No sabemos si estarán entrando en nuestro sistema o sacando información de él. Sin comunicación encriptada, seguridad física o protocolos de privacidad,

[3] Por ejemplo, el PGP (Pretty Good Privacy; privacidad bastante buena) es un programa bastante conocido y seguro. Su finalidad es proteger la información enviada por Internet usando la criptografía de clave pública, y también se usa para autentificar documentos con firmas digitales. Se puede bajar de http://www.pgpi.org/.

cualquiera podría estar accediendo a nuestros archivos, leyendo nuestros correos, y manipulando nuestros documentos sin que lo sepamos. Si nuestra comunicación es abierta podríamos estar poniendo a otras personas en peligro allí donde los ataques o redadas de motivación política ocurren con más probabilidad. Si usamos buenos cerrojos en las puertas, deberíamos encriptar nuestros archivos; es así de simple.

P: No tenemos acceso a Internet y tenemos que ir a un ciber café. ¿Cómo podemos proteger nuestras comunicaciones si utilizamos un ordenador de fuera?

R: A pesar de eso, podemos encriptar los correos y nuestros archivos. Antes de ir al ciber, encriptaremos todos los archivos que vayamos a enviar por correo electrónico y copiaremos la versión encriptada en el CD o disquete. En el ciber, nos registraremos en un servicio de encriptación de correo electrónico, como el de www.hushmail.com, o en un servicio de anónimos, como www.anonymizer.com, y enviaremos nuestros correos desde allí. Recordatorio: quienes reciben estos correos deben ser también usuarias o usuarios de este servicio.

P: Si es tan importante proteger nuestros archivos y nuestras comunicaciones, ¿por qué no lo hace todo el mundo?

R: Esta tecnología es bastante nueva. Aun así, su uso se está popularizando. Los bancos, las multinacionales, las agencias de noticias y los gobiernos lo encriptan todo: lo ven como una inversión sensata y uno de los precios de poder hacer negocios. Las ONGs corren riesgos más graves que las compañías pues a estas últimas las reciben con los brazos abiertos casi todos los gobiernos. Una ONG, con toda probabilidad, será objeto de vigilancia, por lo que las ONGs tienen que ser capaces de poner la tecnología a su servicio. Además, quienes defienden los derechos humanos se preocupan por proteger a personas y grupos que están siendo perseguidos. Para hacerlo, guardan bien los archivos que pueden identificar y localizar a esas personas. Si resulta que se puede tener acceso a esos archivos, estas personas pueden ser asesinadas, torturadas, secuestradas o se las podría "convencer" de que no vuelvan por la ONG en cuestión. La información de estos archivos puede ser también utilizada como prueba contra la ONG y sus clientes en persecuciones políticas.

P: Uno de nuestros principios es la transparencia. Nuestro trabajo incluye presionar al gobierno para que sea también más transparente en sus actuaciones. ¿Por qué tenemos que usar una tecnología de la privacidad?

R: El respeto a la privacidad es coherente con el ser abiertas/os. Si el gobierno desea pedirnos abiertamente nuestros archivos, puede hacerlo, siguiendo procedimientos adecuados y conocidos. Lo que la tecnología de la privacidad evita es que puedan acceder a nuestra información de manera clandestina.

P: Seguimos todos los protocolos de seguridad y privacidad y aun así se filtra información, ¿qué está pasando?

R: Podríamos tener una o un infiltrado en la organización o sencillamente a alguien incapaz de entender que una información sea confidencial. Trabajaremos la jerarquía creada para el tratamiento de la información para conseguir que

menos personas tengan acceso a la información más sensible y vigilaremos estrechamente a esas pocas personas. Las grandes compañías y organizaciones distribuyen cada cierto tiempo, como parte de su trabajo habitual, fragmentos de información falsa a personas concretas que van variando. Si esta información falsa se filtra, la fuente puede ser localizada de inmediato pues sabemos a quién le dimos tal o cual información.

Lo que podemos y no podemos hacer al usar la encriptación

- **SÍ** encriptarlo todo, todo el tiempo. Si sólo encriptamos material confidencial, quien nos esté vigilando el correo sabrá cuándo algo importante va a ocurrir. El que de pronto haya muchos documentos encriptados cuando no suele haberlos puede provocar un ataque o redada.

- **NO** poner información clave en los títulos de los correos. Aunque el mensaje vaya encriptado, la línea del asunto del mensaje no suele ir encriptada.

- **SÍ** utilizar una clave hecha con letras, números, espacios y puntuación que sólo tú puedes recordar. Algunas técnicas para crear claves seguras son trazar dibujos en el teclado o elegir palabras al azar intercalando símbolos. Por lo general, cuanto más larga sea, más segura será.

- **NO** usar una sola palabra o nombre, una frase conocida o una dirección de nuestro listín de direcciones como clave. Las descifran en cuestión de minutos.

- **SÍ** hacer una copia de seguridad de la clave privada (el archivo que contiene nuestra clave privada para encriptar) y guardar, encriptada, en un solo sitio seguro y diferente, como un disquete o en una memoria USB, pequeña y extraíble.

- **NO** enviar material sensible a alguien sólo porque esa persona nos ha enviado un correo encriptado usando un nombre que podemos reconocer. Cualquiera puede imitar un nombre (spoofing) haciendo que su dirección de correo se parezca a la de alguien que conocemos. Siempre hay que verificar la identidad de la fuente antes de confiar en ella: la comprobaremos comunicándonos en persona, haciendo una llamada telefónica o enviando otro correo.

- **SÍ** enseñar a otras personas a encriptar. Cuanta más gente lo use, más seguras y seguros estaremos todos.

- **NO** olvidar firmar el mensaje además de encriptarlo. Queremos que la destinataria o el destinatario sepa si nuestro mensaje ha sido modificado en su tránsito.

- **SÍ** encriptar archivos que se envíen como adjuntos por separado. Por regla general, no se encriptan automáticamente cuando enviamos un correo encriptado.

Gestión más segura de la oficina

El tema de la seguridad en la oficina tiene relación con nuestras costumbres, que pueden ser útiles para nuestra seguridad o peligrosas. Para desarrollar costumbres útiles, tenemos que entender las razones que hay detrás. Hemos elaborado una lista de hábitos que pueden ayudarnos a gestionar la información de una manera más segura. Pero esto sólo ocurrirá si desarrollamos esas rutinas y conocemos su importancia.

¿Qué es lo más importante para la privacidad y la seguridad en la gestión de la oficina?

- Ser conscientes de qué información tenemos y de quién tiene acceso a ella
- Desarrollar rutinas de seguridad y utilizarlas siempre
- Usar las herramientas adecuadamente

Administración

Muchas organizaciones tienen una persona a cargo de la administración de sistemas, o alguien con la responsabilidad y función administrativa de acceder al correo, a los ordenadores en red, y de supervisar la instalación del nuevo software. Si alguien abandona la organización o no está disponible, esta persona puede entonces acceder a la información y asuntos pendientes de quien se ha ido, dando así continuidad y evitando que el trabajo quede a medias o interrumpido. Además, es alguien que se encarga de que todo el software esté limpio y proceda de una fuente acreditada.

El problema radica en que algunas organizaciones piensan que este papel es meramente de apoyo técnico y permiten que una tercera parte se encargue de este trabajo. Este administrador o administradora controlaría de hecho toda la información de la organización, por lo que tendría que ser alguien que disfrute de total confianza en la organización. En algunas organizaciones las labores de administración las comparten la persona que representa a la organización y otra persona de confianza.

Algunas organizaciones recogen en un documento todas las claves privadas PGP, las encriptan y las guardan en un lugar seguro y distinto (una organización de su confianza). Esto evita problemas si a alguien se le olvida su contraseña o pierden su clave privada. No obstante, el lugar donde se guarden esos archivos tiene que ser un sitio totalmente seguro y confiable, y se deben crear protocolos concretos y exhaustivos respecto al acceso a esos archivos.

Las reglas:

1 ◆ NUNCA poner la administración de nuestros sistemas en manos de terceras partes. No solo no merecen la confianza que podamos darle a gente de nuestra organización; sino que puede ser difícil ponerse en contacto con ellas si se produce una emergencia.

2 ◆ Sólo las personas más fiables deberían tener acceso a la administración de nuestros sistemas.

3 ◆ Hay que determinar a cuánta información puede acceder quien(es) asuma(n) la administración: acceso a todos los ordenadores, a sus claves, a las claves de acceso, a las carpetas protegidas y a las claves del uso de PGP, etc.

4 ◆ Si decidimos guardar una copia de las claves y de las claves privadas de PGP en otra organización, tendríamos que desarrollar protocolos de acceso a las mismas.

5 ◆ Cuando alguien se marche de la organización, será preciso cambiar de inmediato sus claves y códigos de acceso.

6 ◆ Cuando alguien de la administración deje la organización, será preciso cambiar de inmediato TODAS las claves y códigos de acceso.

Administración del software

Usar programas piratas puede hacer que la organización quede vulnerable a lo que llamamos "la policía del software". Las autoridades pueden caer sobre una organización que use software ilegal, imponiéndola el pago de multas ingentes e incluso cerrándola. La organización en cuestión no recibirá apoyo de los medios de comunicación occidentales porque esto no se verá como un ataque a una ONG de derechos humanos, sino como una actuación contra la piratería. Debemos tener muchísimo cuidado con el tema de las licencias del software, y no permitir que nadie haga copias de cualquier cosa en la oficina. El software pirata es inseguro también porque contiene virus. Hay que usar siempre un antivirus cuando estemos instalando software.

Quien esté a cargo de la administración tendrá que supervisar la instalación de cualquier programa nuevo, para que podamos comprobar que todo está bien antes de hacerlo. No debemos autorizar la instalación de programas potencialmente inseguros, y sólo debemos instalar los programas que necesitemos utilizar.

Es preciso instalar los últimos parches de seguridad que tengan todos los programas que utilicemos, en especial del Microsoft Office, del Microsoft Internet Explorer y el Netscape. La más grave amenaza a nuestra seguridad procede del software y del hardware que ya tienen puntos débiles conocidos. Mejor aún, podríamos considerar pasarnos al software libre que no se rige por el modelo "seguridad a través de la oscuridad", sino que anima tanto a las y los expertos en seguridad como a las y los hackers a que sometan todos sus códigos a un riguroso examen. Usar el software libre y cualquier software que no sea el de Microsoft tiene el beneficio añadido de hacernos menos vulnerables a los virus más comunes y a los hackers que no tienen un objetivo específico. Se crean menos virus para los sistemas operativos de Linux o Macintosh porque casi todo el mundo usa Windows. Outlook es el programa de correo más utilizado, y por lo tanto, el objetivo más común para los hackers.

Hábitos con el correo electrónico

Deberíamos desarrollar la costumbre de encriptar los correos. Es más fácil acordarnos de encriptarlo todo que tener una política sobre qué se encripta y qué no. No debemos olvidar que si encriptamos siempre nuestros correos, quien lo esté vigilando nunca sabrá cuando nuestras comunicaciones son más importantes o sensibles.

Unos cuantos puntos importantes más:

- Si guardamos una copia de un correo encriptado, la copia debe estar encriptada también. Siempre la podemos desencriptar después; sin embargo, si alguien accede a nuestro ordenador y no lo hemos hecho, la información sería tan vulnerable como si nunca la hubiéramos encriptado.

- Debemos perseverar en nuestro esfuerzo por asegurarnos de que nadie con quien nos comuniquemos usando correos encriptados se dedique a reenviarlos después de desencriptarlos, o a respondernos sin molestarse en encriptar su propio correo. La pereza individual es la más grave amenaza a nuestras comunicaciones.

- Podría ser útil crear varias cuentas seguras para gente que esté en misiones de campo, cuentas que al no tan utilizadas, no serían tan fácilmente identificadas por los servidores de spam. Estas direcciones deberían ser verificadas regularmente, pero no utilizadas, salvo por quienes estén en la misión de campo. De esta manera podríamos destruir las direcciones de correo que están recibiendo mucho spam sin poner en peligro nuestra base de contactos.

Consejos generales para ciber cafés y similares

Los correos que enviamos por Internet en texto sin formato y sin encriptar pueden ser leídos por muchas partes diferentes, si se lo proponen. Una de estas partes puede ser nuestro servidor (Internet Service Provider, ISP) pero también podría hacerlo cualquier servidor por el que pasen nuestros correos. Un correo pasa por muchos servidores en su viaje de remitente a destinatario/a, ignorando las fronteras geopolíticas. Puede pasar por servidores de otro país cuando estamos enviando un correo dentro del país.

Unos consejos generales sobre temas que normalmente no entienden bien las y los usuarios de Internet:

- Proteger un archivo con una contraseña hace tan poco para proteger ese archivo que no merece la pena hacerlo con documentos que contienen información confidencial. Sólo da una falsa sensación de seguridad.

- Comprimir un archivo no lo protege.

- Si queremos enviar un archivo o un correo protegiéndolo, tenemos que encriptarlo (ver www.privaterra.com).

- Si queremos enviar un correo o un documento de forma segura, tenemos que encriptarlo todo en todas las fases del proceso hasta la recepción final. No sirve de nada enviar un correo encriptado, por ejemplo, desde un proyecto de campo a la oficina de Nueva York o Londres o donde sea, y después que se reenvíe ese correo desde ésta ¡sin encriptar!

- Internet es global por naturaleza: no existe ninguna diferencia entre enviar un correo entre de una oficina a otra en Manhattan y enviar un correo desde un ciber café de Sudáfrica al ordenador de una oficina de Londres.

- Debemos encriptar tanto como nos sea posible, incluso si el correo o los datos **no** son confidenciales.

- Debemos comprobar que el ordenador que estamos usando dispone de un programa de protección de los virus. Muchos virus se diseñan para extraer información de nuestro ordenador, ya sea de nuestro disco duro o de los archivos de nuestro correo electrónico, lo que incluye además nuestro listín de direcciones.

- Debemos comprobar que nuestro software tiene todas las permisos que debe tener. Si estamos usando software sin licencias de ningún tipo, de manera inmediata, a ojos de los gobiernos y los medios de comunicación, pasamos a ser piratas y dejamos de ser activistas de derechos humanos. La mejor opción es la de usar software libre (¡es gratis!).

- No hay una solución segura al 100% si estamos usando Internet. Hay que ser conscientes de que una persona puede entrar ilegalmente en un sistema haciendo que es alguien que no es, por teléfono o por correo electrónico. Debemos usar nuestro criterio y sentido común en todo momento.

- Debemos recordar que los interesados en nuestro trabajo no han necesitado esperar a las nuevas tecnologías para tratar de obtener información sobre nosoros.

Resumen

Recordar que las partes interesadas en nuestro trabajo no han esperado a las tecnologías para intentar conseguir información sobre nosotras o nosotros.

Muchas personas dedicadas a la defensa de los derechos humanos son reticentes a usar tecnologías de la información seguras; sin embargo, los procedimientos básicos para poder hacerlo son sencillos.

Esos procedimientos mínimos y sencillos son: discreción por teléfono y en la comunicación en persona, usar PGP en la comunicación por correo electrónico y con los archivos confidenciales, y las contraseñas para acceder a nuestros ordenadores.

No obstante, tener el software adecuado no lo es todo: **nuestro punto débil son normalmente las personas, no la tecnología.**

SEGUNDA PARTE

SEGURIDAD DENTRO DE LA ORGANIZACIÓN

INTRODUCCIÓN:

En la segunda parte del Manual nos centraremos en la seguridad a nivel de organización, es decir, en cómo mejorar la seguridad dentro de las organizaciones de defensores.

Seguridad/protección no quiere decir solamente tener un plan de seguridad. Hace falta controlar todo el proceso, empezando con la mejora del nivel original de seguridad dentro de la organización, para aplicarla, y después gestionar la mejora del proceso en sí mismo.

Estar en control de todo el proceso forma parte de la seguridad.

El proceso de seguridad dentro de la organización es pragmático y global.

Tiene que ser realista y apropiado para el perfil de la organización.

Y, aunque hacen falta recursos, cambiar el comportamiento es gratis y es un factor fundamental en la mejora de la seguridad.

CONTENIDOS DE LA SEGUNDA PARTE:

CAPÍTULO 2.1

Cómo Valorar las actuaciones de una organización en materia de seguridad: la rueda de la seguridad

Objetivo:

Valorar nuestra manera de gestionar los temas de seguridad

Evaluar hasta qué punto la seguridad está integrada en nuestro trabajo de defensa de los derechos humanos

Para conseguir estos objetivos, sugerimos que se parta de dos enfoques:

- Cómo nos percibimos: valorar desde dentro de la organización nuestras actuaciones en materia de seguridad: analizar y evaluar el tema tras reunir información objetiva. El proceso podría ser colectivo y/o individual. Puede ocurrir que diferentes miembros de la organización lleguen a muy distintas conclusiones sobre cómo funciona la organización en materia de seguridad y sería interesante detenerse en eso también.

- Cómo nos perciben: pensar sobre qué perciben los demás respecto a nuestra organización en relación con el tema de la seguridad.

Valoración del tema de seguridad desde dentro de la organización

La rueda de la seguridad

La rueda de la seguridad y sus ocho ejes nos puede ser útil para valorar objetivamente el tema de la seguridad desde dentro de la organización.

Para girar, una rueda tiene que ser redonda; sus ejes deben ser todos de la misma longitud. Lo mismo ocurre con la rueda de la seguridad y sus ocho ejes o componentes, que representan la gestión de la seguridad en una organización o grupo de defensoras o defensores.

La valoración podríamos hacerla en grupos:

- Dibujar una rueda con ocho radios.
- Sombrear cada porción según el nivel de desarrollo del radio (ver líneas punteadas del diagrama).

- Usando la lluvia de ideas, buscar razones que expliquen por qué hay porciones menos desarrolladas; como todas deben ser de la misma longitud que la más desarrollada, hacer propuestas para conseguirlo: establecer objetivos y procesos relevantes, anticipar posibles problemas y proponer soluciones.
- Al terminar el ejercicio, guardaremos nuestra rueda de la seguridad para compararla con otra que hagamos al cabo de unos meses y así averiguar si se han producido mejoras en cada uno de los puntos.

Los 8 radios de la rueda de la seguridad:

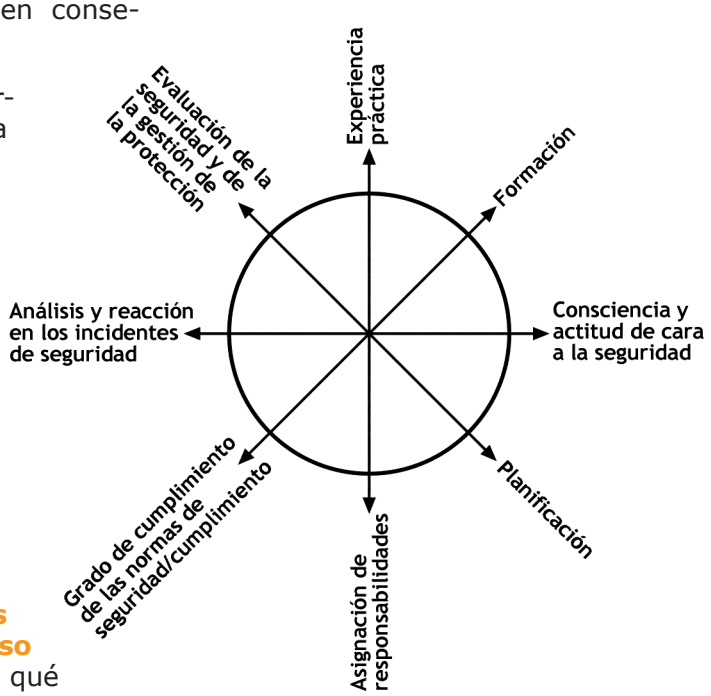
Experiencia y cohesión adquiridas: conocimientos prácticos y compartidos en materia de seguridad y protección adquiridos durante nuestro trabajo. Son los extremos inicial y final de la valoración.

Formación: formación en temas de seguridad adquirida ya sea en cursos o gracias a nuestra propia iniciativa en el trabajo diario.

Sensibilización y actitud: se refiere a si las personas y la organización en su conjunto comprenden lo importante que es abordar la cuestión de la seguridad y la protección, y si están dispuestas a actuar en consecuencia.

Planificación: incorporación del tema de la seguridad y la protección a los planes que guían nuestro trabajo.

Reparto de responsabilidades: ¿quién es responsable de qué aspecto de la seguridad y la protección? ¿Y qué ocurre si hay emergencias?



Respeto a las reglas (y compromiso con ellas): ¿hasta qué punto se respetan las reglas y procedimientos establecidos en materia de seguridad?

Análisis de los incidentes de seguridad y respuestas a los mismos: ¿hasta qué punto es cierto que se analizan los incidentes de seguridad? ¿Son adecuadas las reacciones de la organización?

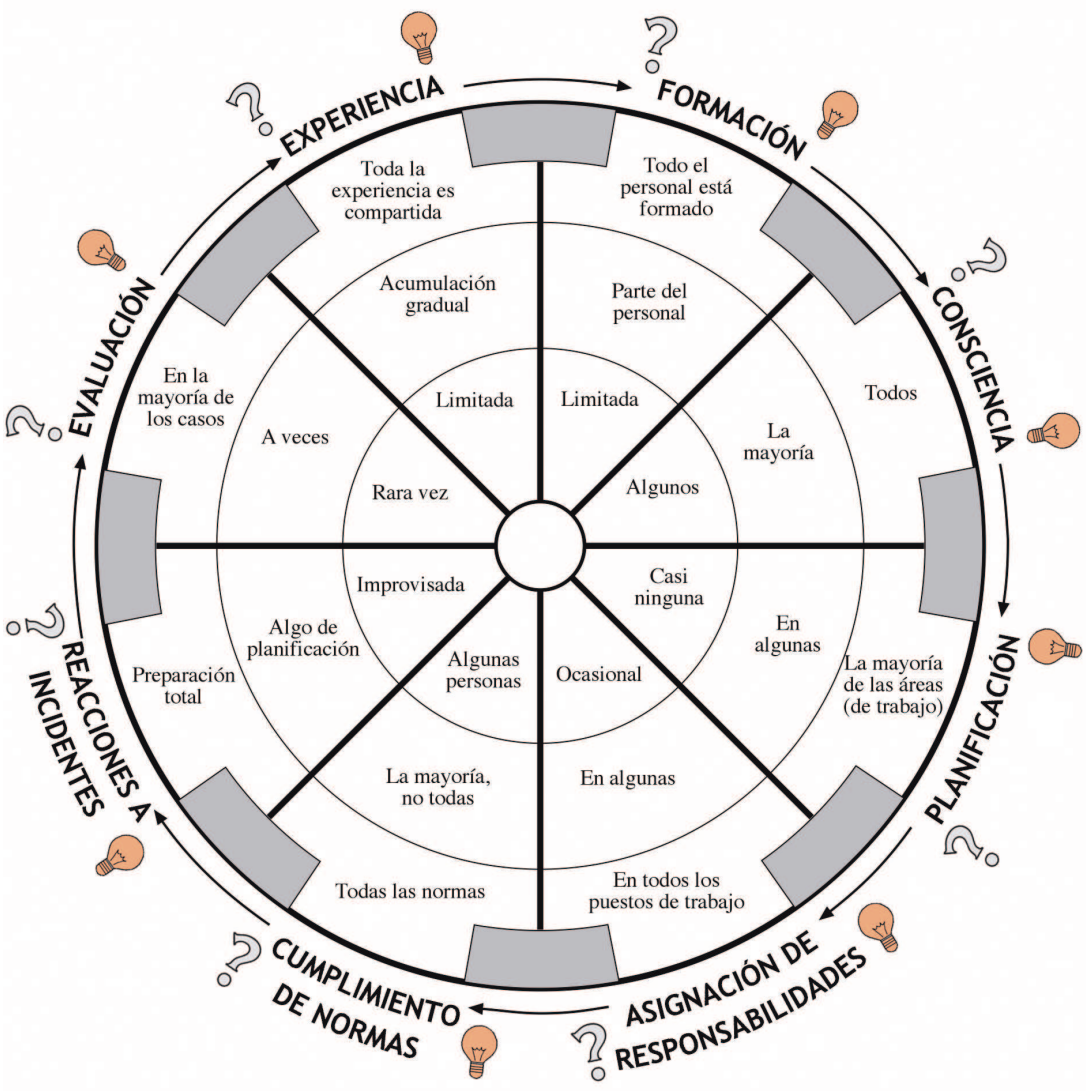
Evaluación de la gestión: ¿evalúa la organización su gestión de los temas de seguridad y protección?, ¿los revisa / actualiza?

A continuación presentamos un ejemplo del uso de la rueda de la seguridad:

La rueda de la seguridad nunca nos sale perfecta: algunos radios estarán más desarrollados que otros. Por eso es fundamental determinar el nivel de desarrollo de cada componente. De esta manera, podremos identificar qué tipos de actuaciones tienen que pasar a ser prioritarias para que podamos mejorar nuestra protección y seguridad. Las líneas de puntos que van del centro al borde exterior ilustran cómo de desarrollada está esa componente de la rueda.

Problemas posibles relativos a esta parte de la rueda...

... y posibles soluciones a esos problemas



Fotocopiar la rueda en papel o acetato y sombrear las zonas entre los radios para representar visualmente el estado de la rueda en nuestro grupo u organización. Así podremos ver mejor el nivel de desarrollo de cada componente.

Análisis de la rueda de la seguridad paso a paso

Hacer una valoración en toda regla de la política de seguridad de una organización requiere tiempo porque es preciso examinar el significado de todos y cada uno de los componentes de la rueda de la seguridad.

1 ● Experiencia en temas de seguridad y cohesión adquiridas durante el trabajo y las puestas en común:

Conocimiento práctico acumulado y cohesión en temas de seguridad y protección. El punto inicial y final de nuestra valoración.

Recordemos que la experiencia de unos cuantos miembros no es equiparable a la experiencia adquirida al nivel de organización, sino más bien a la suma de la de todas y todos los miembros: por lo tanto, compartir nuestras experiencias contribuye a mejorar la cohesión en materia de seguridad.

El conocimiento total quedará reflejado en los radios; cuando hayamos desarrollado todos los componentes al punto que deseamos, el conocimiento total habrá crecido. El radio de la experiencia en temas de seguridad estará entonces mejor desarrollado, con toda probabilidad, y tendremos que pasar a desarrollar los demás. La actividad no será nunca definitiva, por la simple razón de que las y los miembros de la organización van y vienen continuamente, el contexto político cambia, y también lo hacen las cuestiones de seguridad. No obstante, para el caso de este radio, como es el resultado del desarrollo de los otros siete, para éste en concreto no tendremos que hacer nada (aunque sí para los otros siete).

2 ● Formación en materia de seguridad

Marcaremos la formación en seguridad que hayamos recibido en algún curso o que hayamos desarrollado en nuestras iniciativas en el trabajo.

Preguntas para analizar:

¿Puede todo el mundo recibir formación en seguridad? ¿Actualizamos o mejoramos esos conocimientos? ¿Se le ofrece formación a las y los nuevos miembros? ¿Qué dificultades enfrentaríamos si deseáramos formar a todo el mundo? ¿Cuáles son las posibles soluciones?

3 ● Sensibilización en temas de seguridad y desarrollo de las actitudes adecuadas

Preguntas utilizadas para determinar el nivel de sensibilización de ese momento:

¿Tiene todo el mundo alguna noción de la importancia del tema de seguridad y la protección? ¿Cómo podríamos conseguir que así fuera? (Ser consciente de algo no implica actuar en consecuencia; por ejemplo, las personas que fuman saben que fumar es peligroso pero siguen haciéndolo).

Preguntas para sensibilizar:

¿Qué factores nos llevan a revisar los temas de seguridad?

¿Qué historias se cuentan y qué conocimiento informal existe en la organización en materia de seguridad?

¿Qué problemas podríamos tener si intentáramos sensibilizar sobre este tema? ¿Qué soluciones podríamos aplicar?

4 ● Planificación:

Cuestiones para determinar el nivel de planificación en materia de seguridad en ese momento:

- Cuando planificamos nuestro trabajo, ¿integramos en él las cuestiones de seguridad y protección?
- ¿Lo tiene integrado la organización en su visión (misión, planes estratégicos, áreas de trabajo, temas transversales)?
- ¿Tiene el tema de la seguridad un lugar en nuestras agendas (al menos en las reuniones más importantes y no como último tema)?
- ¿Cuál es la estrategia presupuestaria (¿ad hoc, o incluida en otras?) y cómo se gestiona financieramente del tema?
- ¿Analizamos el entorno de trabajo (en grupos de trabajo y a nivel local, regional y nacional)?
- ¿Analizamos el impacto de nuestro trabajo y cómo nos perciben los actores que podrían constituir una amenaza?
- ¿Realizamos un análisis completo de los riesgos: amenazas, puntos vulnerables y capacidades?
- ¿Compilamos todos los documentos de seguridad: revisamos su contenido y vemos cómo se usan?
- ¿Hacemos una primera versión de los documentos de seguridad y los actualizamos? (Comprobar si están al día y cómo podemos ponerlos al día).
- ¿Comprobamos si el impacto del trabajo y los factores de riesgo han sido tenidos en cuenta? (Comprobar si hay vías operativas para poder hacer consultas cotidianas sobre seguridad).

Nuestros planes de seguridad:

- ¿Son claros y sencillos? ¿Contienen toda la información necesaria y en un lenguaje comprensible para todo el mundo?
- ¿Han sido diseñados en cooperación con las personas implicadas?
- ¿Son apropiados para los diferentes contextos del trabajo?

- ¿Son mejorados, desarrollados y actualizados gracias a la iniciativa de diferentes personas del grupo de trabajo?
- ¿Son verdaderos y están adaptados al "mundo real"?

Nuestros planes de seguridad, ¿tienen en cuenta...?

- ¿Todos los puntos necesarios?
- ¿La comunicación, la tecnología de la información (TI) y la gestión de la información?
- ¿La gestión del personal (incluido su reclutamiento o contratación)?, ¿la gestión del estrés?

¿Es todo el mundo consciente de que un grupo de trabajo con una buena estructura, una buena dinámica de comunicación interna, buenas relaciones públicas y una buena capacidad de cooperación constituye un requisito básico de seguridad?

Preguntas para desarrollar más el plan de seguridad:

¿Qué problemas enfrentaríamos si intentáramos abordar cada uno de los puntos anteriores?

¿Cuáles podrían ser las soluciones?

5 ● Atribución de responsabilidades:

Preguntas para determinar el nivel que tenga en ese momento la cuestión de la atribución de responsabilidades en materia de seguridad:

- ¿Sabemos con claridad quién es responsable de qué aspecto de la seguridad y la protección? ¿Y en caso de emergencia?
- ¿Tienen las y los trabajadores y colaboradores responsabilidades y deberes para con la organización (incluido su comportamiento fuera del trabajo y la familia)?
- ¿Asume todo el mundo su responsabilidad en materia de seguridad y existen responsabilidades concretas para los diferentes temas de la seguridad? (¿Con qué dificultades nos topamos?).

Preguntas para mejorar la asignación de responsabilidades en temas de seguridad:

¿Qué problemas encontraríamos si quisiéramos asignar y compartir las responsabilidades en materia de seguridad?

¿Qué soluciones podríamos darles?

Asignar responsabilidades ayuda a que compartamos la cuestión de la seguridad.

6 ● Nivel de compromiso con el cumplimiento de las normas de seguridad:

Preguntas para determinar el nivel de compromiso que se tiene en ese momento con el cumplimiento de las normas de seguridad:

• ¿Hasta qué punto respeta la gente las normas y procedimientos que se han establecido en materia de seguridad?

• ¿Hasta qué punto participa cada cual y el grupo en su conjunto en la elaboración del plan de seguridad y se compromete con el cumplimiento de las normas de seguridad y protección?

• ¿Sabemos cuándo no se están respetando las normas de seguridad? Si no lo sabemos, ¿a qué se debe esto?

• ¿Respetamos las normas de seguridad por miedo a que nos llamen la atención o porque somos conscientes de que seguirlas va a reducir los riesgos a que nos vemos expuestas o expuestos?

Preguntas para mejorar el nivel de compromiso con el cumplimiento de las normas de seguridad:

¿Qué problemas encontraríamos si deseáramos mejorar el nivel del respeto a las reglas?

¿Qué soluciones podríamos darles?

7 ● Análisis de los incidentes de seguridad y reacciones

Preguntas utilizadas para determinar el nivel que tenemos en cuanto a análisis de los incidentes de seguridad y en cuanto a nuestras reacciones:

• ¿Hasta qué punto estamos analizando los incidentes de seguridad, y hasta qué punto es la reacción de la organización adecuada? ¿Qué incidentes ocurrieron? ¿Cómo se manejó esa situación y qué daños se produjeron?

• ¿Redactamos informes (y cómo)?

• ¿Hacemos análisis (cómo y a qué nivel)?

• ¿Qué comentarios y críticas nos hacemos (fechas para tener terminados procesos o tareas, vías para aportarnos valoraciones y críticas, cuestión de las responsabilidades)?

• ¿Qué evaluación hacemos de nuestros comentarios y críticas?

• La formación dentro de la organización, ¿parte del análisis de los incidentes? (¿Hay formación? ¿Existen canales en la organización para que la haya o pueda haberla?).

• En resumidas cuentas, ¿qué se hace con los incidentes?

• ¿Existe un procedimiento para recoger información, investigar y analizar los incidentes de seguridad con el fin de crear una batería de comentarios y críticas que nos sirva de base a la hora de elaborar nuestras estrategias y planes? ¿Se integran las conclusiones en nuestro trabajo y evaluaciones (allí donde proceda)?

• ¿Existen planes claros y un reparto claro de responsabilidades para saber reaccionar en caso de emergencia?

• ¿En qué tipo de emergencia son aplicables?

Preguntas para mejorar el tema del análisis de incidentes de seguridad y las reacciones:

¿Qué problemas existen cuando se intenta mejorar cada una de las situaciones enumeradas anteriormente?

¿Qué soluciones podemos darles?

8 • Valoración de la gestión en temas de seguridad y protección:

Preguntas para determinar el nivel en ese momento de cómo se valora la gestión de la seguridad y la protección:

• ¿Hasta qué punto evalúa la organización su gestión de la seguridad y la protección, y hasta qué punto la actualiza?

• ¿Es esta valoración parte de las actividades rutinarias de la organización?

• ¿Somos conscientes de lo necesario que es que se haga una valoración desde el punto de vista de la seguridad del trabajo y las reacciones producidas en el día a día en torno a los incidentes de seguridad para así enriquecer nuestro conocimiento y experiencia como individuos y como organización?

Preguntas para mejorar la valoración de la gestión en materia de seguridad y protección:

¿Qué problemas encontraríamos si deseáramos mejorar el tema de nuestra valoración de la gestión de la seguridad y la protección?

¿Qué soluciones podríamos darles?

Cómo nos perciben

Nuestra imagen y el tema de la seguridad

Es importante que recojamos información sobre qué imagen tiene nuestra organización en el contexto donde trabajamos y si esa imagen es la que queremos dar como organización. También es importante averiguar cómo perciben los demás que tratamos los temas de seguridad y protección en nuestra organización. Podemos hacer el análisis partiendo de diferentes puntos de vista:

- Desde el punto de vista de la gente con la que trabajamos: contrapartes y beneficiarias y beneficiarios.
- Organizaciones similares a la nuestra.
- Organizaciones e instituciones que financian proyectos (algunas pueden ser más receptivas que otras).
- Las autoridades con las que tenemos contacto.
- Otros actores que podrían ser potenciales agresores.
- ...

Asimismo, es importante determinar con fiabilidad el nivel de cooperación que existe en temas de seguridad con otras organizaciones y redes, con contrapartes, con las personas con las que trabajamos, etc.

Aquí presentamos dos listas no exhaustivas de preguntas útiles, por temas:

I ◆ Imagen de la organización e impacto del trabajo de la organización. ¿Cómo podríamos valorarlo?

- ¿Qué podemos hacer para enterarnos de qué imagen da nuestra organización?
- ¿Cómo explicar nuestro trabajo a otras personas?
- ¿Cuál es el propósito de la organización?
- ¿Cuáles son nuestras actividades?
- ¿Cómo les afectan a los actores armados o a otros?
- ¿Qué capacidades o poder tenemos para mantener nuestro espacio de trabajo?
- ¿Qué hacemos para conservarlo?
- ¿Cómo creemos que nos percibe nuestro potencial agresor?
- ¿Se nos percibe como una organización que maneja bien los temas de protección y seguridad en relación con su trabajo?
- ¿Existe alguien que critica nuestro trabajo o cómo llevamos nuestro trabajo desde un punto de vista de la seguridad? ¿Por qué? ¿Cómo lo sabemos?

II ◆ Imagen de la organización e impacto del trabajo de la organización. ¿Cómo nos perciben?

Intentar responder a estas cuestiones desde los diferentes puntos de vista de otros actores (repetir el ejercicio con todas y cada una de las partes que consideremos necesario analizar. Recordar que "ellos/as" somos nosotras/os y "nosotros/as" es la parte cuyo punto de vista estamos investigando.)

- ¿Quiénes son?
- ¿Qué expectativas tienen?

- ¿Qué hacen? (su trabajo)
- ¿Cómo frenan nuestro trabajo? ¿Qué límites nos ponen?
- ¿Qué podemos hacer? ¿Cómo podemos protegernos?
- ¿Cómo podemos conseguir lo que queremos?

Una vez hayamos valorado la percepción de otras personas necesitamos ver cómo podríamos cambiar nuestra imagen si ésta no se ajusta a la realidad. No podremos cambiarlas todas, esto es evidente. En cualquier caso, ser conscientes de ellas nos ayudará mucho, porque esas percepciones podrían afectar a nuestra seguridad y protección.

Resumen

Para valorar nuestra seguridad tenemos que partir de dos puntos: autocrítica (mirarnos en el espejo) y valoración de cómo nos perciben los demás.

La **autocrítica** podemos hacérnosla usando la rueda de la seguridad con sus ocho porciones:

Será como una instantánea de nuestro nivel de seguridad y protección en ese momento dado.

Nos permite ser conscientes de qué temas necesitan ser más trabajados para que la rueda tenga ejes de la misma longitud y por tanto, ruede.

Para desarrollar nuestra rueda de la seguridad tenemos que empezar con un inventario de la situación en ese momento dado, establecer los objetivos y decidir qué procesos de mejora vamos a emprender. Intentaremos predecir los obstáculos que podríamos hallar en nuestro progreso hacia nuestros objetivos, y también las soluciones que podríamos darles.

Una valoración de **cómo nos perciben los demás** podemos hacerla intentando imaginar cómo hablan de nosotras y nosotros.

También podríamos pasarle un cuestionario a las partes con las que tengamos una buena relación.

Tendríamos que hallar la manera de transformar las percepciones erróneas de nuestro trabajo. No podremos cambiarlas todas, esto es evidente. En cualquier caso, ser conscientes de ellas nos ayudará mucho, porque esas percepciones podrían afectar a nuestra seguridad y protección.

CAPÍTULO 2.2

Cómo Asegurarnos de que se respetan las normas y los procedimientos de seguridad

Objetivo:

Pensar sobre qué es lo que hace que las organizaciones y sus miembros no puedan o no quieran seguir planes y procedimientos de seguridad, y buscar soluciones adecuadas para cada caso.

La seguridad es asunto de todo el mundo

La cuestión de si la gente y las organizaciones siguen de verdad las normas y los procedimientos de seguridad es un tema complicado: podemos disponer de un buen plan de seguridad, con sus normas preventivas y sus procedimientos de emergencia, tener el tema como uno de los puntos principales de nuestras reuniones más importantes, etc., y sin embargo vivir la situación de que la gente no está cumpliendo con las normas de seguridad de la organización.

Parece increíble, pues las y los defensores de derechos humanos están siempre bajo presión y amenazas, pero ocurre.

Si alguien quiere averiguar algo sobre nuestro trabajo, no lo hará acercándose a la persona más cuidadosa de la organización; preferirá recurrir a quien se suele emborrachar los sábados por la noche. De manera parecida, si alguien quiere darle un susto a nuestra organización, probablemente no atacarán a quien haya tomado todas las precauciones necesarias; irán a por quien descuide a menudo su propia seguridad, aunque también podrían atacar a una persona cuidadosa que ha sido víctima del descuido de la no cuidadosa, que dejó la puerta abierta... La cuestión es que los descuidos de una persona pueden poner en más peligro a todo el mundo. El nivel de seguridad vendrá determinado por el elemento más débil, en este caso, la negligencia de una persona.

Por esta razón el tema de la seguridad debería ser asunto de toda la organización al completo, y también de las personas a quienes implica. Si sólo 3 de 12 personas siguen las normas de seguridad, toda la organización, incluidas las personas que sí siguen las normas, corre peligro. Si la situación mejora y 9 personas empiezan a seguir los procedimientos de seguridad, el riesgo se reduce, pero sería menor aún si las 12 personas siguieran las normas.

El tema de la seguridad debería ser asunto de toda la organización al completo, y también de las personas a quienes implica.

Tener un buen plan de seguridad no sirve de nada si no se respeta. Seamos realistas: mucha gente no sigue las normas o procedimientos. Esta falta de cumplimiento viene a ser la diferencia entre las buenas intenciones y las prácticas reales. Sea cual sea el caso, es mucho más fácil enfrentarse a este problema que a sus posibles consecuencias.

¿Por qué la gente no cumple con las normas de seguridad y cómo podemos evitarlo?

En primer lugar, la palabra "cumplimiento" es a menudo asociada a las ideas de sumisión y docilidad, por lo que deberíamos evitarla. La gente sólo sigue las normas que entiende y acepta porque las ha hecho suyas. Así, la mejor manera de expresar esta cuestión sería hablando del 'nivel de compromiso con el cumplimiento de las normas'.

Para que un procedimiento de seguridad sea seguido, todo el mundo en la organización tiene que hacerlo suyo. Esto no ocurre de manera automática. Para que las y los miembros del grupo hagan suyo un procedimiento de seguridad deben haber podido participar en su diseño y puesta en práctica. La formación, comprender y asumir el procedimiento, es otro de los aspectos cruciales.

Tabla 1:
La relación entre individuos y organizaciones en términos de seguridad

Concepto	Enfoque: "¡Tenéis que obedecer las normas!"	Enfoque: "Todas y todos hemos creado estas normas para nuestra organización."
Enfoque	Normativista	Basado en las necesidades en materia de seguridad de las personas y de la organización
Tipo de relación entre el individuo y la organización	Normativa o "paternalista"	Basada en el diálogo
¿Por qué seguimos las normas?	Por obligación, para evitar la expulsión o la sanción	Para observar un acuerdo, que podamos ir criticando y mejorando(el nivel de compromiso con el cumplimiento de las normas y la persuasión se consiguen cuando estamos convencidas/os de que la norma se ajusta a nuestras necesidades, que disminuirá la viabilidad y las consecuencias de un riesgo y que contribuirá a protegernos, tanto a las personas de la organización como a aquellas con o por quienes trabajamos)
Compromiso con la seguridad	No compartido	No compartido

El nivel de compromiso con el cumplimiento de las normas no significa sólo que se "cumpla con las normas": significa establecer un acuerdo sobre las normas que hará que todas y cada una de las personas las respeten porque las entienden, las consideren adecuadas y eficaces y sientan que tienen un interés personal en su cumplimiento. Por esta razón, además de sus necesidades básicas, las normas deben tener en cuenta también los criterios éticos y morales de cada persona (evitando exclusividades y siempre según las normas de los derechos humanos).

El nivel de compromiso con el cumplimiento de las normas no significa sólo "cumplir con las normas": nos habla de la capacidad de respetar un acuerdo sobre seguridad entre la organización y sus miembros.

Con objeto de mantener el acuerdo entre la organización y sus miembros, es importante que **cada persona que esté a cargo de alguna tarea relativa a la seguridad trabaje por mantener implicadas e implicados a los demás,** con sesiones informativas, recordándoles aspectos del acuerdo y preguntándoles qué opinan sobre la eficacia de las normas en la práctica.

No obstante, dicha implicación tendrá poco valor si no existe una **cultura de seguridad** en la organización, la cual sostenga procedimientos y programas de trabajo formales e informales.

En resumen, la base necesaria para que la gente observe las normas y procedimientos de seguridad se puede conseguir siguiendo los siguientes pasos:

- Conseguir comprender en profundidad que la protección de víctimas, testigos, familiares, compañeras y compañeros de trabajo es un tema importante de seguridad del que depende que podamos seguir adelante con lo fundamental de nuestro trabajo.
- Desarrollar una cultura de seguridad de la organización y aprender a valorarla.
- Generar un nivel de compromiso con el cumplimiento de las normas y los procedimientos de seguridad.
- Hacer posible que todo el grupo participe en el diseño y en la mejora de las normas y los procedimientos de seguridad.
- Ofrecer formación en materia de seguridad.
- Comprobar si todo el grupo está convencido de que las normas y procedimientos de seguridad adoptadas son adecuadas y eficaces.
- Redactar y suscribir un acuerdo entre la organización y sus miembros sobre las normas y procedimientos de seguridad.
- Implicar a quienes tienen responsabilidades en el tema de la seguridad en que ofrezcan sesiones informativas y de formación, le recuerden al grupo el acuerdo suscrito si procede, y recojan sus opiniones sobre si las normas son adecuadas o eficaces en la práctica.

¿Por qué no se respetan las normas y los procedimientos de seguridad?

No existe un prototipo de defensor o defensora de derechos humanos que no respeta las normas. Lo que suele ocurrir es que la mayoría de la gente de una organización respeta unas normas y otras no, o bien, que se siguen las normas en determinadas ocasiones.

Existen muchas razones posibles que expliquen estos hechos. Para poder transformar la situación y así conseguir el nivel de compromiso con el cumplimiento de las normas que necesitamos es importante determinar por qué ocurre esto y buscar soluciones con las personas implicadas. Asimismo, será conveniente escuchar las razones que pueda tener cada cual para no respetar las reglas, porque varían.

Algunas razones posibles para no observar las normas y procedimientos de seguridad:

No intencionadas:

El defensor o la defensora...

- No sabe que existe esa norma;
- No sabe aplicar las normas.

Intencionadas:

Problemas generales:

- Las normas son demasiado complicadas y difíciles de seguir.
- La descripción de los procedimientos no está a la mano en la oficina, o se explican de una manera que los hace difíciles de usar en el día a día.

Problemas individuales:

- Las normas son contrarias a las necesidades o intereses del individuo y este conflicto no ha sido resuelto.
- La persona no está de acuerdo con todas o algunas de las normas, y las considera innecesarias, inadecuadas o ineficaces en función de su experiencia personal, información previa o formación, o por sus creencias.

Problemas de grupo:

- La mayoría de las personas del grupo no sigue las normas o las o los "líderes" del grupo no lo hacen, o no lo hacen lo suficiente, porque no existe una cultura de la seguridad en la organización;
- Una falta general de motivación en el trabajo puede llevar a la gente a ignorar las normas de seguridad.

Problemas de la organización:

- No existen suficientes recursos económicos o técnicos para facilitar a las y los miembros del grupo que sigan las normas.
- Existe una contradicción entre las normas y las áreas concretas del trabajo. Por ejemplo, quienes se encargan de coordinar los temas de seguri-

dad han establecido normas que están siendo ignoradas o mal aplicadas por las personas que trabajan en los programas o recogida de testimonios / informes. Unas normas pueden valer para un área de trabajo y no valer para otra.

- Las y los miembros del grupo tienen mucho trabajo y poco tiempo, por lo que no consideran prioritario cumplir con las normas, o al menos con algunas de ellas.

- Una falta general de motivación, que surge del estrés, de las peleas en de la organización, etc.

La cultura de la organización es tanto formal como informal, y debe ser desarrollada no sólo en la organización en su conjunto, sino también en sus equipos. Cuando existe una buena cultura de organización se nota: surgen las conversaciones espontáneas, las bromas, las fiestas, etc.

Cómo supervisar la observancia de las normas y procedimientos de seguridad

Supervisión directa:

Se puede tener una lista con las normas y procedimientos de seguridad y marcar las que se han seguido en tal o cual tema de trabajo; también pueden usarse en las reuniones de antes y después de las misiones de campo, en nuestros informes, en las agendas de nuestras reuniones, etc.

Con el equipo, se podrían hacer repasos periódicos sobre temas como la seguridad de los archivos de información confidencial, las copias y los manuales de seguridad; los protocolos de seguridad para visitas a la sede de la organización; la preparación de las misiones de campo, y demás.

Supervisión indirecta:

Para saber si la gente conoce las normas, si las acepta o si existe algún área de desacuerdo que deberíamos tratar, podemos preguntar qué opina cada cual de las normas y procedimientos, si les parecen adecuadas o fáciles de seguir. También podríamos comprobar si las y los miembros del grupo están usando el manual de seguridad o los materiales que recogen los protocolos y normas existentes.

Merece la pena reunir y analizar, con la gente o los equipos en cuestión, los comentarios y valoraciones que hacen todas esas personas sobre las normas y los procedimientos de seguridad. Esto también podemos hacerlo sin dejar constancia escrita de ello o con la ayuda de una tercera parte.

Revisión a posteriori:

Podemos repasar los temas de seguridad analizando los incidentes de seguridad según vayan surgiendo. Esto hay que hacerlo con especial cuidado en caso de que quienes hayan estado involucradas o involucrados en el incidente puedan estar pasándolo mal al pensar que se produjo por su culpa, y/o al pensar que se les va a sancionar por ello. Eso les podría llevar a no dar ciertos datos importantes que nos permitan usar el incidente para mejorar los temas de seguridad.

¿Quién supervisa?

Dependiendo de cómo funcione la organización, puede ser:

- Quien sea responsable de organizar el tema de la seguridad o áreas concretas del trabajo dentro de la seguridad.
- O quien tenga funciones directivas en la organización (y supervisa la seguridad además de otros aspectos del trabajo).

¿Qué podemos hacer si las normas y procedimientos de seguridad no están siendo respetados?

1 ◆ Determinar las causas de por qué es así, buscar las soluciones y ponerlas en práctica. Podemos usar la lista de opciones del Tabla 1 anterior como guía.

2 ◆ Si el problema es intencionado y de un individuo, debemos intentar:

a • Entablar un diálogo con esa persona para determinar la causa o motivos.

b • Trabajar con todo el equipo de esa persona (en ocasiones esto puede ser una mala opción, por lo que habrá que considerar si procede).

c • Utilizar un sistema de avisos o apercibimientos, para que la persona se dé cuenta de que existe un problema.

d • Utilizar un sistema de sanciones que podría culminar en expulsión o despido.

3 ◆ Debemos incluir una cláusula sobre observancia de las normas y procedimientos de seguridad en todos los contratos de trabajo, con objeto de que todas las personas que trabajen en la organización sean plenamente conscientes de lo importante que es este tema.

En conclusión,

Existen personas que piensan que discutir las razones por las que la gente no respeta las normas de seguridad es perder el tiempo, al haber asuntos más importantes o urgentes que tratar. Quienes así piensan, creen, por regla general, que las normas están ahí para ser obedecidas, punto. Otras personas son conscientes de que el mundo no siempre funciona así.

Al margen de lo que creamos individualmente, os invitamos a que os detengáis un momento y analicéis el grado en que las normas y procedimientos de seguridad son respetados en la organización u organizaciones donde trabajáis. Quizá os sorprendan los resultados de esa investigación, y podría merecer mucho la pena con vistas a evitar problemas en el futuro...

Resumen

La seguridad es asunto de todo el mundo.

La seguridad es un tema de la organización y también de cada persona que trabaja en la organización.

Tenemos que ser conscientes de por qué la gente no sigue las normas de seguridad. Entre las razones posibles están:

No intencionadas
(problema individual).

Intencionadas
(problemas general, individual, de grupo o de organización).

Saber cuáles son nos ayudará a saber cómo lidiar con ellas.

No obstante, se recomienda disponer también de un órgano que supervise el tema (supervisión directa, indirecta y retrospectiva).

Es fundamental desarrollar una cultura de seguridad en la organización.

CAPÍTULO 2.3

cómo Gestionar la mejora de la política de seguridad en la organización

Objetivo:

Aprender a gestionar el cambio dentro de la organización hacia una política de seguridad mejorada.

Pasos y temas en torno a los cuales construiremos el proceso:

- Mejorar la gestión de la estrategia de seguridad
- Mejorar el proceso de aplicación de la gestión de seguridad
- Identificar el punto de entrada. ¿Qué parte de la organización será responsable de él? ¿De dónde partiremos? ¿Cómo procederemos? ¿Cómo llevaremos las cosas a la práctica? ¿Cuáles son los puntos a favor y en contra? ¿Y los obstáculos?

Cómo manejar los problemas de seguridad: la gestión de la seguridad paso a paso

La gestión de la seguridad es un proceso que requiere constantes actualizaciones; siempre pragmático, parcial y selectivo. Esto se debe a lo siguiente:

- No podemos trabajar más que con una cantidad limitada de información: no podemos reunir y tratar al mismo tiempo todos los factores que afectan al tema de la seguridad.

- Es un proceso complejo: requiere mucho tiempo y el trabajo de concienciación, llegar a consensos, formarnos, preparar el traspaso de funciones (rotación), desarrollar las actividades, etc.

La gestión de la seguridad rara vez puede aspirar a desarrollar una perspectiva general total a largo plazo. Lo que aporta es que evita ataques y hace énfasis en la necesidad de que elaboremos estrategias para abordarlos. Puede que este objetivo no parezca muy ambicioso, pero no podemos olvidar que demasiado a menudo los recursos que se destinan al tema de la seguridad son insuficientes.

Cuando examinamos las prácticas de seguridad de un o una defensora, o de una organización, encontramos siempre algún tipo de directrices, planes, medidas o patrones de comportamiento; y también fuerzas en sentido opuesto, que irán desde las ideas estereotipadas sobre las prácticas de seguridad a la reticencia a aumentar la cantidad de trabajo existente con nuevas actuaciones en materia de seguridad.

La práctica de la seguridad es típicamente un trabajo fragmentado e intuitivo siempre en construcción. La gestión de la seguridad tendría el objetivo de realizar cambios paso a paso para mejorar nuestra actuación. Las normas y procedimientos de seguridad tienden a surgir en las áreas concretas del trabajo de una organización, como en sus necesidades logísticas, el equipo que hace trabajo de campo y que está especialmente preocupado por su seguridad, o de un directivo al que los donantes están presionando para saber cómo está el tema de la seguridad, etc.

La gestión de la seguridad paso a paso abre la puerta a los procesos informales y ofrece espacio para que puedan adoptarse nuevas prácticas. Acontecimientos repentinos, como los incidentes de seguridad, provocarán la toma de decisiones urgentes, a corto plazo, que, si son bien gestionadas, podrán ir dando forma a prácticas de seguridad más a largo plazo dentro de la organización en su conjunto.

Mejora de la estrategia de seguridad: posibles puntos de entrada

Una vez hemos determinado que necesitamos mejorar el tema de la seguridad, tenemos que iniciar el proceso. Para ello, buscaremos algún punto de entrada (ya sea fuera o dentro de la organización):

Dentro de la organización:

- nivel directivo o de coordinación
- nivel intermedio o ejecutivo
- plantilla y/o base/miembros
- una combinación de todas estas posibilidades

Fuera de la organización:

- donantes
- compañeras/os, contrapartes
- organizaciones similares que trabajan en la misma red

Comparemos sus ventajas y desventajas

Posibles puntos de entrada para promover la necesidad de cambios	**Ventajas**	**Desventajas**	**Posibles soluciones**
Puntos de entrada **dentro** de la organización			
Nivel directivo o de coordinación (Dirección, junta directiva o líderes)	• Capacidad para convocar reuniones o asambleas generales • Con memoria histórica • Autoridad moral • Apoyo institucional • ...	Cómo se les percibe: • Imponen las cuestiones de seguridad y generan desinterés por ser demasiado formales, rígidos, distantes, paternalistas... • Creen que el tema de la seguridad sólo les corresponde a ellos • Lo descartan porque no lo consideran una prioridad • ...	• Reuniones o asambleas generales • ...
Nivel intermedio / ejecutivo	• Con visión de los niveles superior e inferior • Fácil acceso a ambos • Canal de comunicación cotidiana con ambos niveles • Comunicación • Capacidad técnica para llevar a cabo los cambios en materia de seguridad • ...	• A menudo no existe este nivel • Enfoque parcial: centrarse en un área • Posible distracción por intereses profesionales personales • "Demasiado" técnicos/as si no tienen contacto con actividades de campo o las más políticas • ...	• Procedimientos de participación (tanto hacia el nivel directivo o de coordinación como hacia las y los miembros en general). • ...
Plantilla o base / miembros, ...	• Pueden movilizar a la gente • Conocen los mecanismos y detalles del trabajo diario • ...	• Podrían tener problemas con las o los directores / coordinadores o con la jerarquía • ...	• En general, como grupo, reconocer el problema, la necesidad de que todo el mundo aporte, y de soluciones. Después, delegar la búsqueda de soluciones a un grupo de trabajo • ...
Puntos de entrada desde **fuera** de la organización			
Donantes, organizaciones a las que se pertenece, ...	• Más distancia • Sin intereses directos • Podrían tener una experiencia más completa • Podrían convocar reuniones con cualquiera o todos los niveles mencionados sin sufrir un conflicto de intereses • ...	• Podrían tener problemas de credibilidad o no conocer apenas el trabajo que se está haciendo • Podría ser difícil ponerse en contacto con ellos (proceso demasiado "técnico") • ...	• Señalar intereses comunes en materia de seguridad • La organización donante prefiere invertir en una organización que cuida la seguridad en vez de arriesgarse a perder su inversión en una organización que ignora estas cuestiones. • El tema de la seguridad entre organizaciones depende de que se compartan las mismas actitudes y normas en materia de seguridad

El proceso de entrada puede ser puesto en práctica por todas las organizaciones, al margen de su tamaño, estabilidad, ubicación.

¿Qué parte de la organización es responsable del proceso de mejora?

Una vez hallado el punto de entrada (todo el mundo es más consciente de la necesidad de mejora y se pretende hacer algo al respecto), alguna parte de la organización tendrá que dirigir el proceso. ¿Quién/quiénes serán responsable(s) del proceso de mejora en materia de seguridad? Existen varias posibilidades:

- Miembros ad hoc de la organización (son parte de la organización y se los elige dentro de ella; normalmente tienen también otras responsabilidades). O podría ser un grupo de trabajo (formado por gente de varias áreas del trabajo).
- Una persona de fuera-dentro: alguien que esté parcialmente involucrada/o en el trabajo y que interactúa de cerca y siempre con la gente de la organización (por ejemplo, alguien que solía trabajar para la organización y sigue en contacto).
- Una persona que actúe como asesora: se relacionará con quien asuma de forma ad hoc las cuestiones de seguridad o con el grupo de trabajo (interacción a corto plazo).

Examinemos las ventajas y desventajas de las tres posibilidades

Parte responsable del proceso de mejora	Ventajas	Desventajas	Posibles Soluciones
Persona ad hoc de la organización	• información centralizada • fácil acceso a la información • claridad respecto a responsabilidades • facilidad a la hora de tomar decisiones: menos gente involucrada • elegida/o por sus capacidades • ...	• cantidad de trabajo: compromiso colectivo debilitado • demasiada dependencia en una sola persona • no recibe comentarios y críticas que pueden interesar sobre planes e ideas. • ...	• distinguir entre arrancar con el proyecto (promoción) y puesta en práctica (materialización) • reducción temporal del volumen de trabajo para permitir tiempo para centrarse en temas de seguridad. • personal de apoyo • que las estrategias estén continuamente en circulación para asegurarnos de que se da el intercambio de impresiones sobre las mismas • ...
Grupo de trabajo	• compartir el trabajo en seguridad y darle un enfoque global/inclusivo • experiencia amplia y diversa • más recursos humanos • reparto de responsabilidades: más claridad para iniciativas y actividad. • más probabilidad de que se sigan los protocolos. • ...	• volumen de trabajo; tomas de decisiones por consenso lentas • Circulación de la información menos fluida: más personas que tienen que ser entrenadas para la tarea. • ...	• distribución adecuada de las destrezas y tareas • implicación del nivel de dirección/coordinación • rotación, formación y compromiso con que el output (el trabajo que hagamos) esté siempre abierto a mejoras • ...

UNA PERSONA DE FUERA - DENTRO	• más objetividad en el análisis de los riesgos • persona ya formada en la que confía la organización • compromiso total • probada receptividad: conocedora de los puntos fuertes y las debilidades • ...	• discontinuidad • podría debilitar el compromiso del grupo • podría socavar el nivel de compromiso con el cumplimiento del proceso • ...	• formar a 1 o 2 miembros del equipo • output siempre en construcción y circulación para reunir comentarios y críticas de todo el equipo • construcción del consenso y acuerdos • ...
ASESOR O ASESORA	• puede formar al equipo • asesoría especializada • claridad a la hora de supervisar el proceso • consejos acreditados • proceso de seguimiento activo • le afectan menos los temas internos de la organización • ...	• podría generar dependencia en lugar de ayudar a formar • podría ser visto/a como "alguien que está ahí para sacar adelante tal trabajo" en lugar de "alguien que está ahí para ayudar que se saque adelante el trabajo" • podría socavar la debida confianza en la organización • más gastos • difíciles de encontrar • dificultades para programar el trabajo • podrían no tener suficiente conocimiento del contexto • podría trazar un plan y unas normas inadecuadas para el contexto de trabajo • ...	• explicar las cosas con mucha claridad a todo el mundo (papel del asesor/a, alcance de sus funciones) • elevar la importancia de la seguridad con otras organizaciones o grupos para abordarla con ellos • formación de formadores/as en materia de seguridad dentro de las organizaciones (facilitadores/as) • sesiones informativas sobre el contexto en el que se desarrolla el trabajo • ...

¿Cuál es el punto de partida del proceso?

Una vez que se ha identificado el punto de entrada y se ha designado a quien será responsable de la mejora, ¿cuál es el punto de partida?

El punto de partida tendría que ser evaluar el proceso de aplicación de la política de seguridad de la organización. Empezar por una evaluación (o diagnóstico) determinará las prioridades y las soluciones posibles (las mejores prácticas de acuerdo a las necesidades declaradas, el perfil de la organización y su mandato). Se trazará entonces un plan con el objetivo de estructurar el proceso de mejora. El plan incluirá metas intermedias para posibilitar que se compruebe si se avanza y cómo se avanza. Además, aclarará el papel y las responsabilidades tanto de la(s) persona(s) a cargo del proceso como de las y los miembros de la organización; e incluirá también un calendario. Al final del proceso planeado, se realizará una evaluación de lo conseguido.

Diagnóstico ⇨ Prioridades ⇨ Soluciones posibles
⇨ Plan de mejora ⇨ Evaluación

Una vez hayamos determinado las prioridades, la decisión sobre su orden de ejecución podría ser más fácil si se han establecido unos criterios: emergencias, recursos disponibles en ese momento, etc.

La flexibilidad es un factor esencial a lo largo de todo el proceso. Sin embargo, ¿cuál es el mínimo necesario para que el proceso de mejora tenga posibilidades reales de conseguir resultados? Es vital responder a esta pregunta antes de iniciar el proceso: para ello hacemos un diagnóstico.

Diagnóstico y plan de mejora

El diagnóstico puede hacerse usando las herramientas de la "valoración de riesgos" y la "rueda de la seguridad" que describimos en capítulos anteriores de este manual (también puede servir cualquier metodología para revisiones que se use en organizaciones).

Obviamente, este paso debería implicar a todas las personas y grupos de trabajo de la organización que puedan verse afectados por las medidas.

El plan de mejora tiene que **ser realista** y **encajar adecuadamente** con el perfil y las necesidades de la organización. A continuación presentamos una secuencia de pasos:

1 ◆ Identificar las expectativas de la organización y los resultados que esperamos tenga el plan de mejora para el tema de la seguridad.

2 ◆ Hacer el diagnóstico conjuntamente, alcanzar un consenso y compartir ideas sobre la actual estructura de la gestión de la seguridad (aplicación del "análisis de riesgos" y la "rueda de la seguridad"): indicar el progreso, las insuficiencias y las necesidades.

3 ◆ Indicar y discutir las mejores prácticas que se pueden llevar a cabo para abordar las insuficiencias y las necesidades que hayamos identificado.

4 ◆ Indicar los objetivos deseables y deseados en el plan de mejora.

5 ◆ Dar una idea general de qué actividades se precisan para alcanzar esos objetivos y hacer una valoración sensata de lo que se puede esperar de cada una (esto posibilitará el avance hacia los objetivos).

6 ◆ Dar una idea general de qué recursos se van a necesitar (económicos, humanos, de tiempo y técnicos). Definir las responsabilidades, las tareas y el calendario de trabajo.

7 ◆ Definir qué riesgos surgen al lograr esos objetivos y resultados.

8 ◆ Definir los indicadores para supervisar el progreso y los resultados finales.

9 ◆ Compartir el plan con todas las partes implicadas para conseguir sus comentarios y críticas, mejorarlo y generar la aprobación necesaria para que pueda materializarse.

10 ◆ Materializar el plan y decidir el calendario para supervisar su progreso y los cambios que sea necesario introducir.

El proceso: Puesta en práctica del plan de mejora

El proceso incluye una serie de reuniones y entrevistas con personas o equipos de la organización o que están en contacto con ésta (en este caso, tendremos que contar con un acuerdo previo hecho por la organización que indique con qué personas y/u organizaciones podemos discutir el tema de la seguridad). El intercambio puede empezar con una reunión en la que se haga una introducción general al tema, y después pueden organizarse más reuniones. Estas reuniones proporcionan el espacio en el que definir el diagnóstico y discutir la materialización del plan de mejora. Es más, las reuniones pueden tratar temas concretos o pueden ir acompañando el trabajo específico de la organización desde el punto de vista de la seguridad y la protección.

Resistencia al plan de mejora

Una vez identificado el punto de entrada, designado al responsable, y decidido el punto de partida y el proceso, ¿qué resistencia podrían plantear las personas?

Como ocurre con todos los procesos que suponen cambios en una organización, el plan de mejora podría encontrar resistencia. Sin embargo, también encontrará aprobación y apoyo. La cuestión es, por tanto, ver cómo aprovechar ese apoyo y cómo argumentar una defensa frente a la oposición que pueda darse.

La manera más eficaz de socavar la resistencia es escuchar atentamente e intentar comprender las razones subyacentes. Aquí, una vez más, la participación, la escucha activa de todos los puntos de vista y expectativas son fundamentales para un buen proceso.

Es esencial que el plan de mejora proporcione una manera de abordar la resistencia que pueda plantearse para así evitar tener que improvisar después, corriéndose el riesgo de que el plan falle sólo porque no quisimos ver este posible escenario.

En la siguiente tabla presentamos algunos estereotipos comunes de resistencia, las razones subyacentes a su postura y las posibles respuestas para superarla.

Estereotipos comunes de resistencia	Razones subyacentes de los estereotipos	Respuestas para superar la resistencia
"No estamos amenazados/as" o "nuestro trabajo no supone tanta exposición o no es tan conflictivo como el de otras organizaciones".	• El riesgo no variará, no cambia y no depende de que el contexto del trabajo se deteriore o de que pueda cambiar el escenario.	• El riesgo depende del contexto político, y el contexto político es dinámico, por lo tanto, el riesgo también.

"El riesgo es inherente a nuestro trabajo como defensores/as" y "ya sabemos a qué nos exponemos".	• Como defensores/as aceptamos el riesgo y ese tema no nos afecta en nuestro trabajo. O bien, el riesgo no puede reducirse, el riesgo está allí y no hay más.	• Enfrentarnos a un riesgo inherente no significa que tengamos que aceptar el estado de esa cuestión. • El riesgo, como mínimo, nos afecta psicológicamente en nuestro trabajo, siquiera por el estrés que provoca. • El riesgo se compone de elementos objetivos: amenazas, puntos vulnerables y capacidades. Estos dos últimos puntos dependen de las y los defensores, por lo que son variables sobre las que podemos trabajar. Reduciendo las vulnerabilidades y aumentado las capacidades, el riesgo se puede reducir. Es posible que no podamos eliminarlo, pero esto no significa que no podamos reducirlo en todo lo posible.
"Ya sabemos manejar la cuestión del riesgo", o "ya sabemos cuidarnos" y "tenemos mucha experiencia"	• La actual gestión de la seguridad no puede ser mejorada, por lo que no merece la pena hacer nada al respecto. • El hecho de que no hemos sufrido daños en el pasado garantiza que no pasará nada en el futuro.	• La gestión de la seguridad está basada en elementos objetivos sobre los que se puede trabajar. • Mirar alrededor: veremos cuántas defensoras y defensores han sufrido daños a pesar de su mucha experiencia.
"Sí, el tema es interesante pero tenemos otras prioridades."	• Hay temas más importantes que la seguridad de las y los defensores.	• La prioridad es vivir. Si perdemos la vida, no podremos abordar las restantes prioridades.
"¿Y de dónde sacamos el dinero para pagarnos eso?"	• Los temas de seguridad cuestan dinero y no pueden incluirse en las propuestas de recaudación de fondos.	• ¿Cuánto pensamos que cuesta la seguridad? Bastantes elementos de la seguridad tienen que ver con los comportamientos, por lo que no cuestan un céntimo. • Quienes invierten un dinero preferirán invertir en una organización que se ocupa del tema de la seguridad a correr el riesgo de perder lo que invierten.
"¿Y de dónde sacamos el dinero para pagarnos eso?" "Si le prestamos tanto atención al tema de la seguridad no podremos hacer lo verdaderamente importante, que es trabajar con la gente, y se lo debemos."	• El que tengamos problemas de seguridad no es un problema de las personas con las que trabajamos. La calidad del trabajo que ofrecemos a la gente no depende de si nos sentimos más a salvo o no.	• La seguridad es una cuestión de vida o muerte. • Justamente por debérselo a la gente no podemos correr el riesgo de perder la vida. • La gente corre riesgos al confiarnos sus casos y si no cuidamos nuestra propia seguridad, esto les repercutirá; podrían decidir, por ejemplo, cambiar de organización para trabajar con una que cuide más el tema y que, por lo tanto, inspire más confianza.
"No tenemos tiempo para eso, tenemos ya demasiado trabajo."	• Es imposible encontrarle un hueco al tema en nuestro plan de trabajo.	• ¿Cuánto tiempo pensamos que lleva el tema de la seguridad? • ¿Cuánto tiempo empleamos en reaccionar ante las emergencias y no en prevenirlas en lo posible? (con toda probabilidad, mucho más que el tiempo necesario para planear cómo incluir el tema de la seguridad en nuestro trabajo).

"La comunidad nos respalda: ¿quién va a atreverse a hacernos daño?".	• Somos parte de la comunidad. No está fragmentada, no cambia ni de miembros ni en sus opiniones. • No se puede influir en la comunidad.	• La comunidad no es homogénea y también las personas a las que afecta nuestro trabajo son parte de esa comunidad.
"En nuestro pueblo/poblado, las autoridades comprenden nuestro trabajo y colaboran con nosotras/os."	• Nuestro trabajo de DDHH no afecta a las autoridades del lugar, y no van a cambiar de opinión. • No hay una jerarquía entre autoridades locales y nacionales	• La memoria histórica de la organización podrá ofrecer ejemplos de autoridades locales que se opusieron al trabajo de derechos humanos cuando sintieron que ya no podían tolerarlo más. • Las autoridades locales tienen que ejecutar las órdenes de sus superiores. • Entre las autoridades podría haber personas que tuvieran un interés por proteger a quienes agreden. • Los contextos políticos cambian.

Una vez identificado el punto de entrada, designado al responsable, decidido el punto de partida y el proceso, disuelto la resistencia individual de las personas, ¿qué factores de la organización podrían obstaculizar o facilitar el cambio?

Los factores organizativos pueden obstaculizar o facilitar los cambios dentro de la organización para la consecución de una política de seguridad más eficaz.

Dentro de la organización	Factores que obstaculizan el cambio	Factores que facilitan el cambio
Cultura de la organización	• Superficialidad. Improvisación. Orientada a lo individual. • La seguridad no está integrada en el trabajo •...	• Trabajo en equipo, consciencia del impacto del trabajo, escucha activa, asesoramiento, tomas de decisiones por consenso. • La seguridad integrada en el trabajo •...
Actitud de la dirección	• Autoritaria y dictatorial. Interesada en los resultados. Distante. Sólo se le da importancia a los líderes, de ahí su inclinación a sólo diseñar y respetar normas que les afectan. • La idea de servicio a no es bidireccional: se piensa que el resto de la organización está ahí para servir a la dirección. • Se otorgan privilegios. •...	• Reconocimiento de la importancia de lo que aporta todo el mundo para que se cumpla con el mandato de la organización. • Se le presta atención a las preocupaciones de todas y todos los miembros de la organización, sin importar su cargo. • Apertura/Transparencia. • Respeto a las normas,. •...
Estructura de la organización	• Rígida. • Compartimentalizada. • Inadecuada para el trabajo. •...	• Flexibilidad. • Buena coordinación y comunicación entre niveles. • Se cubren las necesidades de las personas y del trabajo.

CONOCIMIENTO DE LOS TEMAS DE SEGURIDAD	• Centralización. Parcialidad. Baja sensibilización a temas de seguridad en el campo. Falta de objetividad, poco conocimiento corroborado o de los hechos sobre los temas. •...	• Se comparte la experiencia y el conocimiento. Inclusivo. Basado en los hechos. • Recogida sistemática de la información y actualizaciones regulares. •...
FALTA DE ESTABILIDAD EN LA ORGANIZACIÓN; CANSANCIO DE LOS CONTINUOS CAMBIOS.	• Movimiento de personal. • Ausencia de memoria histórica. • Presión debida a los continuos cambios. Ausencia de continuidad en el trabajo •...	• Descripción clara del empleo y contrato con la organización donde se establece por escrito el compromiso de dar aviso previo de la marcha y de posibilitar que quien ocupe el puesto abandonado reciba toda la formación e información que necesita. • Evaluaciones regulares. • Distribución de tareas que puedan realizarse en el horario en el que se ha contratado a la gente. Introducción al trabajo y formación •...
VOLUMEN DE TRABAJO	• Recursos humanos insuficientes y/o inadecuados. Estrés. Descentrarse o perder el sentido de las prioridades. •...	• Hacer una lista de prioridades y (re)distribuir el trabajo. • Espacio para ajustes. •…
PLANIFICACIÓN	• La seguridad no es una prioridad clara. • No se la incluye en el plan de trabajo. • El plan de trabajo se improvisa y no encaja con los objetivos generales y específicos. •...	• Planear adecuadamente la seguridad en el trabajo. Integrarla en los planes de trabajo. Dar la consideración adecuada a las actividades cuyas condiciones de seguridad se ven como insuficientes y decidir después si se llevarán a cabo si no se dan determinadas condiciones de seguridad. •...

Factores que no influyen en el cambio de la organización hacia la mejora de la política de seguridad:

- El tamaño de la organización
- Que los miembros tengan o no educación superior
- La religión
- El género
- ...

Criterios o buenas prácticas a la hora de gestionar la protección y la seguridad

Una vez identificado el punto de entrada, designado a la parte responsable, decidido el punto de partida y planeado el proceso, disuelto la posible resistencia individual al mismo, considerado qué factores de la organización obstaculizan o facilitan los cambios, ¿cuáles son las mejores prácticas de gestión en relación con la seguridad y la protección sabiendo que dependen de los modelos organizacionales estructurales?

Existen varias opciones para gestionar la seguridad dentro de una organización, y puede ser difícil tomar una decisión sobre cuál será la mejor. En la siguiente tabla discutimos tres modelos con sus ventajas e inconvenientes, además de con soluciones posibles para los inconvenientes.

Modelos estructurales estándar en la gestión de la seguridad

Modelos estructurales	Dónde se toman las decisiones en material de seguridad	Ventajas	Desventajas	Soluciones posibles
Modelo centralizado	• En el nivel directivo, en una parte que tiene esta función asignada.	• Puede ser más fácil comprobar que dentro de la organización se dispone de la experiencia y el conocimiento necesarios. •…	• El volumen de trabajo podría impedir que se puedan tomar las decisiones adecuadas. • Podría estar desconectado del trabajo en algunas áreas. •…	• Una persona en el nivel directivo con capacidad ejecutiva actúa en nombre de la dirección. • Se asigna la responsabilidad de seguridad en el nivel directivo pero sin capacidad ejecutiva. •…
Modelo intermedio	• Directrices globales y fundamentales: en el nivel directivo. • Decisiones concretas: por quienes sean responsables de ellas en cada área de trabajo.	• La directiva no se ve sobrecargada. • Las destrezas se relacionan con el nivel donde se desarrollan. Proximidad al trabajo real en cada área. •...	• Podrían surgir problemas entre el nivel de dirección y el de las áreas de trabajo. • …	• Cada responsable de un área concreta se responsabiliza de la seguridad en esa área. Se podría nombrar a un/a asesor/a para toda la organización: una persona vinculada a un área dada, por ejemplo, administración o logística, asume la responsabilidad de la seguridad y se relaciona con las personas responsables de las demás áreas. •…
Modelo descentralizado	• Las decisiones se toman en todos los niveles porque todas y cada una de las personas tienen la responsabilidad de tomar decisiones.	• Mejor cumplimiento, aportación a la cultura de la organización que se ocupa de la seguridad. •...	• Las discusiones pueden llevar más tiempo. Se puede aplicar sobre todo en organizaciones pequeñas. •…	• Puede que haya personas que se dediquen sólo a temas de seguridad. • Cada cual podría tener esa responsabilidad en su descripción de funciones o de su trabajo anterior. •…

Formación de los miembros de una organización

Una vez identificado el punto de entrada, designado al responsable, decidido el punto de partida y planeado el proceso, disuelto la posible resistencia individual, considerado qué factores de la organización obstaculizan o facilitan los cambios, determinado las mejores prácticas de protección y seguridad, ¿cómo formar a las personas de la organización?

La formación se puede hacer con recursos internos de la organización (puede haber personas con formación para dar un taller sobre seguridad); o con otras organizaciones (enviando a la gente a sesiones de formación con gente de otras organizaciones). Si fuera así, el estar construyendo las propias capacidades junto con otras organizaciones podría facilitar el posterior intercambio de información de seguridad e incluso el montar redes que nos ayuden a mejorar la protección. Para participar en talleres con personas de otras organizaciones es necesaria la confianza mutua; es más, es útil que las organizaciones compartan intereses y tengan áreas de trabajo parecidas y entornos de trabajo parecidos (por ejemplo, las organizaciones rurales y las urbanas tienen necesidades muy diferentes en materia de su seguridad).

La formación puede hacerse de maneras muy diferentes. Posiblemente, las más habituales son:

- Talleres (preferiblemente en pequeños grupos de 10 a 15 personas).
- Formación individual (útil para tareas complicadas o para responsabilidades específicas, y van con la formación que se da al asumir ese puesto de trabajo).
- Conversaciones o reuniones semiformales (consultas particulares, consejos sobre temas concretos).

Se recomienda hacer parte de la formación fuera del entorno del trabajo para permitir la gente se concentre con más facilidad al estar evitándoles la tensión diaria del entorno laboral. No obstante, a menudo es contraproducente hacerlo fuera de las horas del trabajo (p.e. los fines de semana) pues se podría estar enviando un mensaje a evitar por ser falso: que cuidar los temas de seguridad supone cargarse con más trabajo y que el tema no es lo bastante importante como para incluirse en el horario de trabajo.

Cómo mejorar el respeto a las normas de seguridad

Una vez identificado el punto de entrada, designado el cuerpo responsable, decidido el punto de partida y planeado el proceso, disuelto la posible resistencia individual, considerado qué factores de la organización obstaculizan o facilitan los cambios, determinado las mejores prácticas de protección y seguridad, y que las y los miembros o la plantilla han recibido formación, ¿cómo podemos mejorar el respeto a las normas de seguridad?

El respeto a las normas de seguridad se consigue creando las condiciones necesarias que generan estos pasos:

- Existencia y desarrollo de una cultura de seguridad en la organización.

- Compromiso individual con las normas y planes de seguridad. Participación en su concepción y en los procesos que las mejoran. Formación para comprender el tema y poder resolver dudas. Certeza de que son adecuadas y eficaces.

- Redactar un acuerdo entre la persona y la organización relativo al cumplimiento de las normas y planes de seguridad.

- Intervención regular de las y los responsables de la seguridad, a modo de recordatorio de los acuerdos alcanzados y para recoger opiniones sobre si las normas están funcionando adecuadamente y si son eficaces.

¿Qué puede hacerse para los casos de incumplimiento de las normas y planes de seguridad?

I ● Identificar y resolver las causas del incumplimiento (ver capítulo 2.2).

II ● Si la causa es intencionada y depende de la voluntad de la persona en cuestión, se pueden tomar las siguientes medidas:

a • Hablar con esa persona (como culminación del proceso previo que pretendía resolver las causas del incumplimiento) para inspirarla/motivarla y fortalecer su compromiso.

b • Tratar el tema con el equipo que proceda tratarlo, en presencia de la persona que nos ocupa (este paso puede ser una mala idea en ocasiones, dependiendo de la situación).

c • Aplicar un sistema de apercibimiento (entre 2 y 3 avisos).

d • Aplicar un sistema de sanciones graduadas que culminan con el despido.

Es importante incluir en el acuerdo una cláusula relativa al cumplimiento con las normas y planes de seguridad, para que todas y todos los defensores sean plenamente conscientes de la importancia que tiene el tema en la organización.

Resumen

Tener un plan de seguridad no significa necesariamente que se esté llevando a la práctica o que se esté respetando. Se debe diseñar un proceso adecuado para gestionar la materialización de ese plan, que se respete y que se pueda mejorar. Cuanto más inclusivo sea el proceso, más información sobre las necesidades relativas a la seguridad podrá reunirse y mejor se desarrollará el nivel de compromiso individual con el cumplimiento de esas normas.

No hay una estructura organizativa mejor que otras: cada tipo tiene sus ventajas y desventajas. Por lo tanto, es útil analizar varias con objeto de diseñar un proceso que nos sirva bien y de que se le den todas las oportunidades posibles para que salga adelante.

El plan de mejora tiene que ser **realista** y **ajustarse** al perfil de las necesidades de la organización.

He aquí los pasos sucesivos del proceso hacia una política de seguridad mejorada:

- Identificar el punto de entrada del tema
- Designar a las y los responsables
- Esas personas tendrán que encontrar el punto de partida y planear el proceso
- Tenemos que disolver la resistencia individual usando la escucha activa, para sí determinar qué razonamientos sustentan esa resistencia y contraargumentar eficazmente (no basta con dar una visión contraria a la del estereotipo que se opone, puesto que el factor determinante es el razonamiento que sostiene ese estereotipo: si el razonamiento es correcto, la resistencia es legítima).
- Considerar qué factores de la organización obstaculizan o facilitan el cambio
- Determinar cuáles son las mejores prácticas o criterios
- Formar a las y los miembros o la plantilla
- Mejorar las normas de cumplimiento en materia de seguridad

TERCERA PARTE

PROTOCOLOS, PROCEDIMIENTOS DE URGENCIA Y OTRAS POLÍTICAS DE SEGURIDAD

INTRODUCCIÓN:

En la tercera parte del Manual presentamos la lógica para elaborar protocolos, procedimientos de urgencia (para usar en situaciones específicas) y otras políticas de seguridad.

Se basan en "buenas prácticas" compartidas y aprendidas en nuestros talleres de formación.

Sin embargo, ni están completas ni garantizan siempre resultados positivos, dado que el Manual no puede reproducir todas las posibles variables en un contexto dado.

El Manual está todavía 'creciendo", por lo que les invitamos a mandarnos sus comentarios y sugerencias de planes y protocolos nuevos.

Las actualizaciones y los cambios se publicarán primero en nuestra página web **www.protectionline.org**, para que los defensores puedan usarlos inmediatamente, y serán incluidos después en la siguiente edición del Manual.

Mientras tanto, por favor consulten el Anexo IV - Resumen de riesgo general para perfiles específicos de defensores de derechos humanos.

CONTENIDOS DE LA TERCERA PARTE:

CAPÍTULO 3.1

Cómo Reducir los riesgos conectados a un posible registro o robo en la oficina

Un registro se describe perfectamente como la entrada forzada a una casa, oficina o espacio privado. Es legal cuando el Estado lo decide y ejecuta respetando la legislación vigente; y es ilegal cuando no lo permite la ley (por ejemplo, un robo de noche, la irrupción de las fuerzas de seguridad sin orden de registro, o la de un actor armado).

Aunque el supuesto que sigue es para casos de un registro legal, se pueden extraer normas aplicables a registros ilegales y también completarlas con la información que presentábamos en el capítulo de la seguridad en casas y oficinas.

El Estado puede realizar registros legalmente. La legislación aplicable tendrá que respetar la legislación internacional sobre derechos humanos y de protección de las libertades democráticas. Sin embargo, los registros rutinarios pueden utilizarse, contraviniendo la legislación internacional, como método para perseguir y acosar sin tregua las y los defensores de derechos humanos y demás miembros del movimiento social, y esto puede convertirse en un grave problema.

No puede decirse que un registro ha sido un hecho "inesperado" (no puede decirse esto de ninguno de los riesgos que corremos), sobre todo cuando además puede ser legal. Ningún riesgo que puede reducirse a cero, pero intentaremos reducir lo más posible las amenazas / consecuencias (los peligros) que se desprenden de un registro.

¿Cómo? Utilizaremos la ecuación del riesgo y haremos una lista de todas las amenazas / consecuencias (estas últimas podrían asimilarse a las primeras). Después, para cada una, identificaremos las vulnerabilidades y capacidades que van asociadas, y empezaremos a trabajar con todo esto...

Peligros vinculados a los registros

Un registro genera una serie de amenazas / consecuencias (peligros):

a • La amenaza de que durante el registro alguien salga herida o herido física o psicológicamente.

b • La amenaza de que se lleven, se pierda o se destruya información.

c • En relación con eso, de que la información sea usada por una tercera parte que no debería tenerla.

d • La amenaza de que se escondan objetos peligrosos (armas, drogas, documentos) para después proceder "legalmente" contra la organización.

e • La amenaza / consecuencia de que roben o destruyan dinero y propiedades como ordenadores, etc.

f • ...

a ◆ La amenaza de que durante el registro alguien salga herida o herido física o psicológicamente

No se puede saber cómo va a ser un registro ni qué impacto tendrá. Sin embargo, reunir previamente toda la información posible sobre los registros puede ayudarnos a evitar actuaciones y sentimientos como el estrés que podrían aumentar el riesgo de que suframos daños físicos o psicológicos. Nos ayudará, además, a sensibilizarnos sobre qué es lo que dispara los riesgos, y a que podamos mantener un comportamiento positivo.

Puntos vulnerables:

- no saber de qué trata un registro
- creer que tratar de impedirlo ayudará
- no tener un seguro médico
- ...

Capacidades:

- saber cómo son los registros legales
- saber qué departamento puede emitir órdenes de registro y conocer el nombre de quien esté a cargo (antes y durante el registro legal)
- haber visto una orden de registro, para saber cómo son
- saber qué derechos tienen las organizaciones / individuos que son registrados (incluido el derecho a pedir que nos enseñen la orden de registro y posiblemente a solicitar asistencia letrada).
- derecho a tener asistencia letrada (durante y después del registro).
- saber qué no hay que hacer
- si el registro es con violencia, es importante mantenerse en grupo para evitar abusos a personas que estén solas
- …

La organización podría publicar en algún tablón o sitio visible:

- Un modelo de orden de registro.

- Toda la legislación que venga al caso (derechos y deberes de ambas partes).

- Una lista con los nombres y teléfonos del abogado o abogada de la organización, de asistencia médica como doctor/a, psicólogo/a, hospital más cercano)… (Esta lista debería ponerse en varios lugares de la oficina para que la información se pueda localizar rápidamente estemos donde estemos).

Esta información es legal y pública, por lo que puede ser expuesta en tablones para que la vean las dos partes. Esto no evitará el registro (sea o no sea con orden de registro) pero podría ayudar a reducir el estrés entre quienes son objeto de ese registro. Además, sirve de información para que quien hace el registro sepa que la persona u organización registrada es plenamente consciente de sus derechos, por lo que si el registro no se ajustara a sus límites legales, procedería a algún tipo de acción (disuasión).

b ◆ La amenaza de que se lleven, se pierda o se destruya información

La información que se considere pública o no peligrosa puede guardarse en la oficina, así, si hay un registro, será esa la que se lleven (como hacemos cuando viajamos con dinero, que dejamos más a la mano una cantidad de dinero y bien guardada otra, por si nos atracan).

Tener una buena política de seguridad con la información implica que se reducen las posibilidades de que se pierda, se robe o destruya, entre ellas, que las y los defensores no sentirán que tienen que exponerse para protegerla (en cualquier caso, la vida es siempre lo primero). Esto reducirá el estrés que genera un registro, y también el riesgo de violencia y daños tanto físicos como psicológicos.

Puntos vulnerables:

- Que la información no se archive/guarde siguiendo la distinción aprobada por todas y todos entre información confidencial y no confidencial
- Información confidencial en papel
- Información electrónica no encriptada (archivos y adjuntos).
- Mala seguridad en la oficina y la casa: insuficientes barreras para impedir el acceso o que ganemos tiempo para cerrar el ordenador o esconder un documento
- …

Capacidades:

- hacer copias de seguridad regularmente (al menos una vez a la semana) de la información almacenada en los ordenadores, y guardarla en un sitio seguro. En caso de registro, sabremos así cuánta información ha quedado expuesta (dependiendo de la fecha del registro, comparándola con la fecha de la última copia de seguridad o del almacenamiento de la información).

- copias o fotocopias, o mejor aun, copias escaneadas, para guardar el archivo de los documentos fundamentales en un sitio seguro. Si fuera necesario, se pueden repartir por otros sitios seguros).
- buenas medidas de seguridad para la casa y la oficina
- comentar al principio del registro la cuestión de la asistencia letrada (abogado/a) y que otras organizaciones estén presentes durante el registro, al menos en el exterior. Así se presiona a quienes estén llevando a cabo el registro para que lo hagan respetando la legalidad vigente.
- ...

COMPARATIVA DE DIFERENTES SISTEMAS PARA HACER COPIAS DE SEGURIDAD (ORDENADORES)

MEDIO DE ALMACENAMIENTO	VENTAJAS	DESVENTAJAS
COPIA EN CDS/DVDS	Muchos ordenadores tienen programas para la copia de CDs y DVDs. Transporte y almacenamiento de los CDs y DVDs más fácil y seguro.	Si la cantidad de información es grande, hacen falta muchos CDs, lo que hace que el proceso lleve mucho más tiempo y sea más complicado. Quien consiga los CDs tendrá acceso a todos los datos.
DISCO FLASH	Como anterior.	Como el anterior, sólo que el objeto es más fácil de guardar y por tanto, menos fácil que caiga en las manos de quien no queremos que caiga.
HARDWARE EXTERNO	Puede almacenar mucha información y no se tarda mucho en copiarla en él. Puede tener códigos de acceso para proteger la información.	El precio (US $200-300)
SERVIDOR EN UN LUGAR REMOTO	Puede guardar toda la información, es veloz, no se puede perder ni robar.	Requiere que tengamos una conexión a Internet de banda ancha y que utilicemos la encriptación Recordar que según la seguridad del Estado se puede obligar a los servidores a entregar los archivos si se los piden.

c ◆ La amenaza/consecuencia de que la información sea usada por una tercera parte que no debería tenerla.

Mucha probabilidad de que repercuta en la organización y las personas mencionadas en esa información.

Consecuencias para la organización que sufre el registro

Puntos vulnerables:

- No haber considerado previamente cómo podríamos reaccionar en diferentes escenarios.
- Descuidar la ética, llevar mal las cuentas, usar software pirata (podrían implicar acciones legales contra la organización).
- ...

Capacidades:

- Copias de seguridad.
- Plan de reacción listo.
- ...

Consecuencias para las personas mencionadas en la información

Puntos vulnerables:

- No haber hablado antes de esta posibilidad con las personas ahora afectadas.
- No poder ponerse en contacto rápidamente con estas personas.
- ...

Capacidades:

- Haber dado explicaciones sobre el riesgo que se corre y haber asegurado en todo lo posible que este riesgo no se dará por negligencia por parte de la organización.
- Haber planeado conjuntamente la reacción para el caso de emergencia (poner el plan en marcha de inmediato, medidas de protección, lugares para esconderse, etc.).
- ...

d ◆ La amenaza de que se escondan objetos peligrosos (armas, drogas, documentos) para después proceder "legalmente" contra la organización.

Puntos vulnerables:

- El espacio de la oficina está lleno de objetos y papeles no relacionados con el trabajo (objetos personales, revistas...). En caso de registro, es más difícil ver si están escondiendo algo o si alguna visita anterior ha dejado un objeto o documento peligroso para que luego lo encuentren "casualmente".

- No existe un inventario del material de la oficina, y menos aún en manos de un abogado o abogada (que es algo muy recomendable).
- Sólo una persona de la organización presente durante el registro.
- ...

Capacidades:

- Cuando sea posible (sólo para el caso de un registro legal),[1] la gente sabrá qué puesto tiene que ocupar en la oficina (por ejemplo, cada cual en su lugar habitual de trabajo) para poder observar así lo que pasa durante el registro desde el máximo de puntos posibles. Podremos notar más fácilmente si se están apropiando de algo ilegalmente.
- Después del registro (no importa de qué tipo sea), la organización debe revisar toda la oficina (si es posible, con la ayuda de observadores/as de fuera de la organización), registrando (incluso sacando fotos) todo lo que se pueda encontrar y asegurándose de que se hace un informe de y no se toca todo lo que no pertenece a la oficina o lo que no estaba allí antes del registro (cuidado con las huellas). Debemos anotar también aquello que haya desaparecido.
- Presentar el informe a la policía y seguir las provisiones legales vigentes.
- ...

e ◆ La amenaza / consecuencia de que roben o destruyan dinero y propiedades como ordenadores, etc.

Con toda probabilidad, un registro ilegal conllevará el robo de algún artículo.

Puntos vulnerables:

- Guardar mucho dinero u objetos valiosos en la oficina.
- Tener artículos desprotegidos.
- Que no exista un inventario del material de la oficina, y menos aún en manos de un abogado o abogada (que es algo muy recomendable).
- Que no exista un seguro contra robos.
- ...

Capacidades:

- Conocer qué puestos debemos ocupar en los diferentes lugares de la oficina para poder observar lo que hacen en el registro.[2]

[1] Para casos de registros con violencia, es fundamental mantenerse en grupo para que nadie sufra malos tratos a solas (sin testigos).

[2] Ver nota anterior.

- Comentar al principio del registro la cuestión de la asistencia letrada (abogado/a) y que otras organizaciones estén presentes durante el registro, al menos en el exterior. Así se presiona para que quienes estén llevando a cabo el registro lo hagan respetando la legalidad vigente.
- ...

Cómo enfrentarse a y reducir la amenaza de que se produzca un registro

Si un registro respeta la legislación internacional y tiene un objetivo legal y legítimo, entonces no tiene sentido siquiera pensar en impedirlo. Sólo cabe dejarles entrar, habiendo considerado los pasos anteriores relacionados con actuar respecto a las consecuencias. No obstante, si se están usando los registros como forma sistemática de perjudicar el trabajo de defensa de los derechos humanos y sus organizaciones sociales, entonces habrá que tomar medidas.

Con objeto de enfrentar y reducir la amenaza de un registro legal, la mejor estrategia es elevar su precio político a través de campañas y de conseguir apoyo activo, preferiblemente en colaboración con otras organizaciones e instituciones.

Si existe el peligro de un registro ilegal (o robo), es importante mejorar lo más posible la seguridad de la casa, la oficina o el local.

Todo esto es aplicable tanto para zonas urbanas como rurales.

Resumen

Cómo reducir el riesgo de un registro:

Los registros pueden ser legales e ilegales (cuando son ilegales, son como un robo).

Y como ocurre con cualquier otro riesgo, pueden aumentar el precio político de los registros.

Usar la ecuación para analizar cada elemento tanto como podamos.

Hacer una lista de las amenazas/consecuencias (los peligros) y sus respectivos puntos vulnerables y capacidades, y trabajarlas:

a • La amenaza de que durante el registro alguien salga herida o herido física o psicológicamente.

b • La amenaza de que se lleven, se pierda o se destruya información.

c • En relación con eso, de que la información sea usada por una tercera parte que no debería tenerla.

d • La amenaza de que se escondan objetos peligrosos (armas, drogas, documentos) para después proceder "legalmente" contra la organización.

e • La amenaza / consecuencia de que roben o destruyan dinero y propiedades como ordenadores, etc.

f • ...

CAPÍTULO 3.2

Retención, detención, secuestro (político o por chantaje) de una o un defensor

"Sin noticias"

Cuando no sabemos nada de dónde puede estar un defensor o una defensora, el primer obstáculo a superar es averiguar qué le ha ocurrido exactamente, y eso puede llevar algún tiempo. Posibilidades sobre lo que pueda haber ocurrido:

- Que el defensor o la defensora **no quiera** ponerse en contacto con la organización, o que se le **haya olvidado:** puede que haya decidido pasar un fin de semana fuera o hacer una visita y que no se lo haya dicho a nadie (o podría querer "desconectar"). Quizá no haya encontrado un teléfono o ningún otro medio de comunicación, o puede que no tenga la intención de enterarse de si lo hay siquiera. Podría ser que no quiera que nadie sepa lo que está haciendo (a veces esto se nos da muy bien). O lo más habitual: que se le haya olvidado avisar, o que no se haya dado cuenta de que sus compañeras y compañeros tienen motivos para estar preocupados pues no saben dónde está.

- Que el defensor o la defensora no haya podido ponerse en contacto con la organización por **causas técnicas:** esto puede ocurrir cuando nos hemos quedado, de manera no planeada o repentina, sin acceso a algún medio de comunicación en un lugar remoto; por ejemplo, durante un viaje al llegar a un sitio sin comunicaciones (y no lo sabíamos), cuando la carretera está bloqueada o tomamos una ruta alternativa, o cuando tenemos que improvisar un plan, cambio que nos lleva a un sitio sin comunicaciones. También puede ocurrir que el medio de comunicación con el que contábamos no funcione (móvil estropeado, sin saldo, sin batería, la red telefónica del lugar no funciona, etc.).

- Que el defensor o la defensora no pueda ponerse en contacto por **enfermedad u hospitalización** (por ejemplo, por un accidente de tráfico, una enfermedad inesperada, o ponerse peor de una enfermedad que ya se tenía).

- Que el defensor o la defensora haya sido objeto de una retención, detención o secuestro. Todas estas acciones tienen en común que el defensor o la defensora han perdido su libertad de movimiento y podrían estar viviendo desde a una presión amable a una seria amenaza a su vida[1]. En algunos casos, el defensor o la defensora podrá avisar a la organización, lo que implicará que ésta dispondrá de alguna información sobre la situación.

Retención significa que las y los miembros de la organización están bajo el control de un grupo (de soldados o milicia, una autoridad local, etc.). Detención es el término utilizado para describir un arresto hecho por las fuerzas de seguridad dentro del marco de la ley, por lo que se tienen derechos (en principio). Aquí usaremos "detención" para referirnos a los dos términos, por simplificar. Secuestro alude a dos casos diferentes que tienen en común la captura y traslado por la fuerza de una persona, pero que puede ser por razones políticas o para conseguir concesiones de la persona capturada o de otras.

En general, en la mayoría de los casos cuando no sabemos nada de un defensor o defensora es por las dos primeras categorías (que no quiera/ que haya olvidado comunicarse, o no poder hacerlo por causas técnicas). Veamos cómo prevenir y reaccionar ante estos casos.

Consejos de prevención para evitar las situaciones de "Sin noticias" respecto al paradero de un o una defensora

El defensor o la defensora no quiere ponerse en contacto con la organización, o ha olvidado hacerlo.

- Todas y todos los miembros de una organización, en especial quienes corran mayores riesgos, tienen que ser conscientes de que otras personas se preocuparán si no saben de su paradero. Si desean que nadie se pueda comunicar con ellos, es preciso que avisen de esto a sus compañeras o compañeros, dejando claro cuándo piensan volver a estar disponibles. Para el caso de defensoras o defensores en situaciones de mucho peligro, podría ser poco aconsejable que decidan no estar para nadie.
- Es importante desarrollar rutinas de seguridad que impliquen informar de dónde estamos cada cierto tiempo (normalmente a una o dos personas a cargo). Esto pasa a ser esencial cuanto mayor sea el riesgo que se esté corriendo (porque el defensor o la defensora viaje a una zona peligrosa, o porque hayan recibido amenazas, etc.).

El defensor o la defensora no puede ponerse en contacto con la organización por causas técnicas

- Acordar de ante mano horas para ponerse en contacto, y hacer un plan de contingencia para el caso en que hubiera problemas de comunicación: por ejemplo, si una de las horas de llamada va a coincidir con un viaje, habrá que pensar cómo y cuándo será posible comunicarse (por móvil o

[1] En este capítulo recurriremos a algunos de los contenidos del muy útil manual de seguridad de van Brabant (2000) (capítulo 1.3).

por teléfono normal, o por cualquier otro medio) para asegurarnos de que podremos hacerlo, y así que no haya nada (ni falta de saldo o de batería, ni averías y similares) que impida la comunicación.

- Prever medios alternativos de comunicación (p.e., a través de terceras partes).

El defensor o la defensora no se puede poner en contacto por enfermedad u hospitalización

- Es preciso tener a mano listas con los números de teléfono y las direcciones de todos los hospitales y centros de salud de la zona visitada, y donde sea posible, de sitios donde den información sobre los accidentes de tráfico (compañías de autobuses, guardia civil o policía de carretera, contactos en diferentes puntos del trayecto, etc.).
- Las y los defensores no deberían viajar si no están bien de salud.
- Utilizar el medio de transporte más seguro posible (incluidos los autobuses u otros medios).
- Las y los defensores deben tener un seguro médico y de accidente válido.

Cómo evitar las detenciones...

No es fácil evitar una detención. El objetivo fundamental es reducir las causas que puedan llevar a una detención de alguien de la organización.

- Para excluir en lo razonable el que se nos detenga por quebrantar el derecho común, debemos mostrar un comportamiento ético / respetar las normas y leyes del lugar donde trabajemos, tanto a nivel individual como de la organización. Ya sabemos que algunas detenciones son pretextos, pero el abogado o la abogada de la organización sabrá qué hacer y además, quien haya sido detenido o detenida sabrá qué pasos va a dar la organización y cuándo, por lo que los podrá repasar mentalmente según se vayan produciendo para "guardar la calma" (impacto psicológico) pues sabrá que afuera se estará haciendo algo. No hace falta enfrentarse a las autoridades o darles una excusa para exponerse a más riesgo del que ya se está corriendo.
- En los casos en que se quebrante la ley por acción política, será necesario realizar antes una valoración de los riesgos y preparar una estrategia de limitación de los daños, porque las y los defensores estarán co rriendo más riesgo.
- Una detención legal puede, sin duda, ser una excusa, no obstante. Puede o no haber una citación y / o una orden judicial, y puede darse en cualquier momento, en la oficina / casa o durante un viaje. Lo que habría que evitar es que nos detenga cuando estamos solas o solos, para ahorrarnos hechos que se relacionan con el momento del arresto. En última instancia, lo que se precisa es una estrategia de acción política cuyo objetivo sea disuadir a las autoridades de que detengan a las y los defensores; no obstante, la tendencia en muchos países parece ser a criminalizarlos, encarcelándolos por diferentes motivos, incluidos algunos que nada tienen que ver con su trabajo.

- No es fácil evitar el secuestro político. Además de realizar una valiosa valoración de riesgos cuando se sospecha que puede producirse, es crucial también reducir la exposición en las zonas donde la amenaza puede ser consumada, asegurarse de que la persona nunca va a estar sola y sopesar cualquier acción que pueda facilitar un posible secuestro.
- El secuestro político pueden llevarlo a cabo delincuentes comunes (sea o no una excusa) o actores legales y/o paralegales, y/o grupos políticos armados, etc. Puede ocurrir potencialmente en cualquier sitio, pero lo más probable es que ocurra cuando los agresores potenciales generen el momento adecuado, o cuando el defensor o la defensora lo facilite, y preferiblemente allí donde no existan testigos. Así, es menos posible que se produzca en la oficina durante las horas de trabajo, en la casa durante el día, etc. (ver ejemplo de amenazas de muerte contra un líder de una organización en el capítulo 1.7).

  La diferencia entre procedimientos ilegales en una detención legal y secuestro político es tan pequeña que recomendamos que las y los defensores de derechos humanos consideren todos los puntos de las dos partes como complementarios y no como excluyentes. No obstante, pensamos que era importante señalar aquí la diferencia entre lo que implica una detención y lo que implica un secuestro político por cuestiones psicológicas y prácticas.
- Para diseñar el procedimiento de prevención de un secuestro político habría que tener en cuenta el trabajo del defensor o la defensora en su día a día y área normal de actividades, su tiempo libre, etc., y sobre todo, sus misiones de campo, sean éstas parte del trabajo de la organización o porque se haya recibido una invitación. Hay que estar alerta en todo momento, y comprobar minuciosamente toda invitación de partes que no conozcamos.

Sospechamos que una defensora o un defensor ha siso detenido (o secuestrado, o que está siendo retenido)...

¿Cuándo podemos sospechar que se han llevado a una defensora o defensor contra su voluntad? Si no hemos tenido noticias de alguien, tendremos que sospecharlo cuando sea razonable descartar las primeras tres opciones... En realidad el procedimiento de reacción a una detención es como el procedimiento que usamos cuando una persona no se pone en contacto cuando debiera.

Por lo tanto, cuando no tengamos noticias de un defensor o una defensora debemos empezar a buscar a esa persona, para descartar cualquiera de las tres opciones. Es importante ponerse un límite de tiempo antes de considerar la cuarta opción (3 horas sin noticias, 6, 12..., según el contexto, las circunstancias, el nivel del riesgo, lo bien que comprenda el defensor o la defensora lo importante que es ponerse en contacto, etc.). Cuanto más breve sea ese tiempo, más riesgos de cometer errores si alertamos a la gente; cuanto más tiempo pase, más se retrasará el poder tomar medidas. ¡No será una decisión fácil!

Advertencia: puede que no se dé aviso de dónde se está porque se nos pase, por negligencia, o porque no se disponga de un medio de comunicación; todo esto lo tendremos que tener en cuenta cuando hagamos el plan de cuándo se van a dar los avisos durante la misión.

Recordar: Podemos reaccionar ante una detención que sospechemos que se ha producido, y también ante una detención confirmada.

Es crucial que la reacción de quienes hayan sido detenidas o detenidos y la de la organización no entren en conflicto, que ambas partes busquen los mismos objetivos. Por eso todas y todos los miembros de la organización deberían conocer a fondo todos los procedimientos de reacción.

Detención (o retención, secuestro, o secuestro político):

Las detenciones pueden tener duraciones muy diferentes, desde unas horas a varios años incluso. El caso se resolvería normalmente con la puesta en libertad de la persona, pero podría convertirse en un secuestro si existiera un objetivo más allá de la mera detención, o en los casos más graves (secuestros políticos) podría conllevar la tortura, la muerte o la "desaparición" de la persona.

Podemos abordar la detención desde tres puntos de vista:

- Desde el punto de vista de la(s) persona(s) detenida(s).
- Desde el punto de vista de la organización de la que depende(n).
- Desde el punto de vista de la familia y personas próximas a la(s) persona(s) detenida(s).

Objetivos generales a la hora de abordar una detención:

- Reducir la probabilidad de que se produzca una detención.
- Informarse cuanto antes de las posibilidades de que se produzca una detención.
- Trazar el plan de cómo reaccionar en una situación así:
  - Reacción inmediata.
  - Reacción a medio plazo.

Para simplificar en este manual, trataremos por un lado la detención (que incluirá la retención) y por otro, los secuestros.

Detención de un/a defensor/a: reacción inmediata

Objetivos y pasos de una reacción inmediata ante una detención:

Establecer un grupo de trabajo ad hoc.

1 ◆ Proteger la vida y la libertad de las y los miembros de la organización.

2 ◆ Localizar geográficamente a las personas detenidas, usando un mapa, el plan del viaje, los últimos contactos que se hicieron, llamar a los contactos y actores del terreno, etc.

3 ◆ Averiguar qué actor armado retiene a la persona, por qué y con qué fin.

• Usar la información de la localización geográfica de la(s) persona(s) detenida(s) y todo conocimiento que tengamos sobre el caso (si no podemos averiguarlo, tendríamos que deducir las causas de la detención). Así, tendríamos que poder imaginar quién está reteniendo a la(s) persona(s), o al menos elaborar la lista de sospechosos.

• Ponerse en contacto con las autoridades (si procede, y es necesario y posible).

4 ◆ Conseguir la puesta en libertad del defensor o de la defensora sin que sufra daños.

□ La regla general es que no hay que centrarse en llegar a un acuerdo sino en conseguir "la salida" de la(s) persona(s), su liberación, y sólo negociar tras su liberación.

□ Hacer una valoración del cuerpo armado en cuestión (en colaboración con las autoridades regionales allí donde sea posible/necesario), ya sea de manera directa si se trata de un cuerpo de las fuerzas de seguridad, o a través de intermediarios, como las iglesias, dignatarios o los ancianos del lugar, el Comité Internacional de la Cruz Roja, etc. Para ello, es fundamental poder confiar en estos contactos. Esta valoración tendrá el objetivo de que confirmemos la razón de la detención, e intentemos conseguir la puesta en libertad inmediata de la(s) persona(s) detenida(s).

□ Considerar el poner en alerta a otras organizaciones de defensoras y defensores o humanitarias, para que tengan esa información y puedan tomar las medidas necesarias de forma conjunta, consiguiéndose así mayor presión. Cuando sospechemos de que se trata de un caso de secuestro político en el que la persona puede ser torturada (como en los secuestros de los "escuadrones de la muerte"), es importante actuar lo más rápidamente posible y centrar la acción al máximo en los líderes obvios (si procede) del grupo responsable, o en cuerpos políticos próximos a los responsables del secuestro que puedan ser más sensibles a la presión nacional o internacional.

□ Alertar a los consulados para el caso de que las personas detenidas sean de otro país.

Detención de un/a defensor/a: reacción a medio plazo

Si detienen a una defensora o defensor y sabemos que no podremos conseguir su puesta en libertad a corto plazo, tendremos que plantearnos qué objetivos y pasos deberemos tomar a medio plazo, sin perder de vista, no obstante, los objetivos del corto plazo.

Objetivos y pasos de una reacción a medio plazo ante una detención:

1 ◆ No perder de vista los objetivos a corto plazo.

2 ◆ En el caso de detención, además de identificar tan rápidamente como nos sea posible quién retiene a la defensora o el defensor, debemos intentar conseguir que se le transfiera a custodia legal o a un servicio de seguridad sobre el

que se pueda influir. En este caso, hay que intentar conseguir un apoyo legal pertinente de inmediato (idealmente, lo habríamos preparado de previamente). Así podría reducirse el riesgo de que las personas detenidas sufran malos tratos y sean torturadas.

3 ◆ Si el defensor o la defensora siguen detenidos, debemos intentar atender a sus necesidades personales: seguridad, comida, atención sanitaria, contactos con sus familiares y con la organización, etc. desde el principio y a lo largo de todo el proceso (esto también puede planearse de antemano; ver más abajo, medidas en relación con las familias y otras personas próximas).

Reacciones de las personas detenidas

- Recordar los pasos y planes preparados antes con vistas a que se pudieran producir estas situaciones. Es importante recordar cuidadosamente la secuencia de pasos a dar si se produce una detención, para así minimizar la incertidumbre, usar la fortaleza de manera controlada, y planear objetivos de resistencia sencillos.
- Guardar la calma. Como defensoras y defensores sabemos que la organización dispone de un protocolo de reacción y que se está haciendo algo; podemos repasar esos pasos mentalmente al tiempo que toque que se den, y esto nos ayudará a guardar la calma.
- Todo lo que se diga y se haga debe tener el objetivo de preservar la vida y la integridad de las personas detenidas.
- Ponerse en contacto con el jefe del grupo armado, e intentar dialogar con él, usando argumentos institucionales básicos con el objetivo de obtener la puesta en libertad de las personas detenidas y su vuelta al sitio de donde vinieron o a cualquier otro lugar seguro (no se debe intentar negociar un "acuerdo").
- Si no se nos permite esto, hay que buscar cualquier medio disponible para alertar a la organización sobre nuestro paradero; no hay que intentar llamar sin permiso si nos están vigilando, pues esto podría ser más arriesgado que no hacer nada.
- Si la detención la hacen las fuerzas de seguridad, podremos usar los argumentos legales que da la organización para estos casos.
- No debe cundir el pánico, y habrá que recordar que la organización estará siguiendo todos los pasos del plan de seguridad.

Medidas relativas a las familias y otras personas próximas:

- Informar a la familia y a otras personas próximas si la persona no va a ser puesta en libertad de inmediato. Establecer y mantener una relación de confianza.
- Mantener una relación clara con la familia: se trata de ofrecer apoyo e información (podemos nombrar a una persona para que actúe de contacto con la familia).

- La familia esperará tiempo y atención de la organización. Debemos saber que sus actitudes y actuaciones podría fluctuar.
- Para el caso de una detención o encarcelamiento a largo plazo, es importante disponer de un plan de apoyo a la familia de la persona detenida.

Secuestro de un o una defensora[2]

Desde el punto de vista de la organización

Ocuparse de una crisis de secuestro supone un proceso en continuo cambio que puede durar desde unas horas a meses, incluso años. Serán temas fundamentales poner en funcionamiento un comité de crisis que dirija la respuesta al secuestro; las relaciones con la familia y/o los otros seres queridos, las autoridades y la prensa; la comunicación y las negociaciones con los secuestradores.

Comunicación y negociación con los secuestradores

El secuestro que no es por motivos políticos suele implicar que los secuestradores se pondrán en contacto en este caso con la organización para transmitir sus exigencias y dar instrucciones.

El comité de crisis tendrá que dirigir las negociaciones evitando tener un contacto directo con los secuestradores; así se puede ganar tiempo para tomar decisiones y hacer consultas tanto internas como externas. Asimismo, se pueden pedir pruebas de que la persona secuestrada está viva, y pruebas de que los secuestradores son quien dicen ser, además de instigar y exigir que se le dé un buen trato a la o las personas cautivas.

Si el secuestro es un escenario muy posible, es importante que en la organización se hayan aprobado normas y procedimientos relativos al rescate y las peticiones de los secuestradores, preferiblemente, si es adecuado, similares a las de otras organizaciones, y además, que todo el mundo las conozca. En cualquier caso, anteriores casos similares nos servirán para reunir información sobre las fases de un secuestro.

Desde el punto de vista del defensor o la defensora secuestrado/a

- Los momentos que entrañan más peligro, cuando los secuestradores estarán más nerviosos, son durante el momento en que se captura a la persona (pues se la tiene que trasladar rápidamente para evitar ser capturados por las autoridades), en las situaciones de cerco y durante la puesta en libertad.

- Los secuestradores querrán que estemos en silencio; podrían taparnos los ojos, golpearnos, incluso drogarnos para que así sea. No tiene sentido gritar o luchar para oponerse a estas tácticas: de hecho, guardar silencio podría evitarnos todo eso (a no ser que sea razonable pensar que durante el secuestro gritar pueda hacer que alguien nos oiga y nos procure ayuda).

[2] Para este tema hemos recurrido a la fuente de van Brabant (2000).

- El lugar y las condiciones en que se tiene a la gente secuestrada pueden variar mucho. Podrían tenernos en un solo sitio o trasladarnos varias veces; podríamos estar solos o solas, o con un grupo de personas secuestradas. Es habitual que se desarrolle una relación con los guardianes, y que nos cueste irnos adaptando a que nos cambien de guardianes.

Conviene:

- Obedecer las órdenes de los secuestradores sin parecer serviles; y evitar sorprenderles o alarmarles.

- Intentar mantenerse en forma físicamente y en un buen estado de salud mental.

- Si estamos en un grupo, intentar que no nos separen de él, pues estar aunque sea con otra persona puede ser de gran ayuda. No obstante, tenemos que estar preparadas/os ante la eventualidad de que nos separen, o de que se produzcan otros cambios, y en general, ante la incertidumbre que pueda traernos, que tendremos que enfrentar y superar.

- Conseguir ser puestas/os en libertad no es la misión de las personas secuestradas, sino la de sus organizaciones. Nunca debemos negociar con los secuestradores por nuestra cuenta, pues esto podría complicar mucho las cosas. Si éstos nos dicen que hablemos por una radio, teléfono o vídeo, sólo tendremos que decir lo que nos dicen o permiten que digamos, y tendremos que negarnos a negociar aunque nuestros captores nos presionen para que lo hagamos.

Procedimientos de prevención: cómo reducir los riesgos de detención o secuestro durante un viaje

Los riesgos de detención o secuestro son particularmente altos durante un viaje o en una misión porque estamos más expuestas y expuestos, tenemos menos contacto con nuestro entorno habitual, y quienes nos rodean podrían tardar en reaccionar ante una amenaza o un ataque. Por esta razón indicamos que los riesgos vinculados a una misión de campo incluyen la mayoría de las amenazas / consecuencias relacionados con nuestro trabajo en su conjunto.

Por ejemplo:

Puestos de control (check points) ⇨ retención ⇨ detención ⇨ ...
Ataques ⇨ secuestro político ⇨ violencia ⇨ ...

Pérdida de información ⇨ impacto en testigos ⇨ impacto en organización ⇨...
Transporte ⇨ público / privado ⇨ ...

Tiempo libre en las misiones de campo ⇨ bajar la guardia ⇨ incidentes de seguridad ⇨...
Comunicación ⇨ teléfono ⇨ en persona ⇨ ...

Desearíamos insistir en el riesgo que existe de detención / secuestro durante una misión de campo y recomendar que el protocolo de prevención para las misiones de campo incluya al menos:

- Preparación para todas las misiones, tanto al campo como a barrios difíciles de zonas urbanas.
- No viajar sola/o.
- Información adecuada sobre la zona y los actores que vamos a visitar (hacer un mapa de los actores, como mostrábamos en el análisis de las fuerzas de campo en el capítulo 1.1).
- Las y los defensores deberían conocer bien las rutas de acceso y salida de los lugares que visiten.
- Todas las personas que participen en la misión deben disponer de documentos de identidad válidos.
- Avisar a los contactos de la red de emergencia de la organización a quienes corresponda estar alerta durante la misión (desde el momento de su salida hasta que esté de vuelta).
- Preparar la misión siguiendo los procedimientos acordados: incluir la agenda y el trabajo que debe realizarse, y seguir todos los puntos del manual de seguridad de la organización.
- Planificar actualizaciones regulares sobre el estado de la misión (normalmente por teléfono, a horas que hayamos acordado previamente). Implica, donde sea posible, comprobar si en la ruta y en los destinos finales existen teléfonos. Si no es posible averiguarlo, podríamos considerar la posibilidad de recurrir a personas de confianza que vivan en puntos de esa ruta para confirmar que el equipo ha pasado por allí.

  Es importante decidir el tiempo que habrá de esperar la persona a cargo de estar pendiente de las llamadas del equipo antes de pasar a preocuparse en la situación de que haya estado intentando ponerse en contacto con el equipo y no lo haya conseguido. Conviene recordar que es más fácil reconstruir un secuestro político cuando han pasado pocas horas.
- Valorar la seguridad del medio de transporte elegido (que podrá ser a veces un vehículo de la propia organización y otro transporte público, para poder estar rodeadas y rodeados de testigos potenciales). Para el caso de transporte público, habrá que valorar si ir juntas/os en él o si hacer como que no nos conocemos. Esto podría hacer posible que, si pasara algo, algún miembro de la organización quedara libre para avisar a la organización; intervenir eliminaría esa posibilidad.
- Si los viajes se realizan en un vehículo propio, éste tendría que estar a punto en todo momento (y respetar el límite de velocidad y el código de circulación). En carretera, no parar para ofrecer llevar a personas que estén haciendo autostop.
- Donde sea relevante, entregar información adecuada a autoridades civiles, militares y de la comunidad, y también a quienes sean responsables de la misión (para que asuman su responsabilidad en temas de seguridad de la misión y no digan que "no lo sabíamos").
- Presentar una explicación bien preparada sobre los objetivos y el mandato de la organización, intentando que ésta pueda serle aceptable a grupos armados y fuerzas de seguridad (es mejor no adaptarla a un grupo

armado con el que nos topemos, pues podría ser difícil identificar quiénes son y podríamos cometer un error).

- Valorar cuál es la mejor hora para salir de viaje. En ocasiones, por el calor, será mejor partir cuando aún es de noche, a pesar de que eso no es lo más recomendable desde el punto de vista de la seguridad, pues si atacan al equipo en esas horas tempranas, es posible que los contactos que se ocupen de las emergencias en la organización no estén aún en la oficina, y las primeras horas de un secuestro político son absolutamente cruciales para que podamos seguirle la pista al curso de los acontecimientos.
- No viajar de noche.
- Nunca ir mostrando abiertamente objetos de valor (cámaras de foto o vídeo).
- Comportarse adecuadamente en el viaje.
- Conviene que la organización consiga algún tipo de permiso para su trabajo en la zona visita (incluido, allí donde sea posible, noticia de que nuestro trabajo será tolerado por los grupos armados).

Además, para el caso de una llamada de una tercera parte tras la partida del equipo a una misión de campo:

- Comprobar la identidad de quien haga la llamada (también llamando a nuestros contactos de otras organizaciones de confianza).
- Comprobar por varios medios que los detalles de los hechos que nos cuentan son verdaderos.
- Valorar si conviene ir al lugar de los hechos o si sería más seguro para todo el mundo que la información saliera de allí hacia la organización (ver gestión de la información: protocolo de prevención y reacción).
- Valorar si es necesario ir allí en ese mismo momento, justo después de la llamada, en especial si no conocemos a la persona que llama (habría que comprobar esa información con alguien más al menos). Además, debería tenerse en cuenta que la misión no va a evitar los hechos, pues ya han ocurrido (por eso nos han llamado).
- En general, el mejor consejo es evitar improvisaciones y cambios de planes cuando se esté visitando una zona peligrosa.

Resumen

Entendemos que detener a una persona puede ser un proceso legal. Cuando el hecho va más allá de lo legal, entonces puede considerarse la privación injustificada de la libertad de una persona. La duración de esta privación puede variar de unas horas a años...

Una detención debería abordarse desde tres puntos de vista:

- Desde el punto de vista de la(s) persona(s) detenida(s).
- Desde el punto de vista de la organización de la que dependen la(s) persona(s) detenida(s).
- Desde el punto de vista de la familia y demás personas queridas de la(s) persona(s) detenida(s).

Objetivos generales a la hora de abordar una detención:

- Reducir la probabilidad de que se produzca una detención.
- Informarse cuanto antes de las posibilidades de que se produzca una detención.
- Trazar el plan de cómo reaccionar en una situación así: reacción inmediata y reacción a medio plazo.

El secuestro político es ilegal y puede producirse en cualquier momento, normalmente, cuando les surge la oportunidad de llevarlo a cabo. Es una de las consecuencias posibles de un ataque. Por lo tanto, las medidas de seguridad que adoptemos tendrán que ser similares a las que usamos para prevenir agresiones o ataques (ver capítulo 1.5): reducir la exposición física al máximo...

CAPÍTULO 3.3

Gestión segura de la información

Las organizaciones de derechos humanos manejan información que en un entorno hostil hacia las y los defensores podría ser utilizada contra la seguridad de la organización, otras personas e instituciones. Por lo tanto, es fundamental establecer un procedimiento de gestión segura de la información y un plan de reacción ante cualquier incidente que afecte la seguridad de la información manejada por la organización.

Gestión segura de la información: procedimiento de prevención

Los datos que guardan las organizaciones de derechos humanos pueden agruparse en dos categorías que se establecen en función de su nivel de sensibilidad: alta confidencialidad y baja confidencialidad.

Cualquier información que manejemos atraviesa cuatro pasos diferentes antes de llegar a nuestras manos y antes de dejarnos (allí donde ocurra). Perfilaremos las medidas de seguridad que se requieren en cada paso.

1 • Fuente: recogida de información en punto de encuentro.

2 • Transferencia de la información.

3 • Procesamiento y almacenamiento.

4 • Distribución.

1 • Fuente: recogida de información en punto de encuentro

El principal problema aquí es la protección de la información y de la gente a la que esta información afecta.

La persona que deja la información necesita una ruta entre su casa/oficina y el punto de encuentro; un punto de encuentro (el lugar donde esa persona se reúne con alguien de nuestra organización), que puede ser su casa, su lugar de trabajo, la oficina de la organización o cualquier otro sitio; y una ruta para marcharse. Hay que disponer de un sitio seguro y de condiciones seguras para reunirse, así como de una ruta para que la información llegue

y deje la fuente y una ruta para la llegada y salida de miembros de la organización que a su vez trasferirán la información (asegurar cuanto mejor los desplazamientos a y de los puntos de encuentro).

Una gestión segura de la información empieza incluso antes de que nos llegue la información.

- ¿Necesita la organización esa información?

¿Podrá usarla para mejorar su trabajo o ser más eficaz en la consecución de sus objetivos generales o específicos? Si no fuera así, es mejor **no recibir** esa información. Si no cae dentro de nuestra esfera de competencia, es mejor remitirla a otra organización y no hacerse cargo ni de la información ni del caso.

- Hay que informar a la persona que nos da la información de quiénes somos, cuáles son nuestros objetivo y trabajo, cómo se gestionará la información en nuestra organización; el tipo de información que necesitamos, cómo la custodiaremos y utilizaremos; y lo que se puede esperar de nosotras o nosotros. Es fundamental y ético que la persona que dé la información sepa de antemano (ya sea directamente o a través de terceras partes) los riesgos que entraña transmitir información, y todos los usos que la organización puede darle a ésta.

No hay que presuponer que ya lo sabe. Es importante explicarlo todo para cerciorarnos de que esa persona es consciente de todo. Asimismo, es importante definir con ella las medidas de seguridad que tendríamos que tomar.

El punto de encuentro debe ser lo más seguro y anónimo posible. Con toda probabilidad, la casa de esa persona no será un sitio seguro, porque la llegada de alguien de una organización sería algo muy visible. Quizá sea un sitio algo más seguro la oficina de la organización (si allí se respeta la confidencialidad) o algún otro lugar bastante público donde haya gente yendo y viniendo todo el rato (p.e. una parroquia, centro comunitario; una vez más, siempre y cuando se respete la confidencialidad). Si se ha quedado en un sitio inadecuado, podría trasladarse la cita a un lugar más seguro según la sensibilidad de la información que vaya a transmitirse. También podría usarse una historia pretexto, que encubra nuestro verdadero objetivo: visita al dentista (mostrar dolor de muelas), visita médica (cualquier enfermedad), mercado, etc., y entonces habrá que volver a casa con pruebas reales de ese pretexto que se ha usado para salir de casa (por ejemplo, con la receta médica o medicinas, cosas que hubiera que comprar y que no hubiera en el lugar de residencia).

Nunca debemos olvidar que para la persona que entrega la información, los problemas de seguridad pueden darse **después** de que nos la haya entregado en el lugar convenido.

2 ● Transferencia de la información

La información puede reunirse en varios formatos: memoria USB, impresa, notas o en un ordenador, como fotos, etc.

El método rutinario más seguro para transferir información es por ordenador portátil, memoria USB o CD-Rom encriptado. La reunión puede grabarse, las fotos almacenarse y se puede mecanografiar la información. Se considera que todos los demás medios son menos seguros, lo que incrementa los riesgos en el proceso de transferencia.

Sólo las y los miembros de la organización que son conscientes de lo que llevan encima puede transportar información confidencial.

A menudo las y los defensores de derechos humanos viajan con cuadernos llenos de información importante que no necesitan en la misión que les ocupa en ese momento. Esto se debe a que usan el mismo cuaderno hasta gastar la última hoja, en lugar de decidir viajar sólo con la cantidad de papel o material que vayan a necesitar. Lo mismo suelen hacer con el contenido de las memorias USB, los ordenadores y demás soportes para la información.

3 ● Almacenamiento y procesamiento de la información

Cuando la información llega a la oficina, por regla general, podemos decir que la información ya está más a salvo (aunque esto dependerá de cómo de segura sea la oficina; ver capítulo sobre la seguridad en las casas y oficinas).

Criterios de particular relevancia para la información son:

Archivo de documentos impresos: sólo debería usarse cuando sea estrictamente necesario; la documentación necesaria de casos concretos debería ser entregada en persona. La información en papel debería almacenarse en cajas de metal con cerrojo; y deberíamos plantearnos disponer de cámara acorazada para guardar nuestros archivos en papel.

También podríamos considerar la posibilidad de repartir los papeles por varios sitios seguros o enviarlos a otros lugares usando las mismas precauciones que se describen en el apartado "Transferencia de información". La información también puede escanearse, encriptarse y enviarse a un organismo de nuestra confianza (por ejemplo, un homólogo internacional).

Los sistemas y códigos para encriptar deberían usarse adecuadamente.

Hacer copias de seguridad semanales, y almacenarlas, tras encriptarlas, en un lugar seguro (p.e., una caja fuerte).

4 ● Distribución de la información

Entre los criterios generales relativos a la distribución de la información encontramos:

- Comprobar varias veces la información.

- Allí donde la organización sea la única fuente de información sobre ciertos datos, se estarán corriendo más riesgos y por lo tanto, tendremos que disponer de planes de contingencia.

- Es preciso tener la autorización informada de quienes nos dan la información, especialmente si a estas personas se las puede identificar en ella como únicas fuentes de información sobre esos datos.

- Cualquier información escrita que vaya a abandonar la organización u organizaciones aliadas deberíamos considerarla "pública" (y tratarla en consecuencia) por el riesgo de que caiga en manos de quien no debería caer, o por las sorpresas que puedan darnos a diario los medios que usamos para comunicarnos.

- Es crucial que la organización que publique la información tenga una muy cuidada política de publicación, que debería incluir los principales criterios de seguridad aplicables al tratamiento de la información (entre ellos, normas sobre cómo redactar esa información).

Acceso a la información de personas que no son miembros de la organización (ayudantes, voluntarias, voluntarios, etc.).

Por la seguridad de la organización "debe restringirse el acceso a estos archivos digitales o fisicos de terceras partes, ayudantes, voluntarias y voluntarios (el grado habrá que decidirlo según el caso), y estará a cargo de ellos alguien con un puesto de responsabilidad en la organización.

Podría ser útil incorporar al contrato o acuerdo de trabajo de ayudantes y gente voluntaria una cláusula de confidencialidad que debería cumplirse en todo momento. Esta cláusula habría que incluirla también los contratos del personal subcontratado por la organización.

Gestión segura de los datos: cómo reaccionar frente a robo o pérdida

El robo o la pérdida (a veces no se sabrá cuál es) de los datos que tiene la organización debería hacernos reaccionar como si la información fuera a caer necesariamente en manos de quien no debería tenerla y como si se fuera a hacer el peor uso de ella, lo que afectaría a terceras partes (a quienes nos la dieron, a personas de otras organizaciones, etc.) o a nuestra propia organización.

Si a pesar de todas las medidas de prevención adoptadas, se produce una pérdida o un robo de información, deberíamos actuar como si se hubiera producido un caso grave de amenaza a la seguridad, ante lo cual seguiremos estos pasos:

1 ◆ Informar de inmediato a la gente de la organización.

2 ◆ Determinar cuánta información se ha perdido y cómo de sensible era, conforme al peligro en que ponga a la gente directamente afectada por la información, a terceras partes o a la organización, y conforme a por qué pone en peligro (o los vectores del riesgo). Esta valoración tendrá que hacerse con cada tipo de información robada, allí donde hayan robado varios tipos (p.e. listas de personas, fuentes e información recogida sobre casos individuales).

3 ◆ Valorar el tema de informar posteriormente a las personas e instituciones potencialmente afectadas para que puedan tomar medidas para protegerse (siempre con la máxima discreción posible).

4 ◆ Valorar la posibilidad de informar a las autoridades y de hacer públicos los hechos.

5 ◆ Allí donde fuera necesario, poner en marcha cualquier otro paso que haya que dar para evitar los daños que pueden producirse si usan la información perdida o robada.

La organización tendrá también que decidir hasta qué punto deben exponerse sus miembros a la hora de proteger la información: por ejemplo, para el caso de un registro violento, habrá que plantearse si realmente conviene presentar resistencia.

Resumen

Una gestión segura de la información requiere protocolos de prevención y reacción.

La prevención debe considerar cuatro momentos:

1 • Fuente: recogida de información en punto de encuentro.

2 • Transferencia de la información.

3 • Procesamiento y almacenamiento.

4 • Distribución.

La reacción debería incluir como poco:

1 • Informar de inmediato a la gente de la organización.

2 • Determinar cuánta información se ha perdido y cómo de sensible era.

3 • Valorar el tema de informar posteriormente a las personas e instituciones potencialmente afectadas.

4 • Valorar la posibilidad de informar a las autoridades y de hacer públicos los hechos.

5 • Dar cualquier otro paso necesario para evitar los daños que pueden producirse si usan la información perdida o robada.

CAPÍTULO 3.4

La Seguridad y el tiempo libre

Reflexión:

En general, las normas de seguridad se siguen cuando no contrarían intereses personales. Por eso es más fácil abordar la seguridad en la oficina, por ejemplo, que en el tiempo libre. Y sin embargo, el tiempo libre es un elemento fundamental tanto de la seguridad de cada persona como de la de la organización. Es necesario discutir y entender cómo las necesidades personales pueden interferir con los temas de seguridad.

El tiempo libre

Aquí os presentamos una serie de preguntas y reflexiones que nos pueden ayudar a diseñar una política para el tiempo libre. Como con cualquier otro elemento de la seguridad, es importante explorarlas lo más a fondo posible, incluso si esto implica abrir una brecha en el ámbito de lo privado (los incidentes de seguridad también pueden hacer eso mismo).

Empezamos con dos reflexiones importantes:

- Si desean hacer daño a una organización, probablemente no atacarán a las y los miembros que mejor se protegen o a quienes respetan las normas de seguridad; irán a por los puntos débiles, en particular, en su tiempo libre (por la noche y los fines de semana, etc.).
- Si una organización tiene 10 miembros, de los cuales uno o dos no respetan las normas de seguridad en su tiempo libre, serán todas las personas de la organización, y no sólo esa una o dos, quienes estén en peligro porque un ataque a esa(s) persona(s) le afectaría a toda la organización.

La pregunta fundamental es siempre: "¿existe un riesgo asociado a...?". Si la respuesta es "no", entonces no pasa nada. Si es "sí", habrá que explorar y decidir si existen maneras de satisfacer una necesidad personal en un entorno protegido, si la necesidad debe ser pospuesta para tiempos más seguros, o si debemos renunciar a ella porque es incompatible con la protección de una defensora o defensor de derechos humanos.

¿Cuidamos la seguridad sólo durante horas de trabajo o las veinticuatro horas del día siete días a la semana?

Aunque es difícil distinguir entre las políticas de la organización y la autonomía de cada miembro en su tiempo libre, al trabajar la prevención de ataques y las reacciones a los mismos no se diferencia entre ataques en horas de trabajo y los que ocurren en nuestro tiempo libre... No debemos olvidar que si deciden hacer daño a una organización atacando a uno de sus miembros, no lo harán en horas de trabajo, sino cuando ese defensor sea más vulnerable. Esperarán su oportunidad: un ataque de noche o cuando salimos de un club es mucho más fácil de disimular o encubrir...

En los países donde beber alcohol es una costumbre, ¿corremos riesgos si nos emborrachamos?

Emborracharse tiene, sin duda alguna, un impacto en las cuestiones de seguridad. El defensor podría ponerse a hablar, su comportamiento cambia y podría no enterarse de que le están sacando información o provocando deliberadamente. Esto tiene un impacto claro en la imagen de la organización, aunque no lo tuviera directamente en la seguridad del defensor. Debemos recordar también que un defensor borracho le está dando la oportunidad a cualquier grupo hostil para atacar a su organización (lo mismo ocurre con el resto de las drogas). Consideramos que el tema del uso del alcohol o demás drogas no debería abordarse desde un punto de vista moral o de la salud, sino desde el punto de vista de la seguridad.

¿Pueden las relaciones secretas y eventuales influir en los temas de seguridad?

- Se han dado casos de defensores de derechos humanos que no volvieron a su organización (y no avisaron) porque tenían un asunto privado. La organización alertó a su red de emergencia, y resultó que esas personas estaban perfectamente, que ni se habían enterado del problema generado. Este tipo de situación da claramente a otros la oportunidad de desacreditar tanto a la organización como a la persona que la genera. Y además, puede ocurrir que haya personas que decidan dejar la red de emergencia.

- El problema no es tener una relación, sino cómo esa relación influye en temas de comunicación y seguridad. Como mencionábamos, no se trata de un problema moral o de salud, sino de un tema de seguridad. Es crucial que en la organización se analicen estos temas para buscar maneras de plantearlos bien.

- **¿Qué pasa cuando en la organización hay quien sospecha del amigo o la amiga de un o una defensora? ¿Puede la organización intervenir?**

- ¿En qué formas puede pasarse información a las amistades, la familia y demás personas cercanas? ¿Sería el o la defensora de derechos humanos responsable de cómo pudiera usarse esa información?

La manera en que disfrutan las y los defensores de su tiempo libre puede tener repercusiones en la seguridad de todo el mundo. La cuestión no es negarle a la gente la posibilidad de disfrutar de su tiempo libre, sino de ver cómo podemos hacer para disfrutarlo.

Todas las organizaciones de defensa de los derechos humanos que corran peligro necesitan disponer de una política sobre el tiempo libre, que incluya la noche y las vacaciones.

Habría que hacer una mención especial sobre el uso público del alcohol y de otras drogas, sobre la cuestión de las relaciones personales secretas, y sobre tiempo libre e imagen, con objeto de evitar que estos temas puedan interferir con los de seguridad en la organización.

¿Cómo manejar la confidencialidad de la información?

Y dado que la información puede filtrarse en cualquier momento, incluido en nuestro tiempo libre, presentamos aquí algunos puntos más a considerar en relación al tema de la información y la seguridad.

La organización debería establecer al menos dos niveles diferentes de confidencialidad de la información:

a • Lo que sólo deben saber unas pocas personas de la organización.

b • Lo que todas y todos los miembros de la organización pueden saber.

Esto contribuye a reducir el riesgo de que se filtre información, sea por negligencia y/o porque existan personas infiltradas. Además, nos ayuda a identificar dónde se produce la filtración.

¿Podrían influir algunos aspectos de nuestro comportamiento en nuestro tiempo libre en la imagen de nuestra organización?

- ¿Cómo nos ven las demás personas?
- ¿Hasta qué punto tienen noticia otras y otros compañeros de lo que hacemos en nuestro tiempo libre?
- ¿Qué impacto tiene la imagen que da la organización en relación con el tema de la seguridad?
- ….

Resumen

Una defensora o un defensor que esté en situaciones de riesgo debe cuidar el tema de la seguridad las 24 horas del día, los siete días de la semana, en todos los aspectos de sus vidas, incluido el tiempo libre.

El tiempo libre es un tema que precisa ser contemplado seriamente.

La pregunta a hacerse siempre es: "¿existe un riesgo asociado a...?" Si la respuesta es "no", entonces, no hay problema. Si es "sí", será necesario explorar el tema y tomar decisiones sobre si existen maneras de colmar una necesidad personal en un entorno protegido, si la necesidad debe ser pospuesta hasta que lleguen tiempos menos peligrosos, o si debe ser abandonada por ser incompatible con las necesidades de seguridad que tiene esa persona como defensora o defensor de derechos humanos.

Todas las organizaciones de defensa de los derechos humanos que corran peligro necesitan disponer de una política relativa al tiempo libre, que incluya la noche y las vacaciones. Habría que hacer una mención especial sobre el uso público del alcohol y de otras drogas, sobre la cuestión de las relaciones personales secretas, y sobre tiempo libre e imagen, con objeto de evitar que estos temas puedan interferir con los de seguridad en la organización.

Como en el tiempo libre también corremos riesgos, es importante no olvidar que es necesario hacer valoraciones muy bien meditadas sobre estos riesgos que corremos.

ANEXO I

Declaración de la ONU sobre Defensores de Derechos Humanos

NACIONES UNIDAS **A**

Asamblea General

Distr.
GENERAL
A/RES/53/144
18 de marzo de 2005

Quincuagésimo tercer período de sesiones
Tema 105 b) del programa

RESOLUCIÓN APROBADA POR LA ASAMBLEA GENERAL

[sobre la base del informe de la Tercera Comisión (A/53/625/Add.2)]

53/144. 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

La Asamblea General,

Reafirmando la importancia de la observancia de los propósitos y principios de la Carta de las Naciones Unidas para la promoción y la protección de todos los derechos humanos y libertades fundamentales para todas las personas en todos los países del mundo, abril de 1998, por la cual la Comisión aprobó el texto del proyecto de 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,

Tomando nota asimismo de la resolución 1998/33 del Consejo Económico y Social, de 30 de julio de 1998, por la cual el Consejo recomendó a la Asamblea General que aprobara el proyecto de declaración,

Consciente de la importancia de la aprobación del proyecto de declaración en elcontexto del cincuentenario de la Declaración Universal de Derechos Humanos,

1. *Aprueba* 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 que figura en el anexo de la presente resolución;

2. *Invita* a los gobiernos, a los organismos y organizaciones del sistema de las Naciones Unidas y las organizaciones intergubernamentales y no gubernamentales a que intensifiquen sus esfuerzos por difundir la Declaración, promover el respeto universal hacia ella y su comprensión, y pide al Secretario General que incluya el texto de la Declaración en la próxima edición de *Derechos humanos: Recopilación de instrumentos internacionales.*

85a. sesión plenaria
9 de diciembre de 1998

ANEXO

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.

La Asamblea General,

Reafirmando la importancia que tiene la observancia de los propósitos y principios de la Carta de las Naciones Unidas para la promoción y la protección de todos los derechos humanos y las libertades fundamentales de todos los seres humanos en todos los países del mundo,

Reafirmando también la importancia de la Declaración Universal de Derechos Humanos y de los Pactos internacionales de derechos humanos como elementos fundamentales de los esfuerzos internacionales para promover el respeto universal y la observancia de los derechos humanos y las libertades fundamentales, así como la importancia de los demás instrumentos de derechos humanos adoptados en el marco del sistema de las Naciones Unidas y a nivel regional,

Destacando que todos los miembros de la comunidad internacional deben cumplir, conjunta y separadamente, su obligación solemne de promover y fomentar el respeto de los derechos humanos y las libertades fundamentales de todos, sin distinción alguna, en particular sin distinción por motivos de raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social, y reafirmando la importancia particular de lograr la cooperación internacional para el cumplimiento de esta obligación, de conformidad con la Carta,

Reconociendo el papel importante que desempeña la cooperación internacional y la valiosa labor que llevan a cabo los individuos, los grupos y las instituciones al contribuir a la eliminación efectiva de todas las violaciones de los derechos humanos y las libertades fundamentales de los pueblos y los individuos, incluso en relación con violaciones masivas, flagrantes o sistemáticas como las que resultan del apartheid, de todas las formas de discriminación racial, colonialismo, dominación u ocupación extranjera, agresión o amenazas contra la soberanía nacional, la unidad nacional o la integridad territorial, y de la negativa a reconocer el derecho de los pueblos a la libre determinación y el derecho de todos los pueblos a ejercer plena soberanía sobre su riqueza y sus recursos naturales,

Reconociendo la relación entre la paz y la seguridad internacionales y el disfrute de los derechos humanos y las libertades fundamentales, y consciente de que la ausencia de paz y seguridad internacionales no excusa la inobservancia de esos derechos,

Reiterando que todos los derechos humanos y las libertades fundamentales son universalmente indivisibles e interdependientes y que están relacionados entre sí, debiéndose promover y aplicar de una manera justa y equitativa, sin perjuicio de la aplicación de cada uno de esos derechos y libertades,

Destacando que la responsabilidad primordial y el deber de promover y proteger los derechos humanos y las libertades fundamentales incumbe al Estado,

Reconociendo el derecho y el deber de los individuos, los grupos y las instituciones de promover el respeto y el conocimiento de los derechos humanos y las libertades fundamentales en el plano nacional e internacional,

Declara:

Artículo 1

Toda persona tiene derecho, individual o colectivamente, a promover y procurar la protección y reali-zación de los derechos humanos y las libertades fundamentales en los planos nacional e internacional.

Artículo 2

1. Los Estados tienen la responsabilidad primordial y el deber de proteger, promover y hacer efectivos todos los derechos humanos y las libertades fundamentales, entre otras cosas, adoptando las medidas necesarias para crear las condiciones sociales, económicas, políticas y de otra índole, así como las garantías jurídicas requeridas para que toda persona sometida a su jurisdicción, individual o colectivamente, pueda disfrutar en la práctica de todos esos derechos y libertades.

2. Los Estados adoptarán las medidas legislativas, administrativas y de otra índole que sean necesarias para asegurar que los derechos y libertades a que se hace referencia en la presente Declaración estén efectivamente garantizados.

Artículo 3

El derecho interno, en cuanto concuerda con la Carta de las Naciones Unidas y otras obligaciones internacionales del Estado en la esfera de los derechos humanos y las libertades fundamentales, es el marco jurídico en el cual se deben materializar y ejercer los derechos humanos y las libertades fundamentales y en el cual deben llevarse a cabo todas las actividades a que se hace referencia en la presente Declaración para la promoción, protección y realización efectiva de esos derechos y libertades.

Artículo 4

Nada de lo dispuesto en la presente Declaración se interpretará en el sentido de que menoscabe o contradiga los propósitos y principios de la Carta de las Naciones Unidas ni de que limite las disposiciones de la Declaración Universal de Derechos Humanos, de los Pactos internacionales de derechos humanos o de otros instrumentos y compromisos internacionales aplicables en esta esfera, o constituya excepción a ellas.

Artículo 5

A fin de promover y proteger los derechos humanos y las libertades fundamentales, toda persona tiene derecho, individual o colectivamente, en el plano nacional e internacional:

a) A reunirse o manifestarse pacíficamente;

b) A formar organizaciones, asociaciones o grupos no gubernamentales, y a afiliarse a ellos o a participar en ellos;

c) A comunicarse con las organizaciones no gubernamentales e intergubernamentales.

Artículo 6

Toda persona tiene derecho, individualmente y con otras:

a) A conocer, recabar, obtener, recibir y poseer información sobre todos los derechos humanos y libertades fundamentales, con inclusión del acceso a la información sobre los medios por los que se da efecto a tales derechos y libertades en los sistemas legislativo, judicial y administrativo internos;

b) Conforme a lo dispuesto en los instrumentos de derechos humanos y otros instrumentos internacionales aplicables, a publicar, impartir o difundir libremente a terceros opiniones, informaciones y conocimientos relativos a todos los derechos humanos y las libertades fundamentales;

c) A estudiar y debatir si esos derechos y libertades fundamentales se observan, tanto en la ley como en la práctica, y a formarse y mantener una opinión al respecto, así como a señalar a la atención del público esas cuestiones por conducto de esos medios y de otros medios adecuados.

Artículo 7

Toda persona tiene derecho, individual o colectivamente, a desarrollar y debatir ideas y principios nuevos relacionados con los derechos humanos, y a preconizar su aceptación.

Artículo 8

1. Toda persona tiene derecho, individual o colectivamente, a tener la oportunidad efectiva, sobre una base no discriminatoria, de participar en el gobierno de su país y en la gestión de los asuntos públicos.

2. Ese derecho comprende, entre otras cosas, el que tiene toda persona, individual o colectivamente, a presentar a los órganos y organismos gubernamentales y organizaciones que se ocupan de los asuntos públicos, críticas y propuestas para mejorar su funcionamiento, y a llamar la atención sobre cualquier aspecto de su labor que pueda obstaculizar o impedir la promoción, protección y realización de los derechos humanos y las libertades fundamentales.

Artículo 9

1. En el ejercicio de los derechos humanos y las libertades fundamentales, incluidas la promoción y la protección de los derechos humanos a que se refiere la presente Declaración, toda persona tiene derecho, individual o colectivamente, a disponer de recursos eficaces y a ser protegida en caso de violación de esos derechos.

2. A tales efectos, toda persona cuyos derechos o libertades hayan sido presuntamente violados tiene el derecho, bien por sí misma o por conducto de un representante legalmente autorizado, a presentar una denuncia ante una autoridad judicial independiente, imparcial y competente o cualquier otra autoridad establecida por la ley y a que esa denuncia sea examinada rápidamente en audiencia pública, y a obtener de esa autoridad una decisión, de conformidad con la ley, que disponga la reparación, incluida la indemnización que corresponda, cuando se hayan violado los derechos o libertades de esa persona, así como a obtener la ejecución de la eventual decisión y sentencia, todo ello sin demora indebida.

3. A los mismos efectos, toda persona tiene derecho, individual o colectivamente, entre otras cosas, a:

a) Denunciar las políticas y acciones de los funcionarios y órganos gubernamentales en relación con violaciones de los derechos humanos y las libertades fundamentales mediante peticiones u otros medios adecuados ante las autoridades judiciales, administrativas o legislativas internas o ante cualquier otra autoridad competente prevista en el sistema jurídico del Estado, las cuales deben emitir su decisión sobre la denuncia sin demora indebida;

b) Asistir a las audiencias, los procedimientos y los juicios públicos para formarse una opinión sobre el cumplimiento de las normas nacionales y de las obligaciones y los compromisos internacionales aplicables;

c) Ofrecer y prestar asistencia letrada profesional u otro asesoramiento y asistencia pertinentes para defender los derechos humanos y las libertades fundamentales.

4. A los mismos efectos, toda persona tiene el derecho, individual o colectivamente, de conformidad con los instrumentos y procedimientos internacionales aplicables, a dirigirse sin trabas a los organismos internacionales que tengan competencia general o especial para recibir y examinar comunicaciones sobre cuestiones de derechos humanos y libertades fundamentales, y a comunicarse sin trabas con ellos.

5. El Estado realizará una investigación rápida e imparcial o adoptará las medidas necesarias para que se lleve a cabo una indagación cuando existan motivos razonables para creer que se ha producido una violación de los derechos humanos y las libertades fundamentales en cualquier territorio sometido a su jurisdicción.

Artículo 10

Nadie participará, por acción o por el incumplimiento del deber de actuar, en la violación de los derechos humanos y las libertades fundamentales, y nadie será castigado ni perseguido por negarse a hacerlo.

Artículo 11

Toda persona, individual o colectivamente, tiene derecho al legítimo ejercicio de su ocupación o profesión. Toda persona que, a causa de su profesión, pueda afectar a la dignidad humana, los derechos humanos y las libertades fundamentales de otras personas deberá respetar esos derechos y libertades y cumplir las normas nacionales e internacionales de conducta o ética profesional u ocupacional que sean pertinentes.

Artículo 12

1. Toda persona tiene derecho, individual o colectivamente, a participar en actividades pacíficas contra las violaciones de los derechos humanos y las libertades fundamentales.

2. El Estado garantizará la protección por las autoridades competentes de toda persona, individual o colectivamente, frente a toda violencia, amenaza, represalia, discriminación, negativa de hecho o de derecho, presión o cualquier otra acción arbitraria resultante del ejercicio legítimo de los derechos mencionados en la presente Declaración.

3. A este respecto, toda persona tiene derecho, individual o colectivamente, a una protección eficaz de las leyes nacionales al reaccionar u oponerse, por medios pacíficos, a actividades y actos, con inclusión de las omisiones, imputables a los Estados que causen violaciones de los derechos humanos y las libertades fundamentales, así como a actos de violencia perpetrados por grupos o particulares que afecten el disfrute de los derechos humanos y las libertades fundamentales.

Artículo 13

Toda persona tiene derecho, individual o colectivamente, a solicitar, recibir y utilizar recursos con el objeto expreso de promover y proteger, por medios pacíficos, los derechos humanos y las libertades fundamentales, en concordancia con el artículo 3 de la presente Declaración.

Artículo 14

1. Incumbe al Estado la responsabilidad de adoptar medidas legislativas, judiciales, administrativas o de otra índole apropiadas para promover en todas las personas sometidas a su jurisdicción la comprensión de sus derechos civiles, políticos, económicos, sociales y culturales.

2. Entre esas medidas figuran las siguientes:

a) La publicación y amplia disponibilidad de las leyes y reglamentos nacionales y de los instrumentos internacionales básicos de derechos humanos;

b) El pleno acceso en condiciones de igualdad a los documentos internacionales en la esfera de los derechos humanos, incluso los informes periódicos del Estado a los órganos establecidos por los tratados internacionales sobre derechos humanos en los que sea Parte, así como las actas resumidas de los debates y los informes oficiales de esos órganos.

3. El Estado garantizará y apoyará, cuando corresponda, la creación y el desarrollo de otras instituciones nacionales independientes destinadas a la promoción y la protección de los derechos humanos y las libertades fundamentales en todo el territorio sometido a su jurisdicción, como, por ejemplo, mediadores, comisiones de derechos humanos o cualquier otro tipo de instituciones nacionales.

Artículo 15

Incumbe al Estado la responsabilidad de promover y facilitar la enseñanza de los derechos humanos y las libertades fundamentales en todos los niveles de la educación, y de garantizar que los que tienen a su cargo la formación de abogados, funcionarios encargados del cumplimiento de la ley, personal de las fuerzas armadas y funcionarios públicos incluyan en sus programas de formación elementos apropiados de la enseñanza de los derechos humanos.

Artículo 16

Los particulares, las organizaciones no gubernamentales y las instituciones pertinentes tienen la importante misión de contribuir a sensibilizar al público sobre las cuestiones relativas a todos los derechos humanos y las libertades fundamentales mediante actividades de enseñanza, capacitación e investigación en esas esferas con el objeto de fortalecer, entre otras cosas, la comprensión, la tolerancia, la paz y las relaciones de amistad entre las naciones y entre todos los grupos raciales y religiosos, teniendo en cuenta las diferentes mentalidades de las sociedades y comunidades en las que llevan a cabo sus actividades.

Artículo 17

En el ejercicio de los derechos y libertades enunciados en la presente Declaración, ninguna persona, individual o colectivamente, estará sujeta a más limitaciones que las que se impongan de conformidad con las obligaciones y compromisos internacionales aplicables y determine la ley, con el solo objeto de garantizar el debido reconocimiento y respeto de los derechos y libertades ajenos y responder a las justas exigencias de la moral, del orden público y del bienestar general de una sociedad democrática.

Artículo 18

1. Toda persona tiene deberes respecto de la comunidad y dentro de ella, puesto que sólo en ella puede desarrollar libre y plenamente su personalidad.

2. A los individuos, los grupos, las instituciones y las organizaciones no gubernamentales les corresponde una importante función y una responsabilidad en la protección de la democracia, la promoción de los derechos humanos y las libertades fundamentales y la contribución al fomento y progreso de las sociedades, instituciones y procesos democráticos.

3. Análogamente, les corresponde el importante papel y responsabilidad de contribuir, como sea pertinente, a la promoción del derecho de toda persona a un orden social e internacional en el que los derechos y libertades enunciados en la Declaración Universal de Derechos Humanos y otros instrumentos de derechos humanos puedan tener una aplicación plena.

Artículo 19

Nada de lo dispuesto en la presente Declaración se interpretará en el sentido de que confiera a un individuo, grupo u órgano de la sociedad o a cualquier Estado el derecho a desarrollar actividades o realizar actos que tengan por objeto suprimir los derechos y libertades enunciados en la presente Declaración.

Artículo 20

Nada de lo dispuesto en la presente Declaración se interpretará en el sentido de que permita a los Estados apoyar y promover actividades de individuos, grupos de individuos, instituciones u organizaciones no gubernamentales, que estén en contradicción con las disposiciones de la Carta de las Naciones Unidas.

ANEXO

Bruselas, 9 de Junio de 2004
(11.06) (OR. EN)
10056/1/04
REV 1
LIMITE
PESC 435
COHOM 17

II

CONSEJO DE
LA UNIÓN EUROPEA

NOTA

de:	Comité Político y de Seguridad
al:	Coreper/Consejo
Asunto:	Proyecto de Conclusiones del consejo sobre las directrices de la UE sobre defensores de los derechos humanos

1. En su reunión de 8 de junio, el Comité Político y de Seguridad llevó a cabo un debate y ultimó el proyecto de Conclusiones del Consejo mencionado en epígrafe, cuyo texto se reproduce en el Anexo.
2. En su reunión de 1 de junio, el Comité Político y de Seguridad respaldó el texto "Garantizar la protección - directrices de la Unión Europea sobre defensores de los derechos humanos", preparado junto con el Grupo "Derechos Humanos" del Consejo (COHOM). Este texto se adjunta ahora al proyecto de Conclusiones del Consejo.
3. Se invita al Coreper a que recomiende al Consejo la aprobación de dicho proyecto de Conclusiones del Consejo y de las directrices adjuntas, como punto "A" de su sesión de los días 14 y 15 de junio.

ANEXO

Proyecto de Conclusiones del Consejo

1. El Consejo acoge con satisfacción y adopta las directrices de la UE sobre defensores de los derechos humanos (que figura como Anexo). Dichas directrices formarán parte integrante del proceso de intensificación de la política de los derechos humanos de la Unión Europea en las relaciones exteriores. El Consejo observa que estas directrices mejorarán las actividades de la Unión Europea por lo que se refiere al apoyo y la protección de los defensores de los derechos humanos.
2. El Consejo observa que el apoyo a los defensores de los derechos humanos constituye un elemento tradicional de la política de relaciones exteriores en materia de derechos humanos de la Unión Europea. El objetivo de las directrices sobre defensores de los derechos humanos es aportar sugerencias prácticas para mejorar la acción de la UE en este ámbito. Pueden utilizarse en los contactos con terceros países a todos los niveles, así como en foros multilaterales de derechos humanos, a fin de apoyar y fortalecer los esfuerzos que está realizando la Unión para promover y estimular el respeto del derecho a defender los derechos humanos. Prevén, además, intervenciones de la Unión a favor de defensores de los derechos humanos en situación de riesgo y proponen medios prácticos para apoyar y asistir a los defensores de los derechos humanos.
3. El Consejo observa que aunque las directrices se refieren a cuestiones concretas de los defensores de los derechos humanos, contribuirán a reforzar en general la política en materia de derechos humanos de la UE.

Anexo del ANEXO

GARANTIZAR LA PROTECCIÓN DIRECCTRICES DE LA UNIÓN EUROPEA SOBRE DEFENSORES DE DERECHOS HUMANOS

I. OBJETIVO

1. El apoyo a los defensores de los derechos humanos constituye ya un elemento tradicional de la política de Relaciones Exteriores de la Unión Europea en materia de derechos humanos. El objetivo de las presentes directrices es aportar sugerencias prácticas para mejorar la acción de la UE en relación con este asunto. Las directrices pueden utilizarse en contactos con terceros países a todos los niveles, así como en foros multilaterales de derechos humanos, para respaldar y fortalecer los esfuerzos en curso por parte de la Unión encaminados a fomentar y estimular el respeto del derecho a defender los derechos humanos. Las directrices aportan también intervenciones por parte de la Unión en favor de los defensores de los derechos humanos en situación de riesgo, y sugieren medios prácticos de apoyar y ayudar a los defensores de los derechos humanos. Un importante elemento de las directrices es el apoyo a los procedimientos especiales de la Comisión de Derechos Humanos de la ONU, incluido el Representante Especial de la ONU para los defensores de derechos humanos y los mecanismos regionales adecuados para proteger a los defensores de los derechos humanos. Las directrices proporcionarán asistencia a las misiones de la UE (embajadas y consulados de los Estados miembros de la UE y delegaciones la Comisión Europea) en su política relativa a los defensores de los derechos humanos. Aunque su objetivo principal es abordar las inquietudes específicas en relación con los defensores de los derechos humanos, las directrices contribuyen asimismo a reforzar la política de la UE en materia de derechos humanos en general.

II. DEFINICIÓN

2. La definición de defensores de los derechos humanos a efectos de las presentes directrices, se basará en el artículo 1 de la "Declaración de las Naciones Unidas 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" (véase Anexo I), en el que se afirma que "toda persona tiene derecho, individual o colectivamente, a promover y procurar la protección y realización de los derechos humanos y las libertades fundamentales en los planos nacional e internacional".
3. Los defensores de los derechos humanos son aquellos individuos, grupos y organismos de la sociedad que promueven y protegen los derechos humanos y las libertades fundamentales universalmente reconocidos. Los defensores de los derechos humanos persiguen la promoción y la protección de los derechos civiles y políticos, así como la promoción, la protección y la realización de los derechos económicos, sociales y culturales. Los defensores de los derechos humanos promueven y protegen asimismo los derechos de los miembros de grupos tales como las comunidades indígenas. La definición no incluye a los individuos o grupos que cometan actos violentos o propaguen la violencia.

III. INTRODUCCIÓN

4. La UE respalda los principios que figuran en 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. Aunque la responsabilidad fundamental de la promoción y protección de los derechos humanos corresponde a los Estados, la UE reconoce que los individuos, grupos y organismos desempeñan un papel importante en la defensa de la causa de los derechos humanos. Las actividades de los defensores de los derechos humanos incluyen:
    - informar sobre las violaciones de los derechos humanos;
    - buscar compensaciones para las víctimas de dichas violaciones prestándoles apoyo jurídico, psicológico, médico o de otro tipo; y
    - enfrentarse a la cultura de la impunidad que sirve para enmascarar las violaciones sistemáticas y continuas de los derechos humanos y las libertades fundamentales.
5. El trabajo de los defensores de los derechos humanos implica con frecuencia la crítica de las políticas y actuaciones de los gobiernos. No obstante, los gobiernos no deben considerar negativa esta actitud. El principio de permitir la independencia de espíritu y el libre debate sobre las políticas y acciones del gobierno es fundamental, y constituye un modo sobradamente comprobado de establecer un nivel más alto de protección de los derechos humanos. Los defensores de los derechos humanos pueden ayudar a los gobiernos a promover y proteger los derechos humanos. Como parte de los procesos de consulta, pueden desempeñar un papel fundamental para contribuir a elaborar la legislación apropiada, y ayudar a establecer planes y estrategias nacionales sobre derechos humanos. Cabría también reconocer y respaldar esta función.

6. La UE reconoce que las actividades de los defensores de los derechos humanos cuentan con un mayor reconocimiento a medida que pasan los años. Han logrado garantizar una protección cada vez mayor de las víctimas de las violaciones de los derechos humanos. No obstante, este progreso ha tenido un precio muy elevado: los propios defensores se han convertido paulatinamente en objetivo de los ataques y en muchos países se violan sus derechos. La UE cree que es importante garantizar la seguridad y proteger los derechos de los defensores de los derechos humanos. En este sentido es importante abordar el asunto de los defensores de los derechos humanos desde una perspectiva de género.

IV. DIRECTRICES OPERATIVAS

7. La parte operativa de las directrices tiene la finalidad de definir formas de trabajar con eficacia hacia la promoción y protección de los defensores de los derechos humanos en los terceros países, en el contexto de la Política Exterior y de Seguridad Común.

Control, información y evaluación

8. Se está pidiendo ya a los Jefes de Misión de la UE que presenten informes periódicos sobre la situación de los derechos humanos en sus países de acreditación. El Grupo "Derechos Humanos" del Consejo (COHOM) aprobó recientemente el esquema de fichas encaminadas a facilitar esta tarea. En consonancia con esas fichas, las Misiones deben abordar la situación de los defensores de los derechos humanos en sus informes, tomando nota en particular de si se producen amenazas o ataques contra defensores de los derechos humanos. En este contexto, los Jefes de Misión deben ser conscientes de que el marco institucional puede tener importantes repercusiones sobre la posibilidad de los defensores de los derechos humanos de realizar su trabajo con seguridad. Son de gran importancia al respecto asuntos tales como las medidas legislativas, judiciales, administrativas u otras pertinentes, adoptadas por los Estados para proteger a las personas contra la violencia, las amenazas y las venganzas, la discriminación adversa de facto o de iure, las presiones o cualquier otra acción arbitraria como consecuencia de su ejercicio legítimo de cualesquiera de los derechos referidos a la declaración de la ONU sobre defensores de los derechos humanos. Cuando la situación lo requiera, los Jefes de Misión deberán presentar recomendaciones al COHOM de posibles actuaciones de la UE, incluida la condena de las amenazas y ataques contra los defensores de los derechos humanos, así como gestiones diplomáticas y declaraciones públicas cuando los defensores de los derechos humanos se encuentren en peligro inmediato o grave. Los Jefes de Misión deberán también informar sobre la eficacia de las actuaciones de la UE en sus informes.
9. Los informes de los Jefes de Misión y otra información pertinente, como los informes y recomendaciones del Representante Especial del Secretario General sobre la cuestión de los defensores de los derechos humanos, los relatores especiales de la ONU y los órganos creados en virtud de un tratado, así como las organizaciones no gubernamentales harán posible que el COHOM y otros grupos pertinentes determinen las situaciones en las que sean necesarias actuaciones de la UE y decidan las acciones que se van a emprender o, en su caso, hagan recomendaciones de actuación al CPS y al Consejo.

Papel de las misiones de la UE en el apoyo y protección de los defensores de los derechos humanos

10. Las misiones de la UE (embajadas de los Estados miembros de la UE y delegaciones de la Comisión Europea) son en muchos terceros países el primer punto de contacto entre la Unión y sus Estados miembros y los defensores de los derechos humanos in situ. Por tanto, desempeñan un papel muy importante en la aplicación de la política de la UE en relación con los defensores de los derechos humanos. Las misiones de la UE deben, por consiguiente, tratar de adoptar un planteamiento anticipativo en relación con los defensores de los derechos humanos. Simultáneamente, deben ser conscientes de que en algunos casos la actuación de la UE podría dar lugar a amenazas o ataques contra los defensores de los derechos humanos. Por tanto, deberán consultar, en su caso, con los defensores de los derechos humanos en relación con las acciones que pueden contemplarse. Entre las medidas que las Misiones de la UE pueden adoptar figuran:

    - Coordinar estrechamente y compartir los datos sobre defensores de los derechos humanos, incluidos los que se encuentren en situación de riesgo;
    - Mantener los contactos adecuados con los defensores de los hechos humanos, inclusive recibiéndoles en las Misiones y visitando sus lugares de trabajo, pudiendo considerarse el nombramiento de funcionarios de enlace específicos, cuando sea necesario, compartiendo las cargas a tal fin;
    - Facilitando cuando sea necesario un reconocimiento visible a los defensores de los derechos humanos, mediante el oportuno recurso a la publicidad, visitas e invitaciones;
    - Asistir, cuando sea preciso, a los juicios contra defensores de los derechos humanos y actuar de observadores.

Fomento del respeto de los defensores de los derechos humanos en las relaciones con terceros países y en los foros multilaterales

11. El objetivo de la UE es influir para que los terceros países cumplan sus obligaciones de respetar los derechos de los defensores de los derechos humanos y protegerles de los ataques y amenazas de agentes no estatales. En sus contactos con terceros países, la UE, cuando lo considere necesario, manifestará la necesidad de que todos los países se adhieran a las normas internacionales correspondientes y las cumplan, en particular la Declaración de la ONU. El objetivo general debería ser la realización de un entorno en el que los defensores de los derechos humanos puedan actuar con libertad. La UE dará a conocer sus objetivos como parte integrante de su política de derechos humanos y destacará la importancia que concede a la protección de los defensores de los derechos humanos. Entre las actuaciones de apoyo a estos objetivos se cuentan:

    - Cuando la Presidencia, el Alto Representante de la PESC o los representantes o enviados especiales de la UE, o un miembro la Comisión Europea visiten un país, cuando sea oportuno incluirán reuniones con los defensores de los derechos humanos y harán referencia a casos individuales de los mismos como parte integrante de su visita a estos terceros países;
    - El componente de derechos humanos de los diálogos políticos entre la UE y los terceros países y organizaciones regionales incluirá, cuando sea oportuno, la situación de los defensores de los hechos humanos. La UE destacará su apoyo a los defensores de los hechos humanos y su trabajo y planteará casos concretos objeto de preocupación cuando sea necesario;
    - La colaboración estrecha con otros países que tengan una visión parecida, en particular en la Comisión de Derechos Humanos de la ONU y la Asamblea General de la ONU;
    - La consolidación de los mecanismos regionales existentes para la protección de los defensores de los derechos humanos, tales como los puntos de contacto sobre defensores los derechos humanos de la Comisión Africana de los Derechos Humanos y de los Pueblos y la unidad especial de defensores de derechos humanos de la Comisión Interamericana de Derechos Humanos y la creación de los mecanismos adecuados en regiones en las que no existan.

Apoyo a los procedimientos especiales de la Comisión de Derechos Humanos de la ONU, incluido el Representante Especial sobre defensores de los derechos humanos

12. La UE reconoce que los procedimientos especiales de la Comisión de Derechos Humanos de las Naciones Unidas (relatores especiales, representantes especiales, expertos independientes y grupos) son fundamentales en los esfuerzos internacionales para proteger a los defensores de los derechos humanos en razón de su independencia e imparcialidad, su capacidad de actuar y hacer declaraciones sobre las violaciones contra los defensores de los derechos humanos a nivel mundial y la de realizar visitas al país. Mientras que el Representante Especial sobre defensores de los derechos humanos tiene un papel fundamental a este respecto, los mandatos de otros procedimientos especiales también son importantes para los defensores de los derechos humanos. Las actuaciones de la UE en apoyo de los procedimientos especiales incluirán:

    - Animar a los Estados a que acepten por principio las peticiones de visitas al país realizadas mediante Procedimientos Especiales de la ONU;
    - Fomentar a través de las misiones de la UE el uso de mecanismos temáticos de la ONU por parte de las comunidades locales de derechos humanos y los defensores de los derechos humanos, incluso facilitando el establecimiento de contactos e intercambio de información entre los mecanismos temáticos y los defensores los hechos humanos, pero sin limitarse a ello.
    - Puesto que los procedimientos especiales no pueden cumplir su mandato en ausencia de recursos adecuados, los Estados miembros de la UE respaldarán la asignación de fondos suficientes a cargo del presupuesto general a la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.

Respaldo en la práctica a los defensores los derechos humanos incluido a través de la política de desarrollo

13. Los programas de la Unión Europea y de los Estados miembros destinados a la asistencia en el desarrollo de procesos e instituciones democráticos, y la promoción y protección de los derechos humanos en los países en vías de desarrollo figuran entre la amplia gama de ayudas en la práctica para ayudar a los defensores de los derechos humanos. Entre ellos se pueden incluir, aunque sin limitarse a ello necesariamente, los programas de cooperación al desarrollo de los Estados miembros. Entre las medidas de asistencia en la práctica cabe citar las siguientes:

    - Los programas bilaterales en materia de derechos humanos y democratización de la Comunidad Europea y los Estados miembros deben tener más en cuenta la necesidad de ayudar al desarrollo de los procesos y las instituciones democráticos y a la promoción y pro-

tección de los derechos humanos en los países en desarrollo, respaldando en particular a los defensores de los derechos humanos en actividades como el desarrollo de las capacidades y las campañas de sensibilización;

- Animar y fomentar el establecimiento y el funcionamiento de órganos nacionales de promoción y protección de los derechos humanos, establecidos con arreglo a los principios de París, incluidas las instituciones nacionales de derechos humanos, los defensores del pueblo y las comisiones de derechos humanos.
- Asistir en el establecimiento de redes de defensores de los derechos humanos a nivel internacional, incluso facilitando reuniones de los defensores de los derechos humanos;
- Tratar de garantizar que los defensores de los derechos humanos de terceros países puedan acceder a los recursos, incluidos financieros, procedentes del extranjero;
- Garantizar que los programas educativos en materia de derechos humanos promuevan, entre otras cosas, la Declaración de las Naciones Unidas sobre defensores de los derechos humanos.

Función de los grupos del Consejo

14. Con arreglo a su mandato, el grupo COHOM supervisará la aplicación y seguimiento de las directrices sobre defensores de los derechos humanos, en estrecha cooperación y coordinación con otros grupos pertinentes del Consejo. Esta tarea supondrá:
    - Propiciar la integración del asunto de los defensores de los derechos humanos en las políticas y actuaciones pertinentes de la UE.
    - Emprender periódicamente revisiones de la aplicación de las directrices.
    - Continuar estudiando, en su caso, nuevas maneras de cooperación con la ONU y otros mecanismos regionales e internacionales de apoyo de los defensores de los derechos humanos.
    - Informar al Consejo, a través del CPS y del Coreper, cuando proceda o con carácter anual, de los avances realizados en la aplicación de las presentes directrices.

Anexo I del Anexo del ANEXO

(Déclaration UN sur les DDH)

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

Anexo II del Anexo del ANEXO

Instrumentos internacionales pertinentes

- Declaración Universal de Derechos Humanos
- Pacto Internacional de Derechos Civiles y Políticos
- Pacto Internacional de Derechos Económicos, Sociales y Culturales
- Convención contra la tortura y otros tratos o penas crueles, inhumanos o degradantes
- Convención sobre los Derechos del Niño
- Convención sobre la eliminación de todas las formas de discriminación contra la mujer
- Convención internacional sobre la eliminación de todas las formas de discriminación racial
- Convenio Europeo de Derechos Humanos, sus protocolos y la jurisprudencia del Tribunal Europeo de Derechos Humanos
- Carta Social Europea y Carta Social Europea revisada
- Carta Africana de los Derechos Humanos y de los Pueblos
- Convención Americana sobre Derechos Humanos
- Convenciones de Ginebra sobre la Protección a las Víctimas de Guerra y sus protocolos, así como el derecho consuetudinario aplicable en los conflictos armados
- Convención de 1951 sobre el Estatuto de los Refugiados y su Protocolo de 1967
- Estatuto de Roma de la Corte Penal Internacional
- 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.

ANEXO III

Recomendaciones de cabildeo de PI para DDHs en relación con Misiones de la UE, Estados Miembros de la UE y Representantes Especiales de la UE (Más consejos en www.protectionline.org)

Desde que se adoptara la Declaración de la ONU, se han establecido los siguientes mecanismos para proteger a defensores en todo el mundo:

- **El mandato de la Relatora Especial para Defensores de Derechos Humanos nombrado por El Consejo de Derechos Humanos de la ONU** (substituye el anterior mandato del Representante Especial del Secretario General de las Naciones Unidas para Defensores de Derechos Humanos, creado por la Comisión de Derechos Humanos de la ONU).
- El mandato de la **Relatora Especial de la Comisión Africana de Derechos Humanos y de los Pueblos.**
- **La resolución sobre protección de defensores de derechos humanos en África, adoptada por** la Comisión Africana de Derechos Humanos y de los Pueblos, reunida en la 35 sesión ordinaria, celebrada del 21 de mayo al 4 de Junio de 2004 en Banjul, Gambia.
- La **Unidad de Defensores de Derechos Humanos de la Comisión Interamericana de Derechos Humanos.**
- La **UE** también ha adoptado las **Directrices específicas para Defensores de Derechos Humanos** como una herramienta que las Misiones de la UE deberían usar para proteger a defensores en terceros países.
- **El Consejo de Europa:** Adopción de la Declaración del Comité de Ministros para una mejor protección de los defensores de derechos humanos, **18 de febrero de 2008.**
- **La Comisión Asiática de Derechos Humanos.**

En 2004, el Consejo de Ministros de la EU adoptó las Directrices de la EU sobre Defensores de Derechos Humanos. Estas Directrices de la UE reiteran la Declaración de DDHs de la ONU y dirigen recomendaciones específicas a todas las Misiones de la UE y a todos los Estados Miembros de la UE. Las recomendaciones de la UE se centran en:

- Adoptar políticas proactivas para la protección de DDHs.
- Usar vías diplomáticas para obtener, por parte de los gobiernos locales y regionales de los DDHs afectados, el compromiso de respetar totalmente los derechos de los DDHs.

Las Directrices de la UE también se pueden obtener en oficinas de la UE y en las embajadas de países miembros.

Las Misiones de la UE (Embajadas de Estados Miembros de la UE y Delegaciones de la Comisión de la UE) son el primer punto de contacto entre la UE, los Estados Miembros de la UE y los DDHs locales.

PI recomienda, como mínimo, que los Defensores de Derechos Humanos...

- Pidan que se traduzcan las Directrices de la UE al idioma de los DDHs y que se distribuyan entre organizaciones de DDHs y autoridades locales y regionales.
- Envíen con regularidad información actualizada sobre su situación a los Jefes de Misión de la UE, así como a ONGs nacionales e internacionales, a fin de concienciarlos y de mejorar la coordinación entre los diferentes actores.
- Mantengan un contacto regular con las Misiones de la UE, para que así los DDHs locales estén informados de las Directrices de la EU y de las iniciativas de las Misiones de la EU para la protección de DDHs. Este contacto regular permitirá a las Misiones de la EU mantenerse informadas tanto sobre la situación de los DDHs como sobre sus recomendaciones con respecto a las medidas de protección y apoyo que deberían tomarse…
- Pidan que las Misiones de la UE compartan e implementen prácticas de protección y estrategias a medio plazo homogéneas.
- Inviten al los Jefes de Misión y a los oficiales de DHs a visitar las zonas de trabajo de DDHs, sobre todo aquellas en las que los DDHs corren mas riesgo (por ejemplo en zonas de conflicto o en lugares donde DDHs ya han sido atacados o amenazados).
- Pidan acción urgente cuando DDHs sean amenazados o detenidos.
- Pidan traslado a sitios seguros y ayuda para DDHs que estén corriendo riesgo.
- Pidan o acepten invitaciones y promoción de Misiones de la UE, una vez que los DDHs hayan llevado a cabo una valoración de riesgo del impacto que supondría la posibilidad de aumentar su visibilidad. Que indiquen los problemas de seguridad que se podrían producir en consecuencia y que pidan apoyo para la protección. Que soliciten ayuda y observación por parte de los Jefes de Misión de la UE en casos de juicios contra DDHs. Esto puede garantizar un juicio justo, pero hace falta mantener a un observador durante todo el proceso (desde la lectura de los cargos, hasta la lectura de la sentencia), para garantizar la independencia. Que pidan que los observadores se comuniquen con el DDH al que se esté juzgando. Que pidan que los observadores de la UE estén también presentes en juicios a violadores de DHs, para evitar que sus crímenes puedan quedar impunes.
- Pidan ser informados de las visitas al país del DDH del Presidente de la UE, del Alto Representante de Política Exterior y de Seguridad Común, representantes especiales de la UE o miembros de la Comisión Europea, y que soliciten reuniones con ellos.
- Pidan que las situaciones de DDHs se incluyan en la agenda del diálogo político entre la UE y las organizaciones locales y regionales de DDHs.
- Pidan que las acciones con otros actores estén coordinadas, sobre todo con el Consejo de Derechos Humanos de la ONU, y con la Asamblea General de la ONU. Que pidan que se coordine la protección con organizaciones regionales de protección de DHs y DDHs, como la Comisión Africana de Derechos Humanos y de los Pueblos, la Unidad de Defensores de la Comisión Interamericana De Derechos Humanos o la Comisión Asiática de Derechos Humanos.
- Que pidan que los informes de los Jefes de Misión de la UE sean públicos y que los DDHs puedan tener acceso a ellos.

Recaudación de fondos

Los DDHs pueden recaudar fondos directamente de las embajadas (Programas de DHs) y de la UE, a través del Instrumento Europeo para la Democracia y los Derechos Humanos. Este último organismo permite a la Comisión Europea dar fondos a ONGS sin necesidad de que el gobierno de un tercer país lo apruebe.

http://ec.europa.eu/europaid/projects/eidhr/index_en.htm

Más información sobre otros instrumentos de financiación en esta misma página web.

Además:

Aunque las directrices de la UE cubren Misiones de la UE, de instituciones de la UE y de estados miembros de la UE, los DDHs deberían recordar que pueden buscar el apoyo de otros cuerpos diplomáticos y organizaciones internacionales, ya que la Declaración de DDHs de la ONU se pude usar con todos los actores.

ANEXO IV

Resumen de riesgo general para perfiles específicos de defensores de derechos humanos

Propósito:

Definir el riesgo para perfiles específicos de DDHs, a fin de tenerlo en cuenta tanto a la hora de diseñar planes de seguridad/protección, como a la hora de promover políticas de organización.

Además de los riesgo comunes a los que se enfrentan todos los HRDs, el capítulo 1.9. se centra en la necesidad de tener en cuenta las características propias de un grupo especifico de DDHs a la hora de definir un plan de seguridad/protección, ya sea individual, para una organización y/o a nivel inter-organizacional.

Este manual no puede ser completamente exhaustivo y estudiar todos los perfiles específicos de DDHs que trabajan en contextos políticos diferentes. Para cada grupo o situación se necesitaría un capítulo, por no decir un manual de protección dedicado únicamente a ellos: instituciones religiosas; comunidades indígenas; grupos que trabajan en derechos económicos, sociales y culturales; grupos que trabajan en derechos del niño; abogados y juristas; periodistas; organizaciones rurales; ecologistas; sindicalistas; minorías; LGBTI,…

Además, dado que el contexto político es dinámico y, por tanto, también el riesgo, habría que hacer actualizaciones continuamente.

Sin embargo, conviene no olvidar que la lógica de fondo del análisis de riesgo es la misma para todos los grupos de DDHs y para todos los defensores. Solo hay que implementarla teniendo en cuenta los perfiles específicos del DDH y las amenazas, vulnerabilidades y capacidades que esto conllevan.

Seguidamente hay una tabla no exhaustiva que explica como datos específicos pueden ilustrarse mediante una "tormenta de ideas". Se puede usar como punto de partida para cada grupo de DDHs, que tendría que explorar los resultados en detalle, ya que cada elemento puede presentar muchas "tonalidades".

Por ejemplo, redes e instituciones religiosas pueden ser cristianas (católicas, apostólicas, evangelistas, mormones, cuákeros), musulmanas (sunnitas, chiítas, sufistas etc.), hinduismo, budismo etc.; pueden trabajar en zonas rurales o urbanas; en un contexto político mas o menos orientado hacia los derechos humanos; o a temas mas o menos polémicos etc.

Una misma amenaza se puede explicar a través de diferentes modelos, por ejemplo, una amenaza de agresión puede ir dirigida a gente, a materiales …

Para complementar la información de cada perfil, hay que usar el capítulo 1.2, Tabla 3.

[1] Protection Manual for LGBTI Defenders, PI©2009

Resumen no exhaustivo de riesgo general para perfiles específicos de defensores de derechos humanos

Perfiles	Áreas de trabajo	Amenaza por trabajo/impacto	Vulnerabilidad / capacidades
Redes religiosas • (…)	• Derechos Humanos, Ley internacional humanitaria, seguridad de alimentos y valores religiosos • Grupo cros-denominacional • (…)	• Etiquetados y desacreditados por "apoyar a grupos armados ilegales". • Agredidos debido a esa etiqueta • (…)	• Aislamiento geográfico • Falta de apoyo institucional • Acceso a redes • Trabajan desde elementos convergentes (creencia religiosa) • (…)
Derechos económicos, sociales y culturales: organizaciones DESC	• Empoderamiento a nivel individual y de organización • Seguridad de los alimentos, gestión y protección medioambiental, proyectos agrícolas, educación • Identidad y derechos de las minorías • (…)	• El fortalecimiento de la organización acaba con la hegemonía de los actores armados • Embargos económicos • Infiltración • (…)	• Expuestos a actores armados en la zona donde trabajan • Aislamiento geográfico • Acceso a redes que abordan los mismos temas, a menudo menos polémicos que otros aspectos de los derechos humanos, como, por ejemplo, prisioneros políticos • Aceptados con facilidad, porque su trabajo produce benificios immediatos para las comunidades • (…)
Organizaciones legales o jurídicas	• Defensa de DHs a menudo a través de casos emblemáticos • Formación sobre DHs • Lucha contra la impunidad y para la observación de juicios • Consultoría jurídica y política • Denuncia pública de violaciones de DHs • Campañas políticas temáticas • (…)	• Desprestigio • Criminalización • Judicialización • Ataques contra su imagen social • Infiltración • (…)	• Distancia de las autoridades políticas y civiles • Apoyo político interno limitado • Perfil institucional relativamente alto • Apoyo institucional • Acceso a redes internacionales homologadas • (…)
Instituciones religiosas	• Asistencia humanitaria • (…)	• Estigmatización y persecución • (…)	• Exposición • Demasiada confianza ("si dios quiere"/ "con la ayuda de dios"/ reencarnación…) • Legitimidad • Redes y recursos • Credibilidad • Incidencia/influencia políticas • Jerarquía • Identidad ideológica • (…)

Resumen no exhaustivo de riesgo general para perfiles específicos de defensores de derechos humanos

PERFILES	ÁREAS DE TRABAJO	AMENAZA POR TRABAJO/IMPACTO	VULNERABILIDAD / CAPACIDADES
COMUNIDADES RURALES	• Pedir la devolución de la tierra y recuperarla • (…)	• Control territorial de terceras partes • Desplazamiento o confinamiento • Intimidación por parte de terratenientes poderos • (…)	• Aislamiento • Liderazgo débil • Pobreza • Técnicas de cultivo • Conocimiento del territorio • Técnicas de organización • Dificultades para acceder a la comunicación y a la educación • Difícil acceso a electricidad y agua • Territorio agrícola compartido • Intereses y composición heterogéneos • (…)
SINDICATOS	• Derechos humanos en el trabajo • (…)	• Desprestigio y criminalización • Despido • (…)	• Organizaciones sociales en todo el mundo con socios registrados • Expuestos a actitudes protagonistas • Partidismo político • Trabajo en redes • Capacidad para movilizar a cantidades grandes de socios y no socios • Capacidad de influencia en áreas económicas y sociales clave • Reconocimiento social • No partidario de colaborar con DDHs • Identidad política • Estructura jerarquizada • (…)
PERIODISTAS	• Investigación y publicación de violaciones de DHs. • (…)	• Desprestigio • Agresión • Asalto • Pérdida de material • Pérdida de información • Ostracismo por parte de los medios de comunicación "oficiales" • (…)	• Expuestos a la corrupción y a los magnates de los medios de comunicación • Acceso a redes internacionales y a asociaciones de periodistas • Acceso a los medios de comunicación • Imagen pública • Defensor de la democracia • Individuos • (…)

Resumen no exhaustivo de riesgo general para perfiles específicos de defensores de derechos humanos

Perfiles	Áreas de trabajo	Amenaza por trabajo/impacto	Vulnerabilidad / capacidades
LGBTI	• Derechos LGBTI • (…)	• Denigración, desprestigio y criminalización • Campaña publica anti-LGBTI • Legislación anti-LGBTI • (…)	• Expuestos a prejuicios morales / religiosos / cultu-rale / sociales • Acceso a redes internacionales • Excluidos a menudo por otros DDHs • A veces visibilidad baja • Dificultades para promover sus propios derechos • Transversal a todas las organizaciones de DDHs • Fácil de reconocer • Expuestos también a homofobia y transfobia de las autoridades que se supone deben proteger a todos los ciudadanos • Expuestos a presión psicológica y estrés • (…)
Grupos de identidad minoritaria • (…)	• Derechos de identidad • (…)	• Desprestigio y exclusión • Restricción de sus derechos civiles • (…)	• Comparten identidad cultural y étnica • Se pueden asentar en diferentes zonas geográficas • Tendencia a trabajar en un círculo cerrado • Aislamiento • Dificultad para acceder a otros grupos de DHs • Dificultad para promover la concienciación con respecto a su caso • (…)

Bibliografía y otros recursos de interés

Bibliografía

- Amnesty International (2003): "Essential actors of our time. Human rights defenders in the Americas". Secretariado Internacional de AI (Index AI: AMR 01/009/2003/s).
- AVRE and ENS (2002): "Afrontar la amenaza por persecución sindical". Escuela de Liderazgo Sindical Democrático. Publicado por Escuela Nacional Sindical y Corporación AVRE. Medellín, Colombia.
- Bettocchi, G., Cabrera, A.G., Crisp, J., and Varga, A (2002): "Protection and solutions in situations of internal displacement". EPAU/2002/10, UNHCR.
- Cohen, R. (1996): "Protecting the Internally Displaced". World Refugee Survey.
- Conway, T., Moser, C., Norton, A. and Farrington, J. (2002) "Rights and livelihoods approaches: Exploring policy dimensions". DFID Natural Resource Perspectives, no. 78. ODI, London.
- Dworken, J.T "Threat assessment". Series de módulos para OFDA/InterAction PVO Security Task Force (Mimeo, incluido en REDR Security Training Modules, 2001).
- Eguren, E. (2000): "Who should go where? Examples from Peace Brigades International", in "Peacebuilding: a Field Perspective. A Handbook for Field Diplomats", by Luc Reychler and Thania Paffenholz (editors). Lynne Rienner Publishers (London).
- Eguren, E. (2000), "The Protection Gap: Policies and Strategies" in the ODI HPN Report, London: Overseas Development Institute.
- Eguren, E. (2000) "Beyond security planning: Towards a model of security management. Coping with the security challenges of the humanitarian work". Journal of Humanitarian Assistance. Bradford, UK. www.jha.ac/articles/a060.pdf
- Eriksson, A. (1999) "Protecting internally displaced persons in Kosovo". http://web.mit.edu/cis/www/migration/kosovo.html#f4
- Lebow, Richard Ned and Gross Stein, Janice. (1990) "When Does Deterrence Succeed And How Do We Know?" (Occasional Paper 8). Ottawa: Canadian Inst. for Peace and International Security.
- Mahony, L. and Eguren, E. (1997): "Unarmed bodyguards. International accompaniment for the protection of human rights". Kumarian Press. West Hartford, CT (USA).
- Martín Beristain, C. and Riera, F. (1993): "Afirmación y resistencia. La comunidad como apoyo". Virus Editorial. Barcelona.
- Paul, Diane (1999): "Protection in practice: Field level strategies for protecting civilians from deliberate harm". ODI Network Paper no. 30.

- SEDEM (2000): *Manual de Seguridad. Seguridad en Democracia*. Guatemala.
- *Sustainable Livelihoods Guidance Sheets* (2000). DFID. London, February 2000
- Sutton, R. (1999): *The policy process: An overview*. Working Paper 118. ODI. London.
- UNHCHR (2004): *About Human Rights Defenders* (extensive information): http://www.unhchr.ch/defenders/about1.htm
- UNHCHR (2004): Human Rights Defenders: *Protecting the Right to Defend Human Rights*. Fact Sheet no. 29. Geneva.
- UNHCHR (2004): *On women defenders*: www.unhchr.ch/defenders/tiwomen.htm
- UNHCR (1999): *Protecting Refugees*: A Field Guide for NGO. Geneva.
- UNHCR (2001): *Complementary forms of protection. Global Consultations on International Protection*. EC/GC/01/18 4 September 2001
- UNHCR (2002): *Strengthening protection capacities in host countries. Global Consultations on International Protection*. EC/GC/01/19 * / 19 April 2002
- UNHCR-Department of Field Protection (2002): *Designing protection strategies and measuring progress: Checklist for UNHCR staff*. Mimeo- Geneva.
- Van Brabant, Koenraad (2000): *Operational Security Management in Violent Environments*. Good Practice Review 8. Humanitarian Practice Network. Overseas Development Institute, London.

Otros recursos de interés

Desde el año 2000, Protection International -PI- ofrece cursos de formación y consultorías de análisis de riesgo, protección y seguridad para defensores de derechos humanos. Para mas información, puede ponerse en contacto con: pi@protectioninternational.org; o mandar una carta a:

PI, Rue de la Linière, 11 -1060 Brussels (Bélgica)

Tel: + 32 (0)2 609 44 05 +32 (0)2 609 44 07

Fax: +32 (0)2 609 44 06

www.protectioninternational.org

www.protectionline.org

Tactical Technology Collective: **www.tacticaltech.org** (desde 2003 - soluciones técnicas de seguridad digital): "NGO in a Box".

Índice de capítulos

Índice temático

Luis Enrique Eguren

(España). Médico y experto en protección, es miembro de la Unidad de Investigación y Formación de Protection International. Ha trabajado con PBI en El Salvador, Sri Lanka y Colombia, así como en misiones cortas en otros países con otras organizaciones internacionales. Consultor, formador e investigador, ha publicado varios artículos y libros sobre el tema de protección.

© Maria Dermitzaki

Marie Caraj

(Bélgica). Intérprete y experta en protección. Miembro de la Unidad de Investigación y Formación de Protection International. Ha trabajado con PBI y su Oficina Europea (1985-2007). Actualmente realiza misiones cortas en África, Asia y América Latina. Consultora, formadora e investigadora.

"(...) los riesgos a los que se enfrentan las y los defensores de derechos humanos son tan graves que también es importante buscar más medios para protegerles. En este sentido, espero que el presente Manual de Protección pueda serles de utilidad a la hora de diseñar estrategias de seguridad y medidas de protección adecuadas para las situaciones que viven. La mayoría de las y los defensores de derechos humanos están tan inmersos en su trabajo de proteger a otras personas que no le prestan la suficiente atención a su propia seguridad. Es importante que quienes trabajamos en los derechos humanos comprendamos que nuestra seguridad y la de las personas hacia las que trabajamos es parte de ese trabajo".

(Hina Jilani, ex Representante Especial para las y los Defensores de Derechos Humanos del Secretario General de las Naciones Unidas).

" Desde que fuimos a esta formación han cambiado muchas cosas en nuestra organización, sobre todo porque la mayor parte de lo que aprendimos allí eran cosas de las que no teníamos ni idea. Ahora somos más fuertes gracias a eso, somos más capaces de analizar los riesgos que corremos a diario, identificar los incidentes de seguridad que se producen, y valorar las amenazas que recibimos y cómo de probable es que se materialicen".
"(...) Nos gusta mucho vuestra metodología, por su dinamismo y por algo muy bueno, que nos incluye como parte del intercambio de información. Sin duda alguna, lo que salga de esto será muy enriquecedor para nuestro análisis".
" Tuve el sentimiento de haber estado en una formación de mucha calidad que me enseñaba a ser un verdadero defensor de derechos humanos. A partir de ahora, mi forma de trabajar no va a ser igual ».

(Defensores en la República Democrática de Congo).

"Felicitar el esfuerzo y la forma en la que se impartió el taller, ya que fue muy didáctico y nos ubicó en nuestras realidades"

(Un defensor en Guatemala).

"Aprendí muchas cosas de un mundo que conozco desde hace tiempo, pero que pocas veces había percibido desde este punto de vista."

(Un defensor en México).

"(...) Es un tema muy nuevo para mí. Aunque trabajamos en un campo donde nuestra seguridad siempre está amenazada, nunca nos habíamos planteado la necesidad de ir a una formación como ésta, o nunca nos habíamos puesto a pensar en temas de nuestra seguridad, por falta de tiempo, pero después de esta formación yo personalmente me di cuenta de que era un tema crucial que teníamos que incluir como prioritario en todos nuestros proyectos. Dicho de otro modo, esta formación ha sido vital para todos."

(Un defensor en Nepal).

PROTECTION international

Con el apoyo de:

ifa Institut für Auslandsbeziehungen e. V.

Auswärtiges Amt

Iniciativa Europea para la Democracia y los Derechos Humanos IEDDH

ROYAUME DE BELGIQUE
Service public fédéral
Affaires étrangères, Commerce extérieur et Coopération au Développement

La impresión en México se hizo posible con el apoyo de:

ACUDDEH
Acción Urgente para Defensores de Derechos Humanos A.C.

Protection Desk México

Nuevo Manual de Protección para Defensores de Derechos Humanos. Investigación y texto de Enrique Eguren y Marie Caraj, Unidad de Investigación y Formación, Protection International. Traducción del inglés de Michelle F. René.

Protection International, Rue de la Linière, 11. B-1060 Bruselas (Bélgica)
Tel: +32(0)2 609 44 09, Fax: +32(0)2 536 19 82
pi@protectioninternational.org www.protectioninternational.org

Portal de Internet sobre protección de defensores y defensoras de derechos humanos: www.protectionline.org