Manual de Protección

para

Defensores de Derechos Humanos

Investigado y escrito por Enrique Eguren,
Oficina Europea de Peace Brigades International (PBI BEO)

Publicado por Front Line
Fundación Internacional para la Protección de los
Defensores de Derechos Humanos

Publicado por Front Line 2005
Fundación Internacional para la Protección de los Defensores
de Derechos Humanos
16 Idrone Place, Off Bath Place, Blackrock, County Dublín, Ireland.

Se pueden pedir copias de este manual a:
info@frontlinedefenders.org y pbibeo@biz.tiscali.be y
manual@protectionline.org
Precio 20 Euros más costes envío

Alternativamente, para pedir un manual por favor contactar

PBI-European Office
11 Rue de la Linière, B-1060 Bruxelles, Belgium
Tel +32 2 260 944 05 Fax +32 2 260 944 06
pbibeo@protectionline.org

Front Line
16 Idrone Place, Off Bath Place, Blackrock, County Dublín, Ireland.
Tel + 353 1212 37 50 Fax + 353 1212 1001
protectionmanual@frontlinedefenders.org

Este manual será traducido por Front Line al inglés, francés, ruso, y árabe (así como a otros idiomas, según posibilidades)

ISBN: 0-9547883-1-1

Prefacio, por Hina Jilani

En mi trabajo como Representante Especial para Defensores de Derechos Humanos del Secretario General he tomado nota con grave preocupación del aumento en el número de informes sobre serios abusos de derechos humanos contra los defensores, 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 sobre 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 de derechos humanos recae en los gobiernos, tal y como está establecido en la Declaración sobre Defensores de las Naciones Unidas[1]. Debemos continuar trabajando para que todos los gobiernos tomen seriamente en consideración sus obligaciones con respecto a esto y tomen medidas efectivas para asegurar la protección de los defensores de derechos humanos.

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 es Manual de Protección apoyará 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 en derechos humanos entendamos que también debemos preocuparnos por nuestra seguridad, no sólo por nosotros sino también por las personas con las cuales y hacia las cuales trabajamos.

Hina Jilani
Representante Especial para Defensores de Derechos Humanos del Secretario General de las Naciones Unidas

[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

Front line

Front Line fue fundada en Dublín en el 2001 con el objetivo específico de proteger a los defensores de los derechos humanos, personas que trabajan, de manera no violenta, por cualquiera de los derechos defendidos en la Declaración Universal de Derechos Humanos. Front Line tiene como objetivo ocuparse de algunas de las necesidades identificadas por los mismos defensores, incluyendo la protección, los contactos, la formación y el acceso a los mecanismos temáticos y nacionales de la ONU y otros organismos regionales.

Front Line se centra principalmente en los defensores de los derechos humanos en situación de riesgo, tanto temporalmente como permanentemente, por su trabajo en nombre de sus conciudadanos. Front Line tiene un pequeño programa de becas para el propósito específico de fortalecer la protección de los defensores de los derechos humanos. Front Line moviliza las campañas y los grupos presión en nombre de los defensores que están en peligro inminente. En situaciones de emergencia, Front Line puede proveer una relocalización temporal.

Front Line investiga y publica informes sobre la situación de los defensores de los derechos humanos en países específicos. También desarrollamos materiales y paquetes de formación en nombre de los defensores de los derechos humanos, además de facilitar contactos e intercambios entre los defensores de diferentes partes del mundo. Los proyectos de Front Line suelen llevarse a cabo en asociación con organizaciones específicas para los derechos humanos.

Front Line promueve la difusión de la Declaración Universal de los Derechos Humanos y actúa para asegurar el conocimiento, respeto y adhesión a los principios y los estándares reconocidos 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" (conocida como la "Declaración sobre defensores de derechos humanos").

Front Line tiene estatus consultativo especial con el Consejo Económico y Social de Naciones Unidas.

Front Line tiene estatus "charitable" (CHY NO 14029), es independiente e imparcial. Para apoyar su trabajo, Front Line depende enteramente de la generosidad de la financiación de organizaciones y personas. Front Line tiene la dicha de haber sido financiado, desde su lanzamiento en el 2001, a partir de una variedad de fuentes de financiación, y también recibe donaciones de personas individuales. Consejo de Administración (Board of trustees): Denis O´Brien (chairman), Mary Lawlor (Directora), Pierre Sané, Kieran Mulvey, Noeline Blackwell, Michel Forst, David Sykes. Consejo de asesoría: Hanan Ashrawi, Robert Badinter, Bono, His Holiness The Dalai Lama, Indai Lourdes Sajor, Wangarai Muta Maathai, Martin O´Brien, Adolfo Pérez Esquivel, Desmond Tutu.

Pbi

Peace Brigades International (PBI) es una organización no gubernamental que protege a los defensores de derechos humanos y promueve la transformación no violenta de los conflictos.

Previa invitación, PBI envía equipos de voluntarios a zonas donde hay conflicto y represión. Los voluntarios acompañan a defensores de derechos humanos y a sus organizaciones que estén amenazados por violencia política. Aquellos que llevan a cabo violaciones de los derechos humanos normalmente no quieren que la comunidad internacional sea testigo de sus actuaciones. La presencia física de los voluntarios como observadores, junto a sus actuaciones de incidencia (advocacy) y de creación de redes, junto a una amplia red de apoyo internacional, contribuye a disuadir de realizar hostilidades y ataques contra los defensores. De esta manera PBI contribuye a crear espacio para que los defensores lleven a cabo su trabajo a favor de los derechos humanos y la justicia social.

PBI tiene un Consejo Internacional, una Oficina Internacional en Londres y Grupos de País o asociados en 17 países, así como varios proyectos en el terreno.

La Oficina Europea de PBI está en Bruselas (Bélgica). Los contenidos de este Manual son uno de los resultados del trabajo de su Unidad de Investigación y Formación.

Para más información sobre PBI, ver http://www.peacebrigades.org.
Para más información sobre la Oficina Europea de PBI, ver http://www.peacebrigades.org/beo.html

Front Line fue fundada con el mandato de trabajar exclusivamente por la protección de los defensores de derechos humanos. Lamentablemente, nuestro trabajo diario nos muestra cuánta más protección y seguridad se necesita para los defensores en un mundo en el que se encuentran cada vez más atacados. Nuestro principal foco es incrementar la presión en torno a los gobiernos que además de ser responsables ante el derecho internacional de proteger a los defensores, son además frecuentemente los perpetradores de ataques y medidas represivas contra los defensores. Sin embargo, es claro que a partir de la información proporcionada por los defensores mismos, se podría hacer mucho más para desarrollar su propia capacidad para mejorar su seguridad.

Por esta razón nos pareció muy interesante cuando supimos del proyecto que bajo el título de "Priorizando la protección" estaba desarrollando Peace Brigades International, y particularmente el manual propuesto para defensores de derechos humanos. Rápidamente nos pusimos de acuerdo con ellos para financiar la investigación y la publicación de este manual.

Ha sido un placer trabajar con Enrique Eguren como autor de este manual. Junto con sus colegas, ha aportado la riqueza de la experiencia sobre temas de protección y seguridad. PBI ha llevado también a cabo un número de talleres con defensores en el terreno, para intentar asegurar que el manual se beneficia de la experiencia de aquellos que están trabajando en primera línea. Dos de estos talleres fueron llevados a cabo con la colaboración de Front Line en Bukavu y Goma, en la región Este de la República Democrática del Congo, en mayo de 2004.

El objetivo de Front Line al publicar el manual es proveer de un recurso práctico que los defensores puedan usar al desarrollar sus estrategias y planes de protección y seguridad. En este sentido el manual se ofrece como un trabajo abierto sobre el cual esperamos poder construir con la experiencia de tantos defensores que trabajan en entornos hostiles. Los contenidos del manual también han tenido en cuenta las discusiones sobre seguriad y protección mantenidas en la Primera y Segunda Plataformas de Dublín para Defensores de Derechos Humanos, celebradas en 2002 y 2003. habrá otra oportunidad para una discusión sistemática y comentarios sobre el manual en la Tercera Plataforma de Dublín de octubre del 2005.

El manual intenta profundizar en cómo analizar riesgos y amenazas y cómo desarrollar estrategias y planes efectivos de seguridad y protección.

Esperamos que sea una herramienta útil para los responsables de seguridad en las ONG de derechos humanos y un apoyo para la formación de defensores. Nuestra intención es publicar un manual mas corto con consejos y sugerencias prácticas para complementar el manual de formación. Front Line está también embarcado en un proyecto con Privaterra para publicar un manual y un conjunto de herramientas especias para el tema de seguridad y comunicaciones electrónicas, en parte resumido en el capítulo 12, que será lanzado en 2005.

Tenemos que reconocer la contribución de varias personas sin las cuales este manual no habría sido publicado.

Marie Caraj, Pascale Boosten, Michael Schools and Christoph Klotz, queridos colegas de la Oficina Europea de PBI, fueron clave para este proyecto: sin su compromiso y experiencia no hubiéramos conseguido nada.

El texto fue revisado y corregido por Mary Lawlor, Andrew Anderson, James Mehigan, y Dmitri Vitaliev (capítulo 12), por Front Line. Kristin Hulaas Sunde revisó una versión anterior del texto.

El capítulo 12 está basado en el trabajo de Robert Guerra, Katitza Rodríguez y Caryn Madden, de Privaterra (Canadá).

Estamos en deuda con los aportes y comentarios recibidos de Arnold Tsunga (Zimbabwe Lawyers for Human Rights), Sihem Bensedrine (Túnez, Conseil National pour les Libertés en Tunisie), Padre Brendan Forde (Franciscanos Itinerantes, Colombia), Indai Sajor (antigua Directora del Asian Centre for Women´s Human Rights, Filipinas), James Cavallaro (Brasil, Director Asociado del Programa de Derechos Humanos de la Harvard Law School), Nadejda Marques (investigador y consultor, Global Justice Center, Rio de Janeiro, Brasil) y Marie Caraj (Oficina Europea de PBI, Bélgica). Otros colegas también han contribuido con su propio trabajo. Tenemos que mencionar a José Cruz e Iduvina Hernández de SEDEM (Guatemala), Claudia Samayoa (Guatemala), Jaime Prieto (Colombia), Emma Eastwood (UK) y Cintia Lavandera (Programa de Defensores de Derechos Humanos de Amnistía Internacional en Londres).

Carmen Díez Rozas diseñó cuidadosamente todo el manual y completó su maquetación, y Montserrat Muñoz colaboró con asesoría en la maquetación e ilustraciones.

Estamos también agradecidos al apoyo proporcionado por Development Cooperation Ireland. Impreso por "Print and Display".
(del autor)

También muchas otras personas han contribuido a reunir el conocimiento necesario para escribir el manual. Es imposible nombrarlas a todas aquí, pero nos gustaría mencionar algunos nombres, como:

Para toda la gente de PBI, y especialmente para mis anteriores colegas en el proyecto PBI Colombia, como Marga, Elena, Francesc, Emma, Tomás, Juan, Mikel, Solveig, Mirjam y tantos otros...

A Danilo, Clemencia y Abilio y sus colegas de la Comisión Intereclesial de Justicia y Paz en Colombia. Ellos me enseñaron cómo vivir dentro del corazón de la gente. A la gente de Santa Marta, en El Salvador, y del Cacarica, Jiguamiandó y San José de Apartadó en Colombia. Ellos, entre otros, me enseñaron cómo la gente del campo vive con dignidad.

A las personas comprometidas en el programa de formación de en

seguridad para defensores de Consejería en Proyectos en Colombia, y a los y las colegas de Pensamiento y Acción Social (PAS) en Colombia. Al consejo y al aprendizaje inicial con REDR (Londres) y Koenraad van Brabant (Bélgica).

Y a tantos defensores con los que he trabajado en El Salvador, Guatemala, Colombia, México, Sri Lanka, Croacia, Serbia, Kosovo, Ruanda, República Democrática del Congo, Ingushetia, etc... un mar de conversiones, lágrmas, sonrisas y aprendizaje y compromiso...

Finalmente, no hubiera podido hacer nada sin el amor y dedicación y apoyo de Grisela e Iker y de mis padres. Con todo mi cariño, para ellos.

Agradecemos su aporte a todas las personas mencionadas, y a los muchos defensores con los que hemos trabajado y de los que tanto hemos aprendido. Sin embargo, el texto final y cualquier error que pudiera haber en él son la sola responsabilidad conjunta de Front Line y del autor. Esperamos que este manual sea una herramienta útil para mejorar la protección y la seguridad de los defensores de derechos humanos, aunque sabemos que el manual no puede ofrecer garantías, y que al final estos son temas sobre los que las personas deben asumir su responsabilidad por sí mismas. Esperamos vuestros comentarios y opiniones.

Front Line
Oficina Europea de Peace Brigades International
7 de marzo de 2005

Exención de responsabilidad respecto al texto

Índice de capítulos

Manual de Seguridad y Protección Para los Defensores de los Derechos Humanos

El riesgo de los defensores de los derechos humanos

Los Derechos Humanos están amparados bajo el derecho internacional, pero el trabajo para asegurar su cumplimiento y asumir los casos de aquéllos cuyos derechos han sido violados puede resultar un ejercicio peligroso en muchos países del mundo. Los defensores de los Derechos Humanos son a menudo la única fuerza posicionada entre el ciudadano de a pie y el desproporcionado poder del estado. Por ello son actores fundamentales en el desarrollo de los procesos e instituciones democráticos, para poder acabar con la impunidad y para la promoción y protección de los derechos humanos.

Los defensores de los Derechos Humanos son a menudo víctimas de acosos, detenciones, torturas, difamaciones, suspensiones laborales, privaciones de libertad de movimiento y obstáculos en la obtención del reconocimiento legal de sus asociaciones. En algunos países son asesinados o "desaparecidos."

En los últimos años ha incrementado la conciencia general del enorme riesgo que corren los defensores de los derechos humanos en su labor. El riesgo es fácil de identificar cuando los defensores trabajan en situaciones hostiles como, por ejemplo, cuando la ley de un país penaliza a las personas que realizan ciertos tipos de trabajo relacionados con los derechos humanos. Los defensores corren también riesgo cuando la ley autoriza plenamente el trabajo en derechos humanos por una parte, pero por la otra no castiga a aquéllos que amenazan o atacan a los defensores. En situaciones de conflicto armado, el riesgo se hace más patente todavía.

Exceptuando algunas situaciones caóticas en las que la vida de un defensor puede estar en manos de unos soldados durante un control de carreteras, la violencia perpetrada contra los defensores no debe considerarse indiscriminada. En la mayoría de los casos los ataques violentos representan una respuesta deliberada y organizada contra el trabajo de los defensores, vinculada a una clara agenda política o militar.

Estos desafíos hacen que los defensores de los derechos humanos deban implementar amplias y activas estrategias de seguridad en el día a día de su trabajo. Ofrecer a los defensores consejos bienintencionados o recomendarles

que "vayan con cuidado" no es suficiente: se hace imprescindible una mejora en el manejo de su seguridad. Este manual no ofrece soluciones “hechas a medida” listas para ser aplicadas en cualquier situación. No obstante pretende proporcionar una serie de maniobras dirigidas a mejorar la gestión de la seguridad de los defensores.

Las lecciones de seguridad más efectivas proceden de los propios defensores - de sus experiencias diarias y de las tácticas y estrategias que van desarrollando con el tiempo para proteger su propio entorno de trabajo y el de los demás. Este manual debe, por lo tanto, considerarse como un trabajo en proceso de elaboración que deberá actualizarse y adecuarse a medida que recopilemos más información por parte de los defensores de los derechos humanos que trabajan en primera línea.

También hay lecciones que aprender de las ONGs humanitarias internacionales, que han empezado recientemente a desarrollar sus propias normas y procedimientos para salvaguardar la seguridad de su personal.

Es importante tener en cuenta que el principal riesgo de los defensores es que a menudo las amenazas de hecho se convierten en ataques. Los agresores poseen la voluntad, los medios y la impunidad para llevar a cabo las amenazas. Por lo tanto, el mejor instrumento para proteger a los defensores es la acción política dirigida a la necesidad por parte de los gobiernos y la sociedad civil de presionar y actuar contra aquéllos que día tras día amenazan, hostigan y matan a defensores. Por ello los consejos facilitados en este manual no pretenden de ninguna manera reemplazar la debida obligación de todos y cada uno de los gobiernos de proteger a los defensores de los derechos humanos.

Dicho esto, los defensores pueden mejorar considerablemente su seguridad observando algunas normas y procedimientos propuestos y probados.

Este manual representa una modesta contribución hacia un fino compartido por muchas y diversas organizaciones: preservar la inestimable labor que realizan los defensores de los derechos humanos. Son ellos quienes están en primera línea, y son también ellos los protagonistas de este manual.

El manual

El objetivo de este manual es el de proporcionar a los defensores de los derechos humanos un conocimiento adicional y algunos instrumentos que puedan serles de utilidad de cara a mejorar su seguridad y protección. El manual les ayudará a realizar su propia valoración de los riesgos y a desarrollar las normas de seguridad y procedimientos que sean màs convenientes para cada situación en particular.

El presente manual es el resultado de un proyecto a largo plazo de PBI sobre la protección de los defensores. Hemos tenido la oportunidad de aprender y compartir experiencias y conocimientos con centenares de defensores en el terreno, al igual que en talleres, reuniones y debates sobre la seguridad. La mayor parte del contenido del manual ya ha sido puesto en práctica, o bien directamente en protección del trabajo de los defensores o bien en los talleres de formación realizados. Este manual es por tanto fruto de todos esos intercambios, y estamos

enormemente agradecidos por la aportación de los defensores que han participado.

La seguridad y la protección son dos cuestiones complejas. Ambas se basan en torno a un conocimiento estructurado, pero también están influenciadas por las actitudes individuales y el funcionamiento de la organización. Uno de los mensajes clave de este manual es el de que hay que otorgar a la cuestión de la seguridad el tiempo, el espacio y la energía que necesita, a pesar de las sobrecargadas agendas laborales y del fuerte estrés e incluso miedo que padecen muchos los defensores. Esto implica ir más allá del conocimiento individuales sobre la seguridad y encaminarse hacia una cultura organizativa donde la seguridad sea parte integral del trabajo.

El apropiado conocimiento del escenario de trabajo es también un aspecto crucial para una correcta gestión de la seguridad de los defensores. El presente manual incluye reflexiones sobre conceptos básicos como el riesgo, la vulnerabilidad y la amenaza, y algunas sugerencias de cómo mejorar y desarrollar la seguridad de los defensores en el día a día del trabajo. Esperamos que los temas tratados ayuden a las ONGs y a los defensores a hacer mejor frente a los crecientes desafíos inherentes al trabajo en derechos humanos.

Dicho esto, lo debemos tener muy presente que los defensores arriesgan su bienestar e incluso sus vidas, y esto es algo realmente serio. Queremos que quede muy claro que todas las técnicas y sugerencias de este manual no son, en absoluto, el único enfoque de la seguridad de los defensores: el manual ha sido escrito con toda la buena voluntad pero lamentablemente no puede ofrecer garantías de éxito...

Mejoremos este manual...

El manual está en continuo proceso de elaboración y será necesario desarrollarlo, mejorarlo y perfeccionarlo. Tu información como defensor sobre cualquier aspecto de este manual nos será de gran valor: Te rogamos nos envíes cualquier comentario y opinión - sobretodo en lo concerniente a tu experiencia en el uso del manual en tu trabajo. Con tu ayuda, podemos transformarlo en un instrumento práctico para los defensores del mundo entero.

Contáctanos vía e-mail:

- protectionmanual@frontlinedefenders.org
- pbibeo@protectionline.org

O por correo a Front Line ó PBI

- **PBI- Oficina Europea,**
  11 Rue de la Linière, B-1060 Bruxelles, Belgium
  Tel +32 2 260 944 05 Fax +32 2 260 944 06
  pbibeo@protectionline.org

- **Front Line**
  16 Idrone lane, Off Bath Place, Blackrock, County Dublin, Ireland
  tel: +353 1212 3750 fax: +353 1212 1001

Una pequeña introducción a los Defensores de los Derechos Humanos.

El "defensor de los derechos humanos" es un término utilizado para describir a personas que, individualmente o con la ayuda de otros, se esfuerzan en promover o proteger los derechos humanos. A los defensores de los derechos humanos se les conoce sobre todo por lo que hacen, y el término puede, por lo tanto, definirse mejor describiendo sus acciones y algunos de los contextos en los que trabajan.

En 1998 la Asamblea General de las Naciones Unidas aprobó la "Declaración sobre el Derecho y el Deber de los Individuos, los Grupos y las Instituciones de la Sociedad de Promover y Proteger los Derechos Humanos y las Libertades Fundamentales Universalmente Reconocidos" (En lo sucesivo la "Declaración de la ONU sobre los Defensores de los Derechos Humanos"). En otras palabras, cincuenta años después de la Declaración Universal de los Derechos Humanos, y tras veinte años de negociaciones sobre un anteproyecto de la declaración sobre los defensores de los derechos humanos, las Naciones Unidas finalmente reconocieron lo que es una realidad: que millares de personas estaban promoviendo y contribuyendo a la protección de los derechos humanos en el mundo entero. Ésta es una Declaración incluyente que honra a la cantidad y variedad de personas comprometidas con la promoción y protección de los derechos humanos.

La Representante Especial del Secretario General de la ONU para los Defensores de los Derechos Humanos tiene la función de "buscar, recibir, revisar y responder a toda información sobre la situación y los derechos de todo individuo, que actúe individual o colectivamente, a promover y proteger los derechos humanos y libertades fundamentales."

Front Line define al defensor de los derechos humanos como "una persona que trabaja, de forma pacífica, para todos y cualquiera de los derechos consagrados en la Declaración Universal de los Derechos Humanos." Front Line busca promover la Declaración sobre los Defensores de los Derechos Humanos de la ONU.
(Véase más abajo fuentes para una mayor información sobre la Declaración de la ONU sobre los DDH)

Quién es responsable de proteger a los defensores de los derechos humanos?

La Declaración sobre los Defensores de los Derechos Humanos subraya que el estado es el principal responsable de proteger a los defensores de los derechos humanos. Asimismo reconoce "el valioso trabajo de individuos, grupos y asociaciones al contribuir en la efectiva eliminación de toda violación de los derechos humanos y libertades fundamentales" y "la relación entre la paz internacional y la seguridad y disfrute de los derechos humanos y libertades fundamentales".

Pero, según Hina Jilani, la actual Representante Especial del Secretario General de la ONU para los Defensores de los 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"[2]. Todos los informes sobre los defensores de los derechos humanos del mundo entero revelan historias de tortura, desapariciones, asesinatos, amenazas, robos, entrada ilegal en oficinas, coacción, detenciones ilegales, estar sometido a actividades de inteligencia y de vigilancia, etc. Lamentablemente, esta es la regla y no la excepción para los defensores.

[1] Report on Human Rights Defenders, 10 Sept 2001 (A/56/341).

Lectura sugerida

Para más información sobre los defensores de los derechos humanos, véase:

- www.unhchr.ch/defender/about1.htm (El Alto Comisionado de la ONU para los Derechos Humanos).

- www.frontlinedefenders.org (Front Line, La Fundación Internacional para los Defensores de los Derechos Humanos).

- www.peacebrigades.org/beo.html (La Oficina Europea de Brigadas de Paz Internacionales en Bruselas).

- El Observatorio para la Protección de los Defensores de los Derechos Humanos, creado por la Federación Internacional de los Derechos Humanos (FIDH; www.fiderechos humanos.org) y la Organización Mundial Contra la Tortura (OMCT; www.omct.org).

- www.amnesty.org y http://web.amnesty.org/pages/hrd-index-eng (Amnistía Internacional).

- www.ishr.ch, véase bajo "HRDO" (La Oficina de los Defensores de los Derechos Humanos del Servicio Internacional para los Derechos Humanos en Ginebra)

Para más información sobre los instrumentos legales internacionales existentes y la Declaración de la ONU sobre los Defensores de los Derechos Humanos, visite:

- www.unhchr.ch : ésta es la página web del Alto Comisionado de la ONU de los Derechos Humanos.

- www.frontlinedefenders.org/manual/en/index.htm (Front Line, Irlanda), para un manual sobre los instrumentos internacionales de los defensores de los derechos humanos. Su página de conexión también es de gran utilidad: http://www.frontlinedefenders.org/links/

- www.ishr.ch/index.htm (Servicio Internacional de los Derechos Humanos, Ginebra) para una recopilación de instrumentos internacionales y regionales para la protección de los defensores de los derechos humanos.

CAPÍTULO 1

Escenarios de trabajo: contextualizando las decisiones sobre seguridad y protección

Objetivos:

Tomar conciencia de la importancia de analizar nuestros escenarios de trabajo y los diferentes actores que intervienen.

Aprender diferentes métodos para ello.

El entorno de trabajo de los defensores de los derechos humanos

Los defensores de los derechos humanos suelen trabajar en escenarios complejos, con una gran variedad de actores, que se ven afectados por procesos de toma de decisiones sumamente políticas. En estos escenarios suceden muchas cosas simultáneamente, y cada una de ellas ejercerá su influencia sobre las otras. Los defensores de derechos humanos necesitan, por lo tanto, poseer información no sólo sobre las cuestiones directamente relacionadas a su labor, sino también sobre las posiciones de los actores claves.

Un ejercicio inicial sería el de organizar una sesión de reflexión en grupo para intentar identificar y enumerar todos los actores sociales, políticos y económicos que puedan ejercer una influencia sobre la situación actual de seguridad.

Análisis del escenario de trabajo.

Es muy importante conocer y comprender lo mejor posible el contexto en el que se trabaja. Un buen análisis de ese contexto permite tomar decisiones contextualizadas sobre qué medidas y qué procedimientos de seguridad poner en práctica. Es también importante prever posibles situaciones futuras para, en la medida de lo posible, poder tomar medidas preventivas.

Sin embargo, el simple análisis del entorno de trabajo no es suficiente. También es necesario observar cómo podría afectar cada intervención a la situación y cómo podrían reaccionar otros actores ante ella. Es también importante considerar las dimensiones de un escenario de trabajo: se puede realizar un macro análisis sobre el país o la región, pero también se debe averiguar cómo funcionan esas macro dinámicas en el área concreta en la que estás trabajando,

es decir su micro dinámica. Por ejemplo, los paramilitares de una zona local podrían actuar de forma diferente a como se pudiera pronosticar siguiendo el análisis nacional. Es por ello necesario ser consciente de esas características locales. También es crucial evitar una visión estática de un escenario de trabajo, porque las situaciones evolucionan y cambian. Por lo tanto estos escenarios deberían ser revisados con regularidad.

Hay, entre otros, tres métodos prácticos a la hora de analizar el escenario de trabajo: "**formular Preguntas**", el "**análisis de fuerzas externas**" y el "**análisis de actores involucrados**".:

Formular preguntas

El simple hecho de formular las preguntas adecuadas puede ayudarte a comprender mejor tu entorno de trabajo. Resulta un instrumento útil para generar debates en un pequeño grupo, pero tan sólo funcionará si las cuestiones son formuladas de forma que faciliten la búsqueda de una solución.

Supongamos, por ejemplo, que el acoso por parte de las autoridades locales se convirtiera en un problema. Si se formula la pregunta como: "¿Qué debería hacerse para reducir el acoso?", tal vez os encontréis buscando simplemente un remedio para un síntoma, es decir el acoso. Pero si se formula la pregunta orientándola hacia una solución, reales proceso se hace más fácil. Por ejemplo, si se pregunta: "¿Es nuestro entorno socio-político lo suficientemente seguro como para poder llevar a cabo nuestra labor?", se obtendrían sólo dos posibles respuestas: "sí" o "no".

Si la respuesta es "sí", es necesario formular otra pregunta que pueda ayudar a determinar con exactitud y comprender debidamente cuáles son los puntos claves en juego para preservar la seguridad. Si, tras una deliberación apropiada sobre todas las actuaciones, planes y recursos disponibles, al igual que sobre la legislación, negociaciones en marcha, las comparaciones con otros defensores de la zona, etc., la respuesta resultara ser que "no", que nuestro entorno no es lo bastante seguro, a partir de este punto podemos seguir analizando por qué no es seguro, y así sucesivamente.

Uso del método de Formular Preguntas:

- Busca preguntas que te ayuden a delimitar y comprender debidamente los puntos clave en juego para preservar tu seguridad;
- Formula las preguntas orientándote en la obtención de una solución;
- Repite el proceso tantas veces como sea necesario (en forma de debate).

Algunas preguntas prácticas a formular:

- ¿Cuáles son las cuestiones claves en juego en el escenario sociopolítico y económico?
- ¿Quiénes son los actores más importantes en relación con estas cuestiones claves?
- ¿En qué medida podría nuestro trabajo afectar de forma negativa o positiva a los intereses de estos actores claves?
- ¿Cómo podríamos reaccionar en caso de que por nuestro trabajo nos convirtiéramos en blanco de estos actores?
- ¿Es nuestro entorno socio-político lo suficientemente seguro como para poder llevar a cabo nuestra labor?

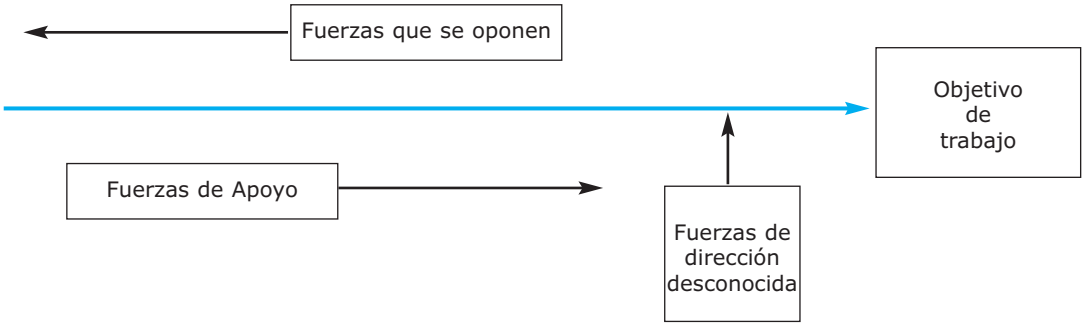
- ¿Cómo han respondido las autoridades locales/nacionales a la labor previa de los defensores de derechos en relación a esta cuestión?
- ¿Cómo han respondido los actores claves a actuaciones similares de los defensores de derechos -u otros- en relación con estas cuestiones?
- ¿Cómo han respondido los medios de comunicación y la comunidaden circunstancias similares?
- Etc.

Análisis de las fuerzas externas

El análisis de las fuerzas externas es una técnica que ayudar a identificar visualmente cómo diferentes fuerzas apoyan o entorpecen el logro de los objetivos de trabajo. Muestra tanto las fuerzas que apoyan como las que se oponen, y se basa en la premisa de que los problemas de seguridad pueden provenir de las fuerzas que se oponen, mientras que se puede sacar provecho de algunas fuerzas de apoyo. Esta técnica puede ser realizada por una persona sola, pero es más efectiva cuando es usada por un grupo diverso, con un objetivo de trabajo claramente definido y un método para lograrlo.

Empieza dibujando una flecha horizontal señalando a un recuadro. Escribe un pequeño resumen de tu objetivo de trabajo en ese recuadro. Esto nos proporcionará un foco para identificar las fuerzas a favor y en contra. Dibuja otro recuadro sobre la flecha central: enumera aquí todas las posibles fuerzas que podrían obstaculizar el logro de tu objetivo. Debajo de la flecha, dibuja un recuadro parecido que contenga todas las fuerzas de apoyo potencial. Dibuja un último recuadro para las fuerzas cuya dirección es desconocida o incierta.

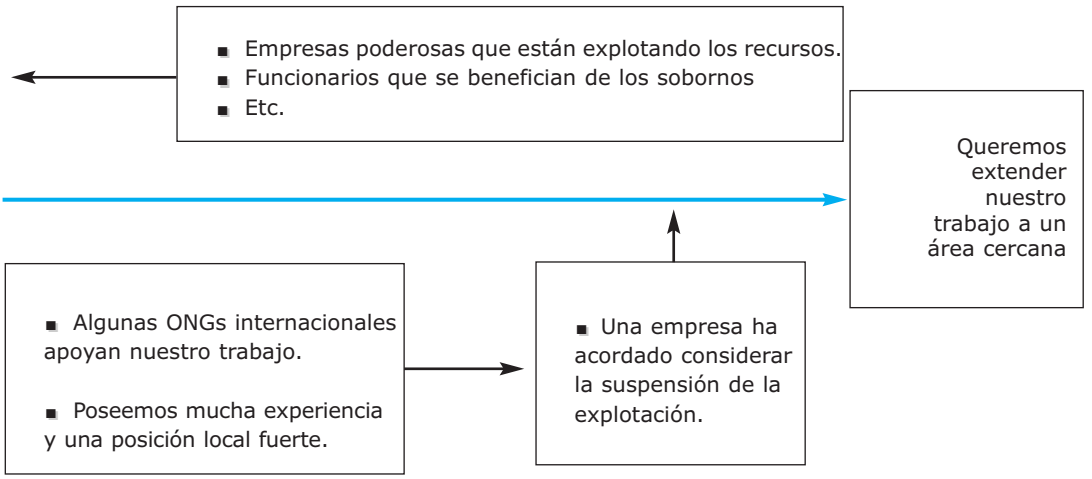
Tabla 1: Análisis de las fuerzas externas para evaluar los escenarios de trabajo



Tras haber completado el gráfico es el momento de los resultados. El análisis de las fuerzas externas te ayuda a visualizar claramente las fuerzas con las que trabajamos. El objetivo es encontrar formas de reducir o eliminar el riesgo generado por las fuerzas de en contra, en parte a través de la ayuda potencial de las fuerzas de apoyo. En cuanto a las fuerzas de dirección desconocida, es necesario decidir si considerarlas de apoyo, o ir analizándolas continuamente para poder así detectar los signos de su conversión hacia oposición o apoyo.

Por ejemplo:

Imaginemos que perteneces a una organización que trabaja sobre los derechos de la población indígena sobre los recursos naturales de su territorio, y que hay varios conflictos con varios acotres interesados en la explotación de esos recursos. Ahora quieres ampliar tu trabajo a un área cercana con problemas similares.



El análisis de actores.

El análisis de actores es una buena forma de aumentar la información que se tiene para tomar decisiones sobre protección. Requiere la identificación y descripción de los diferentes actores implicados y de sus relaciones, con base en sus características e intereses – y todo ello en relación a un tema concreto de protección.

Un actor en protección es toda persona, grupo o institución que esté involucrado o tenga un interés en el resultado de una política en el área de la protección[3].

En otras palabras, el análisis de actores es fundamental para comprender:

- Quién es quién y en qué circunstancias su "interés" ha de ser tenido en cuenta;
- La relación entre los actores, sus características e intereses;
- Cómo éstos se verán afectados por las actuaciones de protección;
- La voluntad de cada actor para implicarse en esas actuaciones en protección.

3 Adaptado de Sustainable Livelihoods Guidance Sheets No. 5.4 (2000)

Los actores que están involucrados en protección pueden ser clasificados de la siguiente manera:

Los actores primordiales. En el contexto de protección, **éstos son los propios defensores, y aquéllos para y con quien trabajan**, porque todos tienen un interés directo en su propia protección.

Los actores con responsabilidades, que tienen obligación de proteger a los defensores, es decir:

- Instituciones gubernamentales y estatales (incluyendo las fuerzas de seguridad, los jueces, los legisladores, etc.)
- Organismos internacionales con un mandato que incluya la protección, como algunos organismos de la ONU, organizaciones regionales, fuerzas de mantenimiento de la paz, etc;
- En el caso de los actores armados de oposición, se les puede asignar la obligación de no atacar a los defensores (como población civil que son), especialmente cuando estos actores armados controlan el territorio.

Los actores clave, que pueden influenciar en gran medida sobre la debida protección de los defensores. Pueden poseer una influencia política o la capacidad de presionar a los actores con responsabilidades si no cumplen con las mismas. (otros gobiernos, organismos de la ONU, etc.), y también pueden ejercer presión sobre otros actores que pueden estar implicados directa o indirectamente en atacar y presionar a los defensores (tales como empresas privadas o medios de comunicación o también otros gobiernos). Todo depende del contexto, los intereses y estrategias de cada:

- Organismos de la ONU (aparte de los que tienen mandato enprotección);
- El Comité Internacional de la Cruz Roja (CICR);
- Otros gobiernos e instituciones multilaterales (tanto como donantes como responsables políticos policy-makers);
- Otros actores armados;
- ONGs (tanto nacionales como internacionales);
- Iglesias e instituciones religiosas;
- Empresas privadas;
- Los medios de comunicación.

Un obstáculo importante a la hora de analizar las estrategias y actuacionesde los actores es que las relaciones entre ellos no estén bien definidas, o que tal vez incluso sean inexistentes. Muchos actores con responsabilidad en protección, especialmente los gobiernos, las fuerzas de seguridad y las fuerzas armadas de oposición, causan (o favorecen) las violaciones de los derechos humanos y la falta de protección de los defensores. Otros actores, que de no ser por ello compartirían las mismas preocupaciones por la protección, podrían tener también intereses opuestos como, por ejemplo terceros gobiernos, organismos de la ONU y ONGs. Todos estos factores, junto a aquéllos inherentes a las situaciones de conflicto, proyectan una visión compleja del escenario en su conjunto.

Análisis de estructuras y procesos variables

Los actores en protección no son estáticos, sino que interactúan entre sí a múltiples niveles, creando una densa red de relaciones. En términos de protección, es importante destacar y prestar atención a las interacciones que moldean y transforman las necesidades de protección de la gente. Para ello hemos de hablar de **estructuras y procesos**.

Las estructuras son las partes del sector público, la sociedad civil o las entidades privadas que se relacionan entre sí. Si los observamos desde el punto de vista de la protección, dentro del sector público, podríamos considerar al gobierno como un grupo de actores con una estrategia unificada o bien con unas estrategias internas enfrentadas. Por ejemplo, podríamos encontrar fuertes discrepancias entre el Ministerio de Defensa y el Ministerio de Asuntos Exteriores durante un debate sobre políticas referentes a los defensores de los derechos humanos, o entre la oficina del Defensor 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 cuerpos diplomáticos) para hacer un seguimiento de la situación de protección de una organización específica de defensores de los derechos humanos.

Los procesos en protección son las series de decisiones y actuaciones llevadas a cabo por una o varias estructuras con el objetivo de mejorar la situación de protección de un grupo específico. Los procesos pueden ser legislativos, culturales y sobre políticas de protección. No todos estos procesos consiguen obtener mejoras en la protección: En ocasiones los procesos de protección entran en conflicto o reducen mutuamente su eficacia. Por ejemplo, las personas supuestamente bajo protección podrían no aceptar una política de protección dirigida por el gobierno por considerar.

Existen muchos métodos para realizar un análisis de actores. Los aquí utilizados siguen una metodología sencilla e inmediata, lo que resulta esencial para obtener unos buenos resultados en los análisis y en los procesos de toma de decisión.

Un análisis de actores en cuatro pasos:

1 ◆ Examina la situación de protección de forma amplia (es decir, la situación de seguridad de los defensores de los derechos humanos en una región específica dentro de un país).

2 ◆ ¿Quiénes son los actores involucrados? Identifica y enumera todos los actores relevantes para este tema de protección (a través de sesiones de reflexión y debates).

3 ◆ Investiga y analiza las características y los aspectos propios de los actores, tales como su poder de influencia sobre la situación de protección, sus fines, sus estrategias, su legitimidad y sus intereses (incluyendo su voluntad de contribuir en la protección).

4 ◆ Investiga y analiza las relaciones entre los actores.

Después de haber efectuado este análisis, sus resultados se pueden visualizar en una matriz como la siguiente (véase Gráfico 2). Copia la misma lista de actores en la primera columna y a lo largo de la primera línea. Una vez copiada, se pueden realizar dos tipos de análisis:

- Para analizar las características de cada actor (objetivos e intereses, estrategias, legitimidad y poder), se rellenan las casillas siguiendo la diagonal donde cada actor intersecta consigo mismo:

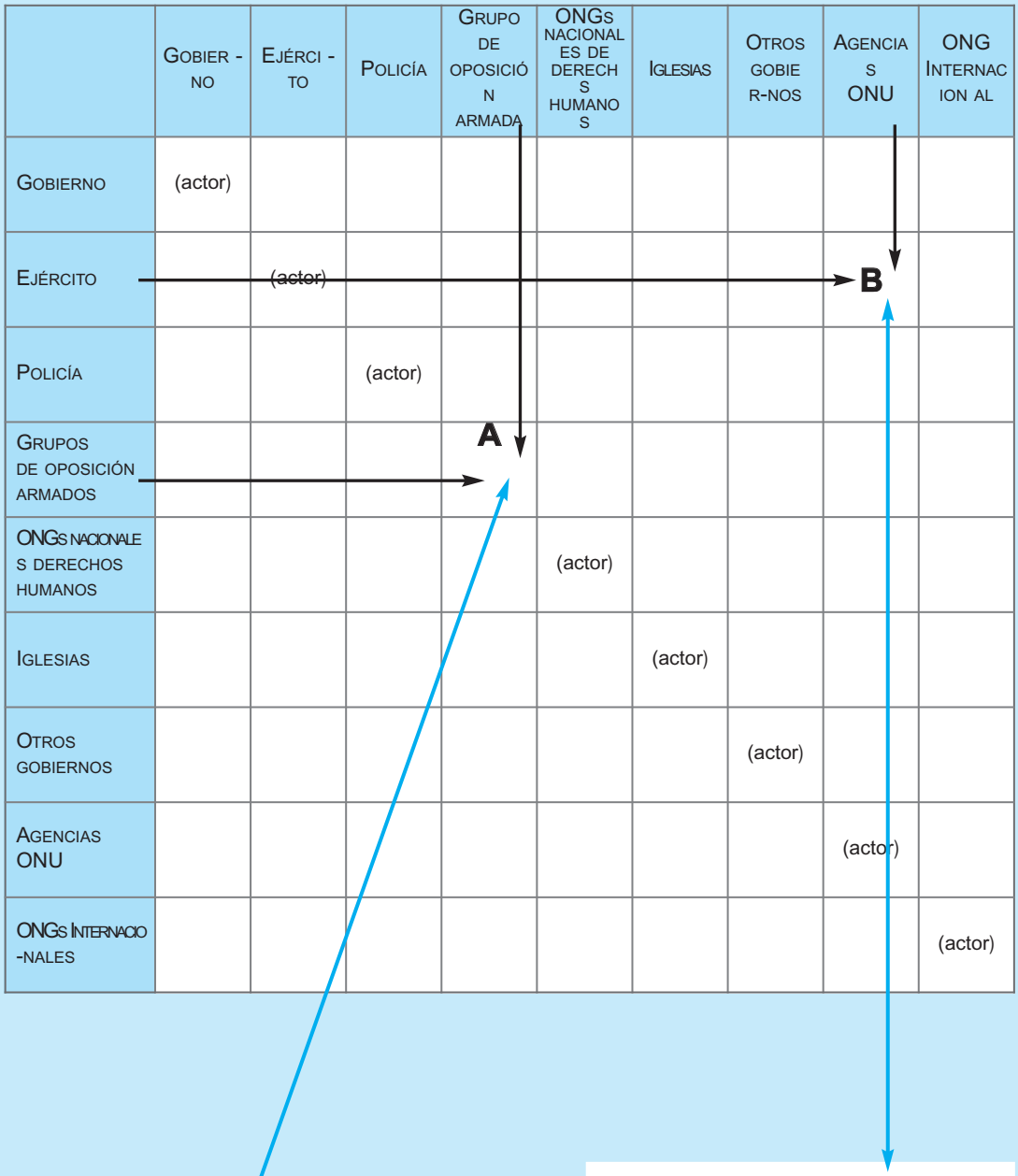
Por ejemplo

se pueden colocar los objetivos e intereses y estrategias de los grupos de oposición armada en la casilla "A".

- Para analizar las relaciones entre todos los actores, se rellenan las casillas que definen las relaciones más importantes relativas a la cuestión de protección, por ejemplo, la casilla de intersección entre el ejército y el Alto Comisionado de las Naciones Unidas para los Refugiados (UNHCR), en la casilla "B", etc.

Tras haber rellenado las casillas más pertinentes, se obtiene una visión general una perspectiva de los objetivos y las estrategias e interacción entre los principales actores respecto a cuestión específica de protección.

Gráfico 2: Sistema matriz para el análisis de actores



Casilla "**A**"

Para cada actor:

- objetivos e intereses
- estrategias
- legitimidad
- poder

Casilla "**B**"

Interrelación entre actores:

(interrelación relativa a la cuestión de protección y a las cuestiones estratégicas de ambos actores).

CAPÍTULO 2

Valoración del riesgo: amenazas, vulnerabilidades y capacidades

Objetivo:

Comprender los conceptos de amenaza, vulnerabilidad y capacidad en la seguridad.
Aprender cómo realizar una valoración del riesgo.

Análisis del riesgo y necesidades de protección

La labor de los defensores de los derechos humanos puede causar un impacto negativo sobre los intereses de ciertos actores, y esto puede a su vez poner en riesgo a los defensores. Es, por tanto, importante subrayar que **el riesgo forma parte inherente de las vidas de los defensores en ciertos países.**

El análisis del riesgo puede desglosarse en los siguientes pasos:

> Analizar los intereses y estrategias de los principales actores involucrados ⇨ Evaluar el impacto de la labor del defensor sobre esos intereses y estrategias ⇨ Evaluar la amenaza contra los defensores ⇨ Evaluar las vulnerabilidades y las capacidades de los defensores ⇨ Establecer el Riesgo

En otras palabras, la labor que los defensores realizan puede incrementar el riesgo al que se enfrentan.

- Lo **que** hacen puede provocar amenazas.
- **Cómo, dónde, y cuándo** trabajen plantea cuestiones sobre sus vulnerabilidades y sus capacidades en seguridad.

No existe una definición ampliamente aceptada del riesgo, pero podemos decir que el riesgo hace referencia a los posibles sucesos, por inciertos que éstos sean, que pueden causar un daño.

En una situación dada, todos aquéllos que trabajen para los derechos humanos pueden compartir un nivel común de peligro, pero el simple hecho de encontrarse en el mismo lugar no significa que todos sean igual de vulnerables a ese **riesgo** general. **La vulnerabilidad** – la posibilidad de que un defensor o un grupo sufra un ataque o daño – varía según los diferentes factores, tal y como estudiaremos seguidamente.

Un ejemplo:

Supongamos que el Gobierno de un país representa una amenaza general para todo tipo de trabajo sobre derechos humanos. Esto significa que todos los defensores corren un cierto riesgo. Pero también sabemos que algunos defensores corren un mayor riesgo que otros; por ejemplo, una gran ONG ya bien establecida, con base en la capital, seguramente no sea igual de vulnerable que una pequeña ONG local. Podríamos decir que afirmar esto es de sentido común, pero sería interesante analizar el por qué para poder así comprender y enfrentar mejor los problemas de los defensores.

El nivel de riesgo al que se enfrenta un grupo de defensores aumenta de acuerdo a las **amenazas** recibidas y a su **vulnerabilidad** de cara a esas amenazas, tal y como indicamos en la siguiente ecuación[1]:

RIESGO = AMENAZAS X VULNERABILIDADES

Las amenazas representan la posibilidad de que alguien dañe la integridad física o moral o la propiedad de otra persona a través de una acción intencionada y a menudo violenta[2]. Evaluar una amenaza significa analizar la posibilidad de que esta amenaza se lleve a cabo en forma de ataque. En una situación de conflicto los defensores pueden enfrentarse a muchas amenazas diferentes, como el "targeting" (amenazas directas con un blanco concreto), la delincuencia común y las amenazas indirectas.

La forma más común de amenaza – **el targeting** – pretende entorpecer o cambiar la labor de un grupo, o influenciar en la actividad de las personas implicadas. El targeting suele estar muy vinculado a la labor llevada a cabo por los defensores en cuestión, así como a los intereses y a las necesidades de las personas que se oponen a la labor de dichos defensores.

Los defensores podrían enfrentarse a la amenaza de **ataques por delincuencia común,** sobretodo si su labor les lleva hacia zonas de riesgo.

En otros casos el targeting se lleva a cabo bajo la apariencia de incidentes "por delincuencia común".

Las **amenazas indirectas** surgen del posible daño causado por combates en conflictos armados, tales como "estar en el lugar equivocado en el momento equivocado", por lo que estas amenazas conciernen sobre todo a los defensores que trabajan en zonas de conflicto armado.

Las amenazas tipo targeting (amenazas **concretas**) puede también considerarse de forma complementaria: Los defensores de los derechos humanos podrían

Sumario de los tipos de amenazas:

- Targeting (amenazas declaradas, amenazas potenciales): amenazas vinculadas a tu trabajo.
- Amenazas por delincuencia común.
- Amenazas indirectas: Amenazas debidas a combates en el caso de conflictos armados.

[1] Van Brabant (2000) and REDR.
[2] Dworken (1999).

enfrentarse a amenazas declaradas al recibir, por ejemplo, una amenaza de muerte (véase el Capítulo 3, sobre cómo evaluar las amenazas declaradas). Existen también casos de **posibles** amenazas, cuando un defensor vinculado a tu labor es amenazado y existen razones para sospechar que tú podrías ser el siguiente.

Vulnerabilidades

La vulnerabilidad es el grado en que las personas son suscetibles a pérdida, daños, sufrimiento o la muerte en caso de un ataque. La vulnerabilidad varía según el defensor o grupo, y cambia con el tiempo. Las vulnerabilidades son siempre relativas, porque todas las personas y grupos son vulnerables en cierto grado. Sin embargo, toda persona posee su propio nivel y tipo de vulnerabilidad, de acorde a las circunstancias. Veamos algunos ejemplos:

- La vulnerabilidad puede estar vinculada a la ubicación. Por ejemplo, un defensor suele ser más vulnerable cuando viaja para realizar una visita de campo que cuando se encuentra en una importante oficina dónde es raro que se lleve a cabo un ataque.

- La vulnerabilidad puede incluir la falta de acceso a un teléfono o a un transporte local seguro o de cerraduras apropiadas en las puertas de una casa. Pero las vulnerabilidades también están relacionadas con la falta de redes de colaboración y de soluciones compartidas entre los defensores.

- La vulnerabilidad puede también estar relacionada con el trabajo en equipo y con el miedo: Un defensor que recibe una amenaza puede sentir miedo, y su labor podría verse afectada por ese miedo. Si el defensor no dispone de un sistema efectivo para enfrentarse al miedo (alguien con quien hablar, un buen equipo de colegas, etc.) existen grandes posibilidades de que cometa errores o tome decisiones inadecuadas que podrían crearle más problemas de seguridad.

(Hay una lista completa de posibles vulnerabilidades y capacidades al final de este capítulo).

Capacidades

Las capacidades son los puntos fuertes y los recursos a los que puede acceder un grupo o un defensor para lograr un nivel razonable de seguridad. Ejemplos de capacidades serían la formación en seguridad o en cuestiones legales, el trabajo en equipo de un grupo, el acceso a un teléfono y a un transporte seguro, a las buenas redes de los defensores, a un sistema efectivo para enfrentarse al miedo, etc.

En la mayoría de los casos, la vulnerabilidad y las capacidades representan dos caras de la misma moneda.

Por ejemplo:

El no conocer suficientemente tu entorno laboral es una vulnerabilidad, mientras que el poseer ese conocimiento es una capacidad. Podríamos decir lo mismo de la falta de acceso a un transporte seguro o a las buenas redes de colaboración de los defensores.

(Hay una lista completa de posibles vulnerabilidades y capacidades al final de este capítulo)

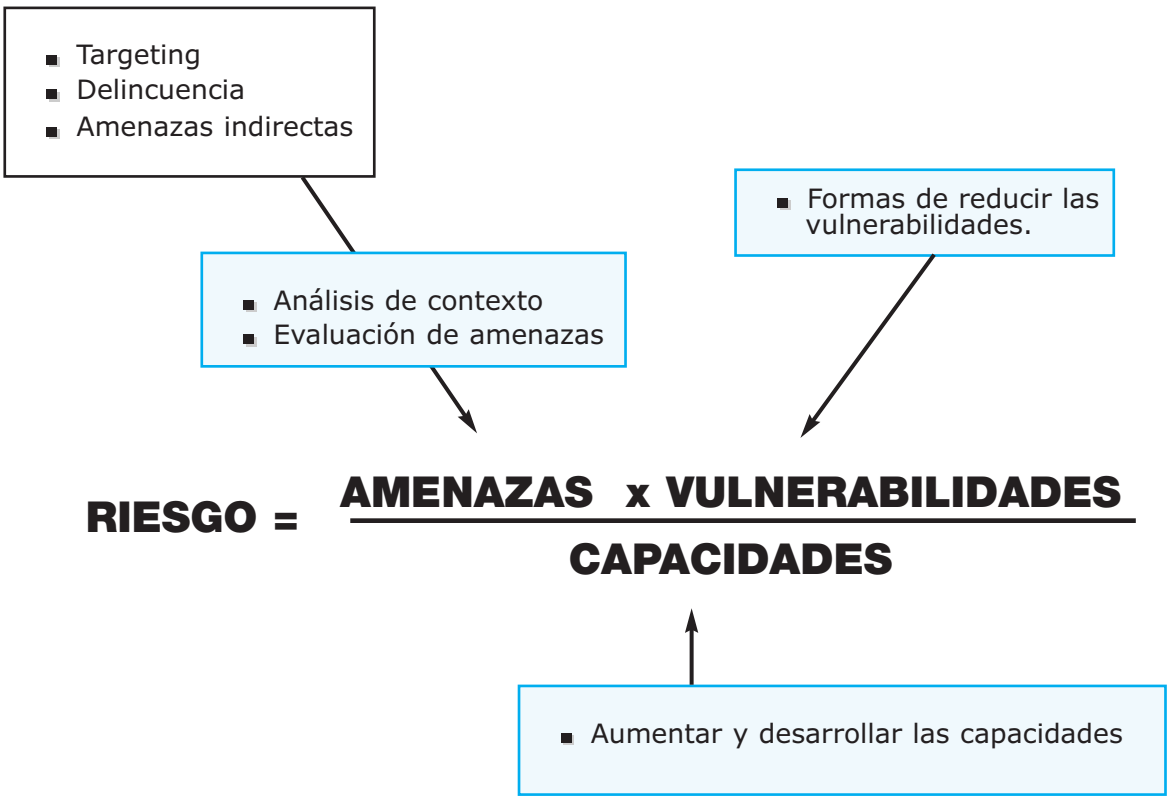
El riesgo creado por las amenazas y las vulnerabilidades puede reducirse si los defensores disponen de suficientes capacidades (a mayor número de capacidades, menor grado de riesgo).

$$\textbf{Riesgo} = \frac{\textbf{amenazas x vulnerabilidad}}{\textbf{capacidades}}$$

En resumen,

de cara a reducir el riesgo a niveles tolerables – es decir, para proteger – es necesario:

- Reducir las amenazas;
- Reducir los factores de vulnerabilidad;
- Aumentar las capacidades de protección.



El riesgo es un concepto dinámico que varía con el tiempo y con los cambios en la naturaleza de las amenazas, las vulnerabilidades y las capacidades. Por ello el riesgo debe ser evaluado periódicamente, sobre todo cuando varíe el entorno de trabajo, las amenazas o las vulnerabilidades. Por ejemplo, las vulnerabilidades también pueden aumentar si un cambio en el liderazgo coloca a un grupo de defensores en una situación más débil que la anterior. El riesgo aumenta drásticamente en el caso de una amenaza presente y clara. En este caso, no es adecuado intentar reducir el riesgo aumentando las capacidades, porque toma su tiempo.

Ciertas medidas de seguridad tales como la formación jurídica o las barreras protectoras, podrían reducir el riesgo al disminuir los factores de vulnerabilidad. Sin embargo, estas medidas no hacen frente a la fuente principal del riesgo, es decir las amenazas, ni tampoco a la voluntad de perpetrarlas, sobre todo en situaciones donde los perpetradores saben que probablemente no serán castigados. Todas las intervenciones importantes en la protección deberían por lo tanto concentrarse en reducir las amenazas, además de reducir las vulnerabilidades y aumentar las capacidades.

Un ejemplo:

> Un pequeño grupo de defensores trabaja en una ciudad en temas relacionados con la propiedad de la tierra. Cuando su labor empieza a afectar a los intereses de un terrateniente local reciben una clara amenaza de muerte. Si se aplica la ecuación de riesgo a la situación de seguridad, se comprobará que el riesgo que corren estos defensores es muy elevado, sobre todo debido a la amenaza de muerte. Si se pretende reducir ese riesgo seguramente éste no sea el momento adecuado para empezar a cambiar las cerraduras de la puerta de la oficina (porque el riesgo no está relacionado con un robo en la oficina), ni tampoco para comprarle un teléfono móvil a cada defensor (aunque la comunicación sea un factor importante para la seguridad seguramente no resultaría suficientemente efectivo si alguien intentara asesinar a un defensor). En este caso, la estrategia más relevante sería la de trabajar en red y generar respuestas políticas para confrontar directamente la amenaza (y si esto pareciera poco efectivo a corto plazo, tal vez la única forma de reducir el riesgo de forma significativa sea disminuir la exposición de los defensores, alejándolos por un tiempo - la capacidad de trasladarse a un lugar seguro es también una capacidad).

Las vulnerabilidades y las capacidades, al igual que algunas amenazas pueden variar según el sexo y la edad. Por lo tanto, es importante ajustar la información de las valoraciones de riesgo también a estas variables.

Valoración de vulnerabilidades y capacidades

Para poder diseñar la evaluación de las vulnerabilidades y capacidades de un grupo (o persona) en concreto, es necesario definir al grupo en cuestión (una comunidad, un colectivo, una ONG, individuos, etc.), la zona geográfica donde está ubicado y el espacio de tiempo (el perfil de vulnerabilidad cambia y evoluciona con el tiempo). Una vez hecho esto se procede a evaluar las vulnerabilidades y capacidades utilizando como guía la **tabla 3** situada al final de este capítulo.

Toma nota: La evaluación de las vulnerabilidades y capacidades debe considerarse como una actividad siempre en marcha, basada en el análisis de la información obtenida para poder mantener una visión clara de una situación que está en constante evolución. Al evaluar las capacidades es importante establecer cuales son las capacidades reales actuales en vez de enumerar las potenciales y/o deseables.

Estrategias de afrontamiento y estrategias de respuesta

Los defensores y los grupos bajo amenaza suelen usar diferentes **estrategias de afrontamiento** para tratar con los riesgos a los que sospechan que deberán enfrentarse. Estas estrategias varían enormemente según su entorno (rural, urbano), el tipo de amenaza, los recursos sociales, económicos y jurídicos disponibles, etc.

La mayoría de las estrategias de afrontamiento pueden ser implementadas de forma inmediata y en respuesta a unos objetivos a corto plazo. Por lo tanto funcionarán más como tácticas que como estrategias de respuesta más elaborada. La mayoría de las estrategias de afrontamiento responden también a unas percepciones subjetivas de riesgo personal, y en algunas ocasiones podrían afectar al grupo, sobretodo si las estrategias utilizadas no tienen marcha atrás.

Las estrategias de afrontamiento están muy relacionadas con la severidad y el tipo de amenaza y con las capacidades y vulnerabilidades del grupo.

Cuando pensamos en la seguridad es necesario tener en cuenta tanto nuestras propias estrategias de afrontamiento como las de los demás. Es importante reforzar las estrategias efectivas, intentar limitar las que puedan afectar negativamente y procurar respetar las restantes (sobre todo las estrategias de afrontamiento vinculadas a creencias culturales o religiosas).

Algunas estrategias de afrontamiento:

- Reforzar barreras protectoras, esconder objetos de valor.
- Evitar comportamientos que pudieran ser cuestionados por otro actor, sobre todo si el control del territorio donde se está ubicado se encuentra en disputa militar.
- Esconderse en situaciones de alto riesgo, incluyendo lugares de difícil acceso, como montañas o jungla, cambiar de casas, etc. A veces se esconden familias enteras y otras veces solo los defensores. El esconderse puede ser sólo durante la noche o podría alargarse durante varias semanas, y podría implicar un aislamiento total.
- Buscar la protección militar o política de uno de los actores armados.
- Suspender el trabajo, cerrar la oficina, evacuar. Desplazarse a otra región o salir al exilio.
- Confiar en la "buena suerte" o recurrir a creencias "mágicas".
- Ser más reservado, incluso con los compañeros; negar las amenazas, evitando hablar sobre ellas; beber en exceso; trabajar demasiado, comportamientos erráticos, etc.

Los defensores también tienen acceso a estrategias de respuesta elaborada. Éstas incluyen: realizar informes para sacar a luz un asunto concreto, presentar cargos, organizar manifestaciones, etc. En muchos casos estas estrategias no representan una estrategia a largo plazo, sino que responden a unas necesidades a corto plazo. En algunos casos las estrategias de respuesta pueden crear unos problemas de seguridad mayores que aquéllos que pretendían abordar inicialmente.

Al analizar las estrategias de afrontamiento y de respuesta, hay que tener en cuenta lo siguiente:

- **Sensibilidad:** ¿Aportarán una respuesta rápida a las necesidades de seguridad individuales o de grupo?

- **Adaptabilidad:** estas estrategias, ¿se adaptarán rápidamente a las nuevas circunstancias, una vez el peligro de ataque haya pasado? Un defensor puede disponer de varias opciones, como por ejemplo esconderse o irse a vivir a casa de otra gente por un tiempo. Estas estrategias podrían parecer débiles o inestables, pero suelen ser muy efectivas.

- **Sostenibilidad:** estas estrategias, ¿servirán a largo plazo, a pesar de amenazas o de ataques no letales?

- **Efectividad:** Protegerán adecuadamente a las personas o al grupo en cuestión?

- **Reversibilidad:** Si lus estrategias no funcionan o la situación cambia, ¿se podrán cambiar o volver atrás?

Tras valorar el riesgo, ¿qué podemos hacer con los resultados?

Una vez valorado el riesgo es necesario prestar atención a los resultados. Como es imposible medir la "cantidad" de riesgo al que uno se enfrenta, es necesario comprender y estimar cuál es el **nivel** de riesgo existente.

Los diferentes defensores y organizaciones pueden estimar diferentes grados de riesgo. Lo que resulta inaceptable para algunos defensores puede ser aceptable para otros, y lo mismo sucede con diferentes personas dentro de una misma organización. Más que debatir sobre lo que "habría que hacer" o sobre si se puede seguir adelante o no, es importante valorar los diferentes umbrales de riesgo de cada persona: Se trata de encontrar un límite aceptable para todos los miembros del grupo.

Dicho esto, existen diferentes formas de enfrentarse al riesgo:

- Puedes **aceptar** el riesgo tal y como está ahora, porque te sientes capacitado para "vivir con él";
- Puedes **reducir** el riesgo, concentrándote en las amenazas, las vulnerabilidades y las capacidades;
- Puedes **compartir** el riesgo, emprendiendo acciones conjuntas con otros defensores para que las amenazas dirigidas sólo a un defensor u organización sean menos efectivas;
- Puedes decidir **evitar** el riesgo, cambiando o paralizando tus actividades o cambiando el planteamiento de trabajo para reducir las amenazas potenciales;
- Puedes **ignorar** el riesgo, mirando hacia otro lado. Ni que decir tiene que ésta no es la mejor opción.

Hay que tener en cuenta que los niveles de riesgo suelen ser diferentes para cada una de las organizaciones e individuos implicados en un caso de derechos humanos, y que los agresores suelen atacar a los puntos más débiles, así que hay que prestar atención a estos diferentes niveles de riesgo y tomar medidas al efecto. Tomemos por ejemplo el caso de un campesino asesinado por sicarios de un terrateniente. Podría haber varias organizaciones e individuos involucrados en el caso, como por ejemplo un grupo de abogados de la capital cercana, un sindicato de campesinos y tres testigos (unos campesinos que viven en un pueblo cercano). Es imprescindible evaluar los diferentes niveles de riesgo de cada uno de estos actores para poder planificar debidamente la seguridad de cada uno de ellos.

Tabla 3: Información necesaria para evaluar las vulnerabilidades y las capacidades de un grupo
(Nota: Por lo general, la información de la columna derecha debería demostrar si un componente en concreto – de la columna izquierda – es una vulnerabilidad o una capacidad de un defensor o grupo de defensores específico)

Componentes de vulnerabilidades y capacidades	Información necesaria para evaluar las vulnerabilidades o componentes
Componentes geográficos, físicos y técnicos	
Exposición	La necesidad de cruzar o quedarse en zonas peligrosas para llevar a cabo actividades rutinarias u ocasionales, con actores amenazantes en esas zonas.
Estructuras físicas	Las características de la vivienda (oficinas, casas, refugios); materiales de construcción, puertas, ventanas, armarios. Barreras protectoras. Alumbrado nocturno.
Oficinas y lugares abiertos al público	¿Están tus oficinas abiertas al público? ¿Existen áreas reservadas únicamente al personal? ¿Debes tratar con desconocidos que acuden a tus oficinas?
Lugares de escondite, rutas de escape	¿Existe algún lugar para esconderse? ¿Son accesibles? (distancia física) y ¿para quién? (para personas específicas o para el grupo entero) ¿Podrías salir momentáneamente del lugar si fuera necesario?
Acceso a la zona	¿Con qué dificultades se pueden encontrar los visitantes de fuera (funcionarios del gobierno, ONGs, etc.) para acceder a la zona? (en el caso de un vecindario peligroso, por ejemplo) ¿Con qué dificultades de acceso se encuentran los actores que generan amenazas?
Transporte y alojamiento	¿Existe algún acceso a transporte seguro (público o privado) para los defensores? Estos transportes, ¿representan alguna ventaja o desventaja en particular? ¿Disponen los defensores de un alojamiento seguro durante sus desplazamientos?
Comunicación	¿Hay sistemas de telecomunicaciones (radio, teléfono)? ¿Disponen los defensores de un buen acceso a éstos? ¿Funcionan correctamente en todo momento? ¿Podrían los actores amenazadores cortarlos antes de un posible ataque?

Componentes de vulnerabilidades y capacidades	Información necesaria para evaluar las vulnerabilidades o componentes
Componentes relacionados con el conflicto	
Vínculos con las partes conflictivas	¿Existe algún vínculo entre los defensores y las partes en conflicto (parientes, vienen de la misma zona, intereses comunes) que pudiera ser utilizado injustamente contra los defensores?
Actividades de los defensores que afectan a una parte conflictiva	La labor de los defensores, ¿afecta de forma directa a los intereses de algún actor? (Como por ejemplo en el caso de la protección de recursos naturales valiosos, el derecho a la propiedad) ¿Trabajas en algún asunto delicado de cara a los actores con poder? (como por ejemplo de nuevo, el derecho a la propiedad de la tierra)
Transporte de objetos y mercancías e información escrita	¿Poseen los defensores objetos o mercancías que puedan ser valiosos para los grupos armados, y que por lo tanto aumenten el riesgo de targeting o de robo? (Gasolina, ayuda humanitaria, pilas, manuales de salud, etc.) ¿Tienen los defensores que llevar consigo información escrita sensible o comprometedora?
Conocimiento sobre zonas de combate y zonas minadas	¿Posees algún tipo de información sobre lo que sucede en las zonas de combate que pudiera causarte algún riesgo? ¿Y sobre posibles zonas seguras para contribuir a tu seguridad? ¿Tienes información confiable sobre las zonas minadas?
Componentes relacionados con el sistema jurídico y político	
Acceso a las autoridades y a un sistema jurídico para reclamar sus derechos	¿Pueden los defensores iniciar un procedimiento legal para reclamar sus derechos? (Acceso a una representación legal, presencia física en juicios o reuniones, etc.) ¿Pueden los defensores obtener una asistencia apropiada de las autoridades de cara a su labor y sus necesidades de protección?
Capacidad para obtener resultados del sistema jurídico y de las autoridades	¿Tienen los defensores derecho a reclamar sus derechos? ¿O están sujetos a leyes internas represivas? ¿Pueden adquirir suficiente poder/influencia para hacer que las autoridades tomen nota de sus reclamaciones?
Registro, capacidad de mantener la contabilidad y los criterios legales	¿Se les niega a los defensores un registro legal o están éstos sujetos a largos retrasos? ¿Es tu organización capaz de mantener la contabilidad en orden según los requerimientos legales nacionales? ¿Empleáis programas informáticos pirateados?
Gestión de información	
Fuentes y precisión de la información	¿Poseen los defensores fuentes de información fidedignas en las que basar sus acusaciones? ¿Publican los defensores información precisa y siguiendo métodos adecuados?
Mantener, enviar y recibir información	¿Pueden los defensores guardar información en un lugar seguro y de confianza? ¿Podría ser robada? ¿Está protegida de virus y piratas informáticos? ¿Puedes enviar y recibir información de forma segura?
Ser testigos o poseer información clave	¿Son los defensores un testigo clave para presentar cargos contra un actor con poder? ¿Poseen los defensores información única y relevante sobre un caso o proceso específicos?
Tener una explicación coherente y aceptable sobre la labor y sus objetivos	¿Tienen los defensores una explicación clara, sostenible y coherente sobre su labor y objetivos? ¿Es esta explicación aceptable, o por lo menos tolerable, por parte de la mayoría o de todos los actores? (sobre todo los armados) ¿Están todos los miembros del grupo capacitados para proporcionar esa explicación cuando se les solicite? (en un retén o en una entrevista)

Componentes de vulnerabilidades y capacidades	Información necesaria para evaluar las vulnerabilidades o componentes
Componentes sociales y organizativos	
Existencia de una estructura de grupo	¿Está el grupo organizado o estructurado de alguna forma? ¿Proporciona dicha estructura un grado aceptable de cohesión al grupo?
Habilidad de tomar decisiones conjuntas	¿Es la estructura del grupo un reflejo de intereses particulares o representa al grupo entero (incluyendo afiliados)? ¿Quién asume las principales decisiones y responsabilidades, una única persona o varias? ¿Se han creado sistemas de emergencia para la toma de decisiones y asunción de responsabilidades? ¿En qué grado es la toma de decisiones participativa? ¿La estructura del grupo permite: a) toma de decisiones conjuntas e implementación de éstas, b) debatir los temas en grupo, c) reuniones esporádicas e inefectivas, d) ninguna de las arriba mencionadas?
Planes de seguridad y procedimientos	¿Se han puesto en marcha normas y procedimientos de seguridad? ¿Existe un buen conocimiento y apropiación de los procedimientos de seguridad? ¿Se cumplen las normas de seguridad? (Para más detalles, véase Capítulo 8)
Gestión de la seguridad fuera del ámbito laboral (familia y tiempo libre)	¿Como manejan los defensores su tiempo fuera del ámbito laboral (familia y tiempo libre)? El consumo de alcohol y drogas representan grandes vulnerabilidades. Las relaciones personales también pueden convertirse en vulnerabilidades (al igual que ventajas).
Condiciones laborales	¿Tiene todo el mundo un contrato laboral adecuado? ¿Se tiene acceso a fondos de emergencia? ¿Y a seguros?
Contratación de personal	¿Se sigue el procedimiento adecuado en la contratación de personal o miembros? ¿Se sigue un plan de seguridad apropiado con los voluntarios ocasionales (como los estudiantes, por ejemplo) o los visitantes de la organización?
Trabajar con gente o con organizaciones conjuntas	¿Se trabaja de cara al público? ¿Se conoce bien a la gente? ¿Se trabajas conjuntamente con alguna organización como intermediaria ante la gente?
Cuidar de los testigos o víctimas con las que trabajamos	¿Evaluamos los riesgos de las victimas y testigos, etc., cuando trabajamos en casos concretos? ¿Tomamos medidas de seguridad específicas cuando les vemos o cuando vienen a nuestra oficina? ¿Cómo reaccionamos si reciben amenazas?
Vecindario y entorno social	¿Están los defensores bien integrados socialmente en el área local? ¿Algunos grupos sociales consideran la labor de los defensores como algo bueno o nocivo? ¿Están los defensores rodeados de gente presuntamente hostil? (vecinos que actúan de informadores, por ejemplo)
Capacidad de movilización	¿Pueden los defensores movilizar a la gente en actividades públicas?

Componentes de vulnerabilidades y capacidades	Información necesaria para evaluar las vulnerabilidades o componentes
Componentes psicológicos (grupo/individuos)	
Capacidad para manejar el estrés y el miedo	Las personas clave, o el grupo en conjunto, ¿confía en su propio trabajo? ¿Expresan los individuos sentimientos de unidad y de tarea común (tanto en palabras como en actos)? El nivel de estrés, ¿afecta en la comunicación y las relaciones interpersonales?
Sentimientos de desaliento o de "sentirse perseguido"	¿Se expresan claramente (tanto en palabras como en actos) los sentimientos de desaliento o de pérdida de esperanza?
Recursos para el trabajo	
Habilidad de comprender el contexto y el riesgo del trabajo	¿Tienen los defensores acceso a una información precisa de su contexto de trabajo, de los actores involucrados y de sus intereses? ¿Son los defensores capaces de procesar esa información y valorar las amenazas, las vulnerabilidades y las capacidades?
Capacidad para definir planes de actuación	¿Pueden los defensores definir e implementar planes de acción? ¿Hay previos ejemplos de ello?
Capacidad para obtener consejo de fuentes bien informadas	¿Puede el grupo obtener consejo fiable? ¿De las fuentes apropiadas? ¿Puede el grupo decidir independientemente qué fuentes utilizar? ¿Se tiene acceso a organizaciones específicas o se posee un estatus que apoye las capacidades de protección?
Personal y cantidad de trabajo	¿Es el número de personas o trabajadores proporcional a la cantidad de trabajo existente? ¿Es posible organizar las visitas al terreno en equipos (de un mínimo de dos personas)?
Recursos financieros	¿Se dispone de suficientes recursos financieros para la seguridad? ¿Se maneja el dinero de una forma segura?
Conocimiento de idiomas y zonas	¿Se dominan los idiomas necesarios para trabajar en esta zona? ¿Se conoce bien la zona? (carreteras, pueblos, teléfonos públicos, centros de salud, etc.)
Acceso a contactos nacionales e internacionales y a los medios de comunicación	
Acceso a redes nacionales e internacionales	¿Tienen los defensores contactos nacionales e internacionales? ¿Con delegaciones, embajadas, otros gobiernos, etc. visitantes? ¿Con líderes de la comunidad, líderes religiosos, u otros personajes influyentes? ¿Se pueden emitir acciones urgentes a través de otros grupos?
Acceso a los medios de comunicación y capacidad para obtener resultados de éstos	¿Tienen los defensores acceso a los medios de comunicación (nacional, internacional)? ¿Y a otros medios (medios independientes)? ¿Saben los defensores relacionarse con los medios de comunicación correctamente?

Una balanza para medir el riesgo.

Una balanza es también útil para entender el concepto de riesgo: es algo que podríamos llamar... un "riesgómetro". Si ponemos dos costales con nuestras amenazas y vulnerabilidades en uno de los platillos de la balanza, y otro costal con nuestras capacidades en el otro platillo, veremos como nuestro riesgo aumenta o se reduce:

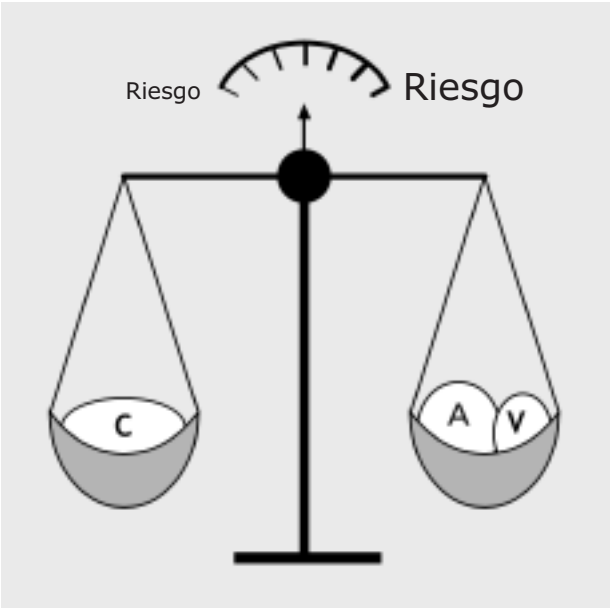


Fig. 1

Cuantas más vulnerabilidades y amenazas tengamos, más riesgo enfrentamos:

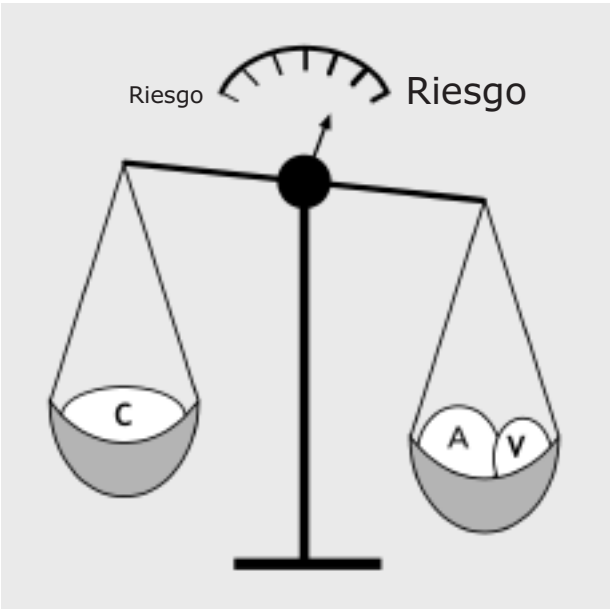


Fig. 2

Cuantas más capacidades tengamos, menos riesgo enfrentaremos. Y para reducir el riesgo, también podemos reducir nuestras amenazas y vulnerabilidades, así como aumentar nuestras capacidades:

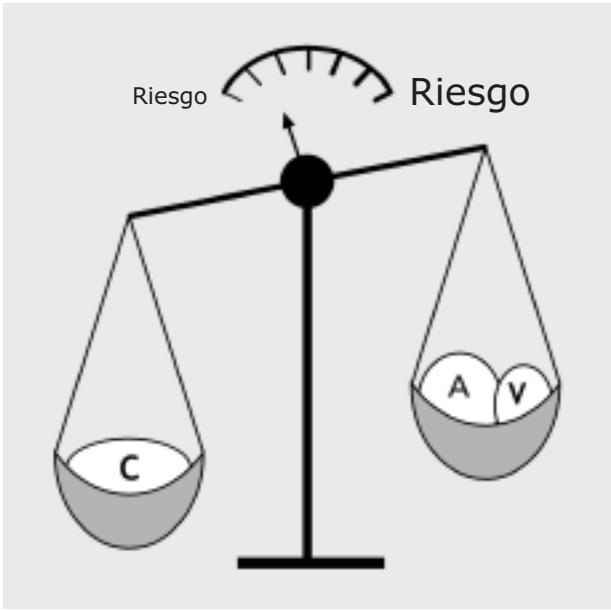


Fig. 3

Pero, miremos lo que sucede si enfrentamos amenazas grandes o severas: No importa que intentemos aumentar nuestras capacidades en ese preciso momento: ¡la balanza mostrará un alto nivel de riesgo de todas maneras!

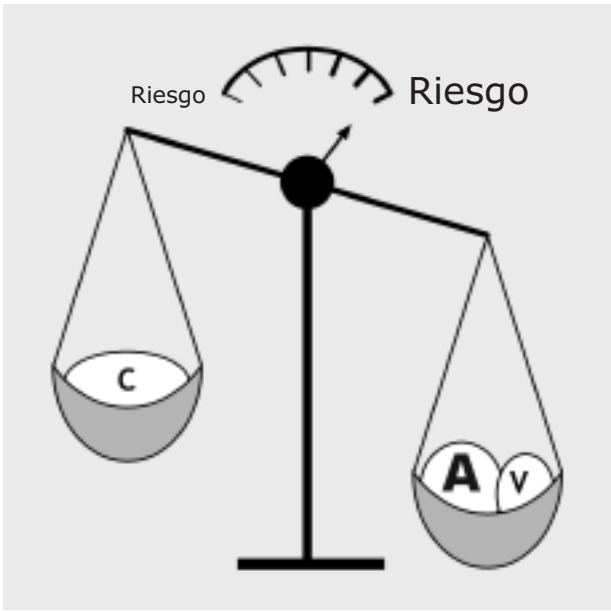


Fig. 4

Capítulo 3

Conocimiento y evaluacíon de las amenazas

Objetivo:

Obtener un conocimiento detallado de las amenazas y de cómo responder ante ellas.

Evaluación de las amenazas: cómo entenderlas en profundidad.

La represión contra los defensores de los derechos humanos se basa sobre todo en la psicología. Las amenazas son una moneda común para hacer que los defensores se sientan vulnerables, ansiosos, confusos e impotentes. En última instancia, la represión también pretende resquebrajar las organizaciones y hacer que los defensores pierdan la confianza en sus dirigentes y compañeros. Por ello los defensores tienen que "hilar fino" para conseguir un manejo cuidadoso de las amenazas al tiempo que intentan mantener una adecuada sensación de seguridad en el trabajo diario. Este es también el principal objetivo de este capítulo.

En el Capítulo 2, definimos las amenazas como "la posibilidad de que alguien dañe la integridad física o moral o la propiedad de otra persona a través de una acción intencionada y a menudo violenta". También hablamos sobre **posibles** amenazas (cuando un defensor cercano a tu trabajo es amenazado y sospechas que tu podrías ser el siguiente), y amenazas **declaradas** (recibir una amenaza de muerte, por ejemplo). Ahora estudiaremos cómo manejar las **amenazas declaradas**.

Una amenaza declarada es **una declaración o el indicio de una intención de infligir daño, castigar o herir, normalmente con la intención de lograr algo**. Los defensores de los derechos humanos reciben amenazas debido al impacto que tiene su trabajo, y la mayoría de las amenazas tienen como objetivo o bien paralizar lo que esté haciendo el defensor o bien forzarlo a que haga algo (u otra cosa). Una amenaza siempre tiene un **origen**, es decir, la persona o grupo que se ha visto afectado por la labor del defensor y que articula la amenaza. La amenaza también tiene un **objetivo** que está vinculado al impacto de la labor del defensor, y una **forma de expresión**, es decir, cómo llega al defensor. Las amenazas son complicadas. Podríamos afirmar con cierta ironía que las amenazas son "ecológicas", porque pretenden obtener el mayor resultado con la menor inversión de energía. Una persona que amenaza elige amenazar antes que entrar en acción – una mayor inversión de energía. ¿Por qué? Existen varias razones, y merece la pena enumerarlas:

- La persona que amenaza tiene la capacidad de actuar pero le preocupa en cierto modo el coste político de actuar abiertamente contra un defensor de los derechos humanos. Las amenazas anónimas pueden producirse por la misma razón.

- La persona que amenaza tiene una capacidad limitada de actuación y pretende lograr el mismo objetivo escondiendo su falta de capacidad tras una amenaza. Esta capacidad limitada podría ser sólo temporal debido a otras prioridades, o permanente, pero en ambos casos la situación podría cambiar y conducirle más adelante a llevar a cabo una actuación directa contra el defensor.

Una amenaza es una experiencia personal, y siempre produce un efecto. O, en otras palabras, las amenazas siempre afectan a la gente de una manera u otra. En una ocasión un defensor afirmaba que "las amenazas logran ejercer algún efecto, incluso el simple hecho de que estemos hablando sobre ellas". De hecho, cualquier amenaza puede causar un doble impacto: emocionalmente y en términos de seguridad. Aquí nos concentraremos en la seguridad, pero no deberíamos olvidar el aspecto emocional de toda amenaza.
Sabemos que la amenaza suele estar relacionada con el impacto de nuestro trabajo. Por lo tanto, la amenaza representa un indicador de cómo el trabajo está afectando a otra persona. Vista bajo esta perspectiva una amenaza representa una fuente de información muy valiosa, y debería ser analizada cuidadosamente.

"Lanzar" una amenaza o "representar de hecho" una amenaza

Son muchas las razones por las que algunos individuos amenazan a los defensores de los derechos humanos, y sólo algunos tienen la intención o capacidad de llevar a cabo una acción violenta. Sin embargo, algunos individuos pueden suponer una seria amenaza sin ni tan siquiera llegar a articularla. Esta distinción entre lanzar y representar de hecho una amenaza es importante:

- Algunas de las personas que **lanzan** una amenaza **representan** de hecho al final una amenaza;
- Muchas de las personas que **lanzan** amenazas no **representan** una amenaza;
- Algunas personas que nunca **lanzan** amenazas sí **representan** de hecho una amenaza.

Una amenaza solo será creíble si la persona que la lanza tiene la capacidad de actuar contra ti. La amenaza debe mostrar un mínimo nivel de fuerza o poseer un elemento amenazador pensado para provocar el miedo. La persona que se esconde detrás de una amenaza puede demostrar su capacidad de actuación muy fácilmente, colocando por ejemplo una amenaza escrita en el interior de un coche cerrado, aunque lo hayas dejado aparcado tan sólo unos minutos, o llamándote justo en el momento en el que acabas de llegar a casa, haciéndote saber que estás siendo vigilando. Pueden intentar asustarte añadiendo elementos simbólicos en las amenazas, enviándote por ejemplo una invitación a tu propio funeral o colocando un animal muerto en el portal de tu casa o sobre tu cama. Muchas amenazas representan una combinación de las características mencionadas. Es importante poder distinguirlas, porque algunas de las personas que envían amenazas fingen disponer de la capacidad de actuación utilizando elementos simbólicos o que causan miedo.

Cualquier persona puede poner una amenaza pero no todas suponen una amenaza.

En fin de cuentas, lo que es necesario es saber si la amenaza se puede llevar a cabo. El enfoque será completamente diferente si llegas a la conclusión razonable de que no es probable, que si sospechas que la amenaza podría ser real.

Por ello los dos objetivos principales a la hora de evaluar una amenaza son:

- Obtener toda la información posible de la razón y el origen de la amenaza (ambos estarán relacionados con el impacto de tu trabajo);
- Alcanzar una conclusión racional sobre si la amenaza puede ser llevada a cabo o no.

Cinco pasos para evaluar una amenaza

1 ◆ **Determinar los hechos que rodean la(s) amenaza(s)**. Es importante saber lo que ha ocurrido exactamente. Esto se puede saber mediante entrevistas o interrogando a las personas clave, y en ocasiones a través de informes relevantes.

2 ◆ **Determinar si existe una pauta de amenazas a través del tiempo**. Si se reciben varias amenazas sucesivas (como es el caso habitual) es importante examinar las pautas o patrones que puede haber, tales como los medios utilizados para amenazar, el momento en el que las amenazas aparecen, los símbolos, la información pasada por escrito o verbalmente, etc. No siempre es posible establecer dichos patrones, pero son importantes a la hora de realizar una buena evaluación de la amenaza.

3 ◆ **Determinar el propósito de la amenaza**. En vista de que la amenaza suele tener un claro propósito relacionado con el impacto del trabajo, es posible que siguiendo el hilo conductor de ese impacto se pueda establecer qué pretende conseguirse con la amenaza.

4 ◆ **Determinar quien está detrás de la amenaza**. (Para ello es necesario haber seguido previamente los tres primeros pasos.) Hay que intentar ser lo más específicos posible. Por ejemplo, puede sostenerse que es "el gobierno" quien está amenazando. Pero, teniendo en cuenta que todos los gobiernos son un actor complejo, sería conveniente descubrir qué parte del gobierno está tras las amenazas. Las "fuerzas de seguridad" o los "grupos guerrilleros" son también actores complejos. Hay que recordar que también una amenaza firmada puede ser falsa: ésta podría ser una buena táctica por parte de quien amenaza para evitar los costes políticos y lograr de todas formas el objetivo de provocar miedo a un defensor e intentar impedir que éste siga con su trabajo.

5 ◆ **Llegar a una conclusión racional sobre si la amenaza puede o no llevarse a cabo**. La violencia es condicionante. Nunca se puede estar completamente seguros de si una amenaza se llevará – o no – a cabo.

Los defensores no son "adivinos" y no pueden pretender saber qué va a ocurrir. Sin embargo, se puede llegar a una conclusión racional sobre si una amenaza en concreto podría llevarse a cabo. Puede que no se haya obtenido suficiente información sobre la amenaza a través de los cuatro pasos previos y por lo tanto no se consiga llegar a una conclusión. También puede llegarse a diferentes conclusiones sobre la definición de una amenaza "real". En todo caso, hay que proceder basándose en el peor de los casos.

Por ejemplo:

> Un defensor de los derechos humanos ha recibido varias amenazas de muerte. El grupo analiza las amenazas y llega a dos conclusiones opuestas, ambas basadas en buenos razonamientos. Algunos opinan que la amenaza es completamente falsa, mientras que otros ven algunas señales preocupantes sobre su gravedad. Al final de la reunión, el grupo decide basarse en el peor de los casos, es decir considerar que la amenaza es viable, y tomar las medidas de seguridad necesarias.

Esta evaluación de amenaza pasa de unos hechos sólidos (paso numero 1) a un razonamiento cada vez más especulativo. El segundo paso requiere ya una interpretación de los hechos, lo que nos lleva a los pasos 3, 4 y 5. Existen buenos motivos para seguir el orden de los pasos. Si pasáramos directamente del segundo al cuarto paso, por ejemplo, perderíamos la información más sólida proveniente de los pasos previos.

Mantenimiento y cierre de un caso de amenaza

Una amenaza genera alarma en un grupo de defensores, pero suele ser difícil mantener esta percepción de alarma hasta que ceda la amenaza. Teniendo en cuenta la constante presión externa a la que están sometidos los defensores por su labor, si la organización hiciera sonar las campanas de alarma demasiado a menudo el grupo podría perder interés y bajar la guardia.

Sólo debería activarse la alarma de un grupo cuando existieran evidencias inequívocas y debería destinarse a prevenir un posible ataque. La alarma sirve entonces para motivar a los miembros del grupo a actuar, y exigir que se realicen una serie de actuaciones específicas. Para ser efectiva, una alarma debería sólo estimular la motivación a un nivel moderado: Uno demasiado bajo no activa la reacción de la gente y uno demasiado alto crea una sobrecarga emocional. Si cabe la posibilidad de que la amenaza se prolongue a través del tiempo, es primordial, una vez activada la alarma inicial, dar el necesario seguimiento a la amenaza y reforzar la confianza del grupo cuando sea necesario.
Para finalizar, si la amenaza no se materializa, es necesario proporcionar algún tipo de explicación del por qué, y el grupo debe ser informado cuando la amenaza disminuya o desaparezca por completo.
Un caso de amenaza puede cerrarse cuando se estime que el atacante potencial ya no supone una amenaza. Antes de cerrar un caso, y para asegurarse de estar en lo cierto, hay que comprobar primero si es posible explicar el por qué se puede cerrar de hecho el caso. También hay que preguntarse qué posibles circunstancias podrían empujar al individuo o actor responsable de las amenazas a repetirlas o a llevar a cabo un ataque directo.

Reacción a las amenazas en relación a la seguridad

- Una amenaza puede ser considerada como un incidente de seguridad. Para más información sobre cómo responder a los incidentes de seguridad, véase Capítulo 4.

- Tras la evaluación de unas amenazas declaradas podrías estimar que corres el riesgo de ser atacado. Véase Capítulo 5, sobre la prevención de ataques.

CAPÍTULO 4

Incidentes de seguridad: definición y análisis

Objetivo:

Aprender cómo reconocer y responder a los incidentes de seguridad.

¿Qué es un incidente de seguridad?

Para simplificar, un incidente de seguridad podría definirse como **cualquier hecho o evento que crees que podría afectar a tu seguridad personal o a la seguridad de tu organización**.
Los incidentes de seguridad pueden consistir por ejemplo en ver el mismo vehículo sospechoso aparcado frente a tu oficina o tu casa durante varios días; que el teléfono suene por la noche y no conteste nadie, que alguien esté haciendo preguntas sobre ti en una ciudad o pueblo cercano, un hurto en tu casa, etc.
Pero no todo lo que detectas representa un incidente de seguridad. Por ello hay que **registrarlo**, tomando nota de ello, para luego **analizarlo**, si es posible con compañeros, y poder establecer si realmente podría afectar a tu seguridad. Llegados a este punto podrás **reaccionar** ante el incidente. La secuencia de eventos es la siguiente:

> Detectas algo ⇨ te das cuenta de que podría tratarse de un incidente de seguridad ⇨ lo registras/lo compartes ⇨ lo analizas ⇨ estableces si se trata de un incidente de seguridad ⇨ reaccionas según convenga.

Aunque el tiempo apremie, debes seguir igualmente esta secuencia, sólo que mucho más rápido de lo habitual para evitar retrasos (véase más abajo).

Cómo distinguir los incidentes de seguridad de las amenazas:

Si estás esperando un autobús y la persona de al lado te amenaza a causa de tu trabajo, esto – aparte de ser una amenaza – constituye un incidente de seguridad. Pero si descubres que un coche de policía está vigilando tu oficina desde el otro lado de la calle, o te roban el móvil, éstos son incidentes de seguridad, pero no necesariamente amenazas. Recuerda: las amenazas tienen un objetivo (véase Capítulo 2), y los incidentes simplemente ocurren.

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

Por qué los incidentes de seguridad son tan importantes?

Los incidentes de seguridad son cruciales a la hora de manejar tu seguridad porque **proporcionan una información vital sobre el impacto que tu labor está teniendo, y sobre la posible acción que podría planearse o realizarse en tu contra**. Al mismo tiempo, este tipo de incidentes te permiten cambiar tu conducta o actividades y evitar lugares que podrían ser peligrosos, o más peligrosos de lo normal. Los incidentes de seguridad pueden, por lo tanto, considerarse como indicadores de la situación de seguridad. Si no detectaras estos cambios sería difícil reaccionar apropiadamente y a tiempo para mantenerte seguro.

Por ejemplo; tras detectar ciertos incidentes de seguridad podrías deducir que estás bajo vigilancia: Ahora ya puedes actuar sobre la vigilancia.

Los incidentes de seguridad representan "la unidad mínima" de las medidas de seguridad e indican la resistencia/presión contra tu labor.
¡No permitas que pasen desapercibidos!

¿Cuándo y cómo se detectan los incidentes de seguridad?

Dependerá de lo obvio que sean los incidentes. Si pudieran pasar fácilmente desapercibidos, la capacidad para detectarlos dependerá de la formación y experiencia en la seguridad y del nivel de concienciación sobre ellos.

A mayor concienciación y formación, menor será el número de incidentes que escaparán a tu atención.

A veces los incidentes de seguridad pasan inadvertidos o reparamos en ellos brevemente para luego dejarlo de lado, o a veces reaccionamos exageradamente ante algo que percibimos como un incidente de seguridad.

¿Por qué un incidente de seguridad podría pasar desapercibido?

Un ejemplo:

Un defensor experimenta un incidente de seguridad, pero la organización para la que trabaja no reacciona en absoluto. Esto podría ser debido a que…

- el defensor no es consciente de que ha ocurrido un incidente de seguridad;
- el defensor es consciente de ello pero lo descarta por su poca importancia;
- el defensor no ha informado a la organización (o bien se olvidó, o no creyó que fuera necesario, o decidió no comentarlo porque ocurrió a causa de un error por su parte);
- el defensor lo anotó en el registro de incidentes pero la organización, tras haber realizado una evaluación en conjunto del incidente, no considera necesario reaccionar.

¿Por qué a veces reaccionamos exageradamente a los incidentes de seguridad?

Por ejemplo,

un/a colega podría explicar constantemente historias sobre incidentes de seguridad, pero al examinarlos detalladamente no parecen tener ningún fundamento ni ser merecedores de esta consideración. En este caso en realidad el incidente de seguridad es el hecho de que tu colega tenga un problema que hace que vea incidentes de seguridad inexistentes. Puede que tenga mucho miedo, o que esté estresado/a, y se le debería ofrecer ayuda para resolver el problema.

No olvidemos que es frecuente que los incidentes de seguridad pasen desapercibidos o sean descartados: !Teng mos cuidado con esto!

Cómo hacer frente a los incidentes de seguridad

Para manejar un posible incidente de seguridad se pueden seguir tres pasos básicos:

1 ◆ **Registrarlo**. Todo incidente de seguridad detectado por un defensor debe ser registrado, o bien en una simple libreta personal, o en una disponible para todo el grupo.

2 ◆ **Analizarlo**. Todos los incidentes de seguridad registrados deberían ser debidamente analizados, bien inmediatamente o bien regularmente. Es preferible analizarlos en equipo que individualmente porque así se minimiza el riesgo de pasar algo por alto. Se debería asignar a alguien la responsabilidad de que estos análisis se lleven a cabo.

Se deben también tomar decisiones sobre si mantener o no la confidencialidad de ciertos incidentes (tales como amenazas, por ejemplo). ¿Es ético y razonable esconder información sobre una amenaza a tus colegas y a otra gente con la que trabajas? No existe una única regla aplicable a todas las situaciones, pero a menudo es preferible ser lo más transparente posible a la hora de compartir información y de manejar las preocupaciones, al igual que los miedos.

3 ◆ **Reacciona**. Los incidentes de seguridad ofrecen información sobre el impacto del trabajo, por lo que deberían generar:

- Una reacción al propio incidente;

- **Retroalimentación**, en términos de seguridad, al menos a tres niveles (de lo concreto a lo más general): sobre cómo realizamos nuestro trabajo en el día a día, sobre nuestros **planes** de trabajo, y sobre nuestras **estrategias** más amplias de trabajo.

Ejemplo

de un incidente que proporciona retroalimentación sobre cómo trabajar más seguro en el día a día:

Es la tercera vez que alguien de tu organización tiene problemas al pasar un control policial porque se suelen olvidar los documentos necesarios. Por lo tanto decides crear una lista que deberá ser consultada por todos los trabajadores antes de salir de la ciudad. También podrías decidir cambiar el recorrido de este tipo de viajes.

Ejemplo

de un incidente que proporciona retroalimentación a nivel de planificación de seguridad:

En el mismo control policial, eres retenido durante media hora y eres informado de que tu labor está mal vista. Te dejan caer algunas amenazas disimuladamente. Cuando te diriges al cuartel de policía exigiendo una explicación se repite la misma escena. Organizas una reunión del grupo para revisar tus planes de trabajo, porque parece evidente que es necesario realizar algunos cambios para poder proseguir con la labor. Acto seguido organizas una serie de reuniones con funcionarios del Ministerio de Interior, cambias algunos aspectos de tus planes y organizas reuniones semanales para ir supervisando la situación.

Ejemplo

de un incidente que proporciona retroalimentación sobre las estrategias más amplias de seguridad:

Al poco tiempo de entrar a trabajar como defensor en una nueva zona recibes amenazas de muerte y uno de tus colegas es agredido físicamente. No habías previsto este tipo de oposición a tu labor, ni tampoco lo pronosticaste en tu estrategia global. Por lo tanto, deberás cambiar tu estrategia para intentar generar un consentimiento local hacia tu labor e impedir más ataques y amenazas. Para ello, tal vez debas suspender tu labor por un tiempo, retirarte de la zona y reconsiderar todo el proyecto.

Reaccionar urgentemente a un incidente de seguridad

Existen muchos modos de responder inmediatamente a un incidente de seguridad. Los siguientes pasos han sido formulados en función a cuándo y cómo reaccionar desde el momento en el que se anuncia un incidente de seguridad, mientras está ocurriendo y una vez ha concluido.

Paso 1. Informar sobre el incidente.

- ¿Qué ocurre/ha ocurrido? (intenta centrarte en los hechos compilados).
- ¿Dónde y cuándo ocurrió?
- ¿Quién está implicado? (en caso de que puedas determinarlo)
- ¿La persona o propiedad ha sufrido algún tipo de daño o perjuicio?

Paso 2. Decide cuándo reaccionar. Hay tres posibilidades:

- Una **reacción inmediata** es necesaria cuando hay que atender a personas heridas o frenar un ataque en marcha.

- Una **reacción rápida** (en las próximas horas o incluso días) es necesaria cuando hay que prevenir que surjan nuevos posibles incidentes (el incidente en sí ya pasó).

- **Una acción de seguimiento** (en varios días o semanas o incluso meses): Si la situación se ha estabilizado, tal vez no resulte necesaria una reacción ni inmediata ni rápida, sino de seguimiento. Por lo mismo, también cualquier incidente de seguridad que haya requerido una reacción inmediata o rápida deberá someterse a observación a través de una acción de seguimiento para poder conservar nuestro espacio de trabajo o revisar nuestro contexto de actuación.

Paso 3. Decide cómo reaccionar y cuáles son tus objetivos.

- Si la reacción debe ser inmediata, los objetivos son claros: Atender a los heridos o frenar el ataque.

- Si la reacción debe ser rápida, los objetivos deberán ser establecidos por la persona encargada o el equipo de crisis (o similar) y deberá **centrarse en restaurar la seguridad necesaria para los afectados por el incidente.**

Las acciones/reacciones posteriores se llevarán a cabo siguiendo los canales habituales de la organización en la toma de decisiones, con el objetivo de restaurar un entorno de trabajo seguro, así como de establecer los procedimientos organizativos internos y mejorar las reacciones posteriores ante los incidentes de seguridad.

Toda reacción debe también tener presente la seguridad y protección de otras personas, organizaciones o instituciones con las que mantengamos una relación laboral (y se puedan ver afectados).

Establece tus objetivos antes de empezar a actuar.
La inmediatez de la acción es importante, pero saber por qué llevas a cabo esa acción es más importante todavía. Al establecer de antemano qué pretendes lograr (objetivos),
podrás decidir cómo quieres lograrlo (táctica a seguir).

Por ejemplo,

si un grupo de defensores descubren que uno de sus colegas no ha llegado a su destino en una ciudad según lo planeado, podrían iniciar una reacción llamando al hospital, a sus contactos de otras ONGs, a una Oficina de la ONU cercana y a la policía. Pero antes de iniciar estas llamadas, es muy importante determinar qué se pretende conseguir y qué se va a decir. En caso contrario, podrían generar una alarma innecesaria (imaginemos que el defensor se hubiera retrasado porque perdió el autobús y olvidó llamar a la oficina) o una reacción opuesta a la pretendida.

CAPÍTULO 5

Prevenir y reaccionar a los ataques

Objetivo:

Evaluar la posibilidad de que se lleven a cabo diferentes tipos de ataque.

Prevenir los posibles ataques directos contra defensores.

Llevar a cabo una contra-vigilancia.

Ataques contra los defensores de los derechos humanos

Los ataques contra defensores son producto de al menos tres factores que interactúan entre sí:

1 ◆ **El individuo que lleva a cabo una acción violenta.** Los ataques contra los defensores suelen ser el producto de procesos de pensamiento y de conductas que podemos descifrar para aprender de ellos, aunque sean ilegítimos.

2 ◆ **Antecedentes y factores desencadenantes que llevan al atacante a considerar la violencia como una opción.** La mayoría de los individuos que atacan a los defensores consideran la acción de atacar como una forma de "lograr un objetivo" o de "resolver un problema".

3 ◆ **Un contexto** y circunstancias que facilitan la violencia, o sea, que permiten que se lleve a cabo o que no la detienen.

¿Quién representa, entonces, un peligro para los defensores?

Por lo general, cualquier individuo (o grupo) que piense que atacar a un defensor es una forma tentadora, aceptable, o potencialmente efectiva de lograr un objetivo puede ser considerado un atacante potencial. La amenaza aumenta si quien considera el ataque también posee, o puede desarrollar, la capacidad de atacar a un defensor.

Algunos ataques vienen precedidos por amenazas, y otros no. Sin embargo, a menudo los individuos que planean un ataque violento denotan sus intenciones en su conducta, puesto que necesitan averiguar el mejor momento para atacar, planear cómo alcanzar el blanco, y cómo escapar.

La amenaza de un ataque puede disminuir si.
surgen cambios en la capacidad potencial del atacante para organizar un ataque,
si cambia su actitud de cara a lo aceptable que es un ataque, o
si aumentan las probabilidades que tiene de ser capturado/a y castigado/a.

Por lo tanto es fundamental detectar y analizar cualquier señal que indique un posible ataque. Esto requiere:

- Determinar la posibilidad de que se lleve a cabo una amenaza (véase capítulo 3);
- Identificar y analizar los incidentes de seguridad (véase capítulo 4).

Los incidentes de seguridad que denotan la vigilancia de los defensores o de su lugar de trabajo están dirigidos a obtener información. Esta información no siempre se recoge con la intención de ser utilizada en un ataque, pero es importante determinar esto (véase Capítulo 4).
El objetivo de vigilar a los trabajadores o las oficinas es el de obtener información que pueda destinarse a varios fines como:

- Establecer qué actividades se están llevando a cabo, cuándo y con/por quien;
- Utilizar esa información más adelante para atacar a personas u organizaciones;
- Obtener la información necesaria para llevar a cabo un ataque;
- Recopilar información para hacer una acusación legal u otro tipo de coacción (sin violencia directa);
- Intimidarnos o intimidar a colaboradores o a otras personas con las que trabajemos, o presionarnos para que dejemos de ver a esas personas o de hacer algo ("vigilancia demostrativa").

Es importante recordar que la vigilancia suele ser necesaria para poder llevar a cabo un ataque, pero que no constituye por sí misma un ataque. Además, no todas las vigilancias implican un ataque posterior. Sin embargo, por otra parte, en algunas ocasiones un individuo puede improvisar un ataque cuando de repente ve una oportunidad para ello, aunque incluso en estos casos suele haber un mínimo de preparación previa.
No hay mucha información disponible que pueda ayudarte a reconocer la fase de preparación de un ataque. La ausencia de estudios sobre este tema contrasta enormemente con el gran número de ataques contra defensores. Sin embargo, los estudios existentes aportan interesantes revelaciones[6].

[6] Claudia Samayoa y Jose Cruz (Guatemala) y Jaime Prieto (Colombia) han realizado unos interesantes estudios sobre ataques contra defensores de los derechos humanos. Mahony y Eguren (1997) también realizaron un análisis de dichos ataques.

- Atacar a un defensor no es fácil y requiere disponer de recursos. La vigilancia es necesaria a la hora de establecer los movimientos de un individuo y el mejor momento para atacar. Dar en el blanco y escapar de forma efectiva y rápida es también primordial (sin embargo, si el entorno es altamente favorable para el atacante le resultará más sencillo llevar a cabo los ataques).

- Quien ataca a los defensores suele mostrar cierto grado de consistencia. La mayoría de los ataques van dirigidos a defensores muy implicados en temas que afectan a los atacantes. Es decir, los ataques no suelen ser casuales o sin objetivo, sino que responden a los intereses de los atacantes.

- Los factores geográficos son importantes. Por lo general, los ataques a defensores en zonas rurales no se divulgan tanto y en consecuencia provocan menos reacciones en la aplicación de la ley y a nivel político que los de las zonas urbanas. Los ataques en zonas urbanas contra oficinas de ONGs o contra organizaciones destacadas generan una reacción mucho mayor.

- Antes de atacar se deben tomar ciertas decisiones y optar por diferentes posibilidades. Los individuos que pretenden atacar a una organización de defensores deben decidir si atacar a los líderes o a los miembros de la base, o escoger entre un único golpe (contra una persona clave e importante lo que a su vez genera un mayor coste político) o una serie de ataques (que afecten a los miembros de la organización). Los pocos estudios realizados al respecto sugieren que suelen aplicarse ambas estrategias.

Establecer la probabilidad de un ataque

Para poder averiguar la probabilidad de que un ataque se lleve a cabo debemos analizar los factores relevantes. Para poder determinar cuáles son estos factores, debemos distinguir los diferentes tipos de ataques, es decir, los ataques directos (targeting), la delincuencia común y los ataques indirectos (estar en el lugar equivocado en el momento equivocado), haciendo uso de los tres cuadros de las páginas siguientes[7].

[7] Esta clasificación de ataques incluye las mismas categorías que en las amenazas: Véase el capítulo sobre amenazas para una aclaración.

Cuadro 1: Determinar el grado de amenaza de un ataque directo (targeting)

(**AP** equivale a atacantes potenciales)

PROBABILIDAD DE ATAQUES DIRECTOS (TARGETING)			
FACTORES	PROBABILIDAD BAJA	PROBABILIDAD MEDIA	PROBABILIDAD ALTA
Capacidad de ataque	Los AP poseen una capacidad limitada para actuar en las zonas donde trabajamos	Los AP poseen capacidad operacional cerca de las zonas donde trabajamos	Las zonas donde trabajamos están bajo control de los AP
Móvil financiero	Los AP no necesitan nuestro material o dinero para sus actividades	Interés en nuestro material, dinero u otras prácticas de ganancia económica (el secuestro, por ej.)	Los AP tienen una necesidad manifiesta de material o dinero
Móvil político o militar	Ninguno – nuestro trabajo no tiene nada que ver con sus objetivos	Interés parcial – nuestra labor limita sus objetivos políticos o militares	Nuestra labor obstaculiza claramente sus objetivos, beneficia a sus oponentes, etc.
Antecedentes de ataques previos	Ninguno o excepcional	Casos ocasionales	Muchos casos previos
Actitudes o intenciones	Actitud favorable o indiferente	Indiferente. Amenazas ocasionales Avisos frecuentes.	Agresiva, con amenazas claras y vigentes
Capacidad de las fuerzas de seguridad de impedir ataques	Existente	Baja	Ninguna, o las fuerzas de seguridad colaboran con los AP (o son los AP)
Nuestro grado de influencia política contra los AP	Buena	Media o baja	Limitada (según las circunstancias) o ninguna.

Ejemplo

de una evaluación del grado de probabilidad de un ataque directo (targeting):

Los AP controlan las zonas donde trabajamos, pero no existe ningún móvil económico para atacarnos. Nuestra labor sólo limita sus objetivos políticos y militares parcialmente, y no existen precedentes de ataques similares en la ciudad. Su actitud es indiferente, y es evidente que no quieren atraer ninguna atención nacional o internacional ni presión alguna atacándote.

En este caso consideraríamos el grado de probabilidad de ataque directo como bajo o medio.

Cuadro 2: Determinar el grado de probabilidad de un crimen por delincuencia común

(**C** equivale a criminal)

PROBABILIDAD DE ATAQUE POR DELINCUENCIA COMÚN			
FACTORES	PROBABILIDAD BAJA	PROBABILIDAD MEDIA	PROBABILIDAD ALTA
MOVILIDAD Y UBICACIÓN DE LOS C	Los C suelen permanecer en sus propias zonas, diferentes a nuestras zonas de trabajo	Los C suelen acceder a otras zonas por la noche (u operan cerca de donde trabajamos)	Los C actúan en cualquier parte, tanto de día como de noche.
AGRESIVIDAD DE LOS C	Los C evitan enfrentamientos (cometen crímenes mayoritariamente donde no hay la presencia de defensores o testigos)	Los C cometen crímenes en la calle (pero no en oficinas con personal)	Los C roban abiertamente en la calle y entran en los lugares cerrados
ACCESO A/USO DE ARMAS	Desarmados, o uso de armas no letales	Armas rudimentarias, inclusive machetes	Armas de fuego, a veces de gran capacidad
TAMAÑO Y ORGANIZACIÓN	Operan individualmente o en parejas	2-4 personas operan juntas	Operan en grupos
RESPUESTA Y DISUASIÓN POLICIAL	Respuesta rápida, con capacidad de disuasión	Respuesta lenta, poco éxito capturando criminales en acción	La policía no suele responder ni con la más mínima efectividad
FORMACIÓN Y PROFESIONALIDAD DE LAS POLICÍA	Bien formadas y profesionales (pueden tener falta de recursos)	Formación regular, salario bajo, recursos limitados	La policía es o inexistente o corrupta (colabora con los delincuentes)
SITUACIÓN GENERAL DE SEGURIDAD	La situación es segura o relativamente segura	Falta de seguridad	No se observan los derechos, impunidad absoluta

Ejemplo

de una evaluación del grado de probabilidad de crimen:

En esta ciudad, los criminales operan en varias zonas, en parejas o en pequeños grupos, a veces durante el día. Suelen ser agresivos y suelen llevar armas. La policía responde, pero lenta e ineficazmente, con formación poco profesional y con falta de recursos. Sin embargo, la jefatura de policía es muy disciplinada. Existe una falta general de seguridad, y si lo aplicamos a los barrios marginales de la ciudad, el grado de probabilidad de crimen está en su punto más álgido ya que todos los indicadores marcan un nivel elevado.

La probabilidad de un ataque criminal en el centro de una ciudad como ésta es de un grado alto a medio.

Cuadro 3: Determinar la posibilidad de un ataque indirecto

(**AP** equivale a atacantes potenciales)

PROBABILIDAD DE UN ATAQUE INDIRECTO			
FACTORES	PROBABILIDAD BAJA	PROBABILIDAD MEDIA	PROBABILIDAD ALTA
Nuestro conocimiento de las zonas en combate	Bueno	Aproximado	Tenemos muy poco conocimiento sobre la ubicación de las zonas de combate
Proximidad a las zonas de combate	Nuestro trabajo está lejos de estas zonas	Nuestro trabajo está cerca de estas zonas y ocasionalmente se accede a ellas	Nuestro trabajo se lleva a cabo en las zonas de combate
Movilidad de las zonas de combate	Las zonas de conflicto son estáticas o varían de forma lenta y verificable	Varían bastante a menudo	Varían continuamente, lo que les hace impredecibles
Nuestro conocimiento de la ubicación de zonas minadas	Poseemos un buen conocimiento o no existen zonas minadas	Conocimiento aproximado	Desconocidas
Proximidad de nuestro lugar de trabajo a las zonas minadas	El trabajo se lleva a cabo lejos de estas zonas o son inexistentes	Trabajamos cerca de estas zonas.	Nuestro trabajo se lleva a cabo en áreas en que hay zonas minadas
Tácticas de combate y armas utilizadas	Discriminadas	Discriminadas, con uso ocasional de artillería, emboscadas y francotiradores	Indiscriminadas: bombardeo, artillería pesada, ataques terroristas o ataques con bombas

Ejemplo

de una evaluación de la probabilidad ataques indirectos:

En esta zona, estás familiarizado con las zonas de combate, que varían de forma lenta y previsible. Trabajas cerca de las zonas donde tienen lugar los enfrentamientos y ocasionalmente visitas o te quedas en las zonas de combate. No estás cerca de zonas minadas. Las tácticas de combate usadas son discriminadas y por lo tanto no suelen afectar a los civiles.

Trabajar en esta zona representa una probabilidad baja de un ataque indirecto.

Prevenir un posible ataque directo

Ahora ya sabemos que una amenaza puede disminuir si surgen cambios en la capacidad potencial del atacante para organizar un ataque, en su actitud de cara a lo aceptable que resulta un ataque o en las probabilidades que tiene de ser capturado y castigado.

Por lo tanto, para prevenir un ataque es necesario:

- Persuadir a un atacante potencial de que un ataque conlleva costes y consecuencias inaceptables;
- Hacer que un ataque sea menos factible de hecho.

Este planteamiento para prevenir ataques es paralelo al análisis del Capítulo 2, que señalaba que el riesgo depende de las vulnerabilidades y capacidades del defensor. También sostenía que para poder protegerse y poder reducir el riesgo, es necesario actuar contra la amenaza, reducir vulnerabilidades y ampliar capacidades.

Cuadro 4: Prevenir un ataque directo: resultados esperables de las actuaciones de protección

PREVENIR UN ATAQUE DIRECTO: RESULTADOS ESPERABLES DE LAS ACTUACIONES DE PROTECCIÓN	
1 **Cambios en el comportamiento del atacante:** disuadir a los atacantes mediente el incremento en el coste potencial de un ataque. →	**Confrontar** y **reducir las amenazas** (actuando directamente contra el origen de la amenaza, o contra cualquier acción desde ese origen)
2 **Cambios en el cumplimiento de la Declaración de la ONU sobre los defensores por parte de las autoridades responsables**[3]: disuadir a los atacantes aumentando la probabilidad de actuación por parte de las autoridades para proteger a los defensores o castigar a los autores de un ataque. →	
3 **Reducir la posibilidad de ataque:** Reducir la exposición del defensor, mejorar su entorno de trabajo, manejar el estrés y el miedo adecuadamente, desarrollar planes de seguridad, etc. →	Reducir **vulnerabilidades**, aumentar **capacidades**

[3] Véase Capítulo 1. Por ejemplo, una vez el defensor haya denunciado las amenazas, o bien el fiscal o la policía o algún otro organismo investigará qué ha ocurrido y esta investigación conllevará una acción contra aquéllos que han estado amenazando al defensor. Bueno, al menos éste podría ser el objetivo de una reacción para prevenir un ataque.

Cuando se es objeto de una amenaza y se quiere reducir el riesgo asociado a ésta, es importante actuar – no sólo contra la propia amenaza, sino que también sobre las **vulnerabilidades** y **capacidades** más **cercanamente vinculadas** a la amenaza. Cuando estamos sometidos a grandes presiones y queremos actuar con la mayor rapidez, a menudo actuamos sobre las vulnerabilidades de fácil solución o las más accesibles, en vez de hacerlo sobre las más relevantes para la amenaza en cuestión.

Ten cuidado: Si el riesgo de ataque es elevado (es decir, si la amenaza es inminente, y tienes varias vulnerabilidades y pocas capacidades), no tiene sentido centrarse en las vulnerabilidades o capacidades para reducir el riesgo, porque cambiarlas requiere tiempo. Si el riesgo es muy elevado (cuando un ataque directo y severo es inminente) tan sólo es posible evitarlo de tres modos:

a ◆ Confrontando la amenaza con inmediatez y efectividad, si se sabe que puedes lograr un resultado inmediato y específico que prevendrá el ataque. (Normalmente es muy difícil estar seguro de que se obtendrá un resultado inmediato y efectivo, porque las reacciones requieren su tiempo, y el tiempo es muy valioso en estos casos).

b ◆ Procurar no exponerse en absoluto (por ejemplo, escondiéndose o abandonando la zona temporalmente[4]).

c ◆ Otra opción sería la de solicitar una protección armada, asumiendo que haya una disponible (inmediata), y que esto podría disuadir al presunto atacante y no incrementa la situación de peligro del defensor a medio o largo plazo (en la práctica, es muy difícil que se cumplan estos tres requerimientos en la protección armada). En ocasiones, tras una presión nacional o internacional, el Gobierno decide ofrecer escoltas armados al defensor; en estos casos, el aceptar o rechazar la escolta podría determinar el grado de responsabilidad estatal en la seguridad de los defensores, pero aunque el defensor no acepte los escoltas armados un Gobierno no puede bajo ningún concepto declararse exento de sus obligaciones. Las empresas privadas de seguridad pueden representar un mayor riesgo si están vinculadas informalmente a las fuerzas de Estado (véase Capítulo 9). En lo referente a la posesión de armas por parte de los defensores debemos señalar que éstas suelen resultar inefectivas en un ataque organizado, y además pueden colocar a los defensores en una situación de vulnerabilidad puesto que el Gobierno podría utilizarlo como justificación para atacarles bajo pretexto de lucha antiterrorista o insurgencia.

Resulta mucho más fácil manejar las situaciones de amenaza que pueden conducir a un ataque cuando otros actores relevantes se implican y trabajan conjuntamente, por ejemplo, con un sistema judicial operativo; redes de apoyo (nacionales e internacionales) que puedan presionar a las autoridades responsables; redes sociales (dentro de las organizaciones o entre ellas), redes personales y familiares, ONU/fuerzas internacionales de pacificación, etc.

Vigilancia y contra-vigilancia

La contra-vigilancia puede ayudarte a determinar si estás sometido a vigilancia. Es difícil descubrir si tus sistemas de comunicación han sido interceptados, y por esta razón deberías presumir siempre que sí lo están[5]. Sin embargo, es posible determinar si alguien vigila tus oficinas y tus movimientos.

[4] Si bien hay situaciones en las que viajar representa una situación de riesgo mayor.
[5] Para más información sobre cómo asegurar las comunicaciones véase el Capítulo 13

¿Quién podría estar vigilándote?

Personas que suelen estar ubicadas en tu zona, como conserjes o porteros de edificios, vendedores que trabajan cerca de la entrada del edificio, gente en vehículos cercanos, visitas, etc., podrían estar vigilando tus movimientos. Hay personas que espían por dinero, o porque les presionan para que lo hagan; por sus inclinaciones, o debido a la combinación de estos factores. Los responsables de la vigilancia pueden también colocar colaboradores miembros de su organización en tu zona.

También puedes ser vigilado desde una cierta distancia. Normalmente son miembros de una organización que suelen practicar la táctica de intentar vigilar sin ser vistos. Esto requiere mantener una cierta distancia, alternarse con otras personas por turnos y observarte desde diferentes lugares, utilizando diferentes vehículos, etc.

Cómo averiguar si estás bajo vigilancia

Puedes averiguar si estás bajo vigilancia observando a aquéllos que podrían estar vigilándote, y adoptando las siguientes normas (sin, evidentemente, caer en la paranoia):

- Si sospechas que alguien podría estar vigilándote, deberías prestar atención a la actividad de la gente de tu zona y a los cambios en su conducta como, por ejemplo, alguien que empieza a hacer preguntas sobre tus actividades. Recuerda que pueden ser tanto hombres como mujeres, al igual que ancianos o gente muy joven.

- Si sospechas que te están siguiendo, podrías poner en marcha una medida de contra-vigilancia que implique a una tercera persona de confianza, desconocida para aquéllos que podrían estar vigilándote. La tercera persona podría observar, por adelantado y desde una buena distancia, los movimientos que se producen cuando llegas, te vas o te diriges a algún lugar. La persona que te esté vigilando probablemente lo realice desde un lugar desde donde te pueda localizar fácilmente, incluyendo tu casa, la oficina y los lugares donde sueles trabajar.

Por ejemplo

Antes de llegar a casa podrías pedirle a un miembro de tu familia o a un vecino de confianza que tome una posición cercana (por ej. cambiando una rueda del coche), para comprobar si alguien está a la espera de tu llegada. Podrías hacer lo mismo cuando salgas de la oficina a pie. Si utilizas un vehículo privado, deberás dejar que salga otro coche después del tuyo para darle tiempo al presunto observador a que se aproxime.

La ventaja de la contra-vigilancia es que, al menos inicialmente, la persona que te observa no es consciente de que está siendo vigilada. Por lo tanto deberías dejar claro a toda persona implicada en la contravigilancia que no es recomendable enfrentarse a la persona que te está observando. De esta forma sabrían que eres consciente de sus actividades, y esto podría desencadenar una reacción violenta. Es importante ser extremadamente precavido y mantener una distancia cuando sospeches que alguien te está vigilando. Una vez detectada la vigilancia, puedes poner en marcha la acción recomendada en este manual (véase Capítulo 9).

La mayoría de nuestros consejos sobre la contra-vigilancia hacen referencia de forma casi exclusiva a las zonas urbanas y semi-urbanas. En las zonas rurales la situación es muy diferente, porque los defensores y las comunidades que viven en estas zonas están más acostumbrados a detectar la presencia de extraños. Por lo tanto la persona que quiera vigilarte en una zona rural tendrá más dificultades para aproximarse a los habitantes - a no ser que la población local sea muy hostil a tu labor.

Nota: Existen situaciones en las que podría resultarte ventajoso relacionarte con las fuerzas de seguridad que te controlan – a veces la vigilancia no es tan secreta, y se exterioriza con el objetivo de intimidar. En algunas ocasiones los defensores establecen relaciones con personas de las fuerzas de seguridad para que les avisen cuando se planee vigilarles o incluso llevar a cabo una acción contra ellos.

Cuándo comprobar si estás siendo vigilado.

Es recomendable comprobar si estás sometido a vigilancia cuando tengas alguna razón para sospecharlo – por ejemplo, por incidentes de seguridad que podrían estar relacionados con la vigilancia. Si tu labor de derechos humanos conlleva un cierto riesgo, es aconsejable organizar de vez en cuando una simple acción de contra-vigilancia, por si acaso.

También debes pensar en el riesgo que representas para los demás cuando estás siendo vigilado – puede suponer un mayor riesgo para un testigo o un familiar de una víctima que visites que para ti mismo. Piensa sobre dónde sería más seguro verles. Tal vez necesites avisarles de que tus movimientos están siendo vigilados.

Reaccionar a los ataques

No existe una única norma aplicable a todos los ataques contra defensores. Los ataques también son incidentes de seguridad, y encontrarás las pautas de cómo reaccionar a los incidentes de seguridad en el Capítulo 4.

En todo tipo de ataque hay dos puntos primordiales a recordar:

- Piensa siempre en la seguridad – tanto **durante** el ataque como **después**. (Si estás siendo atacado y tienes dos posibles alternativas, ¡opta por la más segura!)

- Tras un ataque, deberás recuperarte física y psicológicamente, actuar para solventar la situación, e intentar restaurar un entorno de trabajo seguro para ti y tu organización. Es importante que retengas la mayor información posible sobre el ataque: Qué ocurrió, quién/cuántas personas estaban implicadas, número de matrícula de los vehículos, descripciones, etc. Todo esto podría resultar útil para documentar el caso, y debería ser anotado cuanto antes. Conserva copias de todos los documentos que presentes a las autoridades para documentar el caso.

CAPÍTULO 6

Preparación de una estrategia y un plan de seguridad

Objetivo:

Aprender a diseñar una estrategia de seguridad.

Aprender a trazar un plan de seguridad.

Los defensores de los derechos humanos que trabajan en entornos hostiles

Son muchos los motivos por los que los defensores deben trabajar muy a menudo en entornos hostiles. La mayoría de los casos son debidos al posible enfrentamiento que suscita su labor contra actores poderosos que violan las normas internacionales de los derechos humanos, ya sean autoridades gubernamentales o estatales, fuerzas de seguridad, grupos armados de oposición o bandas armadas privadas. Estos actores pueden tomar todo tipo de represalias para intentar que los defensores cesen en su labor, desde una represión sutil con ataques contra la libertad de expresión hasta amenazas declaradas y ataques directos. El grado de tolerancia del actor puede depender de la labor del defensor- algunas actividades podrían considerarse como aceptables, otras no.

Llegados a este punto deberíamos realizar dos reflexiones importantes: En muchos casos, sólo son hostiles al defensor ciertos componentes **integrantes** de los actores complejos. Por ejemplo, algunos de los componentes integrantes de un gobierno pueden estar relativamente preocupados en la protección de los defensores, mientras que otros componentes quieren atacarlos. Los defensores pueden también experimentar una mayor hostilidad durante momentos de agitación política, tales como las elecciones u otros eventos políticos.

El espacio socio-político de actuación de los defensores

El presente manual está dirigido a la protección y seguridad de los defensores de los derechos humanos que trabajan en entornos laborales hostiles y en medidas para mejorar dicha seguridad. Existen también otras acciones a nivel socio-político que pueden ser aplicadas para mejorar el respeto a los derechos humanos y el entorno de los defensores de los derechos humanos. Las campañas y actividades de promoción de los defensores suelen estar encaminadas a asegurar una aceptación más amplia de los derechos humanos en la sociedad y obtener acciones más efectivas por parte de las autoridades para asegurar la protección de los derechos

humanos. Si bien no solemos relacionar este tipo de actividades con la seguridad, cuando éstas son efectivas pueden causar un impacto positivo en la protección del **espacio socio-político de actuación** de los defensores.

Este espacio socio-político de actuación podría definirse como la **variedad de posibles acciones que puede realizar el defensor exponiéndose a un riesgo personal aceptable**. En otras palabras, el defensor contempla "una amplia variedad de posibles acciones políticas y asocia cada acción a un coste específico o a un conjunto de consecuencias". El defensor considera alguna de estas consecuencias "aceptables y otras inaceptables, definiendo así los límites de un espacio político específico"[1].

Por ejemplo, un grupo de defensores podría estar defendiendo un caso sobre derechos humanos cuando uno de los miembros recibe una amenaza de muerte. Si consideran que tienen suficiente espacio sociopolítico, tal vez opten por hacer pública la amenaza, y continuar más tarde con el caso. Pero si consideran que su espacio político es limitado, quizá decidan que la divulgación de la amenaza representa unos costes inaceptables. Tal vez incluso opten por dejar el caso por un tiempo y mejorar entretanto sus capacidades de seguridad.

La noción del riesgo "aceptable" puede cambiar con el tiempo y varía enormemente para los diferentes individuos u organizaciones. Para algunos, el riesgo más insoportable sería el de la tortura o la muerte de un familiar. Algunos defensores opinan que el encarcelamiento es un riesgo aceptable, siempre y cuando contribuya a lograr los objetivos. Otros alcanzan el límite cuando reciben la primera amenaza.

Este espacio político de actuación, no sólo viene definido de forma subjetiva por los defensores, sino que además es muy sensible a los cambios del entorno político nacional que le rodea. Por lo tanto debemos considerarlo como un espacio relativo y cambiante.

La seguridad y el espacio de actuación del defensor

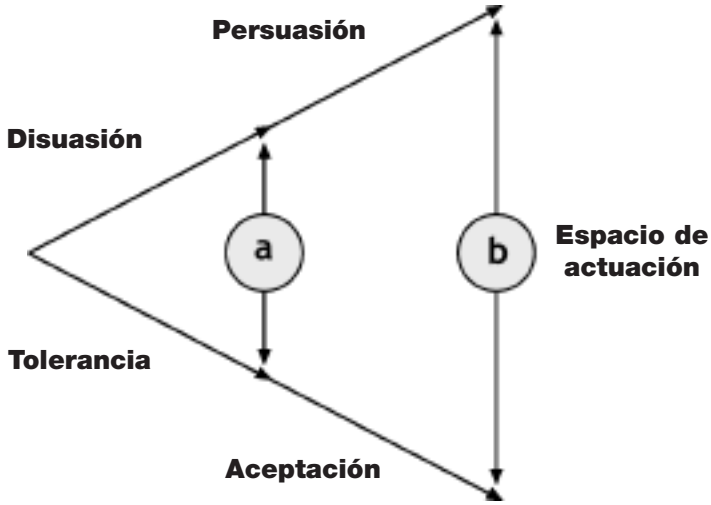
Podemos resumir todas las estrategias de seguridad en unas pocos palabras: expandir el espacio de actuación y mantenerlo así. Si hablamos en términos estrictos de seguridad, el espacio de trabajo del defensor requiere por lo menos un grado mínimo de tolerancia por parte de los actores principales de la zona – especialmente por parte de las autoridades políticas y militares y de los grupos armados a quienes pudiera afectar la labor de los defensores y que podrían actuar en su contra. Esta tolerancia puede ser **explícita**, como un permiso formal de las autoridades, **o implícito**, como por ejemplo en el caso de los grupos armados. La tolerancia será más alta si el actor ve que la labor del defensor le puede aportar algún beneficio, y será más baja si el actor detecta costes relacionados con la labor del defensor. En este caso, su grado de tolerancia dependerá de los costes políticos que representará atacar a los defensores. Todo esto es relevante sobre todo en los conflictos armados donde los defensores se enfrentan a más de un actor armado. Un actor parte en el conflicto podría considerar la labor de los defensores ventajosa para su oponente. La aceptación manifiesta de un actor podría por lo tanto motivar la hostilidad de su oponente.

El espacio de actuación de los defensores puede representarse en dos ejes:

- un eje representa el grado de tolerancia o aceptación del actor hacia la labor del defensor, basándose en el impacto que pueda causar dicha labor a los objetivos o intereses estratégicos del actor (el continuo "tolerancia-aceptación")

[1] Esta definición así como otras partes fundamentales de este concepto han sido tomadas de Mahony y Eguren (1997), p. 93. También desarrollaron un modelo de espacio político que integra el espacio laboral de los defensores con el acompañamiento protector de los defensores.

- otro eje representa en qué medida se puede disuadir los ataques basándose en los costes políticos de un ataque, que aumenta acorde con la probabilidad de disuadir al actor con argumentos racionales/morales o incluso con las ventajas políticas que obtienen al no atacar ni violar los derechos humanos (el continuo "disuasión-persuasión").



Con el tiempo se puede lograr una expansión del espacio de actuación. Para conseguir, por medio de una estrategia de persuasión, la aceptación de la labor del defensor, es necesario tener en cuenta las necesidades de la población, la imagen, procedimientos y la integración del defensor, etc., representados en el espacio "b". Pero en las zonas de conflicto armado el espacio suele limitarse únicamente a la tolerancia de los actores armados, que vendrá parcialmente determinada por los costes que supone atacar a los defensores (disuasión), reduciendo así el espacio a "a".

Expandir el espacio de actuación mediante el aumento de la tolerancia y aceptación.

La labor de los defensores podría afectar a los objetivos o intereses estratégicos de alguien que no está muy interesado en los derechos humanos, lo que causaría un entorno hostil para los defensores. Para ganar la aceptación, o por lo menos la tolerancia hacia la labor de los defensores, es importante reducir la confrontación en lo posible. Algunas sugerencias sobre cómo hacerlo:

- **Proveer información y formación sobre la naturaleza y legitimidad del trabajo de los defensores**. Los funcionarios gubernamentales y otros actores podrían estar más inclinados a cooperar si conocieran y comprendieran el trabajo y las razones por las que se lleva a cabo. No basta con mantener informados a los altos cargos, porque el trabajo diario de los defensores suele abarcar una gran variedad de funcionarios pertenecientes a diversos órganos gubernamentales. Hay que realizar un continuo esfuerzo para informar y formar a los funcionarios de todos los niveles.

- **Aclarar los objetivos del trabajo de los defensores**. En todos los conflictos es recomendable aclarar y limitar el alcance y los objetivos del trabajo. De esta forma se reducirán los malentendidos o enfrentamientos innecesarios que impiden que los defensores logren sus objetivos.

- **Limitar los objetivos de trabajo para ajustarse al espacio sociopolítico de actuación existente**. Si la labor de los defensores afecta a los intereses estratégicos de un actor armado en concreto, éste podría reaccionar con una mayor violencia y una menor consideración por su imagen. Ciertos tipos de trabajo hace a los defensores más vulnerables que otros, así que hay que asegurarse de que los objetivos se ajustan lo máximo posible a la valoración de riesgo y a las capacidades en protección.

- **Conceder un espacio en las estrategias para "salvar la imagen"**. Si hay que enfrentarse a un actor poderoso puede ser útil buscar la manera de que el actor pueda "guardar su imagen" cuando finalmente tome medidas sobre la situación de derechos humanos.

- **Establecer alianzas** de forma amplia, con tantos sectores sociales como sea posible.

- **Buscar un punto intermedio** entre la transparencia en el trabajo, que demuestre que los defensores no tienen nada que esconder, y la protección de información que pudiera comprometer el trabajo o la seguridad.

- **Finalmente**, recordemos que la legitimidad y la calidad del trabajo son condiciones imprescindibles para mantener el espacio de actuación abierto, pero pueden ser insuficientes, y tal vez también sea necesario disuadir a los atacantes potenciales (véase más abajo).

Expandir el espacio de actuación mediante la disuasión y la persuasión

Los defensores de los derechos humanos que trabajan en entornos hostiles deberían ser capaces de generar suficientes costes políticos como para disuadir a un agresor de intentar un ataque: Es lo que denominamos **disuasión**.

Resulta práctico saber distinguir entre la disuasión "general" y la disuasión "inmediata". La **disuasión general** consiste en el efecto combinado de todos los esfuerzos nacionales e internacionales para proteger a los defensores, es decir, todo lo que contribuya a crear una convicción general de que los contra los defensores tienen consecuencias negativas. Para ello se puede recurrir a amplias campañas mediáticas o a la formación e información sobre la protección de los defensores. Por otra parte, la disuasión inmediata envía un mensaje concreto a un agresor determinado para disuadir de los ataques de un blanco específico. La **disuasión inmediata** es necesaria cuando la disuasión general falla o resulta insuficiente, y cuando los esfuerzos de protección se centran en casos específicos.

La **persuasión** es un concepto más amplio. Podría definirse como el resultado de los actos que inducen a un oponente a no llevar a cabo una acción hostil previamente considerada. El argumento racional, el reclamo moral, un aumento de cooperación, una mejora en la comprensión humana, la distracción, la adopción de políticas no ofensivas y y la prevención, todas podrían ser utilizadas para lograr la persuasión. Los defensores utilizan todas estas tácticas a nivel nacional o internacional en diferentes situaciones. Evidentemente, los defensores no pueden utilizar las "amenazas" Directas: La estrategia se basa sobre todo en recordar a los demás que las decisiones que tomen **podrían** acarrear una serie de consecuencias.

Poniendo la disuasión en marcha

Para poder disuadir de ataques, es necesario cumplir con una serie de requisitos:

1 ◆ **Los defensores deben especificar y comunicar claramente al agresor qué tipo de acciones son inaceptables**. La disuasión no funciona si el agresor desconoce las acciones que provocarán una respuesta.

2 ◆ **La organización de los defensores debe expresar su compromiso en disuadir contra la agresión de forma que el agresor sea consciente de ello**. La organización debe también establecer una estrategia para conseguir dicha disuasión.

3 ◆ **La organización de los defensores deber ser capaz de llevar a cabo la estrategia de disuasión, y asegurarse de que el agresor es consciente de ello**. Si una amenaza de movilización nacional o internacional no es creíble, no existe ninguna razón para esperar que tenga un efecto protector.

4 ◆ **Los defensores deben saber quién es el agresor**. Los grupos de ataque suelen trabajar en la oscuridad de la noche y raramente asumen la responsabilidad. Por lo tanto, a menudo nos vemos obligados a analizar quién podría salir beneficiado del ataque. En caso de sospecha de una "responsabilidad estatal", aunque ésta sea correcta, deberá ir acompañada de información más específica sobre qué fracción estatal se esconde detrás del ataque para poder así mejorar la efectividad de una reacción nacional o internacional.

5 ◆ **El agresor debe haber considerado seriamente el ataque y después haber decidido no hacerlo porque los costes** – gracias al compromiso de los defensores – podrían ser mayores que los beneficios.

Es difícil que los defensores logren persuadir a un agresor que no se ve en absoluto afectado por los argumentos de disuasión: Esto sucede cuando la comunidad internacional puede castigar a los gobiernos, pero éstos no pueden castigar al actor violador de los derechos humanos. Por ejemplo, los ejércitos privados o sicarios podrían estar fuera del alcance del gobierno o no compartir sus intereses. En estos casos, al agresor podría incluso beneficiarle atacar a los defensores de los derechos humanos, porque los ataques situarían al gobierno en una posición difícil y dañarían su imagen.

Los defensores nunca sabrán con anticipación si su "compromiso de disuasión" es lo suficientemente fuerte como para disuadir contra un posible ataque. El agresor podría estar a la expectativa de unos beneficios que los defensores ignoran. Evaluar la situación de forma detallada representa un constante desafío y podría incluso resultar imposible debido a la falta de información básica. Las organizaciones de los defensores deben por lo tanto desarrollar unos planes de emergencia extremadamente flexibles y la habilidad de responder con rapidez a acontecimientos inesperados.

Diseñar un plan de seguridad

No es difícil diseñar un plan de seguridad. Aquí está el proceso representado en sólo unos pasos:

1 ◆ **Los componentes del plan**. La finalidad del plan de seguridad es reducir tu

riesgo. Por lo tanto tendrá como mínimo tres objetivos, basados en tu evaluación de riesgo:

- Reducir el grado de amenaza que estés experimentando;
- Reducir tus vulnerabilidades;
- Ampliar tus capacidades.

Resultaría útil que tu plan también incluyera:

- Planes preventivos o protocolos, para asegurar que el trabajo cotidiano se lleve a cabo bajo unos estándares de seguridad (por ejemplo, cómo preparar una denuncia pública o la visita a una zona remota).
- Planes de emergencia para tratar con problemas específicos, como por ejemplo, una detención o una desaparición.

2 ◆ **Responsabilidades y recursos para implementar el plan**. Para asegurarse de la puesta en práctica del plan, debemos integrar la seguridad en las actividades laborales diarias:

- Incluir regularmente en las agendas de trabajo una evaluación del contexto y los puntos de seguridad;
- Registrar y analizar los incidentes de seguridad;
- Asignar responsabilidades en seguridad;
- Asignar recursos, es decir, el tiempo y los fondos, para seguridad.

3 ◆ **Diseñar el plan** – por dónde empezar. Si has realizado una valoración del riesgo de un defensor u organización, seguramente tendrás una larga lista de vulnerabilidades, varios tipos de amenazas y un número de capacidades. Es prácticamente imposible cubrir todo al mismo tiempo. Así que ¿por dónde empezar? Es muy sencillo:

- **Selecciona algunas amenazas**. Da prioridad a las amenazas que has enumerado en la lista, ya sean actuales o potenciales, utilizando uno de los siguientes criterios: La amenaza más seria – las amenazas de muerte, por ejemplo; O la amenaza más seria y probable – si otras organizaciones similares a la tuya han sido atacadas, ésto representa una clara amenaza potencial para ti; O la amenaza que más se aproxime a tus vulnerabilidades – porque corres un mayor riesgo con esa amenaza específica.

- **Haz una lista de las vulnerabilidades correspondientes a la lista de amenazas**. Deberías centrarte primero en estas vulnerabilidades, y recuerda que no todas las vulnerabilidades están relacionadas con todas las amenazas. Por ejemplo, si recibes una amenaza de muerte, no resultará muy práctico empezar a mejorar las puertas de tu oficina del centro de la ciudad (a no ser que se te pueda atacar fácilmente en la oficina, que no suele ser el caso). Podría resultar más práctico reducir tu exposición durante tus desplazamientos de casa a la oficina o durante los fines de semana. No es que mejorar las puertas no tenga importancia, pero esta acción en concreto seguramente no reduzca tu vulnerabilidad ante una amenaza de muerte.

- **Haz una lista de las capacidades que posees que se correspondan con la lista de amenazas.**

Ahora estás en posición de centrarte en las amenazas, las vulnerabilidades y las capacidades seleccionadas en tu plan de seguridad, y puedes estar medianamente

convencido de poder reducir tu riesgo empezando por el lugar adecuado.
No olvides que este es un sistema ad hoc para diseñar un plan de seguridad. Existen otros métodos "formales" para hacerlo, pero este método es sencillo y hace que te centres en los temas de seguridad más urgentes – siempre y cuando tu evaluación de riesgo sea correcta – y que consigas un plan "activo" y "real", y esa es la parte importante de la seguridad. (Véase el final de este Capítulo para una lista detallada de los posibles componentes del plan de seguridad que también pueden ser de utilidad a la hora de evaluar los riesgos.)

Enfrentarse a los desafíos de seguridad: La gestión de seguridad paso a paso

La gestión de la seguridad no se acaba nunca y es siempre parcial y selectiva. Esto es debido a que:

- La cantidad de información que puedes absorber tiene un límite – no se pueden agrupar y manejar simultáneamente todos los factores que afectan tu seguridad;

- Es un proceso complejo – es necesario invertir tiempo y esfuerzo para poder crear una consciencia, desarrollar un consenso, formar a la gente, gestionar la renovación del personal, llevar a cabo actividades, etc.

El manejo de la seguridad es, sobre todo, práctico.

El manejo de la seguridad raramente logra una mirada detallada y a largo plazo. Su aportación se basa en la capacidad para prevenir ataques y desarrollar estrategias organizativas para afrontarlos. Tal vez esto no parezca muy ambicioso, pero cabe recordar que de hecho destinamos muy pocos recursos a la seguridad.
Cuando se examinan las prácticas de seguridad de un defensor o de una organización se encuentran varios tipos de directrices, planes, medidas o pautas de conducta ya establecidos. Habrá muchas discrepancias sobre la seguridad, desde ideas estereotipadas sobre las prácticas de seguridad hasta una reticencia a incorporar nuevas actividades de seguridad por temor a un incremento del volumen de trabajo existente.
La práctica de la seguridad suele ser un trabajo fragmentado e intuitivo, siempre en proceso de elaboración. El objetivo del manejo de la seguridad es el de ir implantando gradualmente diferentes cambios para mejorar la actuación. Las normas y procedimientos de seguridad suelen generarse en las diferentes partes de la organización que cubren ciertas áreas específicas de trabajo, tales como la logística, o un equipo exterior especialmente preocupado por su seguridad, un director bajo presión por las preocupaciones de los financiadores sobre la seguridad, etc.
Poco a poco, el manejo de la seguridad va abriendo puertas a procesos informales y abre un espacio para la práctica de nuevos métodos. Los eventos inesperados, al igual que los incidentes de seguridad, requerirán decisiones urgentes a corto plazo que, si son gestionadas correctamente, podrían convertirse en prácticas de seguridad a largo plazo para toda la organización.

Implementar un plan de seguridad

Los planes de seguridad son importantes, pero no siempre resultan fáciles de poner en marcha. La implementación es mucho más que un proceso técnico – es un proceso organizativo, lo que implica buscar puntos de entrada y

oportunidades para desarrollarlo, al igual que detectar cuáles son los obstáculos y problemas.
Un plan de seguridad debe ser implementado por lo menos a tres niveles:

1 ◆ A nivel **individual**. Cada individuo debe seguir el plan para que éste funcione.

2 ◆ A nivel **organizativo**. La organización en su totalidad debe seguir el plan.

3 ◆ A nivel **inter-organizativo**. Normalmente para mantener la seguridad es necesario un cierto grado de cooperación entre organizaciones.

Ejemplos de puntos de entrada y oportunidades a la hora de implementar un plan de seguridad:

- Han ocurrido varios incidentes menores en tu organización u otra organizacion y algunos trabajadores están preocupados al respecto.
- Existe una preocupación general sobre la seguridad debido a la situación del país.
- Se han incorporado nuevos trabajadores que podrían formarse e implementar así unas buenas prácticas en seguridad con mayor facilidad.
- Una organización nos ofrece una formación sobre la seguridad.

Ejemplos de problemas y obstáculos a la hora de implementar un plan de seguridad:

- Algunas personas piensan que un mayor número de medidas de seguridad equivale a incrementar todavía más el volumen de trabajo.
- Otras opinan que la organización ya dispone de una buena seguridad.
- "¡No tenemos tiempo para estas cosas!"
- "De acuerdo, sacaremos algo de tiempo para discutir el tema de la seguridad el sábado por la mañana, pero ¡que no se hable más!"
- "Debemos centrarnos más en la gente a la que queremos ayudar, no en nosotros mismos."

Formas de mejorar la implementación de un plan de seguridad

- **Aprovecha las oportunidades y los puntos de entrada** para confrontar los problemas y superar los obstáculos.
- **Procede paso a paso**. No vale la pena pretender que se puede hacer todo al mismo tiempo.
- **Subraya la importancia de la seguridad para hacer un buen trabajo por el bien de las víctimas**. La seguridad de las víctimas y testigos es primordial para el trabajo y la mejor manera de manejar esto es integrando unas buenas prácticas de seguridad en todos los ámbitos laborales. Utiliza ejemplos de formación/debate que muestren el posible impacto negativo

que puede ejercer sobre los testigos y las víctimas una seguridad poco rigurosa.

- Si el plan es diseñado por dos "expertos" y presentado a toda la organización es probable que sea todo un fracaso. En la seguridad, la **participación es fundamental**.
- **Un plan debe ser realista y realizable**. Si haces una larga lista de cosas que hacer antes de cada viaje al terreno no funcionará. Enumera sólo las que sean imprescindibles para garantizar la seguridad. Esta es otra de las razones por las que es necesario implicar a aquéllos que realmente hacen el trabajo – como por ejemplo las personas que suelen ir a los viajes al terreno.
- **El plan no es un documento inalterable** – debe ser revisado y actualizado todo a menudo.
- **El plan no debe ser considerado como "más trabajo", sino como "una mejor forma de trabajar"**. La gente tiene que ver las ventajas del plan: evitar por ejemplo duplicar los informes. asegúrate de que los informes de las visitas externas deben tener un apartado de seguridad; haz que los asuntos de seguridad pasen a ser un punto común en las reuniones de equipo, integra aspectos de la seguridad en otras formaciones, etc.
- **Subraya que la seguridad no es una elección personal**. Las decisiones, actitudes y comportamientos individuales que causan un impacto en la seguridad pueden acarrear consecuencias en la seguridad de los testigos, los familiares de las víctimas y colegas. Es necesario llegar a un compromiso colectivo para poder implementar unas buenas prácticas de seguridad.
- **Es necesario asignar el tiempo y los recursos** para poder implementar el plan, puesto que para mejorar la seguridad no debemos hacer uso del "tiempo libre". Para que las actividades de seguridad sean consideradas "importantes", deben colocarse junto a otras actividades "importantes".
- **Todo el mundo debe ser visto siguiendo el plan**, sobre todo los directores y los responsables del trabajo de otras personas. Es necesario implantar sanciones para los individuos que se nieguen a atenerse al plan.

Posibles elementos a incluir en un plan de seguridad

El siguiente "menú" enumera una propuesta detallada de elementos a incluir en un plan de seguridad. Una vez realizada la evaluación de riesgo, podrás escoger y combinar estos elementos con el fin de completar tu plan de seguridad.

- El mandato, la misión y los objetivos generales de la organización.

- Una declaración por parte de la organización sobre la política de seguridad.

- La seguridad debería abarcar todos los aspectos del trabajo diario: el análisis del contexto, la valoración del riesgo y los análisis de incidentes, al igual que la evaluación de la seguridad.

- Cómo asegurar que todos los trabajadores tengan un conocimiento adecuado de la seguridad y que cuando las personas abandonen la organización se transfieran sus responsabilidades de seguridad.

- Asignación de las responsabilidades: Quién debe hacer qué en qué situaciones

- Cómo actuar en una crisis de seguridad: Organizar un comité o grupo de crisis, delegar un responsable para hacerse cargo de los medios de comunicación, comunicarse con los familiares, etc.

- Responsabilidades de seguridad organizacional: Planificación, seguimiento, seguros, responsabilidad civil, etc.

- Responsabilidades individuales de seguridad: Reducir siempre el riesgo, cómo gestionar el tiempo libre o las actividades de ocio, registrar e informar sobre los incidentes de seguridad, sanciones (algunos de estos puntos podrían incluirse en los contratos de trabajo, si procede).

- Políticas organizacionales sobre:

  1- El descanso, el tiempo libre y el estrés 2- Incidentes serios, tales como rapto, desaparición, lesión personal, etc. 3- La seguridad de los testigos 4- La prevención sanitaria y de accidente 5- Relaciones con las autoridades, las fuerzas de seguridad y los grupos armados 6- Gestionar y archivar la información, la gestión de los documentos confidenciales 7- Tu propia imagen en relación a los valores religiosos, sociales y culturales 8- La gestión de la seguridad en oficinas y hogares (visitantes incluidos).

- Planes de prevención y protocolos sobre:

  1- Preparación de viajes al terreno 2- Manejo de dinero en efectivo u objetos valiosos 3- Sistemas y protocolos de comunicación 4- Mantenimiento de vehículos 5- Minas 6- Reducir el riesgo de verse afectado por delincuencia común, incidentes armados o ataques sexuales 7- Reducir el riesgo de accidentes en los desplazamientos por zonas de riesgo.

- Planes y protocolos para reaccionar en las crisis de seguridad, como:

  1- Emergencias médicas y psicológicas (también en el terreno) 2- Ataques, incluyendo los ataques sexuales 3- Robo 4- Reaccionar si una persona no se reporta cuando debe hacerlo 5- Arresto o detención 6- Rapto 7- Incendio y otros accidentes 8- Evacuación 9- Desastres naturales 10- Allanamientos legales o ilegales o entrada ilegal en oficinas u hogares 11- Incidentes armados (si alguien se ve bajo disparos, por ejemplo, o en un bombardeo) 12- Si matan a alguien 13- Si hay un golpe de estado.

CAPÍTULO 7

Evaluar el rendimiento de la seguridad de tu organización: la rueda de la seguridad

Objetivo:

Examinar la forma en la que manejas tu seguridad.

Evaluar en qué grado la seguridad está integrada en el trabajo de un grupo de defensores de derechos humanos .

La rueda de la seguridad

Empecemos por lo más sencillo: para que una rueda gire correctamente, ésta debe ser totalmente redonda. Este punto es evidente. Pero ¿qué ocurre si tiene unos radios más largos que otros? La rueda no será totalmente redonda y por lo tanto no girará correctamente.

Lo mismo ocurre con el manejo de la seguridad de un grupo u organización. Si no desarrollamos al mismo tiempo los principales componentes de seguridad, no podemos pretender que la estrategia global de seguridad funcione correctamente. Partiendo de esta base, podemos dibujar la denominada "rueda de la seguridad" que nos ayudará a analizar cómo manejamos la seguridad, y a evaluar en qué grado ésta está integrada en el trabajo de un grupo de defensores específico.

Esta evaluación puede hacerse en grupo. Podéis realizar una lista con las posibles razones por las cuales ciertos componentes de la rueda no se han desarrollado suficientemente, y proponer diferentes soluciones a estos problemas. Una vez hayáis enumerado las posibles soluciones, podéis iniciar el trabajo de escoger las que más os interesen y ponerlas en práctica.

Una vez completada la evaluación de vuestra rueda de la seguridad, conservad el resultado y el diagrama. Cuando repitáis el ejercicio unos meses más tarde, podréis comparar vuestro nuevo diagrama con el anterior y comprobar punto por punto si la situación ha mejorado o no.

Los componentes de la rueda de la seguridad

La rueda de la seguridad está compuesta por 8 radios, o componentes

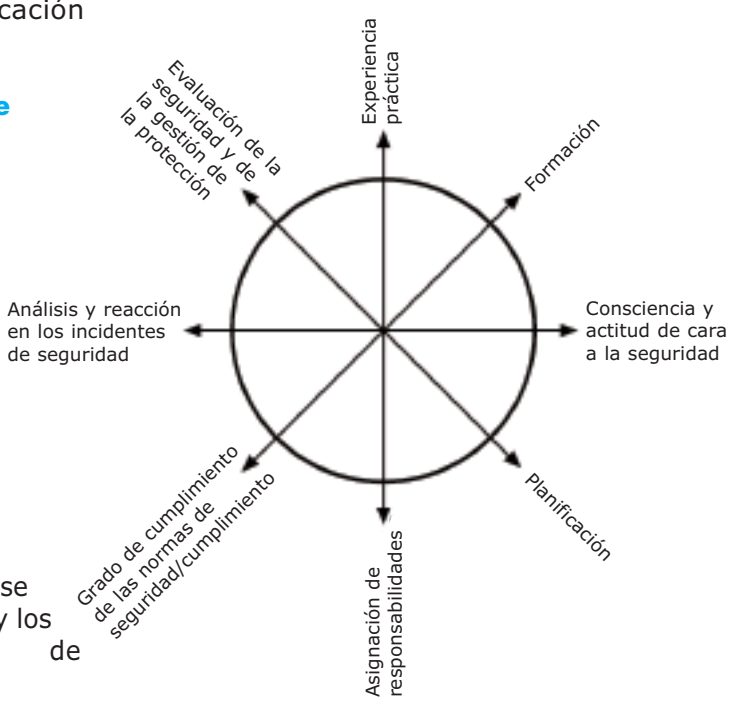
- **Experiencia práctica:** Conocimiento práctico de la seguridad y la protección. Tu punto de partida y tus objetivos.

- **Formación:** Puedes obtener formación en seguridad con un cursillo o por iniciativa propia durante tu trabajo diario.

- **Consciencia y actitud de cara a la seguridad:** Se refiere a si las personas y la organización en su totalidad consideran la protección y la seguridad como una necesidad y si están dispuestos a trabajar para garantizarlas.

- **Planificación:** Capacidad de planificación en seguridad en el trabajo. Planificación para la protección.

- **Asignación de responsabilidades:** ¿Quién es responsable de qué aspectos de la seguridad y la protección? ¿Y en caso de emergencia?



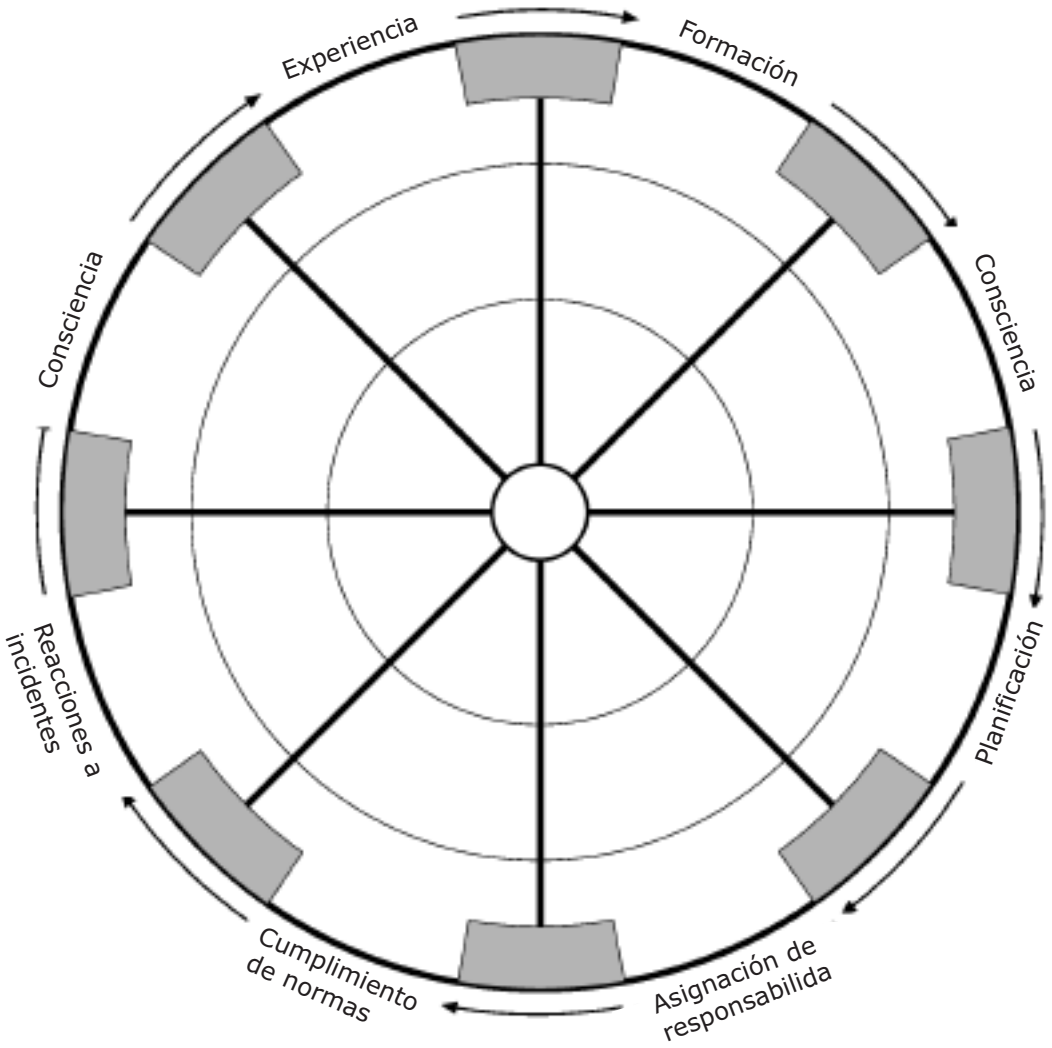
- **Grado de cumplimiento de las normas de seguridad / cumplimiento:** ¿En qué medida se cumplen las normas y los procedimientos de seguridad?

- **Análisis y reacción en los incidentes de seguridad:** ¿En qué medida están siendo analizados los incidentes de seguridad? ¿Está la organización respondiendo correctamente?

- **Evaluación de la seguridad y de la gestión de la protección:** La evaluación de la seguridad en tu trabajo diario, así como la de tus reacciones a los incidentes de seguridad, aportarán un mayor conocimiento y experiencia a las personas y organizaciones.

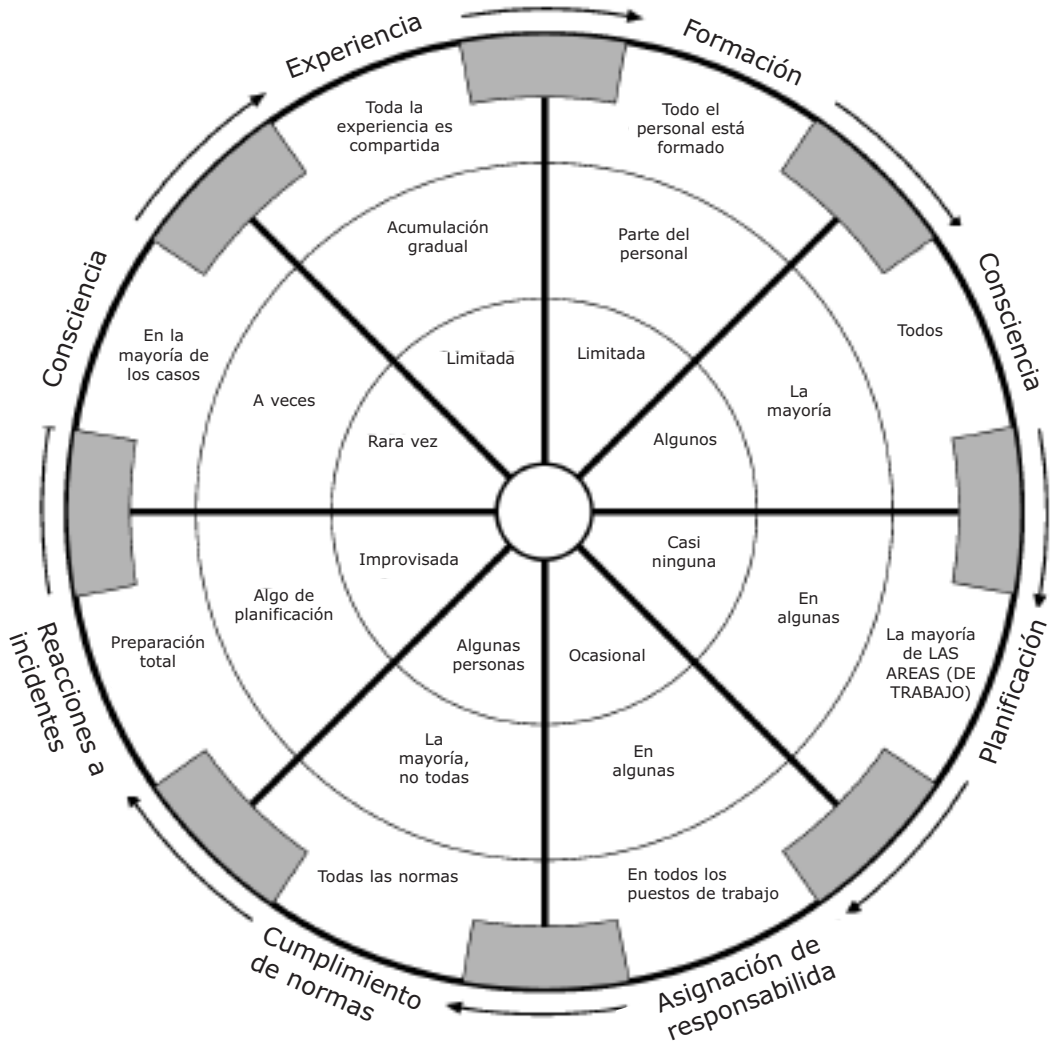
Ahora que estás más familiarizado con los componentes de la rueda de la seguridad, intenta construir un diagrama añadiendo más información. Podría ser algo así como éste:

La rueda de la seguridad y sus ocho componentes, o radios



La rueda de la seguridad nunca es perfecta:

Algunos de sus componentes están más desarrollados que otros. Por lo tanto es mejor examinar el grado de desarrollo de cada uno. De esta forma, podrás identificar cuáles son las acciones prioritarias que debes tomar para mejorar tu protección y seguridad. Las líneas de puntos concéntricas que van del centro hacia fuera ilustran lo desarrollado que está cada componente.

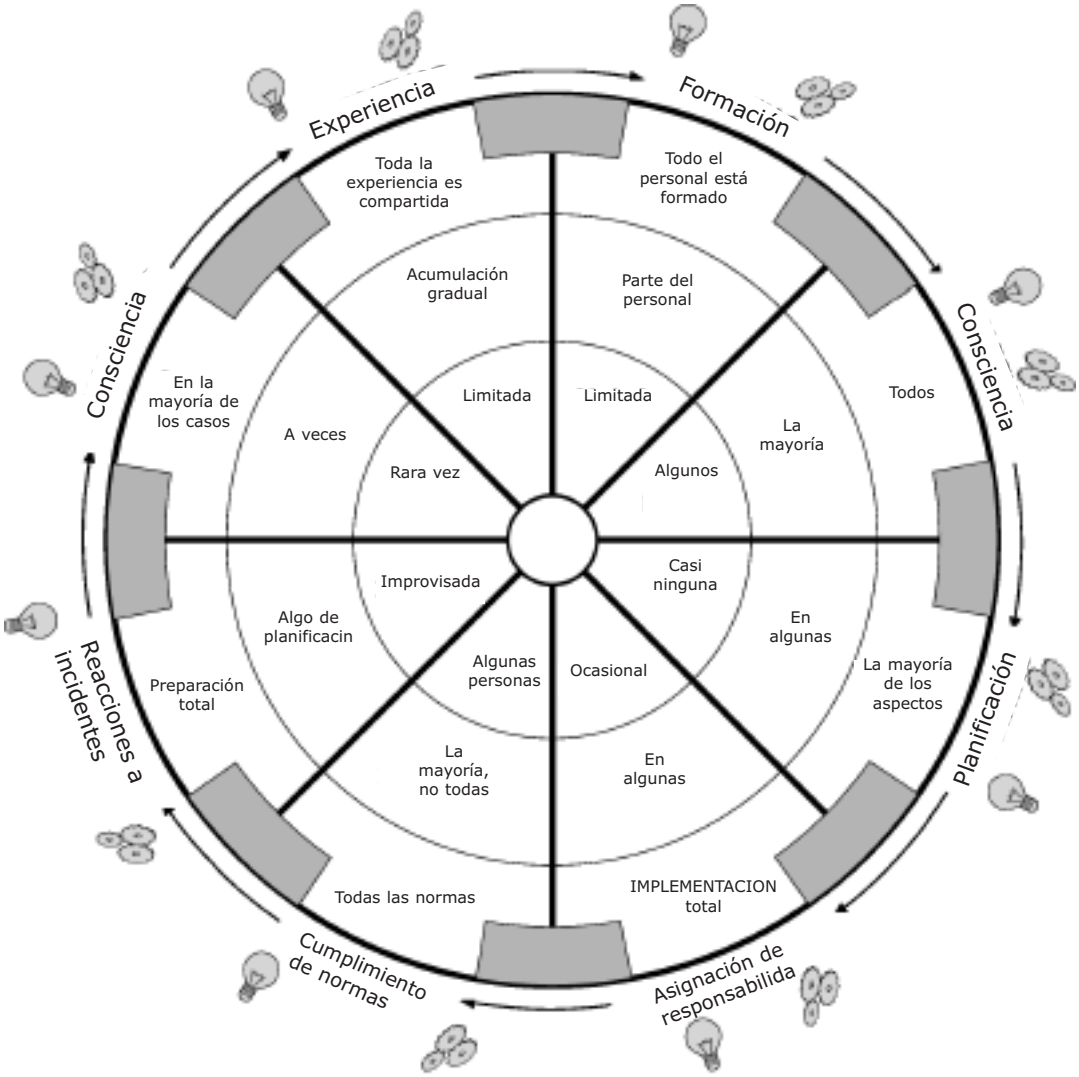


Fotocopia la rueda sobre papel o acetato y colorea los espacios entre los radios. Así obtendrás la estructura de la rueda de tu grupo u organización, y te ayudará a comprobar que partes están más – o menos – desarrolladas.

Si cualquiera de los ocho componentes de la rueda no funcionan deberás establecer:

Cuáles son los problemas de este componente de la rueda…

…y cuáles son las soluciones para estos problemas.



CAPÍTULO 8

Asegurarse del cumplimiento de las normas y procedimiemtos de seguridad

Objetivo:

Pensar en las razones por las que los trabajadores y las organizaciones no pueden o no están dispuestos a seguir los planes y procedimientos de seguridad, y encontrar soluciones apropiadas.

La seguridad concierne a todo el mundo

Resulta complicado conseguir que la gente y las organizaciones cumplan realmente los procedimientos y normas de seguridad. Puedes trazar un buen plan de seguridad, completo, con normas preventivas y procedimientos de emergencia; otorgar a la seguridad una posición capital en la agenda de todas las reuniones importantes, etc., y que a pesar de ello la gente continúe sin observar las normas de seguridad de la organización.

Esto podría parecer increíble, teniendo en cuenta que los defensores de los derechos humanos se encuentran bajo una presión y amenaza constantes, pero ocurre.

Si alguien necesita averiguar algo sobre tu labor, no lo hará a través de la persona más cuidadosa de la organización. Más bien intentarán aproximarse a alguien que suele emborracharse los sábados por la noche. Asimismo, si alguien pretende asustar a tu organización, probablemente no atacará a la persona que ha tomado todas las precauciones necesarias; más bien abordará a alguien que suele ser bastante descuidado con su propia seguridad. Por la misma razon, podría suceder que se ataque a una persona cuidadosa si la persona descuidada dejara la puerta abierta... Lo que viene a mostrar que una persona descuidada puede poner a todos en una situación de mayor riesgo.

Es por ello que deberíamos definir la seguridad como un asunto que no sólo concierne a las personas implicadas sino a toda la organización. Si sólo tres de 12 personas cumplen las normas de seguridad, toda la organización, incluyendo los que respetan las normas, corre un riesgo. Si la situación mejora y nueve personas empiezan a seguir los procedimientos de seguridad, el riesgo disminuye. Pero el riesgo sería todavía menor si las 12 personas siguieran las normas.

La seguridad es un asunto que concierne a toda la organización, y a los individuos que la componen.

Un buen plan de seguridad no tiene sentido si no se cumple. Seamos realistas: Mucha gente no observa las normas o procedimientos. Sin embargo resulta más fácil afrontar este problema que sus posibles consecuencias.

¿Por qué la gente no cumple las normas de seguridad? y ¿cómo podemos evitarlo desde un principio?

En primer lugar, la palabra "cumplir" conlleva unas connotaciones de sumisión y docilidad y por lo tanto debería evitarse. Las personas tienden a cumplir las normas que entienden y aceptan, porque pueden adoptarlas como propias. La palabra clave por lo tanto es "apropiación".

Para que un procedimiento de seguridad se cumpla es necesario que sea acogido por todas las personas de la organización. Esto no ocurre de forma inmediata. Para que el personal haga suyo un procedimiento de seguridad debemos permitir su participación en el diseño y la puesta en práctica del mismo. También son importantes la formación, la comprensión y la aceptación de los procedimientos.

Cuadro 1: La relación entre las personas y las organizaciones en términos de seguridad.

Concepto	Enfoque: "¡Todo el mundo debe seguir las normas!"	Enfoque: "El individuo y la organización han acordado las normas"
Enfoque	Basado en las normas	Basado en las necesidades 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 cumplimos las normas?	Por obligación, para evitar una sanción o una expulsión.	Por respeto a un acuerdo, con un margen de crítica y mejora (porque coincidimos con su propósito/necesidad, para poder ayudar a proteger a nuestros compañeros y a la gente por/con la que trabajamos)
Responsabilidad de la seguridad	No compartida	Compartida

La apropiación no significa simplemente "cumplir las normas", sino establecer un acuerdo sobre las normas que haga que las personas las cumplan porque las entienden, porque consideran que son apropiadas y efectivas, y porque piensan que les afecta personalmente. Por esta razón, las normas deberían ajustarse también al criterio moral y ético y a las necesidades básicas de las personas.

La apropiación no significa simplemente "cumplir las normas", sino respetar un acuerdo entre la organización y los individuos referente a la seguridad.

Para poder mantener el acuerdo entre los individuos y la organización es importante que **la(s) persona(s) responsable(s) de la seguridad mantenga(n) a los demás continuamente implicados** a través de sesiones informativas, recordatorios sobre las normas, y consultando a la gente sobre lo apropiadas y efectivas que resultan las normas en la práctica.

Sin embargo, esta participación no tendrá mucho valor si no existe **una cultura organizacional de la seguridad** que penetre los programas de trabajo y los procedimientos, tantos los formales como los informales.

En resumen, es posible que los individuos se apropien de las normas y procedimientos de seguridad siguiendo estos pasos:

- Desarrollar el concepto de que la seguridad es importante de cara a proteger a las víctimas, testigos, familiares y a los colegas de trabajo, y hacer así posible que el trabajo continúe.
- Desarrollar y valorar una cultura organizacional de la seguridad;
- Promover una apropiación de las normas y procedimientos de seguridad;.
- Asegurarse de que todos los individuos participen en el diseño y la mejora de las normas y procedimientos de seguridad;
- Formar a las personas en temas de seguridad;
- Asegurarse de que todo el personal está convencido de la idoneidad y efectividad de las normas y procedimientos de seguridad;
- Establecer un acuerdo entre la organización y las personas sobre el respeto a las normas y procedimientos de seguridad;
- Instar a los responsables de seguridad a informar y formar a la gente, a recordar al personal los términos del acuerdo y a solicitar sus opiniones sobre lo apropiadas y efectivas que resultan las normas en la práctica.

¿Por qué no se observan las normas y procedimientos de seguridad?

No existe un prototipo del defensor de los derechos humanos que no cumple las normas de seguridad. Mucha gente dentro de una misma organización suele cumplir algunas de las normas pero no todas, o las observan esporádicamente.

Son muchas las posibles razones por las que la gente incumple las normas y procedimientos. Para poder cambiar esta situación y garantizar la apropiación, es importante establecer las causas y buscar las soluciones junto a las demás

personas implicadas. También resultará práctico distinguir las diferentes razones que pueden llevar a la gente a incumplir las normas, ya que varían mucho.

Posibles razones para el incumplimiento de las normas y procedimientos de seguridad:

Incumplimiento no intencionado:

- El defensor desconoce las normas;
- El/ella no aplica las normas correctamente.

Incumplimiento intencionado:

Problemas generales:

- Las normas son demasiado complicadas y difíciles de seguir;
- Los procedimientos no están a mano en la oficina o han sido diseñados de forma que se hace difícil su uso cotidiano.

Problemas individuales:

- Las normas son demasiado complicadas y difíciles de seguir;
- El individuo no está de acuerdo con algunas o todas las normas y las considera innecesarias, inapropiadas o inefectivas basándose en su experiencia personal, en una información o formación previa o en sus creencias personales.

Problemas de grupo:

- La mayoría de los individuos del grupo no cumplen las normas, o los "líderes" del grupo no las cumplen o no lo suficientemente, porque no existe una cultura organizacional de la seguridad;
- Una falta de motivación general en el trabajo puede hacer que la gente ignore las normas de seguridad.

Problemas organizacionales:

- No hay suficientes recursos económicos o técnicos que faciliten el cumplimiento de las normas;
- Existe una discordancia entre las normas y algunas áreas concretas de trabajo. Por ejemplo, las normas han sido establecidas por los responsables de seguridad pero ignoradas o no implementadas correctamente por la gente que trabaja en programas o en la contabilidad. Algunas normas podrían ser adecuadas para algunas áreas e inadecuadas para otras;
- El personal tiene un gran volumen de trabajo y un tiempo limitado, y no priorizan ninguna o algunas de las normas;
- Una falta de motivación generalizada por causa del estrés, las disputas laborales, etc.

La cultura organizacional es tan formal como informal, y debe ser desarrollada no sólo en la globalidad de la organización, sino que también en los equipos de trabajo. Una buena cultura organizacional se reconoce por sus charlas informales, chistes, fiestas, etc.

Seguimiento del cumplimiento de las normas y procedimientos de seguridad

Seguimiento directo:

Podemos incluir las normas y procedimientos en las valoraciones generales del trabajo y en las "listas de control"; al igual que en las reuniones anteriores y posteriores a las misiones de campo, en los informes de trabajo, en las agendas de reuniones, etc.
También se pueden llevar a cabo, conjuntamente con los equipos en cuestión, revisiones periódicas de cuestiones como el cuidado de la información confidencial, de los manuales de seguridad y de las copias; los protocolos de seguridad para visitar las oficinas centrales; la preparación para salir a una misión al terreno, y demás.

Seguimiento indirecto:

Solicitar la opinión de la gente sobre las normas y procedimientos (si son correctas y fáciles de seguir, etc.) puede mostrar si el personal es realmente consciente de las normas, si han sido totalmente aceptadas o si existe un desacuerdo del que hacerse cargo. También puede revisarse así el uso del manual de seguridad por parte de los trabajadores y las normas y protocolos existentes.
Resulta muy provechoso recopilar y analizar, conjuntamente con la gente o los equipos en cuestión, las opiniones y evaluaciones de la gente sobre las normas y procedimientos de seguridad. Esto también podría realizarse de forma confidencial/anónima o a través de una tercera persona.

Seguimiento retrospectivo:

La seguridad puede ser revisada analizando los incidentes de seguridad a medida que van surgiendo. Para ello debemos actuar con una especial precaución. La persona que ha sufrido un incidente de seguridad podría sentirse culpable o pensar que el análisis podría representar sanciones. Podría por lo tanto sentir la tentación de ocultarlo, no informando sobre el incidente o sobre algunos aspectos de éste.

¿Quién realiza el seguimiento?

Según cómo funcione el grupo, el seguimiento puede hacerlo o las personas responsables de seguridad o las personas responsables de áreas de trabajo o de recursos humanos.

¿Qué hacemos si no se respetan las normas y procedimientos de seguridad?

1 ◆ Determinar las causas, buscar soluciones y ponerlas en práctica. La lista de opciones del cuadro 1 anterior ("Posibles razones para el incumplimiento de las normas") puede servir como guía.

2 ◆ Si el problema es intencionado y está relacionado con una persona, procura:

a ◆ Entablar un diálogo con la persona para establecer la(s) causa(s) o motivo;

b ◆ Trabajar junto al equipo del individuo (en según que casos esto puede resultar inapropiado);

c ◆ Establecer un sistema de advertencias o avisos, para que la persona que incumple las normas sea totalmente consciente del problema.

d ◆ Utilizar un sistema de sanciones graduales (que podrían culminar en el despido de la persona).

3 ◆ Incluye una cláusula en todos los contratos laborales o de voluntariado sobre el cumplimiento de las normas y procedimientos de seguridad, para que todos los empleados sean perfectamente conscientes de lo importante que es para la organización.

En conclusión...

Habrá quien sostenga que organizar un debate sobre las razones por las que la gente no cumple las normas de seguridad es una pérdida de tiempo, ya que hay cosas más urgentes o importantes que hacer. Quienes opinan así suelen pensar sencillamente que las normas están hechas para ser cumplidas y punto. Otros personas son conscientes de que las cosas no siempre funcionan así.

Sea cual sea tu opinión, te invitamos a que des un paso hacia atrás y analices hasta qué punto están siendo cumplidas las normas y procedimientos de seguridad en la organización donde trabajas. El resultado podría ser sorprendente, y vale la pena dedicarle algo de tiempo para evitar problemas en un futuro…

CAPÍTULO 9

Mejorar la seguridad en el trabajo y en las casas particulares

Objetivo:

Evaluar la seguridad en oficinas, sedes o en casas.

Planificar, mejorar y supervisar la seguridad en estos lugares.

La seguridad en el trabajo y en la casa

La seguridad de las oficinas centrales de la organización o de las oficinas y los hogares de los trabajadores es de vital importancia de cara al trabajo de los defensores de los derechos humanos. Por lo tanto estudiaremos en profundidad cómo se puede analizar y mejorar la seguridad de una oficina o casa. (Para simplificarlo, a partir de ahora utilizaremos el término de "oficina", si bien la información que sigue hace también referencia a la seguridad en casas particulares).

Aspectos generales de la seguridad en la oficina

Nuestro objetivo para mejorar la seguridad puede resumirse en cinco palabras: **Evitar el acceso no autorizado**. En casos excepcionales también es necesario proteger la oficina de un posible ataque (un atentado con bomba, por ejemplo).

Esto nos lleva a la primera consideración general: las vulnerabilidades de una oficina, porque éstas podrían aumentar el riesgo, dependiendo del tipo de amenaza al que te enfrentes. Por ejemplo, si existe el riesgo de que alguien te robe material o información, debes eliminar las vulnerabilidades correspondientes. Una alarma nocturna no servirá de mucho si nadie se asoma a comprobar lo que ha ocurre. Por otro lado, si se trata de un robo violento en pleno día, los refuerzos de las rejas de la puerta no serán de gran ayuda. En resumen, decide qué medidas tomar de acuerdo con las amenazas a las que te enfrentes y el contexto en el que trabajes.

Las vulnerabilidades de una oficina deben ser evaluadas de acuerdo con las amenazas a las que te enfrentes.

Sin embargo, es importante encontrar un equilibrio entre instaurar las medidas de seguridad apropiadas y dar la impresión a la gente externa de que se "esconde" o "guarda" algo dentro, ya que esto podría de por sí suponer un riesgo. En la seguridad de la oficina a menudo te encontrarás en la obligación de decidir si mantener un perfil bajo o tomar más medidas visibles según convenga.

La seguridad de una oficina es igual a la de su punto más débil.

Si alguien quiere acceder a la oficina pasando desapercibido, no elegirá el punto de acceso más difícil para hacerlo. Recuerda que a veces la forma más sencilla de acceder a una oficina y observar lo que ocurre en su interior es simplemente llamando a la puerta.

La ubicación de la oficina

Los factores a tener en cuenta al instalar una oficina son: El vecindario; si el edificio guarda alguna relación con alguna persona o actividades del pasado; si se pueden implantar las medidas de seguridad necesarias; accesibilidad del transporte público y privado; riesgo de accidentes, etc. (Véase también "puntos a considerar para una buena ubicación más abajo)

Es conveniente revisar las medidas de seguridad adoptadas en el vecindario. Si hay muchas, podría significar que se trata de una zona peligrosa con respecto al crimen común, por ejemplo. También es importante hablar con la gente de la zona sobre la situación de la seguridad local. En todo caso, es importante asegurarse de que es posible tomar medidas de seguridad sin llamar demasiado la atención. También es conveniente relacionarse con la gente local ya que pueden informar sobre cualquier asunto sospechoso que ocurra en el vecindario.

También es importante comprobar quien es el propietario. ¿Qué reputación tiene? ¿Podría ser susceptible a la presión de las autoridades? ¿Aceptará que se adopten medidas de seguridad?

Al elegir la oficina es necesario tener en cuenta quién acudirá a ella. Las necesidades de una oficina donde acudirán víctimas en busca de un asesoramiento jurídico serán completamente distintas a las de una oficina que actúe principalmente como un lugar de trabajo para los empleados. Es importante tener en cuenta el fácil acceso al transporte público, ¿es peligroso el trayecto que va de la oficina a los hogares de los trabajadores, o a las zonas donde se llevan a cabo la mayoría de las actividades?, etc. También hay que evaluar los alrededores, especialmente para evitar tener que cruzar zonas peligrosas durante los desplazamientos.

Una vez seleccionada la ubicación, es importante realizar evaluaciones periódicas de aspectos de la ubicación que pueden cambiar, por si por ejemplo, un "elemento indeseable" se traslada al vecindario.

Puntos a considerar para la elección de una buena ubicación de la ofocina	
Vecindario:	Estadísticas de crimen; proximidad de posibles blancos de ataques armados, como instalaciones militares o gubernamentales; lugares seguros para refugiarse; otras organizaciones nacionales o internacionales con las que relacionarse.
Relaciones:	Tipo de gente en el vecindario; propietario/arrendador, previos arrendatarios; previos usos del edificio.
Accesibilidad:	Una o varias rutas de acceso buenas (cuantas más mejor); accesibilidad de transporte público y privado.
Servicios básicos:	Agua y electricidad, teléfono.
Alumbrado público	de los alrededores.
Susceptibilidad a accidentes o riesgos naturales:	Incendios, inundaciones graves, vertedero de desechos tóxicos, fábricas con procesos industriales peligrosos, etc.
Estructura física:	Solidez de las estructuras, facilidad para instalar el material de seguridad, puertas y ventanas, perímetro y barreras de protección, puntos de acceso (véase más abajo).
Para vehículos:	Un garaje o al menos un patio o un espacio cerrado, con una barrera de estacionamiento.

Acceso de terceros a la oficina: Barreras físicas y procedimientos para las visitas

Ahora ya sabemos que el objetivo principal de la seguridad de oficina es impedir el acceso a las personas no autorizadas. Una o más personas podrían entrar a robar, obtener información, colocar algo que podría ser utilizado en tu contra como drogas o armas, amenazarte, etc. Cada caso es distinto, pero el objetivo es siempre el mismo: Evitarlo.

El acceso a un edificio está controlado a través de unas barreras físicas (vallas, puertas, verjas), de unas medidas técnicas (como alarmas con iluminación) y de los procedimientos de acceso para las visitas. Toda barrera y procedimiento representa un filtro por el que debe pasar todo individuo que desee entrar en la oficina. Lo ideal sería que estos filtros estuvieran combinados, formando varias capas de protección capaces de impedir diferentes tipos de entrada no autorizada.

Barreras físicas.

Las barreras sirven para bloquear **físicamente** la entrada a visitantes no autorizados. La utilidad de las barreras físicas dependerá de su **solidez** y habilidad de cubrir **todos los huecos vulnerables** de los muros.

Tu oficina puede disponer de barreras físicas en tres zonas:

1 ◆ El perímetro **externo**: Vallas, muros o similares, al otro lado del jardín o patio;

2 ◆ El perímetro del **edificio o del local**;

3 ◆ El perímetro **interno**: Barreras que pueden ser instaladas en el interior de una oficina para proteger una o más habitaciones. Es práctico sobre todo en oficinas con un flujo importante de visitantes, ya que permite separar una zona pública de otra más privada que puede estar protegida con barreras adicionales.

El perímetro externo.

La oficina debería estar rodeada por un perímetro externo claramente delimitado, posiblemente con vallas altas o bajas, preferiblemente sólidas y lo suficientemente altas para dificultar más el acceso. Las verjas o mallas metálicas que te permiten ver a través, harán más visible el trabajo de la organización y por lo tanto pueden ser preferibles los muros de ladrillo o algo parecido.

El perímetro del edificio o del local.

Éste incluye paredes, puertas, ventanas y techo o tejado. Si las paredes son sólidas, todas las aberturas y el tejado deberán serlo. Las puertas y ventanas deben tener cerrojos apropiados y deben estar reforzadas con rejas, preferiblemente con barrotes tanto verticales como horizontales bien incrustados a la pared. Si hay un techo, éste debería ofrecer una buena protección – no una simple hoja de zinc o una capa de tejas. Si el tejado no puede ser reforzado bloquea todo los posibles accesos al tejado desde el suelo o desde los edificios vecinos.

En lugares con riesgo de ataque armado, es importante establecer zonas de seguridad en el interior de la oficina (véase Capítulo 11 sobre la seguridad en zonas de conflicto armado).

El perímetro interno

Se aplica lo mismo que en el edificio o local. Resulta muy práctico disponer de una zona de mayor seguridad en el interior de la oficina, y suele ser muy fácil de organizar. Incluso una caja fuerte podría considerarse como un perímetro interno de seguridad.

Una observación sobre las llaves

- Ninguna llave debería ser visible o accesible a las visitas. Mantén todas las llaves en un armario o cajón con un cierre de combinación cuyo código sólo conozcan los trabajadores. Asegúrate de cambiar el código de vez en cuando para mayor seguridad.

- Si las llaves están etiquetadas individualmente, no escribas una descripción de la habitación, armario o cajón correspondientes, ya que esto facilitaría el robo. Es mejor que utilices un código de números, letras o colores.

Medidas técnicas: Iluminación y alarmas

Las medidas técnicas como mirillas, interfonos y video cámaras, sólo refuerzan las barreras físicas o los procedimientos de acceso de visitas (véase más abajo). Ya que **las medidas técnicas sólo son prácticas para disuadir intrusos cuando están activadas**. Para que funcione una medida técnica, es necesario que pueda provocar una reacción en concreto, como por ejemplo, atraer la atención de los vecinos, de la policía o de una empresa privada de seguridad. Si esto no ocurre, y el intruso sabe que no ocurrirá, este tipo de medidas son muy poco prácticas y se limitarán a prevenir hurtos menores o a grabar a la gente que entra.

- La **iluminación** alrededor del edificio (de patios, jardines, pavimento) y de los rellanos es fundamental.
- Las **alarmas** deben tener varias finalidades, que incluyan la detección de intrusos y evitar el ingreso de posibles intrusos o hacer que desistan de un nuevo intento.

Una alarma puede activar un aviso sonoro en el interior de la oficina; una luz de seguridad, un tono, timbre o ruido fuerte y general; o una señal en una empresa externa de seguridad. Una alarma sonora es práctica para llamar la atención pero puede ser contraproducente en situaciones de conflicto o si crees que los residentes locales u otros no reaccionarán a ella. Es necesario elegir cuidadosamente entre una alarma sonora o una luminosa (una potente luz fija, o una luz roja intermitente). Ésta última puede ser suficiente para disuadir al intruso, ya que sugiere que la detección inicial puede desencadenar una reacción contra el mismo.

Las alarmas deben ser instaladas en los puntos de acceso (patios, puertas y ventanas, y en zonas vulnerables tales como los lugares que contengan información confidencial). Las alarmas más sencillas son los sensores de movimiento, que activan una luz, emiten un sonido o activan una cámara cuando detectan algún movimiento.

Las alarmas deberían:

- Incluir **pilas**, para que continúen funcionando en caso de apagón;
- Disponer de un **intervalo** antes de activarse para que pueda ser desactivado por los empleados en caso de activarlo accidentalmente;
- Incluir una opción de activación **manual** en caso de que los empleados necesitaran activarlo;
- Ser de fácil **instalación** y **mantenimiento**;
- Ser fácil de **distinguir** de una alarma de incendio.

Videocámaras.

Las videocámaras pueden ayudar a mejorar los procedimientos de acceso (véase abajo) o grabar a la gente que entra en la oficina. Sin embargo, las cámaras deberían estar colocadas en puntos fuera del alcance de los intrusos porque si no éstos podrían abrir la cámara y destruir la cinta.
Hay que tener en cuenta que las cámaras podrían intimidar a personas que acuden a la oficina, como víctimas o testigos, o por el contrario pueden ser consideradas como un bien lujoso que atrae a ladrones. Es recomendable colocar una nota advirtiendo de la presencia de cámaras activadas (el derecho a la privacidad también es un derecho humano).

Empresas de seguridad privadas

Este tema requiere mucho cuidado. En muchos países, los trabajadores de las empresas privadas de seguridad son antiguos miembros de las fuerzas de seguridad. Existen casos documentados donde estas personas eran responsables de la vigilancia y de los ataques a los defensores de los derechos humanos al mismo tiempo. Por lo tanto, es sensato no confiar en las empresas de seguridad cuando tienes razones para sospechar que estás siendo vigilado o temes un ataque de las fuerzas de seguridad. Si una empresa de seguridad tiene acceso a tus oficinas, podrían instalar micrófonos o permitir el acceso de otras personas.

Si decides usar los servicios de una empresa de seguridad, debes asegurarte de tener un acuerdo conciso sobre lo que su personal puede hacer y no hacer, y a qué partes del edificio pueden acceder. Evidentemente es necesario vigilar para comprobar que estos acuerdos sean respetados.

Por ejemplo:

> Si has contratado un servicio de seguridad que envía a un guarda cuando salta una alarma, este guarda podría acceder a zonas reservadas de tu oficina y activar aparatos de escucha en tu sala de reuniones.

Es preferible que acuerdes (y si es posible controles) exactamente qué empleados trabajarán para ti, pero esto no suele ser posible.

Si los guardas de seguridad van armados es importante para una organización de derechos humanos informarse detalladamente sobre cuáles son sus reglas de uso. Pero es más importante todavía hacer un balance de las posibles ventajas del uso de armas y de sus desventajas. Las armas de mano no representan ningún obstáculo para los atacantes con una mayor capacidad de fuego (tal y como suele ser el caso), pero si los atacantes saben que hay hombres dentro del inmueble con armas de corto alcance, podrían decidir entrar preparados para disparar, para protegerse durante el ataque. En otras palabras, una capacidad armada (armas pequeñas) probablemente incentive a los atacantes a utilizar armas de una mayor capacidad. Llegados a este punto, si necesitas guardas con ametralladoras merece la pena cuestionarse si dispones del espacio socio-político mínimo necesario para poder llevar a cabo tu labor.

Filtros del procedimiento de acceso.

Las barreras físicas deben ir acompañadas por el "filtro" de **un procedimiento de acceso**. Estos procedimientos determinan cuándo, cómo y quién puede acceder a cualquier parte de la oficina. El acceso a espacios privados, como llaves, información o dinero, debe ser restringido.
El método más sencillo para acceder a la oficina donde trabaja un defensor de los derechos humanos es llamando a la puerta y entrando. Mucha gente lo hace cada día. Para poder conciliar el carácter abierto de una oficina de derechos humanos con la necesidad de controlar quién quiere visitarte y por qué, necesitarás unos procesos de acceso apropiados.
Por lo general, la gente que llama a tu puerta o quiere entrar lo hace por una razón concreta. A menudo quieren preguntarte o entregarte algo, sin tener necesariamente que pedir permiso antes. Examinemos caso por caso:

Alguien llama y pide permiso para entrar por una razón en concreto.

Deberías seguir tres simples pasos:

1 ◆ **Pregunta por qué desea entrar**. Si el/ella quiere ver a alguien de la oficina, consulta a éste último. Si la persona no está presente, pídele al visitante que vuelva en otro momento o que espere fuera de la zona restringida de la oficina. Es importante utilizar las mirillas, cámaras o interfonos para evitar abrir o acercarte a la puerta, especialmente si quieres negarle la entrada a alguien o debes enfrentarte a una entrada violenta o forzosa. Por lo tanto, es bueno disponer de una sala de espera físicamente separada de la entrada interna de la oficina. Si es imprescindible disponer de una zona pública de fácil acceso, asegúrate de disponer de barreras físicas que bloqueen el acceso a las zonas restringidas de la oficina.

Alguien podría solicitar entrar para comprobar o reparar la instalación de agua o electricidad o llevar a cabo un trabajo de mantenimiento. También podría afirmar ser un periodista, un funcionario estatal, etc. Antes de permitirles la entrada comprueba siempre su identidad con la compañía u organización a la que dicen representar. Recuerda que ni un uniforme ni una tarjeta de identificación son garantías de una identificación correcta y segura, especialmente en una situación de riesgo medio o elevado.

2 ◆ **Decide si permitir o no el acceso**. Una vez establecida la razón de su visita, deberás decidir si permitirle o no el acceso. El simple hecho de que alguien dé un motivo para entrar no es suficiente razón para dejarle entrar. Si no estás seguro de cuál es su encargo, no le permitas entrar.

3 ◆ **Supervisa a las visitas hasta que salgan**. Una vez la visita ha entrado en la oficina, asegúrate de que alguien las supervise en todo momento hasta su salida. Es conveniente disponer de una zona separada para reunirse con las visitas fuera de las zonas restringidas.

Para cada visitante debería anotarse su nombre, organización, razón de la visita, con quien se reunieron, hora de entrada y de salida. Esta información puede ser de gran utilidad a la hora de analizar los posibles errores tras un incidente de seguridad.

Alguien viene o llama haciendo preguntas.

A pesar de lo que pueda decirte una visita o alguien por teléfono, no comuniques bajo ningún concepto la ubicación de un colega o de otra gente cercana, ni ofrezcas ningún tipo de información personal. En caso de que insistieran, diles que dejen un mensaje, que vengan, que vuelvan a llamar más tarde o que pidan una cita para quedar con la persona que desean ver.

A menudo la gente puede aparecer por error, preguntando si el Señor Tal vive aquí o si se vende algo, etc. Otros a veces quieren vender cosas, y los mendigos pueden venir pidiendo ayuda. Si niegas el acceso y la información a esta gente, estarás evitando todo riesgo de seguridad.

Alguien quiere hacer entrega de un objeto o paquete.

El riesgo que corres con un paquete u objeto es que el contenido podría comprometer o herir al alguien (en el caso de un paquete o carta bomba). Por muy inocente que parezca, no toques o manipules un paquete o carta hasta que no hayas seguido tres simples pasos:

1 ◆ **Comprueba si el destinatario a quien va dirigido está esperando el paquete**. No es suficiente con que el destinatario conozca al remitente, porque la identidad de éste podría ser fácilmente falsificada. Si el destinatario no espera un paquete deberá comprobar si el supuesto remitente realmente le ha enviado algo. Si el paquete está simplemente dirigido a tu oficina, comprueba quien lo envió. Espera y discute el asunto antes de tomar una decisión final.

2 ◆ **Decide si aceptar o no el paquete o la carta**. Si no puedes determinar quien envió el paquete, o si tardarás en saberlo, la mejor opción es no aceptarlo, sobre todo en un entorno de riesgo medio o elevado. Siempre puedes pedir que se te entregue más tarde, o recogerlo en la oficina de correos.

3 ◆ **No pierdas de vista el paquete mientras esté en el interior de la oficina**. Asegúrate de que sabes en todo momento en qué lugar de la oficina se encuentra el paquete hasta que el destinatario lo haya recogido.

Durante actos o fiestas.

En estas circunstancias la norma es sencilla: No puede entrar nadie a quien no conozcas personalmente. Sólo deberían entrar los conocidos de compañeros de confianza, y sólo cuando ese compañero esté presente y pueda identificar a su invitado. Si una persona aparece afirmando conocer a alguien de la oficina que no está presente, no le dejes entrar.

Llevar un registro de llamadas y de visitas.

Es práctico mantener un registro de las llamadas de teléfono y de los números y tomar nota de la gente que visita la organización (algunas organizaciones solicitan a los visitantes nuevos la presentación de un documento de identidad y la organización registra el número del documento)

Horas extras en la oficina.

Deberían existir ciertos procedimientos para el personal que se queda haciendo trabajo fuera del horario normal. Los miembros de una organización que tengan que hacerlo deberían dar parte cada cierta hora a otro miembro designado, tener un especial cuidado al abandonar el edificio, etc.

Lista de revisión: Identificar los puntos débiles de los procedimientos de acceso
◆ **¿Quién** tiene acceso habitual a **qué** zonas y **por qué**? Restringe el acceso a no ser que sea absolutamente necesario mantenerlo público.
◆ Distingue los diferentes **tipos** de visitantes (mensajeros, trabajadores de mantenimiento, técnicos informáticos, miembros de ONG en reuniones, VIPs, invitados a actos, etc.) y **desarrolla unos procedimientos de acceso apropiados para cada uno**. Todo el personal debería estar familiarizado con los diferentes procedimientos de cada tipo de visitas, y asumir la responsabilidad de llevarlos a cabo.
◆ ¿Tiene la visita acceso a los puntos débiles una vez dentro de la oficina? Desarrolla estrategias para evitarlo.
Lista de revisión: Acceso a las llaves
◆ **¿Quién** tiene acceso a **qué** llaves y **cuándo**?
◆ ¿Dónde y cómo **se guardan** las **llaves** y sus **copias** correspondientes?
◆ ¿Hay un control de las copias de llaves que están en circulación?
◆ ¿Existe algún riesgo de que alguien realice una **copia no autorizada de la llave**?
◆ ¿Qué ocurre **si alguien pierde una llave**? Deberás cambiar la cerradura, a no ser que estés totalmente convencido de que se ha perdido accidentalmente y de que nadie puede identificar al propietario de la llave o su dirección. Recuerda que una llave puede ser robada – en un robo organizado, por ejemplo – para poder acceder a la oficina.

Todos los trabajadores tienen la obligación de actuar en relación con cualquier persona que no siga correctamente los procedimientos de acceso. Deberían también registrar en el libro de incidentes de seguridad todos los movimientos de personas o vehículos sospechosos. Esto es también aplicable a cualquier objeto situado fuera del edificio, para descartar el riesgo potencial de una bomba. Si hay una sospecha de bomba, no la ignores, **no la toques**, y asegúrate de Contactar con la policía.

Cuando se mude a una nueva oficina, o si se han perdido o han sido robadas las llaves, es esencial cambiar como mínimo todos los cerrojos de la zona de entrada.

Lista de revisión: Procedimientos generales de la seguridad de oficina

- ☐ Disponer de extintores y linternas (con pilas de repuesto). Asegurarse de que todos los empleados sepan cómo utilizarlos.

- ☐ Disponer de un generador eléctrico si hay una alta posibilidad de apagón. Los apagones pueden poner en peligro la seguridad (luces, alarmas, teléfonos, etc.) sobretodo en zonas rurales.

- Tener una lista a mano con los teléfonos locales de emergencia, de la policía, bomberos, ambulancia, hospitales de urgencias cercanos, etc.

- Si existe un riesgo de combate en las cercanías, mantén un suministro de comida y agua en reserva.

- Confirma la ubicación de otras zonas de seguridad externas a la oficina en caso de emergencia (las oficinas de otras organizaciones por ejemplo).

- Nunca dejes a una persona externa a la organización **sola** en una zona restringida con acceso a llaves, información u objetos de valor.

- **Llaves**: Nunca dejes las llaves en un lugar donde las visitas puedan acceder a ellas. Nunca "escondas" las llaves fuera de la entrada de la oficina – esto las hace accesibles, no escondidas.

- **Procedimientos de acceso**: Las barreras de seguridad no ofrecen protección alguna si se permite el acceso a la oficina a un posible intruso. Los puntos principales a tener en cuenta son:

  - Todos los trabajadores son igual de responsables del control y entrada de las visitas.

  - Todas las visitas deberán estar supervisadas en todo momento mientras permanezcan en el interior de la oficina.

- Si te encuentras con un visitante no autorizado en la oficina:

  - Nunca confrontes a alguien que parece dispuesto a hacer uso de la violencia para obtener lo que quiere (si van armados, por ejemplo). En estos casos, avisa a tus compañeros, busca un lugar seguro para esconderte e intenta pedir ayuda a la policía.

  - Dirígete a la persona con cuidado, o busca ayuda en la oficina, o llama a la policía si fuera adecuado.

- En situaciones de elevado riesgo controla siempre la ubicación de los objetos vulnerables, como la información del disco duro, para que permanezcan inaccesibles o para poder llevártelos en caso de una evacuación urgente.

- Ten en cuenta que en caso de confrontación con un posible intruso, los trabajadores de la oficina están en primera línea. Asegúrate de que reciben en todo momento la suficiente formación y apoyo sobre cómo actuar en cada situación sin ponerse a sí mismos en una situación de riesgo.

Inspecciones regulares de seguridad en la oficina

La supervisión o inspección regular de la seguridad de la oficina es de gran importancia, porque las situaciones y procedimientos de seguridad varían con el tiempo, como por ejemplo, cuando se deteriora el material o cuando hay una gran circulación de personal. También es importante que los empleados adopten un cierto sentido de apropiamiento de las reglas de seguridad de la oficina.

La persona responsable de la seguridad deberá llevar a cabo por lo menos una revisión de seguridad de la oficina **cada seis meses**. Con la ayuda de la siguiente lista tan sólo le llevará una o dos horas. La persona responsable de la seguridad debe asegurarse de obtener la opinión del personal antes de escribir el informe final, y presentar entonces el informe de seguridad a la organización para que se tomen las decisiones y la acción correspondientes. Seguidamente, el informe debería ser archivado hasta la próxima revisión de seguridad.

LISTA DE REVISIÓN DE LA SEGURIDAD EN LA OFICINA

REVISIÓN DE:
REALIZADA POR:
FECHA:

1 ◆ **CONTACTOS DE EMERGENCIA:**

- ¿Tienes una lista actualizada con los números de teléfono y direcciones de otras ONGs locales, hospitales de emergencia, policía, bomberos y ambulancia a mano?

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

- Comprueba el estado y el funcionamiento de las verjas/vallas, puertas que dan al edificio, ventanas, paredes y tejado.
- Comprueba el estado y funcionamiento de la iluminación externa, cámaras o vídeo-interfonos de la entrada.
- Comprueba los procedimientos de las llaves, incluyendo las llaves que están bajo seguridad y etiquetadas en código, asignación de responsabilidad para controlar las llaves y sus copias, y que éstas funcionen correctamente. Asegúrate de que se cambien los cerrojos cuando se pierdan o sean robadas las llaves, y que dichos incidentes sean registrados.

3 ◆ **PROCEDIMIENTOS DE ACCESO DE LAS VISITAS Y "FILTROS":**

- ¿Están activados los procedimientos de acceso para todo tipo de visitantes? ¿Están los empleados familiarizados con ellos?
- Revisa todos los incidentes de seguridad registrados relacionados con los procedimientos de ingreso o "filtros".
- Pregunta a los empleados que suelen encargarse de los procedimientos de acceso si éstos funcionan correctamente, y qué mejoras son necesarias.

4 ◆ **SEGURIDAD EN CASO DE ACCIDENTES:**

- Comprueba el estado de los extintores contra incendios, de las válvulas/cañerías de gas y grifos de agua, de las conexiones eléctricas y cables y generadores de electricidad (si corresponde).

5 ◆ **RESPONSABILIDAD Y FORMACIÓN:**

- ¿Se ha asignado la responsabilidad de la oficina? ¿Es efectiva?
- ¿Existe algún programa de formación sobre la seguridad de oficina? ¿Cubre todas las áreas mencionadas en esta revisión? ¿Todos los empleados han sido formados? ¿Es la formación efectiva?

CAPÍTULO 10

La seguridad y las mujeres defensoras de los derechos hunamos

Objetivo:

Estudiar las necesidades de seguridad específicas de las mujeres defensoras de los derechos humanos.

Seguidamente trataremos de cubrir algunos aspectos básicos sobre las necesidades específicas a las mujeres defensoras de los derechos humanos. Este es un tema que requerirá un análisis más profundo basado en las experiencias de mujeres defensoras de los derechos humanos. Esperamos que se produzcan contenidos más detallados sobre este tema en el contexto de la Conferencia Internacional de Mujeres Defensoras de los Derechos Humanos en 2005.

Mujeres defensoras de los derechos humanos

Las mujeres siempre han jugado un papel importante en la promoción y protección de los derechos humanos, aunque, este papel no siempre ha sido reconocido positivamente. Las mujeres trabajan solas o junto a hombres en la defensa de los derechos humanos[1]. Muchas mujeres pertenecen a organizaciones que trabajan para los desaparecidos y los presos. Otras defienden los derechos de los grupos minoritarios o de las víctimas de la violencia sexual, y otras son sindicalistas, abogadas o hacen campaña por el derecho a la propiedad de la tierra.

Ataques a mujeres defensoras de los derechos humanos

En su **Informe anual del 2002 a la Comisión de Derechos Humanos** Hina Jilani, Representante Especial del Secretario General de la ONU para Defensores de los Derechos Humanos afirma:

> Las mujeres defensoras de los derechos humanos están en igualdad con sus homólogos masculinos al situarse en la primera línea de la promoción y protección de los derechos humanos. Sin embargo, en su actuación, como mujeres, se enfrentan a riesgos específicos para su género que se suman a aquéllos a los que se enfrentan los hombres.

[1] Encontraréis una guía muy práctica sobre mujeres defensores de los derechos humanos en la página web de UNHCHR en http://www.unhchr.ch/defenders/tiwomen.htm Véase también el Informe: Debate sobre las Mujeres DDHs con la Representante Especial del Secretario General de la ONU para los Defensores de los Derechos Humanos, 4-6 abril de 2003, Publicado por Asia Pacific Forum on Women, Law and Development, and Essential actors of our time. Los defensores de los derechos humanos en las Américas, de Amnistía Internacional.

En primer lugar, como mujeres, resultan más visibles. Es decir, las mujeres defensoras pueden despertar una mayor hostilidad que sus colegas masculinos porque como mujeres defensoras de los derechos humanos pueden chocar con las normas culturales, religiosas o sociales sobre la feminidad y el papel de la mujer de un país o sociedad en particular. En este contexto, no sólo deben afrontar violaciones de los derechos humanos debido a su labor como defensoras de los derechos humanos, sino aún más todavía a causa de su género y el hecho de que su labor puede oponerse a estereotipos sociales sobre la naturaleza sumisa de las mujeres, o desafiar los conceptos de la sociedad sobre la condición de las mujeres.

En segundo lugar, no resulta improbable que la hostilidad, acoso y represión a la que se enfrentan las mujeres defensoras pueda por sí misma tomar una forma específica basada en el género, que va, por ejemplo, desde el abuso verbal dirigido exclusivamente a las mujeres por su género hasta el acoso sexual y la violación.

A este respecto, la integridad profesional de las mujeres y su posición en la sociedad puede verse amenazada y desacreditada en formas que son específicas para ellas, tales como los tan conocidos pretextos que cuestionan su probidad cuando – por ejemplo – reivindican su derecho a una salud sexual y reproductiva, o a la igualdad con los hombres, que incluya una vida libre de discriminación y violencia. En este contexto, por ejemplo, las mujeres defensoras de los derechos humanos han sido juzgadas haciendo uso de leyes que penalizan una conducta que viene a ser el legítimo uso y ejercicio de unos derechos protegidos bajo la ley internacional, basándose en cargos falsos presentados en su contra basadas en sus opiniones y labor de apoyo en la defensa de los derechos de las mujeres.

En tercer lugar, los abusos a los derechos humanos perpetrados contra mujeres defensoras de los derechos humanos pueden, a su vez, tener repercusiones que están, de por sí basadas en el género. Por ejemplo, el abuso sexual de una mujer defensora de los derechos humanos bajo custodia y su violación puede representar un embarazo y enfermedades de transmisión sexual, incluyendo el VIH/SIDA.

Algunos derechos específicos de mujeres vienen casi exclusivamente promovidos y protegidos por mujeres defensoras de los derechos humanos. Promover y proteger los derechos de las mujeres puede ser un factor de riesgo adicional, ya que la reafirmación de tales derechos está considerada como una amenaza al patriarcado y como trastornador de tradiciones culturales, religiosas y sociales. La defensa de los derechos de la mujer a la vida y libertad en algunos países ha resultado en la violación de la vida y libertad de las propias defensoras. Del mismo modo, protestas contra prácticas discriminatorias han resultado en una acción judicial contra una destacada defensora de los derechos humanos de la mujer acusada de apostasía.

Factores tales como la edad, la etnia, la educación, la orientación sexual y el estado civil deben también ser tomados en consideración, ya que los diferentes grupos de mujeres defensoras se enfrentan a muchos desafíos diferentes y por lo tanto tienen diferentes necesidades de protección y seguridad.
La evaluación de las necesidades de protección de las mujeres defensoras ayudará a aclarar las específicas y a menudo diversas necesidades, vulnerabilidades y estrategias de resistencia de las mujeres defensoras. De esta forma, sus situaciones podrán ser atendidas más adecuadamente en situaciones de emergencia y en su día a día.

La seguridad de las mujeres defensoras de los derechos humanos.

Las mujeres defensoras de los derechos humanos pagan un elevado precio por su labor de protección y promoción de los derechos humanos de otra gente. Las defensoras tienen que enfrentarse a riesgos que están relacionados con su género, y su seguridad por lo tanto requiere una atención específica. Veamos una lista de las posibles situaciones:

Las mujeres podrían atraer una atención no deseada.

Las mujeres defensoras podrían provocar hostilidad porque el ser mujer y defensor de los derechos humanos podría desafiar las normas locales culturales, religiosas o sociales sobre la feminidad y el papel de la mujer.

Las mujeres defensoras pueden tener que infringir leyes patriarcales y tabúes sociales.

En algunos países, la defensa de los derechos de las mujeres a la vida y la libertad ha resultado en la violación de las vidas y las libertades de las propias defensoras. En muchas culturas, la exigencia de que la mujer muestre respeto al hombre en público puede suponer un obstáculo para las mujeres que cuestionan públicamente actos cometidos por hombres que violan los derechos humanos. A menudo se recurre también a ciertas interpretaciones discriminatorias o sexistas de textos religiosos al formular leyes o establecer prácticas que tendrán una importante influencia en los derechos de la mujer.

Existen formas de ataque específicas contra mujeres defensoras.

La hostilidad, acoso y represión a los que se enfrentan las mujeres defensoras podrían ser específicas al género, y representan desde abusos verbales dirigidos exclusivamente a ellas hasta el acoso sexual y la violación. Las consecuencias de dichos ataques pueden ser también específicos al género, tales como un embarazo y un rechazo social.

Las mujeres defensoras pueden sentirse forzadas a "demostrar" su integridad:

La profesionalidad y posición social de las mujer pueden verse amenazados y desacreditados en formas específicas para ellas, tales como la puesta en duda de su integridad.

Los hombres defensores podrían no comprender, o incluso rechazar el trabajo de las mujeres defensoras:

Los colegas masculinos de las mujeres defensoras de los derechos humanos pueden tener los mismos prejuicios sociales que los mismos hombres que atacan a las mujeres defensoras. Los hombres también podrían sentirse amenazados por la competencia profesional de una mujer. Esto puede conllevar intentos de marginación o debilitación de las mujeres defensoras de los derechos humanos y en algunos casos puede trascender a situaciones de acoso y violencia contra las defensoras perpetradas por sus colegas.

Las mujeres defensoras pueden ser víctimas de la violencia doméstica:

La violencia doméstica puede estar vinculada al cambio de las estructuras de poder en una familia. El ascenso del papel profesional y de la atribución de poder de una defensora podría hacer que su marido, compañero u otros familiares se sintieran amenazados e intentaran frenar sus actividades o actuara de forma violenta. La violencia doméstica contra mujeres incluye todo daño físico, sexual y psicológico que ocurra en el seno familiar, como una paliza, violación marital, mutilación genital femenina y otras prácticas tradicionales que sean dañinas para las mujeres (véase abajo).

Obligaciones familiares adicionales:

Muchas mujeres defensoras, aparte de su labor tienen también a su cargo el cuidado de los niños y otros parientes. Tales responsabilidades, especialmente si incluye niños pequeños, influirá en muchas de las decisiones de seguridad que la defensora deberá tomar en una situación de alto riesgo.

Hacia a una mejor seguridad y protección para las mujeres defensoras de los derechos humanos

Es importante reconocer que las mujeres defensoras constituyen una gran variedad de mujeres enfrentadas a diferentes problemas, con diferentes antecedentes y que requieren diferentes soluciones. El punto más importante a tener en cuenta es que, en cualquier situación determinada, las mujeres son defensoras de los derechos humanos que pueden identificar problemas y encontrar soluciones apropiadas. Para que así sea, es necesaria una mayor participación de las mujeres, un adecuado enfoque en cuestiones de seguridad específicas para el género y una formación adecuada cuando sea necesario.

Una participación mayoritaria de mujeres

En pocas palabras, esto significa Asegurar una mayor participación de mujeres junto a hombres en la toma de decisiones, poniendo las cuestiones de seguridad de las mujeres en la agenda, y situando a las mujeres en igualdad con los hombres en la toma de medidas de seguridad. Es importante incluir las experiencias y opiniones de las mujeres y asegurarse de que las mujeres definan normas y procedimientos de seguridad, al igual que observar su desarrollo y evaluarlos.

Asegurarse de tratar las necesidades de seguridad y protección específicas de género.

Al igual que con otras necesidades de seguridad, es muy importante en toda organización o grupo defensor asignar responsabilidades para tratar con la violencia de género y con los riesgos de seguridad de las defensoras. Las personas responsables de la seguridad deberán tener un buen conocimiento de las necesidades específicas de las mujeres defensoras. En ocasiones quizás sea necesario asignar a otra persona que pueda aportar un conocimiento y percepción específicos para esto. Por ejemplo, una persona podría ser responsable de la seguridad, pero la organización decide más tarde designar a otra persona con experiencia práctica y teórica para manejar la violencia de género. En este caso, ambas personas deberían trabajar conjuntamente para asegurar que todos los procedimientos de seguridad funcionen sin dificultad y respondan a las diferentes necesidades de la gente.

Formación

La formación de todas las personas que trabajan en una organización de derechos humanos es un elemento clave para mejorar la seguridad y protección y debería incluir el generar conciencia sobre las necesidades específicas de las mujeres defensoras.

Como comentario adicional, La violencia de género recibe **insuficiente atención**. La conciencia general sobre la violencia de género en la organización o grupo puede ayudar a que la gente hable sobre amenazas o incidentes de género específicos. Los trabajadores dispuestos a colaborar pueden también actuar como "puntos de acceso" para que mujeres y hombres que quiera buscar soluciones a las amenazas o violencia vinculados al género contra ellos u otras personas pertenecientes a la organización o comunidad.

En resumen,

Las diferencias en las necesidades de seguridad de las mujeres están relacionadas a los diferentes papeles, los diferentes tipos de amenazas y a las diferentes situaciones (tales como la detención, el trabajo de campo, etc.). El propósito es poder desarrollar respuestas sensibles a la violencia de género contra las mujeres y demás defensoras.

Agresiones sexuales y seguridad personal

La prevención de la agresión sexual es similar a la de los demás ataques, sobre todo a aquéllos asociados con el crimen común. Los ataques sexuales pueden ser usados para reprimir al defensor o defensora, y las víctimas pueden ser o bien elegidas o bien agredidas aprovechando una situación oportunista.

Todas las personas – hombres o mujeres - son víctimas potenciales de una agresión sexual, pero las mujeres suelen ser un blanco más frecuente. La agresión sexual es un crimen de poder y violencia, y el contacto sexual es un método más del atacante para demostrar su poder sobre la víctima.

Recordemos que en muchos casos las mujeres que son llevadas consigo por un potencial atacante son violades (y reciben palizas o incluso se les asesina): Por lo tanto las mujeres deberían tomar la decisión firme y rotunda de no desplazarse con un presunto atacante a otra ubicación (a no ser que su rechazo pudiera poner en peligro su vida o la de otros)

Reacción ante una agresión sexual[2]

Las opciones de respuesta en el momento de una agresión sexual son limitadas y dependerán estrictamente de la víctima. No existe una reacción "correcta" o "equivocada". En todo caso, el objetivo primordial es sobrevivir. Las opciones disponibles para la víctima en el momento de una agresión sexual pueden incluir lo siguiente:

1 ◆ **Ceder:** Si la víctima teme por su vida, tal vez escoja someterse a la agresión sexual.

2 ◆ **Resistencia pasiva:** Hacer o decir cualquier cosa desagradable o repugnante para arruinar el deseo de contacto sexual del atacante. Se puede decir que se tiene el SIDA, diarrea, provocarse el vómito, etc.

3 ◆ **Resistencia activa:** Utilizar toda la fuerza posible para deshacerse del atacante, como golpear, dar patadas, morder, arañar, gritar y escaparse.

En cualquier caso, hay que hacer lo que se tenga que hacer para sobrevivir. "Sigue tus instintos". Nadie sabe cómo reaccionará en una situación como ésta y tu reacción será la apropiada para ti y tu situación en concreto.

Tras una agresión sexual

Todas las organizaciones y grupos defensores de los derechos humanos deberían disponer de planes de prevención y reacción en marcha para agresiones sexuales. El plan de reacción debería incluir, como mínimo, el suministro de una **asistencia sanitaria efectiva, que incluya una asistencia psicológica**, (pruebas de análisis inmediatos y regulares de enfermedades de transmisión sexual, la píldora del día siguiente, etc.) y **una asistencia jurídica**.

Es necesario encontrar un justo equilibrio entre asegurarse de que la víctima obtenga el apoyo de especialistas y asegurar el apoyo y la reacción apropiada por parte de la organización.

Véase también Prevención y reacción a los ataques en el Capítulo 5.

[13] La mayor parte de esta información ha sido adaptada del libro Van Brabant: Operational Security in Violent Environments y de los Manuales de Seguridad de World Vision y World Council of Churches.

LA DECLARACIÓN SOBRE LA ELIMINACIÓN DE LA VIOLENCIA CONTRA LA MUJER (1993) DEFINE LA VIOLENCIA CONTRA LA MUJER COMO:

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 1)

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. (Artículo 2)

La seguridad en zonas de conflicto armado

Objetivo:

Reducir los riesgos inherentes a las zonas de conflicto armado.

El riesgo en situaciones de conflicto

Los defensores de los derechos humanos que trabajan en zonas de conflicto están expuestos a unos riesgos específicos, sobre todo en las situaciones de conflicto armado: Muchos de los asesinatos de civiles son debidos a las prácticas indiscriminadas de la guerra, pero muchos otros son el resultado de que los civiles se convierten en objetivos militares directos, y es necesario que reconozcamos estos hechos como tales: la acción política es siempre necesaria para señalar estos hechos e intentar detenerlos.

Es difícil ejercer algún tipo de control sobre una acción militar en marcha, pero puedes adaptar tu conducta para evitar que el conflicto te afecte o para reaccionar apropiadamente si ocurre algo.

Si estás ubicado en una zona donde las acciones armadas son frecuentes, seguramente ya habrás establecido muchos de los contactos necesarios para protegeros a ti, a tu familia y a la gente con la que trabajas al mismo tiempo que prosigues con tu labor.

Sin embargo, si no estás ubicado en la zona de conflicto armado donde trabajas, debes **considerar tres puntos desde un principio**:

a ◆ Qué grado de riesgo estás preparado a asumir? Esto también es aplicable a la organización/personas con la/s que trabajas.

b ◆ Tu presencia en la zona, ¿aporta mayores ventajas que riesgos? La labor de derechos humanos no puede mantenerse a largo plazo cuando equivale a estar continuamente expuesto a un riesgo elevado.

c ◆ El simple hecho de "conocer la zona" o "saber mucho sobre armas" no te ofrecerá ninguna protección de los disparos o de un ataque con morteros o de francotiradores.

Tipos de fuego

Puedes estar expuesto al fuego de rifles, ametralladoras, morteros, bombas y misiles de tierra, aire o mar. El fuego puede estar más o menos orientado, y comprende desde un francotirador o un helicóptero con buena visibilidad hasta morteros o artillería. El fuego también puede ser de la variedad de "saturación", dirigido a "barrer" una zona entera.
Mientras más dirigido esté el fuego, menor será el riesgo que corras – siempre y cuando el fuego no vaya dirigido a ti, a tu zona en general o a una zona vecina, en estos casos el riesgo disminuye si puedes retirarte. **En cualquier caso, recuerda que si te encuentras en la línea de fuego, resultará difícil determinar si va dirigido a ti. Establecer si va dirigido a ti no es una prioridad**, tal y como veremos más abajo.

Tomar precauciones: Reducir tu vulnerabilidad al fuego.

1 ◆ **Evita los lugares peligrosos.**

En una zona de combate o de acción terrorista, evita ubicarte (tener una oficina o permanecer durante un largo periodo) cerca de un posible blanco, como una guarnición o una instalación de telecomunicaciones. Esto también es aplicable a las zonas estratégicas como las entradas y salidas de las zonas urbanas, los aeropuertos o los puntos estratégicos que controlan la zona circundante.

2 ◆ **Busca protección adecuada del ataque.**

Una de las principales causas de heridas son los cristales que salen disparados de las ventanas cercanas. Cubriendo las ventanas con tablas o con cinta adhesiva reducirás el riesgo de que esto ocurra. En caso de ataque, aléjate de las ventanas y busca una protección inmediata en el suelo, bajo una mesa, preferiblemente en una habitación central con paredes gruesas, o, mejor todavía, en un sótano.
Los sacos de arena pueden resultar prácticos, pero sólo si los demás edificios también están equipados con ellos – si no, corres el riesgo de llamar una atención innecesaria.
Si no hay nada más disponible, el suelo o cualquier concavidad en éste pueden ofrecerte al menos una protección parcial.
Un simple muro de ladrillos o la puerta de un coche no pueden protegerte de un rifle o de armas de fuego más pesadas. Los bombardeos y los misiles pueden matar en un radio de varios kilómetros, así que no es necesario estar muy cerca del combate para que éste te alcance.
Las explosiones de bombas o morteros pueden dañar tus oídos: Cúbrelos con ambas manos y abre un poco la boca.
La clara señalización de tus oficinas centrales, tu ubicación o tus vehículos puede ser útil, pero recuerda que **esto es únicamente aplicable si los atacantes respetan tu labor**. Si no es el caso, te estarás exponiendo innecesariamente. Si deseas ser identificado, hazlo con una bandera o con colores y señales en paredes y tejados (si existe un riesgo de ataque aéreo).

3 ◆ **Desplazamiento en vehículos.**

Si disparan directamente a tu vehículo, podrías pensar en analizar la situación, pero es muy difícil realizar una evaluación acertada en estas circunstancias. Por lo general, **es aconsejable asumir que el vehículo es o puede ser un blanco, y que la reacción apropiada es, por lo tanto, salir y ponerse a cubierto inmediatamente**. Un vehículo es un blanco perfecto. No sólo es vulnerable, sino que además del fuego directo puede causarte otras heridas con los cristales que salen disparados o la explosión de los tanques de gasolina. Si el fuego no es cercano, continúa desplazándote en el vehículo hasta que encuentres un lugar próximo donde ponerte a cubierto.

Minas y proyectiles sin detonar (Unexploded ordnance, UXO)[1]

Las minas y proyectiles sin detonar suponen una seria amenaza para los civiles en zonas de conflicto armado. Pueden tener diferentes formas:

- **Minas:**
  - Las minas antitanque suelen estar colocadas en carreteras y caminos y pueden destruir un vehículo normal.
  - Las minas anti-personas son más pequeñas y pueden encontrarse en cualquier lugar donde se supone que circula la gente. La mayoría de las minas anti-personas están enterradas en el suelo. No olvides que quienes colocan minas en una carretera podrían también minar las cunetas y los campos y los caminos próximos a la carretera.
- **Bombas trampa:**
  - Las bombas trampa son pequeños explosivos escondidos en un objeto de aspecto normal o atractivo, (con colores, por ejemplo) que explotan al tocarlos. El término también es utilizado para las minas atadas a un objeto que puede ser desplazado o activado (puede ser cualquier cosa desde un cadáver hasta un coche abandonado).
- **Proyectiles sin detonar:**
  - Hace referencia a cualquier tipo de munición que ha sido disparada pero que no ha explotado.

Prevención contra las minas y los proyectiles sin detonar.

La única forma de evitar las zonas minadas es sabiendo donde están. Si no estás ubicado ni vives en la zona, la única forma de determinar la ubicación de los campos minados es preguntando de forma continua y activa a los habitantes locales, o a los expertos, si ha habido explosiones o combates en la zona. Es aconsejable utilizar carreteras asfaltadas, o caminos transitables de uso habitual, o seguir las huellas de otros vehículos. **No salgas de la carretera, ni siquiera a la cuneta o el arcén, con o sin el vehículo**. Las minas u otra artillería sin detonar pueden permanecer escondidas y activas durante años.

[1] Gran parte de la información de esta sección ha sido adaptada del excelente manual de Koenraad van Brabant: Operational Security Management in Conflict Areas (véase la Bibliografía).

La artillería sin detonar puede encontrarse en cualquier zona donde haya habido un combate o fuego armado, y puede ser visible. La regla de oro es: No te acerques, no la toques, señala el lugar si puedes, y hazlo saber inmediatamente.

Las bombas trampa suelen encontrarse normalmente en las zonas de las que se han retirado los combatientes. En estas zonas es imperativo **no tocar ni mover nada y permanecer alejado de los edificios abandonados**.

Si una mina explota debajo de un vehículo o persona cercanos.

Existen dos reglas de oro:

- Donde hay una mina siempre hay más.
- Nunca actúes de forma impulsiva, aunque haya heridos.

Si tienes que retirarte, vuelve sobre tus pasos si éstos continúan visibles. Si viajas en un vehículo y sospechas que puede haber minas antitanques, abandona el vehículo y retírate siguiendo las huellas de las ruedas.

Si quieres acercarte a una víctima o retirarte de una zona minada, la única forma de hacerlo es arrodillándote o tumbándote e ir examinando el suelo introduciendo un pincho (un palo muy fino de madera o metal) delicadamente en la tierra en un ángulo de 30 grados, para detectar con cuidado cualquier objeto duro. Si te encuentras con un objeto duro, despeja la zona con cuidado hasta que puedas ver lo que es. Las minas también pueden estallar a través de cables atados a éstas. Si te encuentras con algún cable no lo cortes.

Todo esto, evidentemente, requerirá una cantidad de tiempo considerable[2].

2 Podéis encontrar manuales y recursos sobre la concientización y educación sobre las minas en la página Web International Campaign to Ban Ladmines: www.icbl.org (Campaña Internacional para Prohibir las Minas)

CAPÍTULO 12

La seguridad en las comunicaciones y la información tecnológica

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

Objetivo:

Los grandes vacíos de la información tecnológica presentes en todo el mundo afectan también a los defensores de los derechos humanos. Este capítulo se centra principalmente en las tecnologías de la información– es decir, los ordenadores e Internet[1]. Los defensores sin acceso a ordenadores o Internet tal vez consideren parte de su contenido irrelevante. Sin embargo, pueden necesitar obtener urgentemente los medios y la formación necesarios para el uso de las tecnologías de la información en defensa de los derechos humanos.

Manual de los problemas de seguridad en la comunicación y cómo evitarlos

El conocimiento es poder, y conociendo el origen de tus posibles problemas de comunicación, puedes sentirte más seguro al realizar tu labor. La siguiente lista resume las diferentes formas de acceso o de manipulación ilegal de tu información o de tu sistema de comunicación, y sugiere varias medidas para evitar estos problemas de seguridad.

Hablar

No es necesario que la información pase por Internet para que accedan a ella ilegalmente. Cuando discutas temas confidenciales, considera los siguientes puntos:

1 ◆ ¿Confías en la persona con la que estás hablando?

2 ◆ ¿Necesita la información que le estás dando?

3 ◆ ¿Te encuentras en un entorno seguro? A menudo se colocan micrófonos ocultos u otros dispositivos de escucha en zonas que la gente considera seguros, tales como oficinas privadas, calles con mucha circulación, habitaciones de la casa y coches.

[16] El presente capítulo está basado en el trabajo realizado por Robert Guerra, Katitza Rodríguez y Caryn Mladen de Privaterra, una ONG que trabaja por todo el mundo en la seguridad de la Información Tecnológica para los defensores de los derechos humanos ofreciendo cursos e información. En la actualidad Privaterra está realizando un manual más detallado sobre las comunicaciones electrónicas y la seguridad para Front Line que será publicado en 2005 (este texto ha sido ligeramente adaptado en algunos párrafos por Enrique Eguren).

Es difícil responder a la tercera pregunta, porque pueden haber instalado grabadoras o micrófonos ocultos en la habitación para grabar o transmitir todo lo que allí se dice. También puede haber micrófonos láser apuntando a las ventanas para escuchar las conversaciones desde una gran distancia. Las cortinas gruesas, al igual que la instalación de ventanas de doble acristalamiento, pueden protegerte en parte de los micrófonos láser. Algunos edificios seguros tienen dos juegos de ventanas en las oficinas para reducir el riesgo de los aparatos de escucha por láser.

¿Qué puedes hacer?

- **Presume siempre que hay alguien escuchando.** Una actitud de paranoia saludable, podría ayudarte a ser más cauteloso con los asuntos confidenciales.

- **Los detectores de micrófonos o rastreadores pueden detectar los aparatos de escucha**, pero pueden ser caros y difíciles de adquirir. Además, a veces los propios encargados de detectar los micrófonos son los responsables de colocarlos. Durante una barrida, podrían o bien encontrar algunos "desechables" (micrófonos ocultos baratos diseñados para ser encontrados) o curiosamente no encontrar nada y declarar tus oficinas "limpias".

- **El personal de limpieza puede representar una grave amenaza de seguridad**, porque pueden acceder a tus oficinas fuera del horario laboral y se llevan la basura consigo cada noche. Todo el personal debería ser examinado cuidadosa y regularmente por el dispositivo de seguridad, ya que podrían comprometerse una vez incorporados a tu organización.

- **Cambia las salas de reuniones tan a menudo como te sea posible.** A mayor número de habitaciones o lugares donde intercambies información, mayor número de personal y equipo serán necesarios para la escucha.

- **Sospecha de los regalos diseñados para que los lleves contigo a todas horas**, como un bolígrafo caro, un pin o un broche de solapa; o para que los utilices en tu oficina, como un bonito pisapapeles o un cuadro grande. En el pasado se ha hecho uso de este tipo de objetos para escuchar conversaciones.

- **Presume que una parte de tu información está expuesta** en todo momento. Tal vez decidas cambiar de planes y códigos a menudo, ofreciendo a tus oyentes sólo fragmentos de la información verídica. Podrías entregar información falsa para comprobar si alguien hace uso o responde a ella.

- Para minimizar la efectividad de los micrófonos láser, **discute los asuntos confidenciales en un sótano o en una habitación sin ventanas**. Las tormentas u otros cambios climáticos pueden reducir la efectividad de algunos dispositivos de escucha.

- **Pon una grabación de ruido blanco o una canción popular** de fondo para que interfieran en la recepción del sonido. Sólo la alta tecnología puede filtrar los ruidos sobrepuestos a una conversación.

- **Los espacios abiertos pueden resultar tan prácticos como nocivos.** Si te reúnes en un lugar aislado te resultará más fácil comprobar si alguien te sigue u observa, pero te será imposible esconderte entre la gente y escapar. Las muchedumbres pueden ayudarnos a pasar inadvertidos pero también es mucho más fácil ser visto y oído en ellas.

Teléfonos móviles

Si el oyente posee una buena capacidad tecnológica podrá escuchar todo tipo de llamadas telefónicas. Ningún tipo de llamada puede considerarse segura. Los teléfonos móviles digitales son más seguros que los teléfonos móviles analógicos y las líneas fijas son más seguras todavía.

La vigilancia celular puede detectar tu ubicación y tus conversaciones. Para dar con tu paradero no es necesario que estés hablando - con que tengas el teléfono móvil encendido ya es suficiente.

No guardes información confidencial como nombres y números de teléfono en la memoria de tu teléfono. Si te lo robaran, dicha información podría ayudarles a localizar y comprometer a la gente que quieres proteger.

La seguridad del material de información de la oficina

Mantén la oficina cerrada a todas horas, incluyendo puertas y ventanas. Utiliza llaves que requieran una autorización específica para hacer una copia y no pierdas de vista ninguna de las copias. NO des llaves a terceros, ni siquiera al personal de limpieza o de mantenimiento, y asegúrate de que tú o alguien de confianza esté siempre presente cuando haya personas ajenas en la oficina. Si esto no es posible, asegúrate de disponer de una habitación con acceso limitado para guardar los archivos confidenciales. Procura cerrar con llave todas las puertas de la oficina y al finalizar el día deja todos los residuos no-confidenciales en el pasillo.

Utiliza una trituradora de papel para todos los documentos confidenciales. Las tiras de papel trituradas son casi completamente inservibles. Si quieres deshacerte de un material extremadamente confidencial, puedes quemar los desechos, pulverizar las cenizas y tirarlas por el baño.

Seguridad básica de ordenadores y archivos[2]

Si es posible procura guardar los ordenadores bajo llave al salir de la oficina. Aparta las pantallas de los ordenadores de las ventanas.

Utiliza un protector de sobrecarga para todas las tomas de corriente (las variaciones de la corriente eléctrica pueden dañar tu ordenador).

Guarda las copias de seguridad, incluyendo los archivos de papel, en un lugar seguro y apartado. Asegúrate de que las copias de seguridad estén protegidas guardándolas en un disco duro encriptado con datos seguros de la organización, o protegido con sofisticados cerrojos.

Para reducir el riesgo de acceso a tu ordenador protégelo con una frase de pase y apágalo siempre que lo abandones.

Encripta tus archivos por si acaso alguien consiguiera acceder a tu ordenador o averiguar la frase de pase.

2 Si deseas una información más detallada sobre la seguridad de ordenadores consulta a Front Line en info@frontlinedefenders.org o a Privaterra en info@privaterra.org

Crea copias de seguridad diariamente por seguridad y para poder recuperar tus archivos en caso de que te roben o destruyan el ordenador. Mantén los documentos de seguridad encriptados lejos de tu oficina en un lugar seguro.

Los archivos borrados no podrán ser reconstruidos si utilizas el PGP Wipe u otro programa de utilidades, en vez de eliminarlos o colocarlos simplemente en la papelera de reciclado del ordenador.

Tu ordenador puede ser programado sin que te des cuenta para enviar tus archivos fuera o para dejarte indefenso. Para evitar esto, adquiere tu ordenador de una fuente segura, allana el ordenador (es decir, reformatea el disco duro) al estrenarlo, e instálale únicamente el software que necesites. Permite sólo a los técnicos de confianza que se ocupen del mantenimiento de tu ordenador y obsérvalos en todo momento.

Desconecta el módem/conexión telefónica de tu ordenador, o sino desconéctate de Internet, cuando vayas a dejar el ordenador desatendido. De esta forma, los programas maliciosos que llamen en mitad de la noche no funcionarán. Nunca dejes tu ordenador conectado si piensas pasar el día fuera. Procura instalar un software que invalide el acceso tras un tiempo determinado de inactividad. De esta manera, tu ordenador no estará expuesto mientras te tomes un café o hagas unas fotocopias.

En tus preferencias de Internet, activa las extensiones de archivos para saber qué tipo de archivo es antes de abrirlo. Podrías atrapar un virus si abres un archivo ejecutable creyendo que era un archivo de texto. Si utilizas Internet Explorer, haz clic en el Panel de control de tu ordenador y después en Opciones de carpeta. Haz clic en Ver y comprueba que el cuadro de Ocultar las extensiones de archivo para tipos de archivo conocidos NO esté activado.

Problemas de seguridad con Internet

Tu correo electrónico no pasa directamente de tu ordenador al ordenador del destinatario, sino que pasa por varios nodos y va dejando información en el recorrido. **Se puede acceder a tu correo desde cualquier parte del recorrido (¡no sólo desde tu país!)**

Alguien podría estar mirando por encima de tu hombro mientras tecleas. Esto es particularmente problemático en los Internet cafés. Si estás conectado a una red, todo el mundo en la oficina tiene acceso a tu correo electrónico. Tu sistema administrativo puede tener unos privilegios administrativos especiales para acceder a todos los correos electrónicos.

Tu proveedor del servicio de Internet (ISP) tiene acceso a tus correos electrónicos, y cualquier persona con influencia sobre tu ISP podría presionarlo para conseguir que le remita copias de todos tus correos electrónicos o para impedir que pasen ciertos correos electrónicos.

Al pasar por Internet, tus correos electrónicos recorren cientos de sitios inseguros. Los piratas informáticos pueden acceder a los mensajes de correo electrónico mientras transitan. El ISP de tu destinatario también puede ser vulnerable, al igual que su red y su oficina.

Seguridad de Internet básica

Los virus y otros problemas, tales como los Caballos de Troya o los Troyanos, pueden proceder de cualquier parte; incluso tus amigos pueden propagarte un virus sin saberlo. Utiliza un buen programa anti-virus y mantenlo actualizado con conexiones automáticas a la Web. Constantemente se crean y descubren virus

nuevos, así que consulta la Biblioteca de Información sobre Virus en www.vil.nai.com para saber lo último sobre los parches de protección.

Los virus suelen ser propagados a través del correo electrónico, así que procura hacer un uso seguro del correo electrónico (véase abajo). Los virus son programas únicos diseñados para replicar y podrían o no ser nocivos. Los Troyanos son unos programas diseñados para ofrecer el acceso de tu ordenador a terceros (¡o a cualquiera!).

Un buen cortafuegos puede ayudarte a pasar desapercibido ante los piratas informáticos y mantener alejados a los intrusos que intenten acceder a tu sistema. De esta forma desde tu ordenador sólo podrán conectarse a Internet las aplicaciones autorizadas e impide también que programas como el de los Troyanos te envíen información o abran las "puertas traseras" de tu ordenador para dejar pasar a los piratas informáticos.

El sistema de "key logger" puede localizar cada tecla que pulses. Estos programas pueden ser instalados o bien accediendo a tu ordenador en tu ausencia, o a través de un virus o un Troyano que ataca tu sistema desde Internet. Los Key loggers localizan las pulsaciones de tu teclado e informan de tus actividades, normalmente por Internet. Se les puede derrotar utilizando una frase de pase para proteger tu ordenador, haciendo uso del correo electrónico de forma segura, utilizando un programa anti-virus, y un programa para teclear tu contraseña con el ratón. También se puede incapacitar a los Key loggers desconectando físicamente el ordenador del acceso a Internet - normalmente sólo necesitas desenchufar la conexión telefónica del ordenador – cuando no lo estés utilizando.

La dirección de correo electrónico puede ser "spoofed" (manipulada/falsificada) o utilizada por una persona que no es el propietario real. El pirata informático puede conseguir esto accediendo al proveedor de servicios de Internet del ordenador de esa persona y obteniendo el acceso y su contraseña, o utilizando una dirección casi idéntica. Por ejemplo, si intercambiamos la "l" minúscula por el número "1", obtendremos una dirección muy parecida y casi nadie notará la diferencia. Para evitar ser engañado por un spoof, escribe frases coherentes en la línea de Asunto y formula preguntas periódicamente que sólo la persona en cuestión pueda responder. Confirma toda solicitud de información por medio de otro sistema de comunicación.

Mantén la privacidad de tu actividad de navegación no aceptando cookies y eliminando tu caché cada vez que termines de navegar en la web. En Internet Explorer, haz clic en Herramientas, y luego en Opciones. En Netscape Navigator, haz clic en Edición, y luego en Preferencias. Una vez dentro de cualquiera de estos menús borra todo tu historial, todas las cookies que puedas tener y vacía tu caché. Recuerda borrar también todos tus marcadores. Los navegadores también archivan las páginas Web que has visitado en ficheros de caché, así que averigua qué ficheros deberían ser borrados de tu sistema.

Actualiza todos los navegadores de Internet para que adopten una encripción de 128-bits. Esto te ayudará a proteger cualquier información que quieras enviar a través de Internet, incluyendo contraseñas y otros datos confidenciales recogidos en formularios. Instala los parches de seguridad más actuales en todo el software que utilices, sobre todo en Microsoft Office, Microsoft Internet Explorer y Netscape. No utilices un ordenador que contenga información confidencial para conexiones a Internet no esenciales.

Seguridad básica del correo electrónico

Existen métodos seguros de utilizar el correo electrónico que tú y tus amigos y asociados deberíais poner en práctica. Informa a tus amigos y asociados de que no abrirás sus mensajes a no ser que practiquen una correspondencia electrónico segura.

1 ◆ NUNCA abras un mensaje de un desconocido.

2 ◆ NUNCA reenvíes un mensaje de un desconocido, o originado por un desconocido. Todos esos mensajes de "Ten pensamientos felices" que la gente se envía pueden contener virus. Al enviárselos a tus amigos y asociados podrías infectar sus ordenadores. Si tanto te gusta el texto, rescríbelo y envíalo tú mismo. Si no merece la pena perder el tiempo reescribiéndolo, es señal de que no era tan importante.

3 ◆ NUNCA descargues o abras un archivo adjunto sin saber qué contiene y si es seguro. Desconecta las opciones de descarga automática de tu programa de correo electrónico. Muchos virus o Troyanos se autopropagan en forma de "gusanos" y los gusanos modernos suelen ser enviados por un conocido. Los gusanos inteligentes escanean tu agenda de direcciones, sobretodo si utilizas Microsoft Outlook o Outlook Express, y la replican haciéndose pasar por archivos adjuntos legítimos de contactos legítimos. Si haces que el PGP firme tu correo electrónico, con o sin archivos adjuntos, reducirás en gran parte la confusión sobre los archivos adjuntos sin virus que puedas enviar a tus compañeros (PGP es un software diseñado para encriptar información, véase más abajo en "Encripción")

4 ◆ NO utilices HTML, MIME o un formato de texto enriquecido en tu correo electrónico - únicamente un texto normal. Los correos electrónicos enriquecidos pueden contener programas incorporados que permiten el acceso o dañan los archivos de tu ordenador.

5 ◆ Si utilizas Outlook ó Outlook Express, desconecta la opción de vista previa de la pantalla.

6 ◆ Codifica tu correo electrónico siempre que puedas. Un correo electrónico sin encriptar es como una postal que puede ser leída por todo aquél que la ve o que tiene acceso a ella. Un correo electrónico encriptado es como una carta en un sobre dentro de una caja fuerte.

7 ◆ Titula tus mensajes con frases significativas para que el destinatario te reconozca. Pide a todos tus amigos y colegas que hagan siempre un comentario personal en la línea de Asunto para asegurarte de que son realmente ellos quienes te envían el mensaje. Sino alguien podría estar practicando spoofing con ellos, o un Troyano podría haber enviado un programa infectado a toda su agenda de direcciones, incluyéndote a ti. Sin embargo, no utilices las líneas de Asunto para revelar información confidencial de mensajes encriptados. No olvides que la línea de Asunto no está encriptada y podría revelar el tema del mensaje encriptado, lo que puede desencadenar ataques. En la actualidad hay muchos programas de piratas informáticos que escanean y copian mensajes de correo electrónico con títulos "interesantes" como "informe", "confidencial", "privado" y demás para indicar que el mensaje es de interés.

8 ◆ NUNCA envíes un mail a un gran grupo utilizando las líneas "Para" o "CC". Envíate el mensaje a ti mismo e incluye el nombre de los demás en las líneas de "bcc". Esto es por pura cortesía al igual que una buena

práctica de privacidad. Sino, estarás enviando MI dirección a gente que no conozco, una práctica que es maleducada, ofensiva y probablemente igual de frustrante que peligrosa.

9 ◆ NUNCA contestes al correo basura, incluso a las proposiciones de borrarles de la lista. Los servidores de spam envían mensajes a grandes cantidades de direcciones y nunca saben cuáles están "activas" - es decir que la dirección de correo electrónico está siendo utilizada activamente. Al responder, el servidor te reconoce como una cuenta "activa" y consiguientemente te envía más correo basura.

10 ◆ Si es posible, mantén un ordenador separado, que no esté conectado a ningún otro y que no contenga ningún archivo de datos, para la correspondencia electrónica general.

Encriptación: Preguntas y Respuestas

Seguidamente encontrarás una lista con las preguntas y respuestas más frecuentes. Para cualquier consulta no dudes en contactar a la ONG Privaterra en www.privaterra.org

P: ¿Qué es la encriptación?

R: Encriptar significa transformar datos en un código secreto que puede ser descifrado únicamente por la parte interesada. Contando con el tiempo y el poder informático suficientes, todos los mensajes encriptados pueden ser descodificados, pero es necesario invertir enormes cantidades de tiempo y recursos. Para simplificar, la encriptación es una forma de esconder tus archivos y correo electrónico de la vista de los espías. Tus archivos se traducen a un código – aparentemente una colección de números y letras escogidos al azar – que no guardan sentido alguno para quien lo vea. Para encriptar un archivo, lo "bloqueas" con una tecla, que representa una frase de pase. Para encriptar un mensaje, lo bloqueas con un par de teclas utilizando tu frase de paso. Sólo podrá abrirlo su destinatario, utilizando su propia frase de pase.

P: ¿Por qué los grupos de derechos humanos deberían utilizar la encriptación?

R: Todo el mundo debería utilizar la encriptación, porque las comunicaciones digitales son intrínsicamente inseguras. Sin embargo, los trabajadores de derechos humanos corren un mayor riesgo que la mayoría de la gente y sus archivos y comunicaciones son más confidenciales. Es fundamental que los trabajadores de derechos humanos utilicen la encriptación para protegerse a sí mismos y a la gente que intentan ayudar. La tecnología digital representa una ventaja para los grupos de derechos humanos, ya que les otorga una comunicación más fácil, una mayor eficacia y más oportunidades. Sin embargo, toda ventaja conlleva ciertos peligros. El simple hecho de ponerse un cinturón de seguridad no significa que vayas a tener un accidente cada vez que conduzcas. Cuando conduces en una situación más peligrosa, como en una competición, eres más propenso a utilizar el cinturón de seguridad, simplemente por seguridad. Los trabajadores de derechos humanos son conocidos blancos de vigilancia. Desde que es posible acceder y leer los correos electrónicos encriptados con cierta facilidad, resulta casi inevitable que tus mensajes encriptados sean interceptados en algún momento. De hecho, tal vez tu correo ya haya sido interceptado por tus oponentes y tú nunca lo sepas. Los adversarios de la gente que ayudas con tu labor también son tus adversarios.

P: ¿Es el uso de la encriptación ilegal?

R: A veces. En la mayoría de los países del mundo el uso de la encriptación es completamente legal. Sin embargo, existen excepciones. En China, por ejemplo, las organizaciones deben solicitar un permiso para utilizar la encriptación, y cualquier programa de encriptación de tu ordenador portátil debe ser declarado al entrar en el país. Singapur y Malasia tienen leyes que exigen que toda persona que desee utilizar la encriptación notifique sus claves privadas. En India se está tramitando una ley parecida. También existen otras excepciones. El Centro de Información Electrónica Privada (EPIC) expone un Informe Internacional sobre la Política de Encriptación (International Survey of Encryption Policy) que examina las leyes de la mayoría de los países en http://www2.epic.org/reports/crypto2000/. Su última actualización es del 2000. Si te preocupa, antes de utilizar una encriptación en un país en concreto consúltalo con Privaterra.

P: ¿Qué necesitamos para mantener nuestros sistemas de Tecnología Informática (TI) seguros?

R: Depende de tu sistema y de tus actividades, pero por lo general todo el mundo debería tener:

- Un cortafuegos;
- Disco de encriptación;
- Encriptación de correo electrónico que también realice firmas digitales como el PGP;
- Software para la detección de virus;
- Seguridad de reserva: Envía por correo electrónico todo el material a un sitio seguro y realiza copias de seguridad semanalmente en CD-RW. Luego almacénalo en un lugar apartado y seguro;
- Frases de pase que sean fáciles de recordar pero no de adivinar;
- Una jerarquía de acceso – no todo el mundo en la organización necesita acceso a todos los archivos;
- Consistencia – ¡Ninguna de las herramientas funcionarán si no las utilizas todo el tiempo!

Pero no sólo es necesario disponer del software correcto. **Las personas suelen ser la conexión más débil, no la tecnología**. La encriptación no funciona si las personas no la utilizan continuamente, si comparten las frases de pase indiscriminadamente o las hacen visibles en una nota pegada en la pantalla, por ejemplo. En caso de un tiroteo o ataque el software de reserva no se salvará si no mantienes la copia de seguridad en un lugar apartado y seguro. La información confidencial debe ser compartida cuando sea necesario y no con todo el mundo de la organización, por lo que es necesario crear jerarquías y protocolos. Por lo general, es importante tener presentes la privacidad y la seguridad en tus actividades diarias. Es lo que denominamos una "paranoia saludable".

P: ¿Cómo decido qué software de encriptación usar?

R: Normalmente, puedes consultarlo con tus amigos – y confirmarlo con nosotros. Necesitarás comunicarte con ciertas personas y ciertos grupos, y si ya están utilizando un sistema de encriptación específico, deberías utilizar el mismo para facilitar la comunicación. Sin embargo, consúltalo primero con nosotros. Algunos paquetes de software simplemente no funcionan bien, mientras que

otros son tarros de miel. Los tarros de miel te atraen ofreciéndote el uso gratuito de un software aparentemente excelente provisto por la misma gente que pretende espiarte. ¿Qué mejor manera de leer tus comunicaciones más confidenciales que la de ser el supervisor de tu software de encriptación? Aún así, existen muchas marcas de confianza tanto de software privado como de software gratuito – simplemente no olvides informarte antes de utilizarlo[3].

P: ¿El uso de la encriptación no aumenta el riesgo de que se adopten medidas severas en mi contra?

R: Nadie sabrá que estás utilizando una encriptación a no ser que tu correspondencia electrónica ya esté siendo vigilada. Si es así, tu información privada ya está siendo leída. Eso significa que quienes te vigilan ya han adoptado esas medidas severas. Existe la inquietud de que los espías puedan utilizar otras opciones si no pueden continuar leyendo tus correos electrónicos, así que es importante conocer a tus colegas e implementar unas políticas de reserva seguras y una gestión laboral sólida en cuanto empieces a utilizar la encriptación. (Nota: No disponemos de información de casos dónde el uso de la encriptación haya causado problemas a los defensores. Sin embargo, considera esta posibilidad detenidamente antes de iniciar la encriptación, sobre todo si estás en un país con un conflicto armado pesado – la inteligencia militar podría sospechar que estás pasando información relevante bajo un punto de vista militar – o si muy pocos defensores utilizan la encriptación – esto podría despertar un interés no deseado hacia ti).

P: ¿Por qué es necesario encriptar el correo electrónico y los documentos todo el tiempo?

R: Si sólo usas la encriptación para los asuntos confidenciales, aquéllos que te estén vigilando o tus clientes podrían adivinar cuando se está llevando a cabo una actividad crítica, y ser más propensos a tomar medidas enérgicas en esos momentos. Mientras no puedan leer tus comunicaciones codificadas, no podrán saber si los archivos han sido encriptados o no. Un incremento repentino de la encriptación podría incentivar un ataque, así que es aconsejable empezar a utilizar la encriptación antes de iniciar los proyectos especiales. De hecho, es mejor asegurarse de que la comunicación fluye sin problemas. Envía correos electrónicos encriptados a intervalos regulares, incluso cuando no haya nada de qué informar. De esta forma, cuando necesites enviar información confidencial, no llamarás tanto la atención.

P: Si ya tengo un cortafuegos ¿por qué necesito encriptar mi correo electrónico?

R: Los cortafuegos impiden que los piratas informáticos accedan a tu disco duro y red pero, una vez envías el correo electrónico por Internet, éste queda expuesto al mundo. Necesitas protegerlo antes de enviarlo.

P: Nadie va a entrar a robar en mi oficina, así que ¿por qué debería utilizar un software de privacidad?

R: No sabes si alguien ha entrado en tu sistema o está filtrando información. Sin comunicaciones codificadas, seguridad física o protocolos de privacidad, todo el mundo puede acceder a tus archivos, leer tu correo electrónico y manipular tus documentos sin tu conocimiento. Tus comunicaciones transparentes también podrían exponer a los demás a un riesgo, sobre todo en lugares donde pueden sucederse ataques por motivaciones políticas. Si cierras las puertas con llave, deberías encriptar tus archivos. Es así de sencillo.

[3] Por ejemplo, PGP –"Pretty Good Privacy"(Privacidad Realmente Buena) – es un método conocido y seguro. Puedes descargarlo en www.pgpi.org

P: No disponemos de acceso a Internet y debemos recurrir a un Internet café. ¿Cómo podemos proteger las comunicaciones enviadas desde un ordenador externo?

R: Es posible encriptar tu correo electrónico y tus archivos. Antes de ir al Internet café, codifica todos los archivos que vayas a enviar por correo electrónico y cópialos con un formato codificado en tu disquete o CD. Una vez en el Internet café, inscríbete a un servicio de encriptación como www.hushmail.com o un servicio de anonimato como www.anonymizer.com, y utilízalos cuando envíes tus mensajes. Asegúrate de que la gente que reciba tu correo se inscriba también a estos servicios.

P: Si es tan importante asegurar nuestros archivos y comunicaciones, ¿por qué no lo hace todo el mundo?

R: Esta tecnología es relativamente nueva, pero su uso se está expandiendo. Los bancos, las empresas multinacionales, las agencias de prensa y los gobiernos utilizan todos la encriptación, considerándola una inversión sólida y un coste necesario para sus negocios. Las ONGs corren un mayor riesgo que las empresas, que suelen ser bien acogidas por la mayoría de los gobiernos. Cabe una mayor probabilidad que las ONGs sean un blanco de vigilancia y por lo tanto necesitan tomar la iniciativa e implementar la tecnología. Los trabajadores de derechos humanos se dedican a proteger a personas o grupos perseguidos y poseen archivos que pueden identificar y localizar a la gente. Si se accediera a estos archivos, estas personas podrían ser asesinadas, torturadas, secuestradas, o "persuadidas" a no volver a acudir a la ONG. La información de estos ficheros podría también ser utilizada como prueba contra la ONG y sus clientes en procesos judiciales políticos.

P: Uno de nuestros principios es la transparencia. Estamos trabajando para que el gobierno tenga una mayor transparencia. ¿Cómo podemos utilizar la tecnología de privacidad?

R: La privacidad es compatible con la transparencia. Si el gobierno desea solicitar públicamente tus archivos, puede hacerlo siguiendo los procedimientos correctos y reconocidos. La tecnología de privacidad evita que la gente acceda a tu información de forma clandestina.

P: Seguimos todos los protocolos de privacidad y seguridad y nuestra información continúa filtrándose - ¿Qué ocurre?

R: Tal vez tengas un espía dentro de la organización o alguien sencillamente incapaz de guardar información confidencial. Modifica tu jerarquía de información reduciendo el número de personas con acceso a la información confidencial – y estate especialmente alerta con esas personas. Las grandes corporaciones y organizaciones divulgan regularmente varias piezas de información falsas a ciertas personas específicas como simple táctica. Si la información falsa se filtra, descubrirás que la filtración proviene del empleado a quien se le dio esa información.

Reglas básicas del uso de la encriptación:

- **Utiliza** la encriptación continuamente. Si tan sólo codificas el material confidencial, la persona que controla tu correspondencia electrónica sabrá cuando está a punto de ocurrir algo importante. Un aumento repentino en el uso de la encriptación podría causar un ataque.

- **NO** añadas información confidencial en la línea de Asunto. No suelen estar codificadas, aunque el mensaje sí lo esté.

□ **Utiliza** una frase de pase que contenga letras, números, espacios y puntuación que sólo tú puedas recordar. Algunas técnicas de creación de frases de pase son el uso de diseños de tu teclado o palabras al azar juntadas entre ellas por símbolos. Por lo general, cuanto más larga sea la frase de pase, más segura.

□ **NO utilices** una única palabra, un nombre, una frase popular o una dirección de tu agenda como frase de pase. Podrían descubrirse en cuestión de minutos.

□ **Haz** una copia de seguridad de tu clave privada (el archivo que contiene tu clave privada para la encriptación del software) en un único lugar seguro, como codificado en un disquete o en un diminuto disco duro portátil USB o "keychain" (dispositivo de memoria).

□ **NO envíes** material confidencial a alguien simplemente por haber recibido un mensaje suyo encriptado con un nombre reconocible. Cualquiera puede "spoof"(falsificar) un nombre creando una dirección de correo parecida a la de alguien conocido. Comprueba siempre la identidad antes de confiar en la fuente – comunícate personalmente, por teléfono, o envía otro mail para reconfirmarlo.

□ **Enseña** a los demás a utilizar la encriptación. Mientras más personas lo utilicen, más seguros estaremos todos.

□ **NO olvides** firmar y encriptar el mensaje. Necesitas que tu destinatario sepa si el mensaje ha sufrido alteraciones durante el trayecto.

□ **Encripta** separadamente los archivos que quieras adjuntar. Por lo general no se encriptan automáticamente cuando envías un correo encriptado.

Guía para una gestión más segura de la oficina y la información.

Gestión de oficina más segura

Para conseguir una gestión de oficina más segura es necesario crear ciertos hábitos. Los hábitos en la gestión de oficina pueden ser positivos o nocivos. Para desarrollar unos buenos hábitos, conviene comprender el razonamiento que se esconde detrás de ellos. Hemos elaborado una lista de hábitos que podrían serte de utilidad para gestionar tu información de una manera más segura – pero sólo si desarrollas estos hábitos y reflexionas por qué son importantes.

¿Qué es lo más importante para la privacidad y la seguridad en la gestión de oficina?

- Ser consciente de tu información y de quien tiene acceso a ella.
- Desarrollar hábitos seguros y practicarlos constantemente.
- Utilizar las herramientas apropiadamente.

Administración

Muchas organizaciones poseen un sistema administrador o alguien con privilegios administrativos para acceder al correo electrónico, la red de ordenadores y supervisar la instalación del nuevo software. Si alguien abandona la organización o no está disponible, el administrador puede acceder a su información y el proyecto puede continuar sin interrupción. Esto también significa que hay un responsable de asegurar que el sistema de software esté limpio y que provenga de una fuente de confianza.

El problema es que algunas organizaciones consideran este papel como un simple soporte técnico y conceden a un trabajador externo esos privilegios administrativos. Este administrador tiene un control efectivo sobre toda la información de la organización, y debe por lo tanto ser de absoluta confianza. Algunas organizaciones reparten el papel de administrador entre el director de la organización y otra persona de confianza.
Existen organizaciones que optan por agrupar las claves privadas y contraseñas del PGP, encriptarlas y guardarlas de forma segura y en un lugar remoto con otra organización de confianza. Esto evita problemas en caso de que alguien olvide su contraseña o pierda su clave privada. Sin embargo, la ubicación de los archivos debe ser completamente segura y de confianza, y deben crearse protocolos específicos y extensos en relación al acceso a los archivos.

La reglas:

1 ◆ NUNCA otorgues privilegios administrativos a un trabajador externo. No sólo son menos fiables que la gente de la organización, pero en caso de emergencia podría resultar difícil contactar con alguien externo a la oficina.

2 ◆ Sólo deberían otorgarse los privilegios administrativos a las personas de mayor confianza.

3 ◆ Decide a qué información podrá acceder el administrador: a todos los ordenadores, frases de pase del ordenador, frases de pase para iniciar la sesión, claves y frases de pase del PGP, etc.

4 ◆ Si decides mantener copias de frases de pase y claves privadas del PGP en otra organización, deberás crear ciertos protocolos de acceso.

5 ◆ Si una persona abandona la organización, sus frases de pase y códigos de acceso personales deberán ser cambiados inmediatamente.

6 ◆ Si alguien con privilegios administrativos abandona la organización, todas las frases de pase y códigos de acceso deberán ser cambiados inmediatamente.

Administración del Software

El uso de software pirateado puede exponer a una organización a la denominada "policía de software". Los policías pueden tomar medidas drásticas con una organización que usa un software ilegal, imponiendo multas muy elevadas y cerrándola. En estos casos la organización no podrá contar con la simpatía o apoyo de los medios de comunicación occidentales porque más que un ataque a una ONG de derechos humamos verán un ataque contra la piratería. Sé extremadamente cauto con tus licencias de software y no permitas que la gente las copie indiscriminadamente. El software pirateado puede también ser inseguro ya que podría contener virus.
Utiliza siempre un programa anti-virus cuando instales el software. El administrador debería controlar la instalación del nuevo software para comprobarlo primero. No permitas la instalación de un software presuntamente inseguro, e instala solamente el software que necesites. Instala los parches de seguridad más actuales en todo el software, sobre todo en Microsoft Office,

Microsoft Internet Explorer y Netscape. Las peores amenazas a la seguridad provienen de los software y soportes físicos entregados con vulnerabilidades intencionadas. Mejor todavía, plantéate pasarte a un software de Código Abierto, que no está basado en el modelo de "Seguridad por Oscuridad" sino que invita tanto a expertos de seguridad como a piratas informáticos a probar rigurosamente todos los códigos. El uso del software de Código Abierto y de cualquier otro que no sea Microsoft tiene la ventaja añadida de hacerte menos vulnerable a los virus estándar y a los piratas informáticos generales. Son pocos los virus creados para los sistemas operativos de Linux o Macintosh porque la mayoría de la gente utiliza Windows. Outlook es el programa de correo electrónico más conocido, y por lo tanto el blanco más conocido de los piratas informáticos.

Hábitos del correo electrónico

La encriptación del correo electrónico debería convertirse en un hábito. Es más sencillo encriptarlo todo que crear una política de cuando debería encriptarse el correo electrónico y cuando no. Recuerda que si encriptas siempre el correo electrónico, quien vigile tu correspondencia no sabrá nunca cuando tus comunicaciones pasan a ser más importantes y confidenciales.

Otros puntos importantes:

- Guarda siempre el correo electrónico codificado en un formato encriptado. Siempre podrás desencriptarlo luego, pero si alguien obtiene acceso a tu ordenador, será tan vulnerable como si nunca hubiera sido codificado.

- Recuerda a todo el mundo con quien intercambies correos electrónicos encriptados que no descodifiquen y reenvíen los mensajes, o que no los contesten sin encriptarlos. La pereza individual es la mayor amenaza para tus comunicaciones.

- Sería interesante crear algunas cuentas de correo seguras para las personas en el campo que no se utilicen generalmente y así no caerán en manos de servidores de spam. Estas direcciones deberían ser revisadas constantemente pero no utilizadas, excepto por el personal de campo. De esta forma podrás eliminar direcciones electrónicas que obtengan mucho correo basura sin que peligre tu base de contacto.

Consejos generales para Internet cafés y otros

Los correos electrónicos enviados en un texto legible o descodificado por Internet pueden ser leídos por muchas partes diferentes. Una de ellas es tu Proveedor de Servicios de Internet local (ISP) por el que pasan todos tus correos electrónicos. Un correo electrónico recorre muchos ordenadores para poder pasar del remitente al destinatario; ignora fronteras geopolíticas y podría pasar por servidores de otros países aunque el correo electrónico esté dirigido al mismo país.
Algunos consejos generales sobre asuntos comúnmente malinterpretados por los usuarios de Internet:

- Proteger un archivo con una contraseña protege tan poco el archivo que no merece la pena hacerlo con los documentos confidenciales. Tan sólo proporciona una falsa sensación de seguridad.

- Comprimir un archivo no lo protege de nadie que quiera comprobar su interior.

- Si quieres enviar un archivo o correo electrónico de forma segura, utiliza la encriptación (véase www.privaterra.com).

- Si quieres enviar un correo electrónico o un documento de forma segura, utiliza la encriptación durante todo el trayecto hasta su destinatario final. No es suficiente con enviar un correo electrónico codificado desde una oficina externa hasta Nueva York o Londres o cualquier otro lugar si luego se reenvía ese mismo correo descodificado a otra persona.

- Internet es universal por naturaleza. No hay ninguna diferencia entre enviar un correo electrónico entre dos oficinas de Washington o enviarlo desde un Internet café de Sudáfrica a un ordenador de la oficina de Londres.

- Utiliza la encriptación tan a menudo como te sea posible, aunque el correo electrónico o la información que envíes no sea confidencial.

- Asegúrate de que el ordenador que estás utilizando posee un software de protección de virus. Muchos virus son creados para extraer información de tu ordenador, tanto del contenido de tu disco duro como de tus archivos de correo electrónico, incluyendo la agenda de direcciones del correo electrónico.

- Asegúrate de que tu software esté autorizado. Si utilizas un software sin licencia, automáticamente te conviertes en un pirata del software a los ojos del gobierno y los medios de comunicación. La mejor opción es utilizar un software de código abierto - ¡es gratuito!

- No existe una solución 100% segura para el uso de Internet. Ten en cuenta que una persona puede "piratear socialmente" un sistema haciéndose pasar por otra persona que no tiene acceso al teléfono o correo electrónico. Básate en tu propio juicio y sentido común.

The UN Declaration on Human Rights Defenders

NACIONES UNIDAS

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,

Tomando nota de la resolución 1998/7 de la Comisión de Derechos Humanos, de 3 de abril de 1998[1], 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 el contexto del cincuentenario de la Declaración Universal de Derechos Humanos[2],

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[2] y de los Pactos internacionales de derechos humanos[3] 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,

[1] Véase *Documentos Oficiales del Consejo Económico y Social, 1998, Suplemento No. 3* (E/1998/23), cap. II, secc. A.

[2] Resolución 217 A (III).

[3] Resolución 2200 A (XXI), anexo.

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 realización 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[2], de los Pactos internacionales de derechos humanos[3] 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.

Bibliografía seleccionada y otros recursos

Bibliografía seleccionada

- Amnesty International (2003): "Essential actors of our time. Human rights defenders in the Americas". AI International Secretariat (Index AI: AMR 01/009/2003/s)

- AVRE and ENS (2002): "Afrontar la amenaza por persecución sindical". Escuela de Liderazgo Sindical Democrático. Published by the Escuela Nacional Sindical and 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 of modules for OFDA/InterAction PVO Security Task Force (Mimeo, included in 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

- ICRC (1983): Fundamental Norms of Geneva Conventions and Additional Protocols. Geneva.

- International Council on Human Rights Policy (2002): "Ends and means: Human Rights Approaches to Armed Groups". Versoix (Switzerland). www.international-council.org

- Jacobsen, K. (1999) "A 'Safety-First' Approach to Physical Protection in Refugee Camps". Working Paper # 4 (mimeo).

- Jamal, A. (2000): "Acces to safety? Negotiating protection in a Central Asia emergency. Evaluation and Policy Analysis Unit, UNHCR. Geneva.

- 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).

- Martin Beristain, C. and Riera, F. (1993): "Afirmacion 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.

- Slim, H. and Eguren, E. (2003): "Humanitarian Protection: An ALNAP guidance booklet". ALNAP. www.alnap.org.uk. London.

- 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 Managment in Violent Environments". Good Practice Review 8. Humanitarian Practice Network. Overseas Development Institute, London.

- Vincent, M. and Sorensen, B. (eds) (2001) "Caught between borders. Response strategies of the internally displaced". Pluto Press. London.

Otros recursos.

La Oficina Europea de Peace Brigades International ofrece desde el año 2000 formación y asesoría sobre protección y seguridad para defensores de derechos humanos, dependiendo de la disponibilidad de tiempo y recursos para ello.

Por favor contactar pbibeo@protectionline.org o pbibeo@biz.tiscali.be, dirigirse a PBI- European Office, 11 Rue de la Linière B-1060 Bruxelles, Belgium Tel +32 2 260 944 05 Fax +32 2 260 944 06 pbibeo@protectionline.org

Ver también una completa página web con recursos sobre protección y seguridad de defensores de derechos humanos en www.protectionline.org

Front Line apoya la formación y la creación de capacidades en seguridad y protección para defensores y publica manuales y materiales en relación con ello. Para más información ver www.frontlinedefenders.org o contactar info@frontlinedefenders.org, o escribir a Front Line, 16 Idrone lane, Off Bath Place, Blackrock, County Dublin, Ireland
tel: +353 1212 3750 fax: +353 1212 1001

Índice alfabético por temas