UNA GUÍA DEL EISF PARA ORGANIZACIONES NO GUBERNAMENTALES

eisf

Gestión de riesgos de seguridad:

una guía básica para las ONG pequeñas

EUROPEAN INTERAGENCY SECURITY FORUM

European Interagency Security Forum (EISF)

EISF es una plataforma independiente de referentes de seguridad que actualmente representan más de 100 ONG humanitarias que operan a nivel internacional. El EISF está comprometido a mejorar la seguridad de las operaciones y del personal humanitario. Tiene como objetivo incrementar el acceso seguro por parte de organizaciones humanitarias a personas afectadas por emergencias. Es clave para su trabajo el desarrollo de investigaciones y herramientas que promueven la concientización, la preparación y las buenas prácticas.

EISF se creó para establecer un rol más destacado de la gestión de riesgos de seguridad en operaciones humanitarias internacionales. Facilita el intercambio entre las organizaciones miembro y otros organismos como la ONU, los donantes institucionales, las instituciones académicas y de investigación, el sector privado y un amplio rango de ONG internacionales. La visión de EISF es convertirse en un punto de referencia global para una práctica aplicada y un conocimiento colectivo, siendo esencial para su trabajo el desarrollo de una investigación práctica para la gestión de riesgos de seguridad en el sector humanitario.

El EISF es una entidad independiente actualmente financiada por la Oficina Estadounidense de Asistencia para Desastres (US Office of Foreign Disaster Assistance, OFDA), el Departamento Federal Suizo para Asuntos Externos (Swiss Federal Department of Foreign Affairs, FDFA), el Departamento para el Desarrollo Internacional del Reino Unido (Department for International Development, DFID) y las contribuciones de los miembros.

www.eisf.eu

Diseño y maquetación : www.wave.coop

Agradecimientos

La presente guía ha sido elaborada por Shaun Bickley (Tricky Locations) con las aportaciones de Lisa Reilly (directora ejecutiva del EISF). La dirección y edición del proyecto a cargo de Adelicia Fairbanks, asesora de investigación en el EISF.

El autor y el EISF desean expresar su agradecimiento a las siguientes personas, que contribuyeron con su tiempo y experiencia a la elaboración de esta guía: Gonzalo de Palacios, Marta Iglesias (MPDL), Nathanael Jarrett, Andrew Parkes (Malaria Consortium), Laky Pissalidis, Emmanuelle Strub y Lotta Westerberg.

Para la traducción al español de esta edición, han participado Angelo Pirola y Fernando Mazarro.

Esta traducción recibió apoyo financiero de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID).

Sugerencia para citar

Bickley, S. (2019) *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*. European Interagency Security Forum (EISF).

Contenido

Introducción

La seguridad del personal es uno de los mayores desafíos a los que se enfrentan las organizaciones no gubernamentales (ONG) humanitarias y de desarrollo, ya sean pequeñas o grandes, a medida en que aumenta la inseguridad, las amenazas y la violencia.

Aunque trabajar y desplazarse en entornos tan impredecibles siempre va a conllevar ciertos riesgos, las organizaciones pueden hacer mucho por desarrollar un entorno de trabajo más seguro para su personal. No obstante, eso implica que la organización otorgue más prioridad y asigne más recursos a la gestión de riesgos de seguridad. Para muchas ONG, los diagnósticos de riesgos de seguridad, los planes de seguridad, los procedimientos de seguridad en viaje, la formación sobre seguridad y los sistemas para reportar incidentes son una parte básica en el lenguaje operativo y son cruciales en su forma de trabajar en todo el mundo.

Sin embargo, tales mecanismos pueden parecer una exageración o demasiado costosos para una ONG más pequeña, debido al tamaño de la organización, en los entornos en los que trabaja, al personal y las actividades que se desempeñan. Aun así, independientemente de su tamaño, todas las ONG tienen la obligación de cumplir el deber de cuidado con su plantilla. A menudo, el personal de organizaciones más pequeñas se encuentra trabajando en las mismas zonas y expuesto a amenazas sin mucho apoyo en comparación con sus homólogos de organizaciones más grandes que cuentan con una estructura notable de seguridad. A muchas personas les resulta frustrante y estresante la falta de prioridad y de apoyo que se presta a temas de seguridad, o la disparidad en enfoques de seguridad entre organizaciones, y a menudo sienten que su organización les está exponiendo a más riesgos. Por todo ello, es fundamental que se establezca un marco eficaz para integrar las prácticas de gestión de riesgos de seguridad en toda la organización.

Aun cuando las organizaciones reconocen que necesitan mejorar su planteamiento sobre la seguridad del personal, puede parecer una tarea abrumadora. ¿Por dónde empezar? ¿Cuáles son las prioridades? ¿Quién se encargará del trabajo? A menudo, las personas que reciben esta responsabilidad poseen poca experiencia y formación en la gestión de riesgos de seguridad y hacen malabarismos con otras prioridades y funciones. Aunque suponga desafíos, mejorar la seguridad del personal

debe ser una prioridad esencial para las ONG, independientemente de su tamaño. Las organizaciones que gestionan con eficacia los riesgos tendrán más acceso a entornos inseguros, lo que conllevará un mayor impacto de sus programas, al tiempo que salvaguardan a su personal.

"Security" en comparación con "safety"

Los términos "security" y "safety" se suelen utilizar indistintamente como "seguridad", pero poseen definiciones distintas. "Security" suele referirse sobre todo a acciones violentas, agresivas o delictivas contra el personal, los activos o las propiedades de la agencia, mientras que "safety" hace relación a acciones, acontecimientos o peligros involuntarios o accidentales.

Se solapan muchas de las medidas necesarias para gestionar los riesgos de ambas seguridades ("security" y "safety") y, a veces, los incidentes de seguridad críticos, como los accidentes de tráfico, pueden conllevar repercusiones adicionales. Aunque algunas organizaciones hacen una distinción clara entre ambas e incluso cuentan con estructuras de gestión separadas, la mayoría de las organizaciones más pequeñas utilizarán los mismos recursos para gestionar ambas cuestiones. Por lo tanto, a efectos de la presente guía, se entiende también "safety" cuando se mencione "security", por eso ambas se traducen como "seguridad".

Sobre esta guía

La presente guía pretende ser un recurso de seguridad sencillo y fácil de usar que sirva a las ONG más pequeñas para romper mitos sobre la gestión de riesgos. Al establecer los elementos de un marco de gestión de riesgos de seguridad, esta guía va dirigida a apoyar a las ONG a traducir sus obligaciones del deber de cuidado en procesos y acciones clave que no solo contribuirán a la seguridad de su personal nacional e internacional, sino que también supondrán una mejora en la reputación y la credibilidad de su organización. Aunque se intenta que la guía se pueda aplicar a ONG nacionales e internacionales, algunos elementos pueden ser más pertinentes para las que trabajen en terceros países.

Muchos de los recursos que existen sobre seguridad en las ONG, tienden a centrarse en los requisitos de las organizaciones grandes de ayuda humanitaria y al desarrollo, es decir, aquellas con grandes equipos multinacionales que trabajan en múltiples países, a menudo con parte de su personal dedicado a la seguridad. La presente guía considera los recursos limitados y los desafíos concretos a los que se pueden enfrentar ONG más pequeñas al intentar establecer y mantener un marco de gestión de riesgos de seguridad.

La presente guía complementa otras guías cruciales, como la de EISF, "Seguridad en práctica", que se centra en sistemas de gestión de la seguridad en un contexto o una ubicación concretos; no obstante, esta guía ofrece una perspectiva más amplia sobre el marco general con el que una organización debería aspirar a contar para mejorar su gestión de riesgos de seguridad. Esta guía también va dirigida a complementar la guía "Auditorías de seguridad" de EISF, que permite que las organizaciones hagan balance de lo que tienen, en lo relativo a seguridad del personal, y de lo que han de mejorar.

¿A quién va dirigida esta guía?

La presente guía va dirigida, sobre todo, al personal de ONG más pequeñas que sea responsable de la seguridad de la plantilla o que busque mejorar la gestión de riesgos de seguridad dentro de su organización.

Aunque se haya escrito pensando en ONG más pequeñas, la guía es pertinente para organizaciones de cualquier tamaño, incluso para organizaciones grandes y consolidadas cuyo personal viaje y trabaje en entornos complicados. La guía también puede resultar de utilidad a ONG internacionales que no tengan presencia en el país, pero que estén ejecutando acciones en remoto a través de organizaciones locales a las cuales formar en gestión de riesgos.

¿Cómo utilizar esta guía?

Esta guía se estructura en torno a los elementos fundamentales de un marco de gestión de riesgos de seguridad. Las personas que lean esta guía podrán manejarla con facilidad y consultar aspectos concretos en función del área de gestión de riesgos de seguridad que quieran abordar.

En el texto encontrarán:

- Actividades cruciales y sugerencias; identificables con
- Testimonios de expertos; identificables con
- Referencias cruzadas dentro de la guía; identificables con
- Referencias cruzadas a otros recursos, herramientas e información de apoyo en materia de seguridad, incluso a publicaciones del EISF que están disponibles en www.eisf.eu; identificables con
- Se proporcionan los hipervínculos para facilitar la consulta.
- Consulte la bibliografía para tener toda la información, y los enlaces, de los recursos que se mencionan en el texto.

1 Cumplir el deber de cuidado

A pesar de que la mayoría de las ONG, grandes y pequeñas, admiten que tienen la responsabilidad de proteger a su personal, muchas organizaciones siguen sin ser conscientes de todo lo que implican sus obligaciones del deber de cuidado y cómo afectan estas a la gestión de los riesgos de seguridad. Los parámetros del deber de cuidado han ido creciendo considerablemente en los últimos diez años y, lo que en su momento se consideró suficiente, ya no basta en la actualidad. Aunque el deber de cuidado es un término jurídico sobre las responsabilidades que tienen las organizaciones para con su personal, existe también una obligación moral de deber de cuidado que las organizaciones deberían tener en cuenta.

Básicamente, el deber de cuidado significa asegurar que se cuenta con las medidas de mitigación adecuadas para prevenir incidentes y responder ante ellos, y que todo el personal es debidamente informado sobre los riesgos y las medidas de mitigación correspondientes.

Es importante resaltar que el deber de cuidado es más que mera seguridad. La gestión de los riesgos de seguridad es solo uno de los elementos de la responsabilidad general que tiene una organización sobre la salud, la seguridad y el bienestar de su personal.

Las obligaciones del deber de cuidado no se limitan a relaciones contractuales entre empleador/a y empleado/a. Las organizaciones también tienen un deber de cuidado para con quien actúa en nombre de la organización, tal como contratistas independientes, consultorías, personal voluntario, personas a cargo y visitantes oficiales.

A menudo, el grado de responsabilidad que tiene una organización para con una persona va determinado por la medida en la que dicha persona controla su entorno de trabajo y las tareas que lleva a cabo, y su acceso a información sobre riesgos eventuales; cuanto mayor sea el grado de control o de influencia que tiene una organización, mayor será su responsabilidad. Por ejemplo, cuando una ONG concierta la visita de una consultoría —incluso mediante la planificación de itinerarios, los preparativos del viaje y la reserva de su alojamiento y transporte—, pasa a tener más responsabilidad

sobre la seguridad de dicha persona. Esto es cierto sobre todo cuando la organización, por su presencia o por sus actividades en el país, está en mejores condiciones que la persona visitante para supervisar los riesgos.

Con frecuencia, las ONG más pequeñas no tienen oficinas fijas en el país, sino que el personal viaja a título individual o se integra en una organización colaboradora local. La organización empleadora sigue teniendo las responsabilidades jurídicas del deber de cuidado y debe asegurarse de que la gestión de riesgos de la organización local es adecuada para cumplir dichas responsabilidades.

Su deber de cuidado

Todas las organizaciones tienen una obligación legal y moral de proporcionar un cuidado estándar que proteja a sus empleados y a quienes actúen en nombre de la organización ante un riesgo de daños razonablemente previsible. Para cumplir su deber de cuidado básico debe:

- **Conocer los riesgos:** las organizaciones deben ser capaces de demostrar que han identificado y tenido en cuenta todos los riesgos previsibles en relación con un lugar o una actividad en concreto. El análisis de los riesgos debe ser realizado y documentado regularmente.
- **Establecer las medidas de mitigación:** las organizaciones deben adoptar todas las medidas razonables para gestionar los riesgos. Han de contar con planes integrales y actualizados, procedimientos y mecanismos, y cumplirlos para abordar los riesgos que existan en un lugar concreto o en relación con una actividad específica. Respetar las normas de la comunidad local les permite demostrar que son conscientes de lo que se consideran buenas prácticas comunes entre otras ONG en la zona donde están trabajando.
- **Elaborar planes de emergencia:** debe contar con planes minuciosos, así como con medidas y asistencia para responder a situaciones sobrevenidas que involucren al personal, independientemente del lugar.
- **Asegurar el consentimiento informado:** el personal debe entender y aceptar los riesgos a los que se enfrenta y las medidas existentes para gestionarlos. Debe existir un proceso para documentar e interiorizar los riesgos y las funciones en la gestión de la seguridad colectiva. Sin embargo, tales documentos no proporcionan exención legal ante los tribunales.

- **Sensibilizar:** el personal debe recibir información y orientación detalladas y actualizadas y, en muchos casos, formación referente a los riesgos a los que está expuesto.
- **Proporcionar el apoyo adecuado:** las organizaciones deben contar con el apoyo y los seguros adecuados para atender al personal afectado por un incidente.

Las responsabilidades del deber de cuidado son de aplicación tanto en entornos de alto riesgo como en los de bajo. Sin embargo, se espera que las organizaciones se responsabilicen aún más del personal que trabaja en situaciones de riesgo más elevado. Se admite que no se pueden eliminar todos los riesgos, sobre todo en entornos de alto riesgo. Por lo tanto, se hace hincapié en que las actuaciones sean "razonables" y en que el personal reciba la información necesaria para tomar una decisión fundamentada sobre los riesgos residuales a los que todavía puede estar expuesto.

Más información

Guía del EISF "Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications", de Edward Kemp y Maarten Merkelbach

Guía del EISF "Auditorías de seguridad"

'Can you get sued? Legal liability of international humanitarian aid agencies toward their staff', de Edward Kemp y Maarten Merkelbach

'Voluntary Guidelines on Duty of Care to Seconded Civilian Personnel', de Maarten Merkelbach

'Duty of Care under Swiss law: how to improve your safety and security risk management processes', de Adelicia Fairbanks

Definir las actitudes ante el riesgo

Las ONG tienen grados muy distintos de exposición ante los riesgos y diferentes actitudes en función de su mandato y sus valores, la percepción de la necesidad y beneficios para la comunidad respecto a las actividades y, finalmente la capacidad de mitigar y gestionar los riesgos a los que está expuesto su personal.

Ser conscientes de los riesgos en lugar de tener aversión a ellos.

Resulta vital que todas las organizaciones identifiquen su nivel de riesgo y determinen el grado que están dispuestas a aceptar. Los riesgos a los que se enfrenta el personal siempre deberán guardar relación con la

necesidad o las ventajas de actividades concretas, la capacidad de la organización para gestionar estos riesgos y las consecuencias si sucediera algo. Dar al personal unos parámetros sobre la actitud ante el riesgo de la organización, lo que a veces se denomina "umbral de riesgo", servirá como orientación en decisiones tales como si autorizar visitas o iniciar actividades en determinadas ubicaciones con un grado mayor de riesgo o cuándo detener o suspender las actividades o retirar al personal porque empeora la seguridad o se dan amenazas concretas.

Todo el personal debe tener una comprensión compartida sobre el grado de riesgo que su organización está dispuesta a asumir para actividades concretas, así como de cuándo y cómo acelerar las decisiones y de acuerdo con la jerarquía interna a la organización. Los documentos organizacionales claves de seguridad, como la política de seguridad de la ONG, deberían incluir una declaración clara sobre la actitud de la organización ante el riesgo, junto con información sobre cómo se evalúan los umbrales de riesgo y cuáles son los procesos de toma de decisión y autorización y las medidas de seguridad que se requieren para distintos grados de riesgo.

▶ *Véase el Apartado 6 – Gestión de viajes y apoyo*

Más información

Documento informativo "Risk Thresholds in Humanitarian Assistance"

"Whose Risk Is It Anyway? Linking Operational Risk Thresholds and Organisational Risk Management", de Oliver Behn y Madeleine Kingston

ISO 31000:2009

Establecer una cultura de seguridad

Una cultura de seguridad positiva es clave para mejorar la seguridad del personal de las organizaciones. La "cultura" de una organización se puede definir, sencillamente, como "la manera en la que hacemos las cosas aquí". Cada organización posee una actitud cultural hacia la seguridad y sobre los riesgos en general. La diferencia es que algunas organizaciones alientan a trabajar con seguridad, mientras que otras no lo hacen. No basta que una organización declare que se toma en serio la seguridad y que cuenta con políticas y procedimientos al respecto si la cultura de la organización no genera un enfoque positivo sobre seguridad. Todo el personal dentro de la organización tiene que entender y demostrar los valores de la organización en cómo procede con sus actividades en el día a día.

"Si las organizaciones no han incorporado una cultura de seguridad, esta dependerá de las personas en un determinado lugar, lo que significa que existirán múltiples planteamientos de seguridad en toda la organización, algunos buenos y otros insuficientes, lo que vendría a ser que la organización carece de su propia cultura de seguridad, algo que el personal identifica con rapidez y utiliza para hacer frente a la organización."

Asesor/a de seguridad en una ONG

Crear una cultura de seguridad positiva en su organización exigirá un sentido colectivo de consciencia y responsabilidad de todo el personal, donde todo el personal, incluso el personal directivo y altos cargos, se responsabilizan personalmente de su seguridad y velan por que esté realmente integrada en todos los aspectos de los programas y de las actividades. Acciones sencillas, como un premio anual de cumplimiento o incluir a los conductores en el plan de seguridad, por ejemplo, pueden tener un impacto palpable sobre la actitud y el comportamiento sin necesidad de tener que implementar recursos adicionales.

Una cultura de seguridad positiva no se puede crear de la noche a la mañana: lleva tiempo cambiar la actitud y el comportamiento del personal y, con ello, el enfoque general de la organización sobre la gestión de los riesgos de seguridad. Sin duda, habrá obstáculos y dificultades, y cierto grado de resistencia interna, incumplimiento y limitaciones de recursos. Es importante ser realista, reconocer que establecer una cultura de seguridad positiva es un proceso a largo plazo y planificarlo acorde a ello. Es mejor empezar con objetivos que se puedan conseguir con facilidad, lo que sirve para impulsar un "cambio cultural" y construir desde ahí. No cabe duda de que un sistema de gestión de riesgos de seguridad parcial es mejor que no contar con ningún sistema.

"Contábamos con todas las medidas y los procedimientos de seguridad, pero la cultura organizativa no cambió hasta que la dirección general no asistió al curso de seguridad personal."

Coordinador/a de una ONG humanitaria

11 pasos hacia una cultura positiva de seguridad

1. **Desarrollar un marco:** detallar el planteamiento sobre seguridad que sigue la organización, incluyendo las políticas, los procedimientos y los mecanismos que se han aplicado para velar por una gestión eficaz de los riesgos de seguridad.
2. **Redactar una política:** enmarcar la actitud de la organización ante el riesgo y sus principios claves de seguridad, así como definir funciones y responsabilidades. Incluir responsabilidades y obligaciones de seguridad en las descripciones de los puestos de todo el personal y de la dirección.
3. **Sensibilizar:** involucrar a todo el personal para que todo el mundo sea consciente de las prioridades para mejorar la gestión de los riesgos de seguridad, entre todos los rangos de la organización. Velar por que la dirección emita declaraciones inequívocas sobre la importancia de la seguridad de las personas. El personal debe "apropiarse" de las medidas, y no percibir que le son impuestas desde los superiores sin consultar al personal ni acordarlas con él.
4. **Liderar desde la primera línea:** asegurarse de que todas las prácticas de seguridad, tales como la formación personal sobre seguridad o los formularios de planificación de viaje, sean de obligado cumplimiento para todo el mundo, sin distinciones de rango.
5. **Proporcionar opciones flexibles:** la gestión de riesgos de seguridad no es un criterio único. Velar por que se establezcan las medidas y los planes locales pertinentes en distintos contextos de seguridad y entornos de riesgo.
6. **Buscar "victorias rápidas":** identificar medidas o requisitos que se puedan establecer con rapidez, en un plazo breve y con recursos limitados, pero que puedan tener un efecto positivo en la seguridad del personal.
7. **Informar, informar e informar:** resaltar ante el personal la importancia de informar sobre incidentes o conatos, y de compartir sus percepciones individuales de la seguridad. Velar por que se cuente con mecanismos sencillos y eficaces para reportar y recopilar incidentes.
8. **Establecer foros de seguridad:** asegurarse de que existan diversas reuniones o mecanismos dentro de la organización donde se puedan plantear y tratar cuestiones y desafíos en materia de seguridad. Velar por que la seguridad sea un punto permanente del orden del día en reuniones clave.

9. **Monitorear y revisar:** llevar a cabo revisiones periódicas del planteamiento de seguridad de la organización y su marco de gestión, así como su puesta en práctica, para verificar que el marco sigue siendo eficaz.
10. **Hacer cumplir la rendición de cuentas:** establecer un mecanismo para que las personas rindan cuentas sobre seguridad y velar por que las responsabilidades en la gestión de riesgos de seguridad se incluyan en las revisiones de desempeño del personal.
11. **Celebrar los éxitos:** identificar planteamientos positivos y encontrar ejemplos que sirvan de motivación sobre las repercusiones positivas de una mejor seguridad: cuanto mejor sea la seguridad, mejor será el acceso y mejores serán los resultados.

Más información

"Developing a security-awareness culture – improving security decision making", de Chris Garrett

Dotar de recursos la gestión de riegos de seguridad

Existen costes inevitables relacionados con la gestión de la seguridad. Desarrollar y emprender un planteamiento integral sobre la gestión de los riesgos de seguridad puede llevar mucho tiempo y recursos financieros, que suelen ser limitados en todas las organizaciones.

Para las ONG más pequeñas, una capacidad y una financiación limitadas se suelen percibir como los principales obstáculos para abordar la seguridad con eficacia. No obstante, existen muchos aspectos de la gestión de riesgos de seguridad que se pueden abordar sin que esto suponga demasiado tiempo ni grandes presupuestos para la seguridad. Por ejemplo, están disponibles varias plantillas, herramientas y recursos de "código abierto" para la gestión de riesgos (a través del EISF e InterAction, por ejemplo) y las ONG los pueden adaptar y utilizar con facilidad. Además, aunque la formación sobre seguridad puede ser una inversión considerable para las organizaciones más pequeñas, existen varios cursos gratuitos online que pueden servir para sensibilizar sobre seguridad y para capacitar al personal.

▶ *Véase el Apartado 7: Sensibilización y capacitación*

También los donantes aceptan cada vez mejor que la seguridad del personal es un elemento crucial en el desarrollo de programas en zonas inseguras. Muchos grandes donantes están dispuestos a financiar algunos de los costes

de seguridad. Por ejemplo, realizar diagnósticos de seguridad, establecer posturas sobre seguridad, comprar equipos básicos relacionados con la seguridad, mejorar la seguridad de instalaciones clave y ofrecer formación son costes que muchos donantes ahora están dispuestos a financiar. Para las ONG resulta esencial identificar y justificar los costes de seguridad a través de un diagnóstico de riesgos y velar por que las propuestas y los presupuestos de programa contengan las consideraciones y los gastos de seguridad, y que estos no se incluyan dentro de los gastos generales (es decir, indirectos).

Véase el documento informativo del EISF "The Cost of Security Risk Management for NGOs"

Aunque su organización saldrá ganando de varias maneras al mejorar su enfoque sobre la seguridad del personal, al fin de cuentas se trata de asignar prioridades y recursos. Crear un marco eficaz para la gestión de riesgos de seguridad precisará de que se destinen suficientes recursos humanos y financieros; es importante que se hable con antelación y que la dirección busque el compromiso para dar prioridad y recursos adecuados a la seguridad.

Más información

Documento informativo del EISF "The Cost of Security Risk Management for NGOs"

"The Risk Management Expense Portfolio (RMEP) Tool" en el documento informativo "The Cost of Security Risk Management for NGOs"

2 Desarrollar un marco

El primer paso para establecer un sistema eficaz para salvaguardar al personal es desarrollar un marco de gestión de riesgos de seguridad que explique la arquitectura, las funciones, las responsabilidades y las disposiciones con las que se cuenta para respaldar el acceso del personal en las mejores condiciones de seguridad.

Un marco de gestión de riesgos de seguridad es un conjunto de medidas, protocolos, planes, mecanismos y responsabilidades que respalda la reducción de riesgos de seguridad para el personal.

Su organización necesita gestionar un amplio abanico de riesgos; entre ellos, financieros, operativos, jurídicos y de reputación. La gestión de riesgos de seguridad solo es un elemento en la gestión general de riesgos que hace la organización y debe ser acorde al enfoque más amplio de la organización sobre gestión de riesgos, junto con las políticas y los procesos existentes. Un marco básico de gestión de riesgos de seguridad es un sistema integrado con dos elementos principales:

- **los fundamentos**, donde entra una buena gobernanza de seguridad y una estructura responsable, así como una política de seguridad y sus principios;
- **los mecanismos**, donde se incluyen los diversos procedimientos, planes, actividades de seguridad y recursos de apoyo que se utilizan para gestionar los riesgos de seguridad para el personal.

Para que no haya duda, el marco de gestión de riesgos de seguridad NO es un único documento. Sin embargo, habrá que desarrollar un documento de orientación o "mapa" que explique cómo plasmar en el marco, el enfoque que adopta la organización sobre la gestión de riesgos de seguridad y cómo se relacionan entre sí todos los diversos documentos y procesos que forman parte del marco de gestión de riesgos de seguridad.

El diagrama siguiente muestra las piezas esenciales de un marco de gestión de riesgos de seguridad.

Marco de gestión de riesgos de seguridad

2. Desarrollar un marco

3 Gobernanza y rendición de cuentas

Una buena estructura de gobernanza y rendición de cuentas es la espina dorsal de un marco de gestión de riesgos de seguridad que sea eficaz. Cualquier persona en cada nivel de la organización —desde el Consejo de Administración hasta los integrantes individuales— tiene la responsabilidad colectiva de gestionar y reducir los riesgos para el personal. Todas las personas tienen responsabilidades sobre su propia seguridad individual, al mismo tiempo que todas las organizaciones, independientemente de su tamaño, deben velar por que se cuente con una estructura de gestión eficaz para impulsar una cultura de seguridad positiva y que ayude a la organización a cumplir sus obligaciones del deber de cuidado.

Crear una estructura eficaz de gestión de riesgos de seguridad

La responsabilidad última por la seguridad del personal reside en el Consejo de Administración o similar, quien a su vez delega la responsabilidad en la dirección ejecutiva o en un puesto de jerarquía similar para asegurar

contar con una gestión eficaz de riesgos de seguridad. Entonces, la gestión y la responsabilidad colectivas respecto a la seguridad se comparten en distintos niveles de la organización y suelen seguir un modelo de jerarquía administrativa. En las descripciones de los puestos de trabajo se deben constar con claridad los deberes de todo aquel personal que tenga responsabilidades de seguridad y, para que rindan cuentas, se deben evaluar en sus evaluaciones de desempeño.

Para conseguirlo es fundamental elegir a las personas correctas para gestionar la seguridad. La mayoría de las organizaciones grandes cuentan con asesores que se dedican a la seguridad o incluso con equipos de seguridad para supervisar el marco de seguridad de la organización y para proporcionar apoyo y asesoramiento en materia de seguridad para todo el personal implicado en ella. No obstante, este modelo no es realista para ONG más pequeñas.

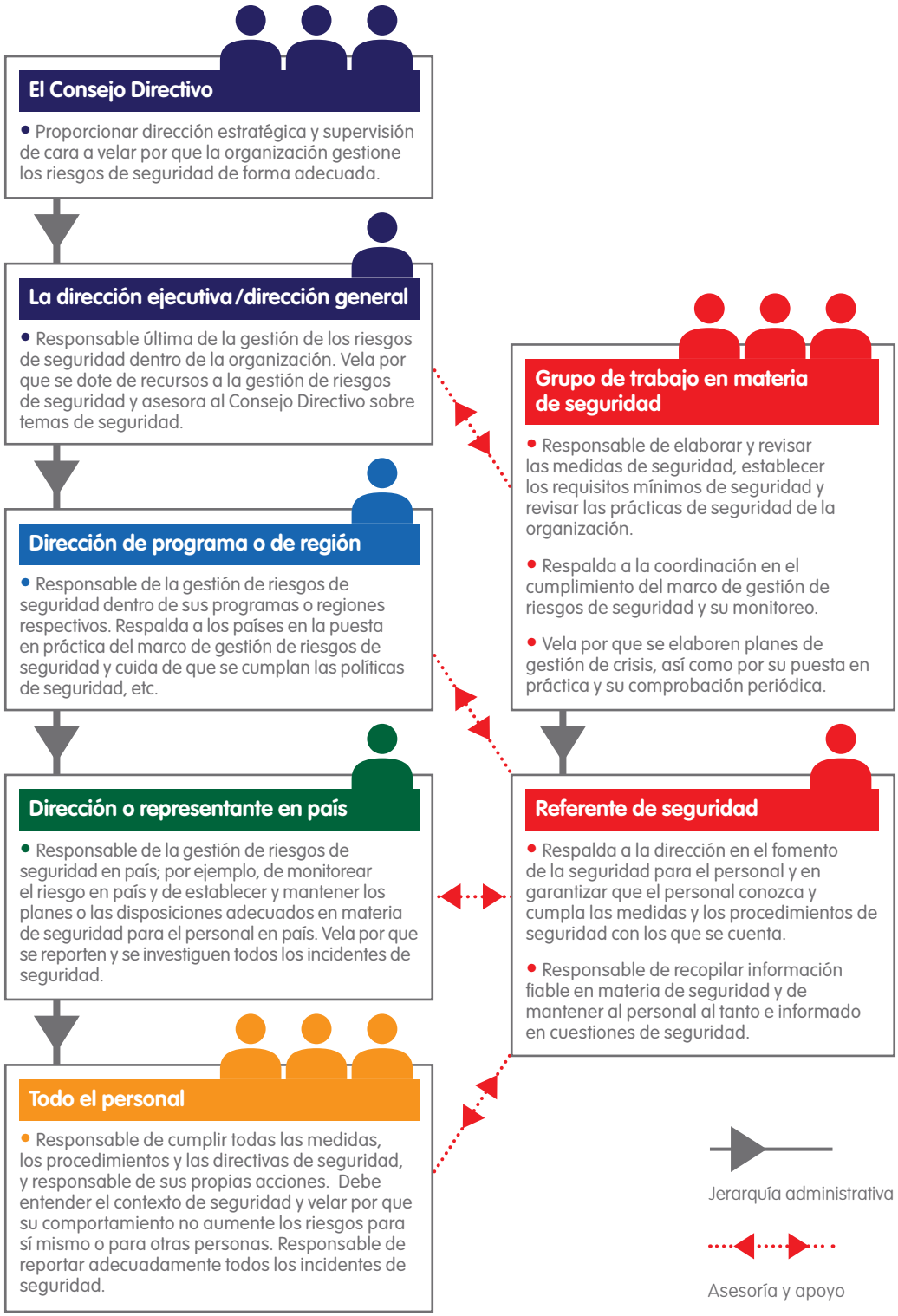
Cabe identificar a alguien o incluso a un grupo del personal dentro de su organización que pueda actuar como referente de seguridad y dirigir el desarrollo y la aplicación del marco de seguridad. Es importante que estas personas tengan el tiempo, el apoyo y la formación necesarios para realizar esto como parte de sus tareas habituales.

Gestionar los riesgos para el personal es una responsabilidad compartida. Para incorporar una buena gestión de riesgos de seguridad es preciso definir con claridad funciones y responsabilidades, así como estructuras con capacidad suficiente para proporcionar y mantener un apoyo eficiente.

Muchas organizaciones utilizan un grupo de trabajo en materia de seguridad o un comité de representantes con distintas funciones y cargos dentro de la organización. Este planteamiento colectivo sirve para compartir la carga, aporta un amplio abanico de experiencias y perspectivas, y fomenta un mayor sentimiento de pertenencia, lo que acaba respaldando aplicación y cumplimiento de las normas de protección.

Es importante percatarse de que no es responsabilidad del referente o del grupo de trabajo en materia de seguridad gestionar los riesgos de seguridad (es decir, que no son "propietarios" del riesgo). En lugar de eso, las responsabilidades de gestión de la seguridad deben quedar incorporadas en la gestión habitual de los programas. La función del referente o del grupo de trabajo en materia de seguridad es respaldar que se elabore el marco de gestión de riesgos de seguridad de la organización y garantizar que se cuente con políticas y procedimientos acordados, así como aconsejar a cada nivel si necesario o si solicitado.

Ejemplo de estructura y responsabilidades



Al identificar funciones y responsabilidades específicas en materia de seguridad, se necesita contemplar qué es lo adecuado y realista para la organización, sin perder de vista el tamaño, la complejidad de su estructura, las funciones y la capacidad existentes, y el tipo de trabajo que desempeña.

Primero, se deben identificar los puestos existentes que cumplan una función crucial en la seguridad del personal, desde la dirección en sede hasta los equipos en el país (si la organización tiene presencia permanente). Después, se definen con claridad las responsabilidades y las funciones específicas de toma de decisiones en materia de seguridad que debería tener cada puesto. Estos y sus responsabilidades en materia de seguridad deberían exponerse con claridad en la política de seguridad de la organización para que todo el personal esté informado de ello.

Más información

Ejemplo de perfil de puesto: Logistics and Security Officer

Ejemplo de perfil de puesto: Field Security Coordinator

Ejemplo de perfil de puesto: Deputy Director of Global Security

Ejemplo de perfil de puesto: Director of Staff Safety and Security

4 Política y principios

La política de seguridad de la organización será la piedra angular del marco de gestión de riesgos de seguridad. Establecer una política global de seguridad servirá para demostrar el compromiso de la organización con la seguridad del personal. Dicha política también manifiesta con claridad el planteamiento que sigue la organización en materia de riesgos de seguridad, los principios clave en los que se basa dicho planteamiento, y las funciones y las responsabilidades que tiene el personal en la gestión de dichos riesgos.

Una política de seguridad es una obligación para todas las organizaciones, independientemente de su tamaño. Informa al personal de los principios, los criterios y las responsabilidades relativas a la gestión de riesgos de seguridad y vela por que el personal actúe de una manera que sea adecuada para la organización.

Elaborar una política de seguridad

Al elaborar o revisar la política de seguridad de la organización, se deberían aclarar los alcances:

- ¿Se centra solo en la seguridad o en la seguridad (security) y la protección (safety)? Las políticas de seguridad de algunas ONG no incluyen la protección porque esta se aborda en una política por separado de salud e higiene en el trabajo.
- ¿A quién cubre dicha política? Aunque esté claro que se aplica al personal, ¿qué pasa con las consultorías, contratistas, personal voluntario, visitantes, familiares acompañantes u otras partes asociadas? La política debería abordar la seguridad de cualquier colectivo, explicitando cualquier distinción por cada grupo de pertenencia.

La política de seguridad debería ser un documento breve y accesible que esté traducido a los principales idiomas de trabajo de la organización. La mayoría de las políticas de seguridad se estructuran entorno a cuatro apartados clave:

1. Una **declaración** sobre la importancia de la seguridad del personal, el alcance de la política y a quién se aplica.
2. Un apartado de **"principios"** sdonde se explican la cultura en materia de seguridad, la actitud ante el riesgo y los principios clave de la organización, que dan forma al planteamiento de la organización sobre la seguridad del personal.
3. Un apartado de **"responsabilidades"** donde se establecen la estructura de gestión de riesgos de seguridad de la organización y las funciones y las acciones asignadas a los puestos específicos.
4. Un apartado de **"requisitos mínimos de seguridad"** donde se establecen los requisitos de seguridad organizacionales específicos con los que se debe contar (por ejemplo, cada país debe tener un plan de seguridad).

La política de seguridad es un documento de gobernanza clave que necesitará el aval de la dirección ejecutiva, o de una persona en un puesto similar, y luego la aprobación del Consejo de Administración o similar. La política de seguridad debe hacer referencia a las demás políticas y procedimientos que rijan la organización y donde se describan los requisitos relativos a la gestión de riesgos de seguridad, como la política de salud y protección, el código de conducta para el personal, los protocolos para denunciar irregularidades, así como políticas sobre el bienestar y cuidado del personal, el fraude y la corrupción, y la seguridad de la información.

Principios de seguridad

- **Responsabilidad compartida:** gestionar y reducir los riesgos para el personal es una responsabilidad compartida que involucra a todo el personal de la organización.
- **Reconocimiento del riesgo:** gestionar la seguridad no va a eliminar los riesgos. Cada persona empleada tiene que ser consciente, como parte de su consentimiento informado, de que todavía está expuesta a riesgos.
- **Prioridad de la vida:** la protección del personal es de máxima importancia para la organización y el equipo nunca debería colocarse en un riesgo excesivo para cumplir los objetivos del programa ni para proteger propiedades.
- **Riesgo proporcional:** deben evaluarse con constancia los riesgos para el personal y han de ser en proporción a la necesidad de ejecutar determinadas actividades, a las ventajas de hacerlo y a la capacidad de la organización para gestionar dichos riesgos.
- **Seguridad equitativa:** algunas personas pueden ser más vulnerables que otras ante determinadas amenazas. Hay que informar a dichas personas de los riesgos, pero las medidas o restricciones de seguridad no deberían discriminar a nadie por sus características personales.
- **Derecho a retirarse:** todo el personal debe tener derecho a retirarse de trabajar, o a rechazar hacerlo, en una zona específica por problemas de seguridad.
- **Sin derecho a permanecer:** la organización tiene derecho a suspender las actividades o a retirar al personal de aquellas situaciones que considere demasiado peligrosas. El personal no tiene el derecho a permanecer en un lugar del que la dirección le haya indicado que se retire.
- **Estrategias de seguridad:** el planteamiento de una organización para mitigar riesgos se denomina estrategia de seguridad. Para la mayoría de las ONG, será un equilibrio entre "aceptación" y "protección", con la "disuasión" como criterio meno habitual.

Véase la guía del EISF "Seguridad en práctica" y la guía de ODI "IBP8 – Gestión de la seguridad de las operaciones en entornos violentos"

La política de seguridad debería explicar también con claridad la postura de la organización sobre armas y personal armado, su relación con agentes armados y el uso de recursos militares, así como su punto de vista sobre rescates y sobornos.

Más información

Ejemplo de una política de seguridad (en inglés)

"Open NGO Security Policy", del Centre for Safety and Development

Guía del EISF "Seguridad en práctica: herramientas de gestión de riesgos para organizaciones de ayuda humanitaria"

Guía del EISF "Auditorías de seguridad"

Guía del ODI "IBP8 – Gestión de la seguridad de las operaciones en entornos violentos"

Página temática del EISF "Policy, Procedure and Practice in SRM"

Establecer requisitos de seguridad

La política de seguridad debería determinar los requisitos básicos de seguridad con los que espera contar la organización como estándares en todos los lugares a los que viaja o en los que haya personal. Por ejemplo, ¿deberían celebrarse inducciones a la seguridad o reuniones informativas para todo el personal? ¿Existe un tipo específico de formación sobre seguridad que se exija para visitar o trabajar en determinados lugares? ¿Las visitas a lugares de riesgo elevado precisan de una autorización del viaje específica? ¿Se exige a todas las oficinas en país que realicen diagnósticos de riesgos y elaboren planes de seguridad?

▶ *Véase "Planes de seguridad" en el Apartado 5: Operaciones y programas*

"Sea realista sobre la capacidad y los recursos de los que dispone su organización. No tiene sentido establecer unos requisitos mínimos de seguridad amplios que su organización no pueda proporcionar por falta de capacidad o de recursos. Aunque se pueda reconocer una regla como buenas prácticas, la credibilidad de la política de seguridad se verá perjudicada si el personal se ve obligado a pasar por alto dicha regla porque no existen los recursos para cumplirlo. Dicho esto, siempre han de cumplirse unas determinadas normas de deber de cuidado, más allá de los recursos o de la capacidad que tenga la organización."

Asesor/a de seguridad en una ONG

Dado el abanico de países y, por lo tanto, de contextos de seguridad en los que se trabaja o a los que viaja el personal, es evidente que no todos los contextos van a precisar el mismo grado de medidas de seguridad. Los requisitos de seguridad se deberían ajustar en función de los distintos grados de riesgo. Sin embargo, los sistemas deberían mantenerse lo más sencillos posible para que el personal no se confunda demasiado y se anime a cumplirlos. Por ejemplo, la política puede afirmar que todo el personal

ha de asistir a una reunión informativa antes de partir al terreno, pero el contenido puede variar. De esta manera, el personal que vaya a entornos con más riesgos precisará de una reunión informativa minuciosa antes de la salida; y el personal que viaje a destinos con un riesgo moderado necesitará únicamente de los consejos básicos de viaje.

Otro elemento que puede repercutir en cómo se pone en práctica la política es si el personal viaja a un país donde la organización tiene oficina propia o si está viajando, apoyándose a una organización local colaboradora.

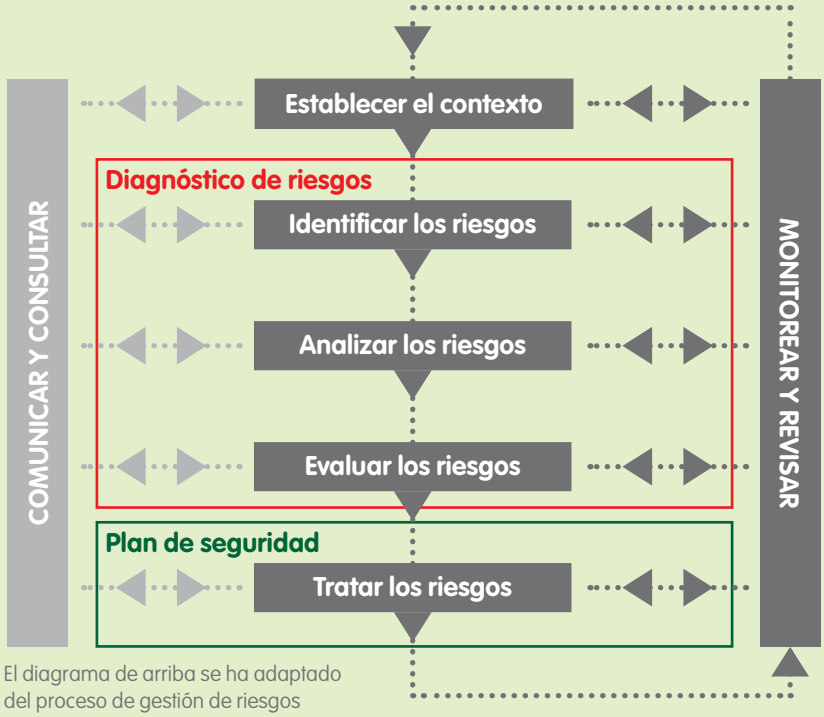
Es importante percatarse de que los recursos de seguridad en sí no constituyen un sistema de gestión de riesgos de seguridad; son el **mínimo** requerido y un punto de partida desde el que construir una gestión de riesgos de seguridad sólida que plasme las buenas prácticas y que sea adecuada para el grado de riesgo al que se enfrenta el personal.

5 Operaciones y programas

Contar con planes, procedimientos y recursos realistas es fundamental para gestionar los riesgos en las operaciones y programas. Debe establecerse un proceso sistemático de gestión de riesgos que permita a la coordinación analizar el entorno operativo, identificar los riesgos para el personal y para las operaciones, y determinar los planteamientos y las medidas más eficaces para gestionar los riesgos en ese contexto específico.

"Es importante reconocer que, al elaborar los planes y los procedimientos para gestionar los riesgos, el objetivo es facilitar que el personal consiga un acceso seguro, y lo mantenga, para realizar los programas; no se trata de gestionar la seguridad en aras de la mera seguridad. Si no es posible utilizar medidas que permitan que el personal trabaje dentro del umbral de riesgo aceptable para la organización, se debería repensar si sus objetivos son adecuados y si debería estar trabajando en dicho contexto."
Coordinador/a de seguridad en una ONG

Proceso de gestión de riesgos



El diagrama de arriba se ha adaptado del proceso de gestión de riesgos de la ISO 31000:2009

Existen diversos modelos del proceso de gestión de riesgos que pueden adoptar las ONG. Por ejemplo, la ISO 31000:2009, que es una norma internacional que muchas ONG han incorporado. La ISO 31000:2009 define el riesgo como el efecto de la incertidumbre sobre los objetivos y describe las siguientes etapas clave en la gestión de riesgos:

- **Establecer el contexto:** revisar tanto el contexto externo como interno. Una comprensión exhaustiva del entorno operacional y de las distintas partes interesadas involucradas, junto con un entendimiento minucioso del impacto de su ONG sobre el contexto a través de las actividades y del personal involucrado, así como de las capacidades de su organización, facilitarán que perciba los posibles desafíos en materia de seguridad para el personal, los programas y la organización.
- **Identificar los riesgos:** identificar todas las posibles amenazas de seguridad que podrían afectar al personal, a los programas o a la organización (incluso su reputación) y entender cómo, cuándo y porqué puede producirse cada amenaza.
- **Analizar los riesgos:** realizar un diagnóstico exhaustivo para determinar la exposición del personal a las distintas amenazas identificadas. Debería evaluarse cada riesgo (la amenaza y la exposición al mismo) para

determinar su gravedad, teniendo en cuenta la probabilidad de que se produzca y las repercusiones potenciales que tendría, dadas las medidas y los procedimientos con los que se cuenta.

- **Evaluar los riesgos:** comprendiendo bien la exposición al riesgo de la organización, se pueden tomar decisiones informadas sobre si aceptar determinados riesgos o si actuar de otra manera para evitar o minimizar los mismos.
- **Tratar los riesgos:** algunas de las opciones para evitar, minimizar o mitigar los riesgos consisten en reducir los riesgos, transferir los riesgos o compartirlos con otras partes o, por último, evitar el riesgo al no emprender esa actividad. Reducir los riesgos de seguridad implica utilizar distintas estrategias que minimicen la probabilidad o las repercusiones de determinadas amenazas. Dichas estrategias se ponen en práctica al desarrollar planes de seguridad por país o zona.
- **Monitoreo y revisión:** deben revisarse continuamente cada uno de los elementos del proceso de gestión de riesgos para velar por que los enfoques y las medidas actuales siguen siendo adecuadas a la situación cambiante.

Una comunicación y una consulta eficaces son fundamentales para el proceso de gestión de riesgos. Nadie puede retener toda la información necesaria para identificar, analizar y mitigar los riesgos. Por lo tanto, resulta crucial identificar a una serie de partes interesadas, tanto internas como externas, que puedan ayudar en este proceso.

El proceso de gestión de riesgos también se puede utilizar como una herramienta para diagnosticar organizaciones colaboradoras que su personal pueda visitar o a las en que se puedan incorporar.

Más información

Guía del EISF "Seguridad en práctica: herramientas de gestión de riesgos para organizaciones de ayuda humanitaria"

ISO 31000:2009

Guía del ODI "IBP8 – Gestión de la seguridad de las operaciones en entornos violentos"

Documento informativo del EISF "Security Management and Capacity Development: International Agencies Working with Local Partners"

Documento informativo del EISF "Género y seguridad: Directrices para la transversalización del género en la gestión de riesgos de seguridad"

Documento informativo del EISF "Security Risk Management and Religion: Faith and secularism in humanitarian assistance"

Documento de investigación del EISF "Managing the Security of Aid Workers with Diverse Profiles"

Guía del EISF "Managing Sexual Violence against Aid Workers: prevention, preparedness, response and aftercare"

Diagnósticos de riesgos de seguridad

Los diagnósticos de riesgos aportan la visión sobre los peligros a los que se enfrentan la organización, los programas y, lo que es vital, el personal en un lugar específico. Un diagnóstico de riesgos de seguridad es un elemento fundamental del proceso de gestión de riesgos y debe verse como una parte integral de los análisis útiles para establecer operaciones y programas en cualquier país, ya se apliquen directamente o a través de colaboraciones locales.

Matriz de análisis de riesgos

		IMPACTO				
		Insignificante	Menor	Moderado	Grave	Crítico
PROBABILIDAD	Segura/ Inminente					
	Muy probable					
	Probable					
	Posible					
	Improbable					

Riesgo extremo	Es preciso actuar de inmediato. ¿Se puede aceptar el riesgo?
Riesgo elevado	Aplicar medidas concretas de seguridad y planes de contingencia
Riesgo medio	Es preciso reforzar la sensibilización y procedimientos adicionales
Riesgo bajo	Se gestiona a través de los procedimientos rutinarios de seguridad

Una comprensión minuciosa de los riesgos en un contexto específico es fundamental para que la organización tome decisiones mejor fundamentadas sobre seguridad.

El diagnóstico de riesgos no debe ser un acontecimiento puntual. Una reevaluación continua de todos los riesgos posibles servirá para asegurar que se cuenta con las medidas de seguridad adecuadas en todo momento.

El proceso de diagnóstico de riesgos primero identifica las amenazas de seguridad en un contexto determinado y la posible vulnerabilidad del personal, de los activos, de los programas que se están desarrollando y finalmente de la propia organización. Luego, se analiza todo conforme a la probabilidad y las repercusiones para calcular el grado de riesgo que implica. Por último, se identifican y evalúan las distintas opciones que se podrían adoptar para gestionar dichos riesgos. Tras haber identificado medidas de mitigación, es probable que queden algunos riesgos residuales, que deberían contrastarse con el umbral de riesgos de la organización para ver si se puede aprobar la continuación del programa. Si una organización lleva a cabo un proceso de diagnóstico de riesgos, pero no lo aplica, puede estar expuesta al incumplimiento del deber de cuidado.

Debe documentarse el proceso de diagnóstico de riesgos de seguridad y se deben incluir los hallazgos clave y las medidas propuestas para gestionar los distintos riesgos. Los diagnósticos de riesgos también deben actualizarse con constancia. Además, el personal necesitará orientación sobre lo que significan las distintas probabilidades y las calificaciones de riesgo para analizar con más precisión las diversas amenazas y garantizar coherencia en toda la organización. Por ejemplo, "probable que suceda" ¿quiere decir que va a ser semanal o diario? Asimismo, es preciso aclarar en qué medida el "impacto" predicho contempla los efectos sobre las personas, las actividades del programa o la organización en su totalidad, ya que pueden ser distintos. Al considerar la vulnerabilidad ante amenazas, deberían contemplarse las particularidades de la organización y de las personas. Por ejemplo, tanto el puesto como la edad, el género, el grupo étnico, la nacionalidad o la identidad sexual pueden tener repercusiones diferenciadas en cada riesgo.

"Los diagnósticos de riesgos se suelen percibir como una carga burocrática, algo que tachar de la lista de papeleos. Por eso se ha perdido la conexión esencial entre dichos análisis y los programas."
Asesor/a de seguridad en una ONG

No existe un formato obligatorio para los diagnósticos de riesgos de seguridad, pero existen muchas pautas sobre buenas prácticas, así como

herramientas y plantillas útiles. Lo importante es proporcionar al personal una plantilla de diagnóstico de riesgos estándar que se utilice en todas las misiones, que sea fácil de rellenar y que capte la información esencial.

Los diagnósticos de riesgos documentados también pueden proporcionar unos fundamentos a la hora de solicitar recursos y financiación para poner en práctica los planteamientos y las medidas de seguridad que son necesarios para respaldar al personal que trabaja en un contexto específico.

Más información

"Módulo 3: Herramienta de diagnóstico de riesgos" en la guía del EISF "Seguridad en práctica"

"Security Assessment Tool", de ACT Alliance

Planes de seguridad

Los planes de seguridad son los documentos clave por país donde se describen las medidas y los procedimientos con los que se cuenta, así como las responsabilidades y los recursos necesarios para ponerlos en práctica. Deberían establecerse planes de seguridad en todos los lugares donde la organización tenga una presencia considerable o donde participe con regularidad. Un documento básico que describa las disposiciones de seguridad y los procedimientos de emergencia, incluso en situaciones en las que su organización no tenga presencia fija, pero que el personal visite con regularidad, o donde haya un equipo pequeño o un único representante, servirá para velar por que el personal entienda las medidas con las que cuenta y, lo más importante, las respecte y las siga.

Si en el diagnóstico de riesgos se identifica una amenaza, el plan de seguridad debe aconsejar al personal cómo gestionar el riesgo que plantea dicha amenaza.

Los planes de seguridad deberían mantenerse como documentos pertinentes y accesibles, deberían abordar los riesgos específicos que existen en ese lugar y, si conviene, ser concretos sobre a quién se aplican las medidas y dónde; por ejemplo, a grupos étnicos determinados en regiones concretas. Se deberían actualizar los planes con regularidad, sobre todo tras incidentes significativos o cambios en el entorno operativo o en las actividades. Donde sea necesario, se deberían traducir a los idiomas del lugar.

Plan de seguridad de país

Entre los elementos clave de un plan de seguridad para un país o para una zona geográfica concreta se deberían incluir:

- **Información crítica:** un resumen de una página de información pertinente para acceder con facilidad y consultar con rapidez, por ejemplo, cualquier restricción como horas de toque de queda, zonas en las que no entrar o contactos clave.
- **Descripción general:** la finalidad y el ámbito del documento, quién es responsable del plan de seguridad, la actitud de la organización ante el riesgo, la fecha de elaboración y la fecha de revisión, y un resumen de la estrategia o de la política sobre seguridad de la organización.
- **Contexto actual:** un resumen del contexto operativo actual y de la situación general de seguridad, los principales riesgos para el personal, los activos y los programas (sistema de diagnósticos de riesgos), las amenazas prevalentes en el presente contexto, la evaluación de amenazas y la calificación de riesgo.
- **Procedimientos operativos estándar (SOP, por sus siglas en inglés):** procedimientos de seguridad sencillos y claros a los que el personal debería atenerse para evitar incidentes y que explican cómo responder si surgen problemas. Los SOP deberían ir vinculados a los riesgos clave identificados y abordar temas tales como el trasporte de efectivo, el reporte de incidentes, los viajes a terreno y la seguridad en los vehículos, instalaciones y emplazamientos, control de acceso a las oficinas y a las instalaciones, robos, accidentes de tráfico, conducta personal, salud y bienestar del personal, y la seguridad de la información.
- **Salud y bienestar:** la protección del personal ante amenazas para la salud, así como ante accidentes, estrés y trastornos de estrés postraumático.
- **Recursos humanos:** medidas relativas a la contratación, a la comprobación de antecedentes, contratos, confidencialidad, iniciaciones, diagnóstico de riesgos de puestos, etc.
- **Reuniones informativas sobre seguridad:** qué información debería proporcionarse a personal nuevo y a visitantes, y cuándo debería proporcionarse dicha información.
- **Seguridad administrativa y financiera:** medidas para evitar robos, fraude y corrupción, así como la manipulación de efectivo y las adquisiciones.
- **Grados de seguridad:** los grados o las fases de seguridad de la organización, con indicadores circunstanciales que plasmen los riesgos que aumentan para el personal en ese contexto y ubicación, y actuaciones o medidas concretas que son necesarias para responder a esa inseguridad creciente.

- **Reporte de incidentes:** los procedimientos y las responsabilidades en el reporte de incidentes en materia de seguridad; por ejemplo, el tipo de incidentes del que se reporta, la estructura para informar de ellos y el formato.
- **Gestión de crisis:** integrantes de su equipo de gestión de crisis y las normas de activación. Incluye planes de contingencia que anticipen amenazas previsibles o incidentes críticos, como la reubicación o la evacuación de personal, catástrofes naturales y urgencias médicas.
- **Anexos:** información adicional, documentos y listas de comprobación que ayuden al personal en la puesta en práctica de procedimientos y planes; por ejemplo, listas de contactos, listas de comprobación para reuniones informativas y formularios para reportar incidentes.

Involucrar el personal afectado por riesgos en la preparación de los planes de seguridad incrementa la probabilidad de que este personal adhiera a dichos planes, ya que entenderán el por qué de las medidas de seguridad.

Más información

"Country Security Plan Example", de InterAction

"Módulo 6: Plan de seguridad" en la guía del EISF "Seguridad en práctica"

Disposiciones de seguridad y soporte

Puede que la organización no tenga presencia en un país, pero que el personal lo visite con regularidad, o que solo cuente con una persona representante o un equipo reducido; en consecuencia, el personal dependerá de los socios locales o de las organizaciones de acogida —cada uno con distintas normas de seguridad y distintas actitudes ante el riesgo— como apoyo en materia de seguridad al realizar visitas a los programas o actividades en el país.

Aunque transfiera alguien del personal a otra organización, no puede traspasar sus responsabilidades de deber de cuidado. Como organización contratante, mantiene siempre la responsabilidad de garantizar que se cuenta con las medidas de seguridad adecuadas y que estas se ponen en práctica.

Por lo tanto, el grado y la calidad del apoyo en materia de seguridad disponible para el personal están determinados por el apoyo que los socios locales o las organizaciones de acogida pueden prestar o al que estén dispuestas a facilitar. Puede ser que el socio o la organización de acogida no estén familiarizados con los riesgos a los que está expuesto o con el grado de apoyo que va a necesitar. Los riesgos para el personal aumentarán si las organizaciones locales colaboradoras o de acogida cuentan con pocos procedimientos de seguridad (o carecen de ellos) o no tienen equipos de comunicación. También puede ser que proporcionen un alojamiento inseguro o vehículos inestables.

Dado que la elección de organizaciones locales colaboradoras o de acogida es claramente estratégica y en ella influyen distintos factores, se debe evaluar la capacidad y las disposiciones de seguridad habituales. Cuando sea necesario, la organización local colaboradora o de acogida debería recibir apoyo en el desarrollo de planes y procedimientos de seguridad y, si es posible, se les debería facilitar el acceso a formación sobre gestión de seguridad. Además, de proporcionar soporte para la recepción de la información en materia de seguridad necesaria para las tomas de decisiones de seguridad para la organización y su personal. Puede que los socios locales carezcan de experiencia en realizar un diagnóstico de riesgos de seguridad o en elaborar planes de seguridad, pero sin duda poseen información minuciosa sobre el contexto que puede ser de suma ayuda para diagnosticar los riesgos y a planificar reglas de seguridad para el personal.

Incluso en situaciones donde no haya ninguna organización colaboradora o de acogida establecida, se debería pedir al personal a desarrollar relaciones con otras ONG en la zona, algunas de las cuales pueden estar dispuestas a proporcionar información, actualizaciones de seguridad y apoyo en caso de emergencia. Como mínimo, dichos contactos pueden ser un "ojo atento" para el personal y alguien con quien conectar mientras el personal esté en el país.

Apoyo en seguridad por parte de organizaciones locales colaboradoras o de acogida

- **Selección:** el proceso de selección de organizaciones potenciales que acojan a su personal debería incluir una evaluación de la capacidad general en materia de gestión de seguridad de la organización local colaboradora o de acogida, su actitud y planteamiento ante los riesgos, los grados de aceptación locales, y los procedimientos y planes existentes sobre seguridad.
- **Responsabilidades y límites:** asegurarse de que cualquier acuerdo sobre apoyo sea explícito en lo que respecta a las responsabilidades en materia de seguridad de ambas partes y a cualquier limitación, en concreto sobre las diversas responsabilidades en caso de incidentes de seguridad o de urgencias médicas que afecten al personal.
- **Planes y procedimientos de seguridad:** velar por que tanto las organizaciones locales colaboradoras como las de acogida cuenten con planes y procedimientos de seguridad adecuados, y que los compartan con el personal. Si es preciso, aportar ejemplos o consejos que apoyen a las contrapartes en la elaboración de documentos de seguridad.
- **Compartir información:** mantener un diálogo habitual con colaboradoras u organizaciones de acogida sobre la situación de seguridad para asegurar un consenso sobre el grado de riesgo y cuál es la mejor manera de gestionar la seguridad del personal. Se debería solicitar a las organizaciones locales colaboradoras o de acogida que compartan con la organización los informes de incidentes pertinentes.
- **Redes:** debería alentar a las colaboradoras u organizaciones de acogida y, si fuera preciso respaldarlas en la creación de vínculos a redes de seguridad locales y con mecanismos para compartir información (por ejemplo, los que coordinan INSO o Naciones Unidas).
- **Financiación en materia de seguridad:** en contextos de riesgo más elevado, puede ser preciso aportar financiación adicional a las colaboradoras u organizaciones de acogida para asegurar que se cuente con recursos de seguridad esenciales.

Más información

"La seguridad de los cooperantes solitarios", de Gonzalo de Palacios

Guía del EISF "Office Opening: A guide for non-governmental organisations"

Documento informativo del EISF "Security Management and Capacity Development: International Agencies Working with Local Partners"

"Humanitarian Safety and Security: Obligations and responsibilities towards local implementing partners", de Christopher Finucane

6 Gestión de viajes y apoyo

Viajar es una necesidad para gran parte del personal de las ONG. Ya sea para visitar programas o para asistir a reuniones y eventos, el personal viaja regularmente a zonas del mundo con riesgos que le son desconocidos o con un mayor grado de riesgo inherente. En cuando el personal pone un pie fuera de su entorno de trabajo habitual, suele aumentar su exposición a diversos riesgos de seguridad o de salud, así como las responsabilidades del deber de cuidado de la organización. Eso significa que la gestión de riesgos de seguridad debe ser un elemento fundamental en el enfoque general de toda organización sobre la gestión de viajes.

La gestión eficaz de los riesgos de seguridad en viaje es un proceso continuo que comienza antes de la salida, sigue mientras la persona que viaja está en su destino y se mantiene después de que vuelva sana y salva.

Pueden agravarse los riesgos de viaje para el personal en países donde exista poca o ninguna presencia de la organización. Un conocimiento limitado del contexto y de información actualizada sobre las amenazas presentes, junto con la carencia de planes de seguridad o de redes, aumentan los riesgos para el personal que viaja.

Al planificar el viaje, es crucial que el personal y los visitantes sean plenamente conscientes de los riesgos a los que pueden enfrentarse y que reciban información al respecto. No se trata solo de contar con unas medidas adecuadas de seguridad antes del viaje, sino también de disponer del apoyo apropiado (incluso reuniones informativas en materia de seguridad, alojamientos seguros, transporte seguro, atención médica adecuada) cuando se llega, mientras se está en el país y cuando se vuelve.

Determinar los riesgos en viaje

Por supuesto, el grado y los tipos de riesgo para quien viaja variarán mucho en función de su destino, el carácter del viaje y su perfil personal. No todos los lugares y trayectos precisarán de las mismas medidas de seguridad. Si el marco de gestión de riesgos de seguridad de la organización no es lo suficientemente flexible para atender las distintas exposiciones a riesgos en los distintos lugares a los que viaja el personal, existe el riesgo de que los procedimientos y las medidas existentes se perciban como una carga o como ineficaces, o como un estorbo para las operaciones, y el personal será reacio a cumplirlos.

Acceder a un sistema actualizado de calificación de riesgo del país permite a su organización, y al personal individual, determinar con rapidez el grado general de riesgo en un país o en un lugar concreto. En función de esta calificación de riesgo, se puede especificar cuáles son las medidas de seguridad necesarias antes de viajar y qué grado de autorización es adecuado para el viaje, siguiendo la política de seguridad y los procedimientos de seguridad en viaje de la organización.

Aunque algunas organizaciones más grandes son capaces de llevar sus propias calificaciones de riesgo por país, esto requiere bastantes recursos, sobre todo para obtener la información necesaria para mantenerlas actualizadas con regularidad. Puede ser más eficaz para su organización utilizar las calificaciones de riesgo en viaje que proporciona un proveedor externo de información sobre seguridad; por ejemplo, una empresa vinculada con su seguro de viaje o con su servicio de reservas para viajes, si fuera el caso. Otra opción serían las calificaciones de riesgo en viajes de código abierto disponibles a través de las páginas web sobre viajes de las embajadas u otros proveedores.

▶ *Véase "Información sobre seguridad y análisis" más abajo en este apartado*

Ejemplos de calificaciones de riesgo por país

Las calificaciones de riesgo de un país o zona suelen basarse en una categorización de cuatro —o cinco— niveles. Se formulan las calificaciones mediante la evaluación de varios tipos de riesgo, incluyendo conflictos, disturbios políticos o civiles, terrorismo, delincuencia, sanidad e infraestructuras. El ejemplo más abajo resume algunos de los indicadores amplios que se utilizan.

Bajo	Países o zonas que suelen ser seguros y donde las autoridades mantienen la seguridad apropiada. Existen unos índices bajos de delitos violentos, y se manifiestan algunos disturbios violentos políticos o civiles durante las elecciones o en otros acontecimientos significativos. No son habituales los atentados. Los riesgos relativos a catástrofes naturales son limitados y las amenazas para la salud se pueden prevenir en su mayoría. Se requiere una seguridad personal básica, así como precauciones sanitarias y en viaje.
Moderado	Países o zonas que experimentan inestabilidad política o protestas violentas. Existen grupos activos contra el gobierno, insurgentes o extremistas con atentados esporádicos. El personal corre riesgos ante delitos comunes y violentos. Los servicios de transporte y comunicaciones no son fiables y los registros de seguridad son escasos. El país es propenso a las catástrofes naturales o a las epidemias. Se precisa de una mayor vigilancia y de procedimientos de seguridad rutinarios.
Elevado	Países o zonas que tienen periodos regulares de inestabilidad política o protestas violentas, que pueden tener como objetivo al personal extranjero. Existen grupos muy activos contra el gobierno, insurgentes o extremistas y plantean una amenaza para la estabilidad política o económica del país. Los índices de delitos violentos son altos y es habitual que tengan como objetivo al personal extranjero. Las infraestructuras y los servicios de emergencias son escasos y pueden existir alteraciones habituales de los servicios de transportes y comunicaciones. Determinadas zonas no son accesibles para el personal extranjero. Las agencias de cooperación pueden verse sometidas a amenazas y acoso por parte de las autoridades y de agentes armados, militares o no estatales. Países y zonas que experimentan una catástrofe natural o una epidemia sanitaria que se considera de alto riesgo. Existe un riesgo persistente para el personal y es necesario un elevado grado de vigilancia y precauciones de seguridad específicas para ese contexto.
Extremo	Países o zonas que pueden estar viviendo un conflicto activo o unos disturbios civiles violentos y persistentes. El riesgo de verse atrapado en un incidente o ataque violento es muy elevado. El gobierno puede haber perdido el control de partes considerables del país y puede que se haya roto el orden público. Las líneas entre criminalidad y violencia política e insurgente están difuminadas. Es probable que el personal extranjero no pueda acceder a partes considerables del país. Los servicios de transporte y comunicaciones están muy degradados o no existen. El grado de violencia supone una amenaza directa a la seguridad del personal. Es fundamental tomar precauciones rigurosas y puede que no sean suficientes para evitar incidentes graves. Pueden verse suspendidas las actividades de programa o los movimientos, y puede que se retire al personal sin mucha antelación.

Deberían elaborarse diagnósticos de riesgos específicos para el personal que viaja a destinos con un mayor riesgo o cuando el carácter de la visita suponga problemas de seguridad. Se necesita orientar con claridad al personal cuando es necesario realizar un diagnóstico de riesgos en viaje y aclarar quién es responsable de aprobar el diagnóstico y de autorizar los desplazamientos. En un diagnóstico de riesgos en viaje debe constar el destino, el itinerario y la información personal de quién viaja y su experiencia. Además, debería evaluarse el contexto general y los riesgos de seguridad clave en las distintas ubicaciones que se van a visitar y las distintas disposiciones específicas con las que se cuenta para gestionarlos.

Más información

Ejemplo de un formulario para diagnosticar los riesgos de viaje (en inglés)

Procedimientos de seguridad en viaje

Muchas ONG pequeñas no tienen oficinas de país permanentes, pero su personal viaja mucho. Para estas organizaciones, los procedimientos de seguridad al viajar deben ser una prioridad. Los procedimientos de seguridad en desplazamientos reflejan el planteamiento de la organización sobre la gestión de riesgos para el personal (y otras personas colaboradoras) cuando se viaja en nombre de la organización. Mientras que los planes de seguridad se centran sobre todo en lugares donde la organización tiene presencia o participa habitualmente, los procedimientos de seguridad en viaje deberían cubrir todas las ubicaciones a las que se mueva el personal, incluso lugares donde la organización tenga poca o ninguna presencia, y también zonas en las que se trabaja con una organización local colaboradora o de acogida. En los procedimientos han de incluirse también medidas para mantener un registro de lugares seguros para el personal en países con menos riesgo donde, no obstante, existe una amenaza de incidente con múltiples víctimas, como las capitales europeas.

Es más probable que el personal cumpla los procedimientos de viaje si participa en su elaboración y entiende sus razones.

Puede que dentro de la política de viaje más amplia de su organización ya existan procedimientos de seguridad en desplazamientos. Si no fuera así, los procedimientos de seguridad en viaje deben describirse con claridad en un documento individual, que debe abordar todo tipo de viaje que realiza el personal y otras partes interesadas, y proporcionar información sobre las

medidas de seguridad y sobre qué espera la organización antes, durante y después del viaje.

Los gobiernos pueden respaldar la evacuación de sus ciudadanos en caso de inestabilidad política o de seguridad, aunque no está garantizado y es muy variable. Toda respuesta diplomática corresponderá a la nacionalidad de la persona y no a la sede de la organización. Antes de que se produzca un incidente, debería comprobarse la capacidad de respuesta de los gobiernos de cada uno de sus trabajadores si se diera una crisis.

Procedimientos de seguridad en viaje

Un procedimiento básico de seguridad en viaje debería incluir:

- **Introducción:** para aclarar a quién se aplican los procedimientos. Debe destacarse cualquier diferencia en los requisitos de seguridad en viaje o en el apoyo que se proporciona al personal, consultorías, personas asociada, y visitantes oficiales.
- **Calificaciones de riesgos en viaje:** explica el sistema de calificación de riesgo en viaje o por país que se utiliza, cómo accede el personal a la información, las distintas categorías e indicadores que se utilizan, y sus consecuencias.
- **Funciones y responsabilidades:** aclara las responsabilidades de quien viaja, sus responsables directos o puntos de contacto, y la dirección en lo que respecta a la seguridad en viaje y cómo esto varía para destinos con calificaciones de riesgo más elevadas.
- **Autorización de viaje:** determina quién autoriza el viaje en la organización, las diversas medidas de cumplimiento y cómo esto cambia para destinos con calificaciones de riesgo más elevadas.
- **Diagnóstico de riesgos en viaje:** explica cuándo son precisos los diagnósticos de riesgos en viaje, qué plantilla debería utilizarse y quién aprueba los diagnósticos terminados.
- **Información y reuniones informativas antes del viaje:** explica la información que ha de proporcionarse a todo el personal antes de que partan, el tipo de reunión informativa precisas y quién la dirige, y cómo dichos requisitos cambian según aumenta la calificación de riesgo.
- **Formación en materia de seguridad:** esclarece si es precisa una formación en materia de seguridad antes de viajar y qué curso debe realizarse. Esto puede variar en función de la calificación de riesgo del país. También debe incluirse información sobre cualquier sistema de exención de la formación y quién autoriza las exenciones. Sin embargo, es importante percatarse de que el deber de cuidado requiere que se justifique la exención.

- **Prueba de Identidad del personal / la persona que viaja:** el personal y las demás personas que viajen por la organización deberían rellenar un formulario de perfil del personal/la persona que viaja. Entre la información recopilada cabe incluir datos personales (nombre, nacionalidad, religión, idiomas que maneja, identificadores físicos o marcas, etc.), contactos en caso de emergencia (familiares o contactos alternativos), datos médicos (problemas de salud preexistentes, medicación habitual, tipo sanguíneo, datos de contacto de su médico, etc.), la huella en redes sociales (las principales redes sociales que utiliza, en caso de incidentes críticos) y preguntas de prueba de vida (en contextos donde exista riesgo de rapto o secuestro). Debe ser fácil acceder a los formularios de perfil fuera del horario laboral habitual.
- **Protocolo de verificación:** especifica con quién deben contactar las personas que viajan mientras lo hagan y con qué frecuencia, así como el proceso necesario en caso en que se pierda el contacto. La frecuencia de la verificación debería plasmar la subida de la calificación de riesgo del destino.
- **Procedimientos de emergencia:** explica los procedimientos de emergencia de la organización para urgencias médicas y en materia de seguridad, incluso quién contactar y cómo hacerlo.

Los procedimientos de seguridad en viaje también deberían especificar qué sucede cuando el personal añade un viaje privado a su viaje de trabajo para cubrir cuestiones como el seguro, verificación, horarios de viaje reales, etc.

"También debería proporcionarse, en la medida de lo posible, información clave sobre el personal que viaja (p. ej. compañía aseguradora) a la organización de acogida en el país ya que, en caso de emergencia, el retraso en acceder a esta información a través de la sede puede tener repercusiones graves sobre el resultado de un incidente."

Director/a de seguridad de una ONG

Información de seguridad y su análisis

Todo el personal y otras personas que viajen en nombre de la organización deberían tener acceso a información y a orientación minuciosa y actualizada sobre los riesgos de seguridad y para la salud, relacionados con el destino antes de que se emprenda el viaje. Para ONG con poca o ninguna presencia en el país, la información está disponible a través de diversas páginas gubernamentales con consejos sobre viajes y otras páginas abiertas de noticias y consejos de viajes; sin embargo, requiere bastante tiempo y

esfuerzo por parte del personal encontrar y cotejar análisis de calidad. Incluso cuando se consigue, la información disponible no siempre plasma los acontecimientos actuales o la situación específica en el terreno, y los consejos suelen ir dirigidos a personas que viajan por negocio o de turismo, más que a personal de ONG.

Muchas organizaciones utilizan servicios informativos externos en materia de seguridad o viajes, bien a través de su seguro de viaje (como servicio gratuito o con costes adicionales), bien directamente de proveedores específicos. La mayoría de los proveedores externos ofrecen información de viaje detallada sobre países y ciudades e informes a través de plataformas online, e incluyen información y consejos sobre acontecimientos significativos que repercuten en la seguridad del personal o que es probable que conlleven posibles alteraciones del viaje. Sin embargo, puede variar mucho la calidad y la exhaustividad de la información disponible entre distintos proveedores y un análisis más profundo tiende a estar vinculado a servicios de pago. Si la organización quiere utilizar servicios informativos externos en materia de seguridad, es aconsejable probar varias plataformas y distintos servicios antes de decidir cuál se va a utilizar y si adquirir los servicios de pago. Cabe contemplar acceder y unirse a iniciativas sin ánimo de lucro, como la Aid Worker Security Database (Humanitarian Outcomes) o el proyecto Aid in Danger de Insecurity Insight, que recopilan y difunden información sobre incidentes de seguridad que experimenten organizaciones humanitarias y de desarrollo. Los órganos de coordinación de seguridad en ONG (p. ej., EISF, INSO, etc.) también pueden ayudar a las organizaciones acceder a información específica para ONG.

Elegir a proveedores externos de información

Si contempla utilizar servicios informativos externos en materia de seguridad, tener en cuenta lo siguiente:

- **Seguro:** identificar qué servicios informativos y de soporte ya están a disposición del personal a través de las disposiciones del seguro existentes de su organización.
- **Servicios:** averiguar qué servicios informativos y de apoyo en viaje ofrece cada proveedor y contemplar si se ajustan a su perfil de riesgo y necesidades.
- **Reputación y experiencia:** hablar con otras organizaciones para cerciorarse de cómo son los distintos proveedores de servicios informativos de seguridad en términos de experiencia y credibilidad en lo que se refiere al análisis, la información o el asesoramiento que proporcionan.
- **Costes:** contemplar qué proveedores ofrecen la mejor relación calidad-precio por la amplitud y la calidad de sus servicios.

- **Multiproveedores:** decidir si centralizar servicios a través de un proveedor, para utilizar los servicios existentes además de comprar otros, o contemplar servicios concretos por país. Sin embargo, utilizar múltiples proveedores para acceder a información distinta puede resultar confuso y conllevar una subutilización de los servicios.
- **Plataforma online y aplicaciones:** comprobar cuán accesibles son los servicios informativos sobre seguridad, ya que es más probable que el personal utilice un servicio si se puede acceder con facilidad a través de aplicaciones de móvil o páginas web que ya utiliza quien viaja, como las páginas de reservas de viajes en línea.

Se debe informar lo antes posible al personal y a quien viaje sobre incidentes y eventos que se produzcan en el país y que puedan influir en la seguridad. La mayoría de los proveedores de servicios informativos en materia de seguridad o viajes mandan alertas por correo electrónico y por SMS y aconsejan según se va desarrollando la situación. Algunos de estos servicios de alertas van incluidos en los paquetes normales de los proveedores, pero algunos cobran una cantidad adicional por dichos servicios. Para recibir directamente estas alertas, cada persona ha de inscribirse y elegir recibir alertas según una selección de países o vincular sus planes de viaje al servicio a través de una correduría de viajes.

Algunos proveedores han desarrollado aplicaciones para móviles que permiten acceder con más facilidad a sus servicios informativos y que quien viaje reciba alertas de seguridad en sus teléfonos. Algunos de estos proveedores incluyen el acceso a estas aplicaciones para móviles en sus paquetes normales, mientras que otros cobran una cantidad adicional por dicho servicio. Es importante percatarse de que estos servicios no tienen por qué ir dirigidos a personal de ONG. La organización ha de examinar los anuncios y los consejos que emiten estos proveedores y, si es necesario, ofrecer orientación adicional al personal.

Reuniones informativas en materia de seguridad

El personal y visitantes que se embarquen en un viaje deben recibir información sobre seguridad específica del país o la zona antes de embarcar y también al llegar, y será la propia organización quien se la proporcione cuando tenga presencia en país o bien la organización local colaboradora.

Puede que no sea realista para la organización celebrar una reunión informativa presencial en materia de seguridad para cada integrante del

personal y visitantes que viajen. Por lo tanto, es importante vincular los requisitos sobre reuniones informativas a un sistema de calificación de riesgo por país o viaje para asegurar que quienes viajan a contextos con un riesgo más alto siempre reciben información minuciosa sobre seguridad. De todas maneras, toda persona que viaje debería recibir al menos información sobre las amenazas clave y las precauciones que deben tomar para evitarlas.

Lista de comprobación para una sesión informativa en materia de seguridad

- **Situación actual:** ofrecer una panorámica de la situación actual en materia de seguridad, incluso agentes y grupos clave, motivos de agitación o conflicto, estado del orden público, niveles de criminalidad y las zonas específicas afectadas.
- **Riesgos de seguridad:** subrayar las principales amenazas de seguridad para el personal, cualquier incidente reciente y cómo el personal debería evitarlos o responder ante ellos. Además, hay que destacar cualquier preocupación o riesgo en materia de seguridad para el personal particularmente en relación con su nacionalidad, grupo étnico, identidad de género, orientación sexual o diversidad funcional.
- **Salud y protección:** resaltar los principales peligros naturales y riesgos para la salud en el país o en determinadas zonas, las precauciones básicas que debería tomar el personal y cómo responder ante problemas de salud o urgencias médicas.
- **Conducta y comportamiento:** destacar toda la legislación importante del lugar, las normas y costumbres locales y remarcar qué comportamiento se espera del personal.
- **Viajes y movimientos:** explicar los documentos identificativos y de viaje precisos para moverse dentro del país o en determinadas zonas, el proceso de autorización y cualquier restricción de movimientos (por ejemplo, toque de queda o zonas prohibidas).
- **Comunicación:** explicar los sistemas que se utilizan para mantener el contacto con el personal y qué sucederá si pierden un punto de contacto acordado con antelación, así como los problemas o las restricciones de seguridad en materia de comunicación.
- **Alojamiento:** ofrecer una visión general del alojamiento y de las medidas de seguridad clave con las que se cuenta.
- **Contactos claves:** proporcionar al personal la lista de contactos esenciales y asegurarse de que se entiendan cómo y a quién informar en caso de incidente.

Quienes viajan con frecuencia pueden argumentar que no necesitan estas reuniones, pero a pesar de su experiencia, pueden correr más riesgos, ya que los cambios en el contexto y en las amenazas pueden no serles evidentes de inmediato.

Las sesiones informativas en materia de seguridad con análisis de contextos específicos deberían proporcionar a quienes viajan, la información actualizada y las orientaciones sobre riesgos de seguridad y para la salud, de forma que puedan entender la situación del lugar lo suficiente como para operar en términos seguros en él.

Más información

Documento informativo del EISF "Género y Seguridad: directrices para la transversalización del género en la gestión de riesgos de seguridad"

Monitoreo de viajes

La organización tiene que ser capaz de mantener contacto con el personal y con otras personas que viajen en nombre de la organización, y seguir sus movimientos. Con qué frecuencia será necesario contactar, va a depender del grado de riesgo en esa ubicación. En la mayoría de los casos, se trata de una mera llamada de teléfono o un mensaje SMS que se envía a un punto de contacto predefinido. Hay que acordar un horario aproximado para que el personal establezca ese contacto y también con quién han de contactar, aunque no tenga nada de lo que informar. Como mínimo, la organización debería saber: que las personas llegaron bien; si hay cambios en su itinerario previsto; cuando salen; y que han vuelto a casa bien. El personal debe conocer las consecuencias de no cumplir los puntos de control acordados, es decir, un proceso que va en aumento. Dicho aumento debe aplicarse uniformemente a toda la organización o cualquier sistema de seguimiento podría dejar de tener sentido.

Si se produce un incidente o un evento importante de seguridad en el país al que viaja el personal, la organización deberá ser capaz de identificar con rapidez dónde está todo el personal y si es probable que se hayan visto afectados por el incidente. Ahora es más fácil hacerse con soluciones tecnológicas de seguimiento en viaje y muchos sistemas son capaces de monitorear la ubicación exacta de personas gracias al GPS por satélite o del teléfono móvil. Parte del personal puede ser reacio a que le sigan tan de cerca y dichas soluciones de rastreo suelen considerarse solo en contextos de riesgo extremo. Una solución de rastreo en viaje más habitual, y que podría ser más adecuada para ONG más pequeñas, rastrea la ubicación amplia de quienes viajan según sus reservas de vuelo. Muchas empresas de reservas de viajes

y proveedores de ayuda en materia de seguridad ofrecen servicios de rastreo en viaje; los servicios básicos pueden ser gratuitos, pero las soluciones más integrales supondrán costes adicionales.

"Si le proporciona al personal un número de teléfono en caso de emergencia, es fundamental que las llamadas se respondan con rapidez 24 horas al día, 365 días al año. No es aceptable que se devuelva la llamada dos horas después con un '¡Lo siento, es sábado!'"

Cooperante de una ONG

Seguro de viaje

Concertar el seguro recae en diferentes posiciones dentro de las muchas ONG existentes y puede no obtener la ponderación del grado de seguridad que merece. Existen muchísimas opciones de seguros. Es peligroso elegir el seguro solo en función del precio, y supone un ahorro en falso. Por ejemplo, las pólizas más baratas suelen tener restricciones de cobertura y pueden no incluir conflictos, inestabilidad y acciones terroristas o determinados destinos. Suelen restringir lugares en función de las evaluaciones gubernamentales sobre los riesgos de viajar. Por lo tanto, hay que comprar ampliaciones específicas para velar por que el personal tenga cobertura total.

Al comprar o revisar los seguros, hay que asegurarse de que las pólizas que se están considerando se adecúan al destino y al perfil de riesgo, que los países y los lugares a los que debe viajar el personal no estén excluidos, y que el personal y otras personas que viajen en nombre de la organización están, al menos, debidamente aseguradas para tener cobertura médica. El tratamiento y la repatriación de una persona trabajadora, consultoría o visitante con una lesión grave sin seguro cuesta muchísimo dinero. Muchas compañías de seguros también incluyen oportunidades de formación o de acceso a otros servicios de gestión de riesgos que pueden ayudar a reducir el riesgo organizacional, por lo que sin duda merece la pena hablar con el proveedor de seguros para ver de qué servicios o apoyo dispone.

Aunque los seguros sean caros, sin duda, el grueso de dicho coste corresponde a elementos de cobertura que no son negociables dado el tipo de trabajo que desempeñan las ONG. Por lo tanto, incluir servicios adicionales como información de viajes y alertas, evacuaciones de seguridad y apoyo en crisis no supondría un gran incremento de los costes generales de la prima anual de la organización, pero puede aportar unas ventajas considerables en la gestión de riesgos de seguridad, sobre todo para ONG más pequeñas con capacidad y recursos limitados por país.

La información sobre el seguro de quienes viajan ha de proporcionarse a la organización de acogida en el país cuando sea posible, incluso en visitas a

las oficinas de la propia organización, ya que el seguro de viaje puede ser de un proveedor distinto para quienes estén basados en el país.

Tipos de seguro

- **Viaje internacional y accidente/enfermedad personal:** cubre seguro de viaje por negocios y por accidente o enfermedad, incluso cubre evacuación médica o repatriación, para las personas aseguradas (personal y partes asociadas) que viajan en representación de la organización. Salvo que la póliza incluya cobertura de "riesgos de guerra", muchas pólizas excluyen determinadas amenazas y destinos de alto riesgo (según los consejos de viaje gubernamentales o la lista que emita la compañía de seguros) y, por lo tanto, la cobertura para estos lugares o riesgos puede requerir primas adicionales.
- **Seguro internacional de salud:** cubre beneficios sanitarios y evacuación médica o repatriación para el personal internacional (y familiares acompañantes) que esté destinado en el extranjero. Cuando el personal viaja fuera del país en el que está destinado, lo habitual será que le cubra el seguro de viaje de la organización.
- **Planes de seguros nacionales de salud:** planes de atención sanitaria local o regional. La disponibilidad y la extensión de la cobertura varían, pero la mayoría reembolsa los gastos médicos en los que incurra el personal contratado en el país. Cuando se incluya la cobertura de evacuación médica, suele limitarse al traslado dentro del país.
- **Seguro de respuesta de emergencia y evacuación:** cubre el apoyo no médico y la evacuación a consecuencia de la inestabilidad política, conflicto o catástrofe natural. Puede incluirse como parte de su paquete de seguro de viaje principal o se puede adquirir como cobertura adicional.
- **Seguro de riesgos especiales:** cobertura ante secuestro, rescate y extorsión (o gestión de crisis), que reembolsa los costes que incurra una organización al responder a un incidente concreto. El seguro también incluye acceso a consultores especialistas en respuesta que puedan asesorar y respaldar a la organización en la gestión de un incidente.

Más información

"Guide to selecting appropriate Crisis Management Insurance", de Harry Linnell

"Módulo 11: Apoyo médico y evacuación" en la guía del EISF "Seguridad en práctica"

"Anexo 5: Seguros" en la guía de ODI "Informe de Buena Práctica 8 – Gestión de la seguridad de las operaciones en entornos violentos"

Documento informativo del EISF "Engaging Private Security Providers: A Guideline for Non-Governmental Organisations"

7 Sensibilización y capacitación

Una parte integral de mejorar la sensibilización en materia de seguridad de su personal y la cultura de seguridad de su organización es ofrecer al personal acceso a una formación adecuada sobre seguridad que sea pertinente para su puesto y para el entorno en el que trabajan, junto con orientación y apoyo continuos.

Todo el personal debe estar sensibilizado y contar con la destreza en materia de seguridad que le permita gestionar su propia seguridad, así como la de sus compañeros.

Iniciación a la seguridad

Debe informar a su personal en términos adecuados sobre las políticas y el enfoque de seguridad de la organización, por el que debe conocer y estar preparado para los riesgos y los desafíos a los que puede enfrentarse durante su trabajo.

Para ello, resulta crucial contar con un proceso de iniciación a la seguridad para todo el nuevo personal al comienzo de su contratación. Lo ideal sería incluir la aproximación a la seguridad dentro de un proceso de iniciación más amplio de RR. HH. y que guiase a los nuevos integrantes del personal sobre la cultura de seguridad de la organización, sus políticas y planteamientos, a la vez que se explicasen sus puestos y responsabilidades concretos en relación con todo esto.

Lista de comprobación para la iniciación a la seguridad

- **Planteamiento de seguridad:** explicar cómo enfoca la seguridad la organización, su perfil de riesgo y su actitud general hacia el riesgo.
- **Política:** presentar la política de seguridad de la organización, sus principios clave y los requisitos mínimos de seguridad, al igual que cómo se aplican en distintas situaciones.
- **Estructura de gestión de riesgos de seguridad:** explicar las funciones y las responsabilidades en materia de seguridad dentro de la organización.
- **Responsabilidad individual:** destacar la responsabilidad de cada persona sobre su propia seguridad y la de sus compañeros, la importancia del consentimiento informado y su derecho a decir que no si consideran que una situación es insegura.
- **Seguridad en viaje:** tratar con el personal que viaja las disposiciones de seguridad con las que se cuenta. Presentar los procedimientos de seguridad y viaje, así como explicar los requisitos de autorización, reunión informativa, formación y monitoreo de viaje con los que se cuenta.
- **Procedimientos de emergencia:** explicar los procedimientos de emergencia de la organización. Informar al personal sobre el proveedor de atención médica y cómo contactarle.
- **Informar de incidentes:** explicar de qué incidentes de seguridad se debería informar y los procedimientos que hay que seguir.
- **Recursos adicionales:** familiarizar al personal con los recursos de seguridad adicionales, tales como guías, manuales y materiales de formación.

Formación en materia de seguridad

La formación es una parte esencial para mejorar la sensibilización en materia de seguridad y la capacidad de gestión del personal. Muchas ONG entienden la importancia de la formación sobre seguridad; sin embargo, en la práctica, los costes y la disponibilidad siguen siendo obstáculos significativos para que las organizaciones lleguen a aplicar y a mantener una formación en materia de seguridad. En concreto, a las ONG más pequeñas puede costarles dotar de

recursos o justificar los gastos que implica ofrecer una formación en materia de seguridad. No obstante, con los avances de las herramientas de seguridad en línea y de recursos de *e-learning*, ahora existe una amplia gama de opciones que pueden contemplar las organizaciones que quieran mejorar la sensibilización y la capacitación de su personal en materia de seguridad.

Tipos de formación en materia de seguridad

Se pueden dividir los cursos de formación en materia de seguridad en cuatro tipos principales:

- **Sensibilización personal sobre seguridad:** dirigido a personas que trabajan en entornos de riesgo moderado o viajan a ellos. Proporciona una sensibilización personal básica sobre los posibles riesgos de seguridad y cómo mitigarlos y responder ante ellos.
- **Sensibilización personal avanzada en materia de seguridad o formación sobre entornos hostiles (HEAT, por sus siglas en inglés):** dirigido a personas con sede en entornos de riesgo alto o que viajan a ellos. Proporciona una formación exhaustiva sobre seguridad personal y ante amenazas específicas, incluso con ejercicios de simulacro.
- **Gestión de riesgos de seguridad:** dirigido a personas con responsabilidad en la gestión de riesgos de seguridad (referentes de seguridad, gestores de programas e integrantes de la dirección). Presenta los conceptos principales de la gestión de riesgos de seguridad y sirve para desarrollar destrezas en el diagnóstico de riesgos de seguridad, la gestión de riesgos de seguridad operativa y la gestión de incidentes críticos.
- **Gestión de crisis:** dirigido a la dirección o a los equipos de gestión de crisis (en sede o en país). Proporciona sensibilización sobre los principios y las actuaciones en la respuesta a incidentes críticos o a situaciones de crisis. Se imparte combinando ejercicios o talleres tanto en vivo como teóricos.

Ha de tenerse en cuenta la financiación de la formación en materia de seguridad al formular propuestas y presupuestos de proyectos. Los costes asociados a la formación sobre seguridad pueden sufrir grandes variaciones en función del proveedor, el lugar y el tipo de formación necesaria.

Antes de empezar a contemplar una formación sobre seguridad, debe averiguar qué formación necesita su personal, según los lugares donde trabaja o a los que viaja dicho personal, sus funciones y responsabilidades, el perfil de riesgo y el trabajo que desempeña su organización. Por ejemplo, no tiene sentido someter al personal a un curso caro de inmersión en entornos hostiles de cuatro días si suelen viajar a países con un riesgo moderado durante periodos cortos, están sobre todo en capitales y pasan la mayor parte de su tiempo en reuniones o en un hotel.

Al llevar a cabo un análisis de las necesidades básicas de formación, es importante tener en cuenta:

- Las competencias y destrezas de seguridad necesarias para puestos y actividades específicos dentro de su organización;
- El grado de experiencia en materia de seguridad y de formación previa que posee el personal existente;
- La cantidad de personal que precisa de un tipo específico de formación en materia de seguridad;
- La distribución geográfica del personal y dónde debería impartirse la formación en materia de seguridad para llegar al máximo de personal con el coste mínimo;
- El presupuesto disponible y los costes de las diversas opciones de formación.

Después de haber identificado y asignado prioridades a los requisitos de formación en materia de seguridad en su organización, debe contemplar cuál es la mejor manera de ajustar dichas necesidades con los recursos y las opciones de formación disponibles, lo que variará de un país a otro. Entre los recursos de formación potenciales se encuentran:

- **Cursos en línea.** Varias organizaciones ofrecen cursos en materia de seguridad gratuitos en línea, que proporcionan recursos útiles y baratos de formación en materia de seguridad para el personal. Aunque los cursos en línea no ofrecen las mismas ventajas que la formación presencial, proporcionan una introducción integral sobre seguridad y no es difícil ponerlos como un requisito de formación obligatorio para el personal.

Cursos en línea sobre seguridad

Estos son algunos de los cursos en línea y gratuitos que están disponibles en la actualidad (todos los cursos requieren inscripción individual):

- **DisasterReady.org**: una plataforma de aprendizaje en línea gratuita para cooperantes con una serie de cursos sobre seguridad (incluso los cursos sobre seguridad de Save the Children y RedR).
- **Kayaconnect.org**: la plataforma de formación de Humanitarian Leadership Academy, que ofrece varios cursos en línea y gratuitos sobre seguridad (incluso cursos sobre seguridad de UNHCR y de Save the Children).
- **Plataforma de aprendizaje de IFRC**: proporciona acceso a los cursos en línea de *Stay Safe - Personal Security* y *Stay Safe - Security Management* de IFRC.
- **Formación de UNDSS**: proporciona acceso a los cursos en línea de la ONU, *Basic Security in the Field* y *Advanced Security in the Field*.

- **Cursos abiertos.** Varios proveedores externos de formación organizan cursos regulares abiertos, en Europa y en núcleos regionales, que suelen ser más baratos que los cursos a medida (pero el personal tendrá que desplazarse al lugar donde se imparta la formación). Para organizaciones con restricciones financieras, los cursos abiertos pueden suponer una opción más sostenible, ya que elaborar y mantener una formación propia en materia de seguridad precisa de bastante capacidad de seguridad.
- **Cursos a medida.** Existen cada vez más proveedores externos y formadores particulares que ofrecen un amplio abanico de cursos y servicios de formación en materia de seguridad a medida. Muchos proveedores o formadores pueden organizar la formación tanto en sede como en las oficinas en país. Aunque los cursos a medida sobre seguridad suelen ser más caros que los cursos abiertos, también es más probable que se adecuen al planteamiento de seguridad específico de la organización y a los riesgos a los que se enfrenta el personal.
- **Formación entre agencias.** En algunos países, órganos de coordinación entre agencias o el Departamento de Seguridad de Naciones Unidas (UNDSS) -dentro del marco Salvar vidas entre todos (*Save Lives Together*, SLT)- ofrece formación de seguridad para personal de ONG. Si su organización tiene personal con sede en distintos países, puede que consigan acceder a estos cursos de formación en materia de seguridad local a tarifas con bonificación o, en algunos casos, gratis.

▶ *Para obtener más información sobre Saving Lives Together, véase el Apartado 10: Colaboración y redes en material de seguridad.*

Compruebe que la formación externa es adecuada para una ONG. Muchos proveedores y cursos se dirigen sobre todo a quienes viajan por negocios, periodistas o estudiantes y por eso no abordan los desafíos de seguridad singulares a los que se enfrenta el personal de ONG ni los planteamientos necesarios para gestionar dichos riesgos.

Se aconseja utilizar mecanismos de coordinación de seguridad para descubrir qué formación externa están utilizando otras ONG. La página web de EISF proporciona una lista de cursos de formación sobre seguridad, que sólo se anuncian una vez que el proveedor de formación haya recibido dos referencias positivas y por dos distintas organizaciones que forman parte de EISF.

Elegir proveedores externos de formación

Cuando esté identificando proveedores externos de formación, tenga en cuenta lo siguiente:

- **Perfil:** ¿Sus valores, su motivación, su ética y su cultura encajan con las de su organización y las de su personal?
- **Reputación y experiencia:** ¿Pueden proporcionar referencias y testimonios creíbles? ¿Cuáles son sus clientes previos y actuales? ¿Tienen la capacidad y la experiencia para proporcionar cursos adecuados?
- **Contenido:** ¿Cuál es el contenido, el planteamiento y la metodología de la formación? ¿Encajan con su perfil y con su planteamiento sobre seguridad? ¿La formación incluye ejercicios de simulacro? ¿Qué tipo de incidentes y grado de ataque se van a utilizar durante estos ejercicios?
- **Costes:** ¿Los costes incluyen la preparación, el viaje, la impartición y la labor tanto previa como posterior? ¿Son razonables y comparables a los de otros proveedores para la formación solicitada?
- **Formadores:** ¿Qué destrezas, conocimientos y experiencia poseen los formadores? ¿Cuál es la composición de género de los formadores? ¿Puede solicitar a formadores concretos?
- **Lugar e idioma:** ¿Dónde se va a impartir la formación? ¿Su personal la puede acceder? ¿Existen gastos de viaje adicionales? ¿Qué idioma se necesita para la formación? ¿Cuentan con formadores que pueden impartir la formación en los idiomas de los que precisa su organización?

Más información

"NGO Safety and Security Training Project: How to Create Effective Security Training for NGOs", de EISF e InterAction

Documento informativo del EISF "Engaging Private Security Providers: A Guideline for Non-Governmental Organisations"

Página web del EISF sobre formación y eventos

8 Monitoreo de incidentes

Es crucial informar a tiempo de los incidentes para proteger al personal. Eso asegura que el personal recibe ayuda con rapidez y que se gestiona con eficacia la respuesta ante el incidente y sus consecuencias. Un buen sistema para monitorear incidentes servirá para que otros compañeros puedan evitar incidentes parecidos y que reaccionen adecuadamente a cambios en el entorno operativo. También mejorará la comprensión que se tienen del contexto y respaldará la toma de decisiones sobre gestión.

Informar y monitorear incidentes con regularidad permite a las organizaciones determinar dónde y cómo cambian las situaciones de seguridad, por qué están cambiando y que implican dichos cambios para la seguridad del personal.

Para la mayoría de las ONG más pequeñas, no suele presentar demasiado valor invertir en sistemas amplios para informar de incidentes, ya que lo más probable es que no tengan que lidiar con demasiados incidentes. Sin embargo, establecer un sistema básico para informar y registrar incidentes

de seguridad resulta esencial para todas las organizaciones, grandes y pequeñas. Un sistema básico para monitorear incidentes cuenta con dos componentes clave:

1. Un proceso para el informe inicial sobre un incidente o una situación;;
2. Un sistema para manejar la información de la que se ha informado.

Procedimientos para reportar incidentes

Los procedimientos para informar de incidentes deberían indicar con claridad qué incidentes hay que reportar, a quién y mediante qué mecanismos.

No resulta sencillo introducir un sistema para informar de incidentes en una organización: lleva tiempo y perseverancia para que cale y para que se informe de todos los incidentes. En todas las organizaciones existe el desafío de infra informar, así que deberá comunicar con claridad al personal la finalidad, la justificación y las ventajas previstas de informar sobre incidentes. Resultan cruciales una mejor sensibilización sobre la necesidad de informar, la confianza en cómo maneja la información la organización, comentar con el personal sus informes sobre incidentes y un mecanismo fácil de utilizar para establecer un sistema para informar que sea eficaz.

De qué informar

Para muchas organizaciones, un *incidente de seguridad* es: **cualquier situación o evento que haya provocado o que pueda conllevar daños para el personal, empleados asociados o terceros, una alteración significativa de programas y actividades, o daños o pérdidas considerables para el patrimonio o la reputación de la organización**.

También han de reportarse conatos, ya que eso puede evitar que otras personas se vean envueltas en un incidente y ayudar al personal a entender si el contexto de seguridad está cambiando y, en ese caso, cómo lo hace.

Aunque se alentará al personal para que informe de todos los incidentes, se tendrá que dejar muy claro cuál es un incidente del que informar. Las percepciones sobre qué es un incidente variarán mucho entre distintos integrantes del personal y lugares, en función de lo que se considere la norma en dicho contexto. Si bien puede estar seguro de que se informará de los incidentes principales, existe el riesgo de que el personal pase por alto o deseche incidentes que parecen aislados o insignificantes y que, si se contemplan en su conjunto, pueden conllevar un cambio en su situación de seguridad.

También ha de informarse sobre "conatos". Un conato es un evento donde, ya sea por suerte o por una respuesta adecuada, se ha evitado un incidente grave.

Deben examinarse todos los incidentes graves en su integridad para entender los acontecimientos que llevaron a ellos o que se produjeron durante o después del incidente. Una investigación tras el incidente —a poder ser dirigida por alguien que no guarde relación con el incidente— contemplará todas las causas o motivos posibles, la actuación y el comportamiento del personal, y la respuesta ante el incidente. Al investigar el incidente, deberían identificarse recomendaciones clave o actuaciones de seguimiento, incluso procedimientos disciplinarios posibles, para mejorar constantemente la gestión de los riesgos de seguridad.

Informes sobre incidentes

Como mínimo, los informes deben abordar las **5W** (como se dice en inglés): ***Quién*** hizo ***Qué*** a ***Quién***, ***Dónde*** y ***Cuándo***.

Normalmente, existen tres tipos de informes sobre incidentes:

- **Informe inmediato de incidente:** se envía cuando se produce el incidente o lo antes posible justo después (cuando sea seguro hacerlo), lo más habitual es que sea oral por teléfono o radio y que sea un resumen breve de lo que ha sucedido y cualquier actuación o apoyo necesarios.
- **Actualizaciones del incidente:** se envían con la frecuencia que sea precisa para proporcionar más información sobre el incidente o la situación.
- **Informe tras el incidente:** se envía una vez se estabilice o cese el incidente, con una narración por escrito del incidente y de las distintas actuaciones que se emprendieron.

Formularios para informar sobre incidentes

Un formulario informativo sobre incidentes estándar y fácil de utilizar puede aportar claridad y coherencia al proceso para informar de la organización. Debe elaborarse un informe formal tras el incidente para todos los incidentes de seguridad que impliquen a su personal directamente o a otras personas que trabajen en nombre de su organización. También han de elaborarse informes después de un incidente que conlleve daños o pérdidas sustanciales de propiedades o que cause lesiones o daños a terceros.

Un informe sobre un incidente de seguridad proporcionará una narración por escrito completa del incidente y de las diversas actuaciones que se adoptaron. Se debería crear una plantilla estándar para todos los informes tras los incidentes.

Habrá información que se deba tratar con confidencialidad, como algunas condiciones de salud, incidentes de agresión sexual, nombres de víctimas, etc. Se debe orientar al personal sobre cómo manejar información delicada o confidencial para proteger la confidencialidad; por ejemplo, directrices acerca de quién tiene permiso para acceder a los informes sobre incidentes, así como cuándo y cómo ha de restringirse el acceso a dichos informes.

Formulario para informar sobre incidentes

Un formulario para informar de incidentes debería incluir:

- **Tipo de incidente:** aclarar el tipo de incidente; por ejemplo, hurto, robo o robo a mano armada.
- **Lugar:** dónde se produjo el incidente, lugar exacto.
- **Fecha, día y hora:** cuándo se produjo el incidente, con toda la precisión posible.
- **Quién estuvo involucrado:** a quién afectó el incidente, incluido su puesto, tipo de programa, nacionalidad, género, etc., para entender mejor las vulnerabilidades específicas.
- **Descripción del incidente:** una descripción minuciosa del carácter de los acontecimientos, las repercusiones en las personas afectadas y datos sobre cualquier pérdida material.
- **Análisis del incidente:** una evaluación inicial sobre quién puede haber perpetrado el incidente, qué provocó el incidente, si el objetivo concreto era la organización o su personal, y las repercusiones potenciales para la seguridad del personal en un futuro.
- **Decisiones y actuaciones adoptadas de inmediato:** información sobre las decisiones y las actuaciones adoptadas, y por quién, justo después del incidente.
- **A quién se ha informado:** una lista donde se detalle a quién se ha informado del incidente en términos locales; por ejemplo, las autoridades, otras agencias humanitarias, donantes u otras partes interesadas.
- **Otras acciones pendientes:** detallar las decisiones y las actuaciones que deben adoptarse en respuesta al incidente. Dar algunas recomendaciones para mejorar la seguridad del personal.

Más información

Ejemplo de un formulario para informar sobre incidentes (en inglés)

"Capítulo 5: Notificación de incidentes y gestión de incidentes críticos" en la guía del ODI "IBP8 - Gestión de la seguridad de las operaciones en entornos violentos"

"Herramienta práctica F: Buenas prácticas en el informe de incidentes en materia de género" en el documento de EISF "Género y Seguridad: Directrices para la transversalización del género en la gestión de riesgos de seguridad"

Registro y análisis de incidentes

Los registros de todos los incidentes de seguridad deberían centralizarse y analizarse periódicamente. Además de proporcionar un registro institucional del incidente y de la respuesta de la organización en caso de litigio o de investigaciones externas, el análisis de esta información almacenada permitirá que la organización desarrolle una comprensión más amplia y global de las cuestiones de seguridad que afectan al personal.

El análisis regular de los informes sobre incidentes de su organización se puede utilizar para:

- Sensibilizar a su personal sobre seguridad y así reforzar la cultura de seguridad de la organización;
- Conseguir que la dirección y el consejo de administración entiendan mejor, según el perfil de riesgo de la organización, las principales amenazas que afectan al personal y brechas en procedimientos, apoyo y formación;
- Proporcionar análisis para mejorar la toma de decisiones en el diseño y la aplicación de programas;
- Negociar con aseguradoras. Los seguros suelen fiarse de las "estadísticas globales" para establecer las primas, pero si se pueden demostrar los riesgos específicos a los que está expuesta la organización y las medidas con las que cuenta para gestionarlos, se pueden convencer de rebajar las primas (o, al menos, de no subirlas).

Ahora existen múltiples conjuntos de programas informáticos comerciales y herramientas de software de código abierto que se pueden utilizar para registrar y analizar los datos sobre incidentes, y muchas organizaciones han creado su propia base de datos integral sobre informes de incidentes. Sin embargo, para algunas ONG esto puede suponer demasiado dinero o puede resultar demasiado complejo su creación y mantenimiento. Puede considerar que para su organización basta con utilizar meras hojas Excel para registrar la información clave de distintos informes sobre incidentes.

Se aconseja compartir la información entre agencias, cuando sea posible, para que su organización pueda aprovechar una mayor comprensión del contexto —por ejemplo, al acceder y contribuir al proyecto Aid in Danger de Insecurity Insight y a la base de datos Aid Worker Security Database, de Humanitarian Outcomes.

Más información

"Applicability of Open Source Systems (Ushahidi) for Security Management, Incident and Crisis Mapping: Acción contra el Hambre (ACF-Spain) Case Study", de Gonzalo de Palacios en el documento informativo del EISF "Communications Technology and Humanitarian Delivery"

Documento informativo del EISF "Incident Statistics in Aid Worker Safety and Security Management"

Proyecto Aid in Danger de Insecurity Insight

Aid Worker Security Database de Humanitarian Outcomes

Incident Dashboard de INSO

9 Gestión de crisis

El fallecimiento, la detención o el secuestro del personal es un gran desafío para cualquier organización. La organización no sólo tiene que responder ante incidentes, gestionar las relaciones con las autoridades y ofrecer apoyo a familiares y compañeros, sino que también debe al mismo tiempo continuar gestionando sus actividades y personal en otros lugares.

Resolver y gestionar con éxito cualquier situación de crisis depende de la capacidad de la organización de adoptar las decisiones adecuadas con rapidez, lo que requiere preparación, un buen flujo de información y canales claros de comunicación que todo el personal entienda.

La preparación es esencial para gestionar con éxito cualquier incidente, sobre todo cuando es necesaria una respuesta coordinada y eficaz en varios lugares e involucra a distintas partes interesadas.

Establecer una estructura de gestión de crisis

La mayoría de los incidentes de seguridad se tratarán a través de la jerarquía administrativa habitual de la organización. Sin embargo, pueden surgir situaciones excepcionales que, a causa del carácter y de la gravedad del incidente o sus repercusiones más amplias, requieran que su organización establezca una estructura específica para responder. Esto se suele denominar crisis.

Una parte fundamental de la planificación previa ante dichos eventos es identificar un equipo que coordinará y gestionará la respuesta de la organización. Un elemento clave de esto es el Equipo De Gestión de Crisis (EGC) en sede o a nivel regional, aunque varía mucho su composición y la terminología que utilizan las distintas organizaciones, así como sus responsabilidades. En muchos casos el equipo responsable estará compuesto por integrantes clave del equipo directivo de la organización. No obstante, las funciones dentro del EGC suelen ir determinadas por la experiencia, la capacidad y las destrezas que aportan las personas al equipo, en lugar de basarse solo en el puesto que ocupan.

Es más fácil desactivar un EGC cuando resulta evidente que el incidente no es tan grave como se preveía de lo que es montar un equipo después de que el incidente haya avanzado.

Tendrá que crear un equipo y una estructura general de gestión de crisis que se adecúe a su organización. Sin embargo, las buenas prácticas según la experiencia suelen incluir un pequeño EGC en sede y un Equipo de Gestión de Incidentes (EGI) lo más cerca de donde se haya producido el incidente (o se esté produciendo) que sea seguro estar. La autoridad en la toma de decisiones estratégicas es de la categoría profesional más alta y es externa al EGC. El personal de respaldo fundamental, que sería el personal de apoyo familiar, una persona portavoz y la plantilla de logística debería considerarse parte de la estructura de respuesta para gestionar una crisis, pero no son integrantes del EGC. No está de más identificar personas que puedan ser una alternativa para cada una de las funciones principales para así velar por que la cobertura durante un incidente prolongado, o si alguien está enfermo, de baja o de viaje, sea la adecuada. No obstante, como ONG más pequeña puede considerar que esto es un todo un desafío y por lo tanto necesita identificar un equipo adecuado, teniendo en cuenta la capacidad, la destreza y la experiencia de la que dispone.

Equipo de gestión de crisis (EGC)

Se trata de un equipo pequeño que se dedica a gestionar todos los aspectos de un incidente o una situación, y que hace de enlace con todas las partes interesadas involucradas.

La composición y las responsabilidades del equipo varían en función del tipo de incidente o situación, su ubicación y el grado de ayuda necesario.

Principales funciones del EGC	
Coordinación de crisis	Coordinación y gestión general del EGC y principal autoridad en la toma de decisiones dentro del equipo. La coordinación de crisis suele reportar al director ejecutivo o CEO, en quien recae la toma de decisiones ejecutiva.
Recursos humanos	Asesora sobre la política de RR.HH. y coordina todos los aspectos relacionados con personal, apoyo familiar y seguros en la respuesta ante un incidente crítico.
Programas y operaciones	Asesora sobre el contexto del país, las actividades del programa y las partes interesadas pertinentes en país, y coordina toda la comunicación con el equipo en país.
Comunicaciones y medios	Asesora sobre cuestiones mediáticas y coordina todas las actividades en medios y toda la comunicación interna.
Gestión de información respaldo	Respalda al EGC y mantiene los registros de información durante la respuesta.

Un miembro del EGC puede desempeñar varias funciones. Dependiendo del carácter del incidente y de la capacidad dentro de la organización, puede que sean necesarios puestos de apoyo adicionales, incluso en seguridad, finanzas, seguros, asesoría jurídica, redes sociales, comunicaciones internas e informática.

El equipo de gestión de incidentes (EGI) tendrá funciones internas parecidas a las del EGC, aunque se centrará en una gestión más localizada al incidente. Es crucial una comunicación definida y gestionada con claridad entre el EGC y el EGI para responder con éxito a cualquier crisis. Para países donde la ONG no cuenta con personal permanente en el país en cuestión del incidente, se tendrá que incluir alguna disposición sobre cómo proporcionar una respuesta localizada en el plan de gestión de crisis.

¿Cuándo es una crisis?

El momento en el que un incidente o una situación pasan a ser críticos o una crisis depende sobre todo de su gravedad, pero también influye la capacidad, el grado de planificación previa y la experiencia de la organización al tratar con tales incidentes. Para algunas ONG, los incidentes o las situaciones menos graves pueden considerarse también críticos a causa de la limitación en capacidad, experiencia y recursos que la organización puede reunir para responder. Se suele identificar como "crisis" cuando las estructuras de gestión habituales ya no se consideran suficientes para hacer frente al incidente y por eso se inicia la respuesta de gestión de crisis.

La dirección debe evaluar con rapidez cualquier incidente o situación que afecte a su personal y sus programas para determinar sus repercusiones potenciales y para aclarar el grado de participación y apoyo necesario para gestionar la situación. Se debe identificar con claridad qué es lo que desencadena el mecanismo de gestión de crisis y, dentro de la organización, quién toma esa decisión. Entre los ejemplos de incidentes críticos que seguramente activan su equipo de gestión de crisis están:

- El fallecimiento o la lesión grave de alguien del personal;
- El fallecimiento o la lesión grave de terceros a consecuencia de las acciones del personal o de las actividades de la organización;
- Un deterioro grave de la seguridad o una amenaza concreta que afecte directamente a la seguridad del personal;
- Un incidente con múltiples víctimas (por ejemplo, catástrofes naturales, bombas o atentados) que afecte al personal;
- Un ataque físico o violencia sexual contra alguien del personal;
- El rapto, secuestro, detención o arresto que afecte al personal;
- Cualquier incidente de seguridad que tenga probabilidad de dañar la representación en los medios.

Principios para gestionar una crisis

Al responder ante cualquier incidente crítico que involucre al personal, deben utilizarse los siguientes principios clave:

- Minimizar daños mayores y velar por la seguridad y el bienestar de la(s) víctima(s) y de otro personal que se haya visto afectado por el incidente.
- Reafirmar a las familias y a otras personas de la plantilla en que la respuesta de la organización es la adecuada y proporcionar apoyo a los familiares afectados.
- Minimizar posibles daños o pérdidas de bienes y recursos; reducir cualquier repercusión negativa para la reputación de la organización y para la continuidad de programas o actividades existentes, siempre que esto no ponga en riesgo la seguridad y el bienestar del personal.
- Mantener una comunicación eficaz con todas las partes interesadas, internas y externas, para permitir su colaboración, sin perder de vista la necesidad de confidencialidad.

Planes de gestión de crisis

Cada incidente es único y, por lo tanto, es difícil prepararse por completo, pero existen mecanismos y disposiciones fundamentales que se pueden planificar con antelación.

Aunque un plan de gestión de crisis es un documento de sede que ayuda a la dirección a movilizar y a centrar recursos para responder a incidentes críticos o situaciones de crisis que involucran al personal, también debe existir un elemento de país para el EGI. Definir con claridad funciones y responsabilidades, y elaborar puntos de acción clave, listas de verificación y herramientas como parte de un plan de gestión de crisis, permitirá que el personal responda con más rapidez y adecuación. Debería empezar a mantener un registro de decisiones y actuaciones en cuanto se active el mecanismo de respuesta ante crisis.

El personal experimentará bastante estrés al responder ante una crisis, por lo que los planes para gestionar una crisis deberían ser sencillos y con listas a las que acceder con facilidad.

Planes para gestionar una crisis

Los elementos clave de un plan básico para gestionar una crisis deberían incluir:

- **Presentación:** explicar a quién va dirigido el documento, a quién cubre el plan, las definiciones clave que se utilizan, y quién y cuándo debería revisarse el documento.
- **Activación y desencadenantes:** especificar cómo se activa el mecanismo de respuesta ante crisis de la organización y cómo se desactiva, quién decide y qué criterios se utilizan.
- **Gestión y toma de decisiones:** exponer la estructura para gestionar incidentes críticos, las partes interesadas clave involucradas, los principios para gestionar una crisis de la organización y las cuestiones de confidencialidad. Incluir un diagrama de decisiones que explique la comunicación y la toma de decisiones.
- **Labores y responsabilidades:** describir las labores y las responsabilidades específicas para las distintas funciones dentro de la estructura de respuesta ante crisis, incluso el EGC, el EGI y el personal de apoyo. En los términos de referencia se especificarán las responsabilidades de cada labor antes, durante y después del incidente.
- **Protocolos de incidentes:** incluir procedimientos y orientación sobre las posibles acciones inmediatas, las cuestiones de gestión de partes interesadas y las necesidades de apoyo tras el incidente referentes a escenarios de incidentes concretos; por ejemplo, urgencias médicas, violencia sexual, catástrofes naturales, evacuaciones de seguridad, incidentes de raptos y secuestros, y fallecimiento del personal.
- **Recursos y herramientas:** incluir listas de comprobación, formatos y herramientas que refuercen la respuesta de la organización, incluso plantillas para registrar comunicados y decisiones, listas de contactos clave, etc.

Proveedores de asistencia y apoyo

Los proveedores especializados de asistencia externa pueden desempeñar una función vital como apoyo a su organización durante una crisis al asegurar acceso a conocimientos y consejos especializados cuando es más necesario. En algunos casos, en función de la nacionalidad de las personas involucradas, los gobiernos de origen también pueden proporcionar apoyo especializado.

Incluso organizaciones más grandes, que tienen equipos de seguridad en plantilla y una amplia capacidad en materia de seguridad, utilizan a proveedores de asistencia externos durante situaciones de crisis. Para ONG

más pequeñas, que pueden carecer de la experiencia de tratar con este tipo de incidentes o de la capacidad para cubrir las distintas funciones del EGC, establecer acceso a asistencia externa de antemano a un incidente puede ser un factor principal en la mejora de la capacidad de respuesta ante crisis de la organización.

Las organizaciones pueden acceder a servicios integrales de apoyo en gestión de crisis y de asistencia en emergencias de proveedores y consultores comerciales, a través de su seguro o al captar directamente a empresas y personas. Es importante velar por que todos los expertos que se utilicen sean adecuados para la organización y que tengan los conocimientos precisos. Existe una amplia gama de servicios disponibles, incluso asistencia médica y apoyo para evacuación por motivos médicos, evacuación del personal por deterioro de la situación de seguridad o por catástrofe natural, acceso a consultoras en caso de rapto o secuestro, y apoyo y formación en materia de gestión de crisis. Al contemplar un apoyo adicional, debería tener claro el tipo de servicios de apoyo que se incluyen en su seguro existente y qué empresas de respuesta prestan dichos servicios.

Su organización no puede delegar la gestión de incidentes críticos ni ceder su responsabilidad decisoria a un proveedor externo de asistencia o a otras partes interesadas. Su organización debe mantener su compromiso activo y su responsabilidad de velar por que todas las respuestas y actuaciones sean adecuadas. Cualquier mecanismo externo de apoyo debería complementar la propia respuesta de la organización ante un incidente crítico.

Los países pueden ayudar a repatriar a sus ciudadanos en caso de evacuación provocada por un incidente de seguridad (por ejemplo, un golpe de estado); no obstante, eso dependerá del país, tanto de origen como de destino, y no ha de darse por hecho.

La ONU tampoco garantiza la evacuación de cooperantes que no sean empleados de la ONU. Incluso si lleva a cabo una evacuación, es probable que cobre el coste íntegro de su ayuda.

Más información

Ejemplo de un plan de gestión de crisis (en inglés)

Guía del EISF "Managing the Message: Communication and Media Management in a Crisis"

Guía del EISF "Family First: Liaison and Support During a Crisis"

Documento informativo del EISF "Crisis Management of Critical Incidents"

Documento informativo del EISF "Engaging Private Security Providers: A Guideline for Non-Governmental Organisations"

10 Colaboración y redes en materia de seguridad

Las ONG, cada vez más preocupadas por la seguridad de su personal, están haciendo más hincapié en la colaboración y en compartir información en materia de seguridad con otras organizaciones. El acceso a información fiable, el análisis y el asesoramiento pueden aumentar la sensibilización sobre la situación, respaldar una mejor toma de decisiones y más fundamentada, y al final reforzar los planteamientos de seguridad de todas las organizaciones, grandes y pequeñas. No obstante, la colaboración en materia de seguridad supone tiempo e inversión por parte del personal para que sea eficaz. A fin de cuentas, los mecanismos de colaboración son tan buenos como sea la participación de las organizaciones involucradas.

Compartir información de seguridad y colaborar de manera activa con otras organizaciones mejora la seguridad colectiva de todos.

Redes de seguridad entre agencias

En los últimos años, las ONG han formado diversas redes y plataformas entre agencias en materia de seguridad, tanto por país, como por región y en sede. Dichas colaboraciones facilitan el intercambio de información en materia de seguridad, sensibilizan mediante formaciones y talleres sobre seguridad, y fomentan las buenas prácticas. Existe un amplio abanico de mecanismos, con diversos grados de formalidad. Entre ellos se incluyen: reuniones informales entre unas cuantas ONG para conversar sobre los desafíos de seguridad, oficinas dedicadas a la seguridad que proporcionan información y apoyo a la comunidad de ONG en un contexto concreto, y redes de membresía en sede para los referentes de seguridad de distintas ONG (como EISF e InterAction).

La gama de servicios que prestan tales iniciativas en país puede incluir:

- Convocar reuniones o sesiones informativas en materia de seguridad;
- Emitir alertas de seguridad o avisos y advertencias sobre amenazas;
- Proporcionar informes de seguridad con regularidad;
- Preparar informes analíticos sobre tendencias de incidentes o desafíos específicos de seguridad;
- Hacer de enlace con UNDSS y otros agentes de seguridad (las fuerzas nacionales de seguridad, incluso la policía y el ejército, las fuerzas militares internacionales, etc.);
- Facilitar el acceso a formación y talleres sobre seguridad;
- Prestar ayuda y respaldo durante situaciones e incidentes críticos.

En sede o en región, los servicios suelen incluir:

- Convocar reuniones para tratar cuestiones relacionadas con la seguridad;
- Facilitar que se comparta información sobre buenas prácticas en la gestión de riesgos de seguridad;
- Apoyar a las organizaciones a desarrollar estrategias y políticas adecuadas para una gestión de riesgos de seguridad eficaz;
- Hacer de enlace con agentes de seguridad, como la ONU, en sede o en términos estratégicos;
- Abogar por que se mejore y que se preste más atención a la seguridad de los cooperantes dentro del sector humanitario en su amplitud.

European Interagency Security Forum (EISF)

El EISF es una red independiente de referentes de seguridad que actualmente representan a ONG humanitarias con operaciones internacionales. Su compromiso es mejorar la seguridad de las operaciones de ayuda y del personal, así como reforzar la gestión de riesgos de seguridad humanitaria para lograr un mayor acceso a poblaciones afectadas por crisis.

El secretariado del EISF trabaja en colaboración con sus miembros para realizar investigaciones originales, celebrar encuentros bianuales del foro y talleres regulares, así como para facilitar que se comparta información entre los miembros y la comunidad de ONG más amplia. Visite EISF en www.eisf.eu

Una información a tiempo y fiable, así como los consejos y el apoyo que prestan estos mecanismos, podrían suponer contribuciones significativas para la seguridad del personal. No obstante, dado que la información y las advertencias que proporcionan estos mecanismos de coordinación son generales de contexto y no a medida de una organización concreta, resulta crucial que usted evalúe la pertinencia de dichos consejos para su organización en función de su perfil y su capacidad específicos. Se debe alentar a los compañeros con responsabilidades sobre seguridad en país y en sede a identificar y forjar relaciones con las diversas redes de seguridad entre agencias.

"Aun si una organización decide no participar en un mecanismo de coordinación formal en materia de seguridad, debería procurar compartir información y tratar las cuestiones de seguridad en terreno. Como ONG no trabajamos aisladas y, por lo tanto, la seguridad de nuestro personal depende mucho de la información y el apoyo que recibimos de otras organizaciones."

Referente de seguridad en una ONG

En términos globales, existen varias iniciativas encaminadas a reforzar la colaboración sobre seguridad entre organizaciones, incluso el marco Salvar vidas entre todos - Saving Lives Together, que pretende mejorar la colaboración sobre seguridad en terreno entre la ONU y las ONG.

Marco Salvar vidas entre todos (Saving Lives Together)

Saving Lives Together es un conjunto de recomendaciones destinadas a perfeccionar la colaboración en materia de seguridad entre el sistema de gestión de la seguridad de la ONU y las organizaciones internacionales/ONG, e incluye:

- El establecimiento de disposiciones y foros para coordinar la seguridad;
- Compartir información pertinente sobre seguridad;
- La cooperación en formación sobre seguridad;
- La cooperación en disposiciones operativas y logísticas;
- Identificar los requisitos de recursos para mejorar la coordinación en materia de seguridad entre la ONU, las ONG internacionales y las organizaciones internacionales, y promover la financiación;
- La asesoría en normas básicas comunes para la acción humanitaria.

Más información

"Saving Lives Together - A Framework for Improving Security Arrangements Among IGOs, NGOs and UN in the Field", de IASC

"Guidelines for the Implementation of the Saving Lives Together Framework", de Saving Lives Together

European Interagency Security Forum (EISF) Strategic Security Coordination Mechanisms (página temática del EISF)

International NGO Safety Organisation (INSO)

International NGO Safety and Security Association (INSSA)

InterAction

11 Monitoreo de cumplimiento y eficacia

Toda iniciativa para perfeccionar la seguridad en su organización correrá el riesgo de perder apoyo e impulso después de su lanzamiento. Los riesgos a los que se enfrenta su personal cambian constantemente y, por lo tanto, su gestión de riesgos de seguridad debe ser revisada y mejorada continuamente.

La gestión de los riesgos de seguridad ha de responder a los cambios, tanto en el entorno externo como dentro de la organización. Las ONG deben controlar y revisar su marco de gestión de riesgos de seguridad para asegurarse de que sigue siendo el adecuado para tal fin.

Su organización debería monitorear el cumplimiento y llevar a cabo revisiones y auditorías de seguridad periódicas para determinar si las políticas y procedimientos mantienen su eficacia y si se siguen en la práctica, así como que se gestionan adecuadamente los riesgos de seguridad en toda la organización para permitir el acceso y la aplicación de los programas.

Monitoreo de cumplimiento

Entonces, ¿qué está monitoreando? Básicamente, está comprobando si el personal está cumpliendo las políticas y los procedimientos de seguridad, y que estos funcionan como se esperaba. Un monitoreo rutinario, tanto del cumplimiento como del número de incidentes que se producen, servirá para velar por que se gestionan los riesgos con eficacia conforme al marco, a las políticas y a los procedimientos de seguridad de su organización. Eso también servirá para evaluar la eficacia (por ejemplo, el acceso, las repercusiones, las ventajas y los costes) de su planteamiento general sobre seguridad. Existen distintas maneras para monitorear el cumplimiento, entre ellas:

- **Listas de comprobación de cumplimiento:** una lista de comprobación puede servir a los directores o a los representantes de país para evaluar el cumplimiento de políticas de seguridad y requisitos mínimos existentes. Aunque dichas listas de cumplimiento no pueden sustituir por completo a una auditoría o a una revisión integral, pueden ser de ayuda cuando una organización está desplegando un marco de gestión de riesgos de seguridad para supervisar el progreso que se ha logrado o los obstáculos encontrados.

  Véase "Herramienta 3 – Lista de comprobación para la revisión de documento" en la guía del EISF "Auditorías de seguridad"

- **Indicadores clave de desempeño (KPI, por sus siglas en inglés):** crear KPI relativos a seguridad puede servir para supervisar si se ponen en práctica distintos elementos del marco de gestión de riesgos de seguridad y si, en efecto, minimizan los riesgos para el personal. Algunos ejemplos de KPI para esta supervisión serían: planes de seguridad actualizados (% completado); el personal que viaja a destinos de riesgo elevado recibe información sobre seguridad (% de éxito); personal que recibe formación (cifra total); e incidentes de los que se ha informado (cifra total).

  Para conocer más indicadores de ejemplo, véase Herramienta 6 – Plantilla para la auditoría del sistema de gestión de seguridad en la guía del EISF "Auditorías de seguridad"

- **Análisis de incidentes:** el seguimiento y la revisión de incidentes que afectan al personal supondrán una mejora en cómo la organización evalúa su perfil de riesgo. Entender qué tipo de incidentes suceden que involucren al personal, con qué frecuencia y por qué servirá para identificar problemas potenciales de cumplimiento o brechas en procedimientos, apoyo y formación.

  Véase el Apartado 8: Monitoreo de incidentes

Si el grado de cumplimiento es bajo, puede ser necesario endurecer la postura ante infractores. No obstante, un escaso cumplimiento puede ser una advertencia de que el personal considera que no es práctico aplicar algunas partes del marco de gestión de riesgos de seguridad y los procedimientos con los que cuenta. Habrá que revisar estos puntos y ajustarlos como parte de la

puesta en práctica continúa del marco de gestión de riesgos de seguridad de la organización.

Auditorías y revisiones de seguridad

Aunque en el monitoreo de cumplimiento se utilizan comprobaciones rutinarias, tendrá que realizar una auditoría o revisión de seguridad más minuciosa en algún punto. Una auditoría de gestión de riesgos de seguridad es una revisión interna o externa con pruebas del marco de gestión de riesgos de seguridad de una organización y su puesta en práctica, y evalúa si la organización cumple sus responsabilidades de deber de cuidado con el personal.

Existen dos tipos de auditoría de gestión de riesgos de seguridad:

- **Auditorías organizacionales**, que revisan las disposiciones para gestionar los riesgos de seguridad en toda la organización;
- **Auditorías por país o ubicación**, que revisan el planteamiento y los sistemas de gestión de riesgos de seguridad en un país o área concretos, a menudo como respuesta a un aumento de la inseguridad o a cambios en el entorno operativo. Dichas auditorías han de realizarse conforme a las políticas en términos organizacionales y no de forma aislada.

El objetivo de la auditoría o revisión debería ser examinar cuán efectivo es el planteamiento de la organización sobre gestión de riesgos de seguridad para lograr los objetivos del programa y para elaborar un plan de acción que potencie la seguridad de todo el personal. Asegúrese de elegir un amplio elenco de personal para la auditoría o revisión (sobre todo, a los "propietarios del riesgo", es decir, las personas que se responsabilizan y que rinden cuentas sobre las decisiones de gestión de riesgos de seguridad), no solo para evaluar la consciencia y la comprensión que tiene el personal de los sistemas con los que se cuenta, sino también para permitirles destacar los riesgos y los desafíos de seguridad a los que se enfrentan en su trabajo.

Para lograr una opinión no sesgada y comparar su organización con otras ONG, o por tener una capacidad limitada, puede resultar útil recurrir a una consultora externa para que realice la auditoría o revisión de seguridad. Emprender una revisión externa supone unos costes considerables y sacarle el máximo partido al proceso resulta vital.

Una alternativa a recurrir a una consultora puede ser trabajar con otra ONG y llevar a cabo un proceso de revisión entre pares (*peer review*).

Asegúrese de que se comunican los hallazgos y las recomendaciones a las personas que hayan participado, así como con el personal en sentido más amplio. Compartir dichos resultados con el personal no solo respalda la transparencia, sino que también sirve para sensibilizar sobre la importancia de la gestión de riesgos de seguridad dentro de la organización.

Muchas organizaciones han utilizado con éxito la caja de herramientas que incluye la guía "Auditorías de seguridad" del EISF para realizar auditorías tanto internas como externas, y puede proporcionar un punto de referencia útil, así como ayuda para identificar áreas a las que destinar recursos.

Revisiones de seguridad externas

Una buena revisión externa de seguridad precisa de que la consultora y el cliente trabajen bien juntos y que ambos sean francos sobre expectativas y responsabilidades desde el comienzo. Al encargar una revisión externa de seguridad, debería:

- asegurarse de que existe una necesidad auténtica de apoyo externo o de un punto de vista independiente;
- redactar unos términos de referencia claros y concisos. Poner de manifiesto el alcance de la revisión, las entregas precisas y los plazos;
- ser realista respecto al tiempo, la cantidad de días que implica y el presupuesto preciso;
- identificar consultoras apropiadas mediante un proceso de selección que sea adecuado para la escala de la revisión;
- estar preparado para hablar de prioridades y requisitos con la consultora. Confirmar todos los acuerdos sobre modificaciones de los términos de referencia por escrito;
- identificar un único punto de contacto dentro de la organización al que informará la consultora y al que mantendrá al tanto de los avances;
- proporcionar a la consultora acceso a la información. Entre los documentos clave de los que precisa la consultora están las políticas de seguridad existentes, las pautas para la gestión de riesgos de seguridad, procedimientos para viaje, planes de seguridad por país, documentos de gestión de crisis e información sobre incidentes previos;
- velar por que los compañeros aporten tiempo y materiales a respaldar la revisión. Decidir quién va a disponer las entrevistas con las partes interesadas y enviar un correo electrónico al personal con antelación para solicitar su apoyo y disponibilidad;
- gestionar las expectativas de los compañeros sobre la revisión, difundir los términos de referencia y elaborar una manera práctica de solicitar comentarios sobre los hallazgos y las recomendaciones del informe;
- proporcionar comentarios a la consultora sobre los resultados del informe y las recomendaciones, y sobre la experiencia general de la consultoría.

Más información

Guía del EISF "Auditorías de seguridad"

12 Recursos de apoyo

Como refuerzo de la gestión de riesgos de seguridad de su organización, todos los cargos directivos y el personal deberían tener acceso a orientación, herramientas y plantillas pertinentes en materia de seguridad. Un elemento esencial para desarrollar el marco de gestión de riesgos de seguridad de su organización es recopilar y dar acceso a una biblioteca de recursos útiles relacionados con la seguridad. Utilice las guías en temas de seguridad personal y recursos para la gestión de seguridad en ONG que ya existen, en lugar de reinventarlos.

Páginas web útiles

www.eisf.eu

www.eisf.eu/themes

www.eisf.eu/themes/other-coordination-mechanisms/

www.eisf.eu/training-and-events/

www.ngosafety.org

www.ngosafety.org/keydata-dashboard

https://inssa.org

www.insecurityinsight.org/aidindanger

https://aidworkersecurity.org/incidents

www.disasterready.org/

https://kayaconnect.org

https://ifrc.csod.com/

https://training.dss.un.org/

Orientación sobre seguridad personal

Stay Safe. Manténgase a salvo. Guía de la Federación Internacional para una misión más segura, de IFRC, 2009.

Seguridad primero. Una guía de seguridad para trabajadores humanitarios de campo, de Shaun Bickley, Save the Children, 2014.

Staying Alive: Safety and Security Guidelines for Humanitarian Volunteers in Conflict Areas, de David Lloyd Roberts, ICRC, 2005.

Manual de seguridad para periodistas: guía práctica para reporteros en zonas de riesgo, de Reporteros Sin Fronteras y la UNESCO, 2015.

Orientación sobre gestión de riesgos de seguridad

Seguridad en práctica: herramientas de gestión de riesgos para organizaciones de ayuda humanitaria, 2º edición, de James Davis et al, EISF, 2017.

Informe de Buena Práctica 8 – Gestión de la seguridad de las operaciones en entornos violentos, edición revisada por Koenraad van Brabant, Overseas Development Institute (ODI), 2010.

ISO 31000:2009: Gestión del riesgo: principios y directrices, de la Organización Internacional de Normalización (ISO), 2009.

Auditorías de seguridad, de Christopher Finucane, EISF, 2013.

Mainstreaming the Organisational Management of Safety and Security (HPG Report 9) de Koenraad van Brabant, Overseas Development Institute (ODI), 2001.

Documentos de ejemplo

Example Job Description: Logistics and Security Officer. Disponible en: https://www.eisf.eu/library/job-description-example-logistics-and-security-officer/

Example Job Description: Field Security Coordinator. Disponible en https://www.eisf.eu/library/job-description-example-field-security-coordinator/

Example Job Description: Deputy Director of Global Security. Disponible en https://www.eisf.eu/library/job-description-example-deputy-director-global-security/

Example Job Description: Director of Staff Safety and Security. Disponible en https://www.eisf.eu/library/job-description-example-director-of-staff-safety-and-security/

Organisational Security Policy Framework Example. Disponible en: https://www.eisf.eu/library/organisational-security-policy-framework-example/

Open NGO Security Policy. Centre for Safety and Development. Disponible en: https://www.eisf.eu/library/open-ngo-security-policy/

Security Assessment Tool. ACT Alliance. Disponible en: www.eisf.eu/library/security-assessment-tool/

Security Plan Example. InterAction. Disponible en: https://www.eisf.eu/library/security-plan-example/

Travel Risk Assessment Form Example. Disponible en: www.eisf.eu/library/travel-risk-assessment-form-example

Incident Report Template Example. Disponible en: https://www.eisf.eu/library/incident-report-template-example/

Crisis Management Plan Example. Disponible en: https://www.eisf.eu/library/crisis-management-plan-example/

Glosario

Aceptación: generación de un ambiente operativo seguro a través del consentimiento, la aprobación y la cooperación de personas, de comunidades y de autoridades locales.

Actitud ante el riesgo: el planteamiento de la organización sobre el diagnóstico de riesgos y, en consecuencia, enfatizarlos, mantenerlos, asumirlos o evitarlos.

Amenaza: cualquier desafío en materia de seguridad u otros al que se enfrente la organización, su personal, sus activos, su reputación o programas que existan en el contexto donde opera dicha organización.

Auditoría de seguridad: una revisión interna o externa basada en pruebas del marco de gestión de riesgos de seguridad de una organización y su puesta en práctica, que evalúa la eficacia del marco de gestión de riesgos de seguridad para permitir que se satisfagan los objetivos de la organización y si la organización cumple su responsabilidad del deber de cuidado respecto al personal.

Crisis: un acontecimiento que altera bastante las operaciones habituales, que ha provocado o que es probable que provoque un sufrimiento grave, o que tenga consecuencias graves para las personas, el personal o las organizaciones, y que precisa de medidas extraordinarias para restaurar el orden y la normalidad, por lo que demanda una actuación inmediata por parte de la dirección.

Cultura de seguridad: la cultura de una organización se puede definir simplemente como "la forma en la que hacemos aquí las cosas". Cada organización posee una cultura hacia la seguridad y los riesgos en general.

Deber de cuidado: obligación legal y moral de una organización de tomar todas las medidas posibles para reducir el riesgo de daños a aquellas personas que trabajan para la organización o en su nombre.

Diagnóstico de riesgos: proceso para que la organización identifique las distintas amenazas de seguridad que podrían afectar al personal, a los bienes y a los programas, y analice su probabilidad e impacto a fin de determinar el grado de riesgo que implican.

Disuasión: reducción del riesgo al contener la amenaza contrarrestándola (p.ej., protección armada, presión diplomática/política, suspensión temporal).

Equipo de gestión de crisis: un equipo que gestiona una situación de crisis (es decir, un incidente crítico) en sede o a nivel regional.

Estrategia de seguridad: el planteamiento general de la organización sobre la gestión de riesgos de seguridad; por ejemplo, a través de una estrategia de aceptación, de protección o de disuasión.

Gestión de riesgos: las actividades coordinadas que dirigen y controlan una organización respecto a los riesgos.

Incidente crítico: un acontecimiento, o una serie de ellos, que amenaza gravemente el bienestar del personal, que puede acabar en fallecimiento, lesiones o enfermedades mortales, y que desencadena la respuesta de gestión de crisis de una organización. Un incidente crítico también puede ser un acontecimiento que tenga graves repercusiones para los programas, los activos o la reputación de una organización.

Incidente de seguridad: cualquier situación o evento que haya provocado o que pueda derivar en daños para el personal, asociados o terceros, una alteración considerable de los programas o de las actividades, o pérdidas y daños para las propiedades o la reputación de la organización.

Marco de gestión de riesgos de seguridad: un conjunto de políticas, protocolos, planes, mecanismos y responsabilidades que respaldan la reducción de los riesgos de seguridad para el personal.

Plan de seguridad: documentos clave para país que explican las medidas y los procedimientos de seguridad con los que se cuenta y las responsabilidades y los recursos precisos para ponerlos en práctica.

Política de seguridad: un documento global que declara con claridad el planteamiento de la organización sobre los riesgos de seguridad, los principios clave que sustentan dicho planteamiento y las funciones y las responsabilidades que tiene todo el personal en la gestión de dichos riesgos.

Protección: reducir la vulnerabilidad de la organización ante una posible amenaza; por ejemplo, a través de la construcción de muros o la contratación de guardias.

Riesgo: cómo una amenaza podría afectar a la organización, a su personal, a sus activos, su reputación o sus programas, teniendo en cuenta las vulnerabilidades específicas.

Seguridad (security): salvaguarda ante riesgos y daños derivados de actos de violencia, agresión o delitos intencionados contra el personal, los bienes o las propiedades de la organización.

Seguridad (safety): salvaguarda ante riesgos o daños derivados de actos, acontecimientos o peligros no intencionados o accidentales.

Vulnerabilidad: exposición de la organización a una amenaza. Variará dependiendo del carácter de la organización, cómo trabaja, qué programas emprende, las características de su personal y su capacidad para gestionar riesgos.

Referencias

A. Fairbanks, "Duty of Care under Swiss law: how to improve your safety and security risk management processes", EISF, 2018. Disponible en: https://www.eisf.eu/library/duty-of-care-under-swiss-law-how-to-improve-your-safety-and-security-risk-management-processes/ [Accedido el 21 de febrero de 2019]

ACT Alliance, *Security Assessment Tool*, EISF, 2011. Disponible en: www.eisf.eu/library/security-assessment-tool/ [Accedido el 25 de abril de 2017]

C. Finucane, *Auditorías de seguridad*, EISF, 2014.

C. Finucane, *Humanitarian Safety and Security: Obligations and responsibilities towards local implementing partners*, Church World Service, 2011. Disponible en: https://www.eisf.eu/library/humanitarian-safety-and-securiy-obligations-and-responsibilities-towards-local-implementing-partners/ [Accedido el 25 de abril de 2017]

C. Finucane, *The Cost of Security Risk Management for NGOs*, EISF, 2013.

C. Garrett, *Developing a security-awareness culture – improving security decision making*, SANS Institute, 2005. Disponible en: https://www.eisf.eu/library/developing-a-security-awareness-culture-improving-security-decision-making/ [Accedido el 25 de abril de 2017]

C. Persaud, *Género y seguridad: directrices para transversalización del género en la gestión de riesgos de seguridad*, EISF, 2012.

C. Persaud, *NGO Safety and Security Training Project: How to Create Effective Security Training for NGOs*, EISF e InterAction, 2014.

Centre for Safety and Development, *Open NGO Security Policy*, EISF, 2011. Disponible en: https://www.eisf.eu/library/open-ngo-security-policy/ [Accedido el 25 de abril de 2017]

Comité Permanente entre Organismos (IASC), "Saving Lives Together - A Framework for Improving Security Arrangements Among IGOS, NGOs and UN in the Field", IASC, 2015. Disponible en inglés en: https://interagencystandingcommittee.org/collaborative-approaches-field-security/content/saving-lives-together-framework-improving-security-0 [Accedido el 10 de mayo de 2017]

E. Jones, et al., *Managing the Security of Aid Workers with Diverse Profiles*, EISF, 2018.

E. Kemp y M. Merkelbach, "Can you get sued? Legal liability of international humanitarian aid organisations towards their staff", *Security Management Initiative*, 2011. Disponible en: https://www.eisf.eu/library/can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/ [Accedido el 25 de abril de 2017]

E. Kemp y M. Merkelbach, "Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications", EISF, 2016. Disponible en: https://www.eisf.eu/library/duty-of-care-a-review-of-the-dennis-v-norwegian-refugee-council-ruling-and-its-implications/ [Accedido el 25 de abril de 2017]

G. de Palacios, "Applicability of Open Source Systems (Ushahidi) for Security Management, Incident and Crisis Mapping: Acción contra el Hambre (ACF-Spain) Case Study", en *Communications Technology and Humanitarian Delivery*, EISF, 2014. Disponible en: https://www.eisf.eu/library/communications-technology-and-security-risk-management/ [Accedido el 25 de abril de 2017]

G. de Palacios, "La seguridad de los cooperantes solitarios", EISF, 2016. Disponible en: https://www.eisf.eu/news/the-security-of-lone-aid-workers/ [Accedido el 10 de enero de 2019]

G. Dhoot, et al., *Managing Sexual Violence against Aid Workers: prevention, preparedness, response and aftercare*, EISF, 2019.

H. Linnell, "Guide to selecting appropriate Crisis Management Insurance", EISF, 2017. Disponible en: https://www.eisf.eu/news/guide-to-selecting-appropriate-crisis-management-insurance/ [Accedido el 25 de abril de 2017]

I. Singh, *Security Management and Capacity Development: International Agencies Working with Local Partners*, EISF, 2012.

InterAction, *Security Plan Example*, EISF, 2017. Disponible en: https://www.eisf.eu/library/security-plan-example/ [Accedido el 24 de abril de 2017]

J. Davis et al, *Seguridad en práctica: herramientas de gestión de riesgos para organizaciones de ayuda humanitaria, 2º edición*, EISF, 2017.

K. van Brabant, *IBP8 – Gestión de la seguridad de las operaciones en entornos violentos, edición revisada*, Overseas Development Institute (ODI), 2010. Disponible en: https://odihpn.org/wp-content/uploads/2011/04/GPR8_revised_edition_Spanish.pdf [Accedido el 10 de enero de 2019]

K. van Brabant, *Incident Statistics in Aid Worker Safety and Security Management*, EISF, 2012. Disponible en: https://www.eisf.eu/library/incident-statistics-in-aid-worker-safety-and-security-management/ [Accedido el 25 de abril de 2017]

L. Hodgson et al. *Security Risk Management and Religion: Faith and secularism in humanitarian assistance*, EISF, 2014.

M. Glaser, *Engaging Private Security Providers: A Guideline for Non-Governmental Organisations*, EISF, 2011.

M. Merkelbach, *Voluntary Guidelines on the Duty of Care to Seconded Civilian Personnel*. Swiss Federal Department of Foreign Affairs (FDFA), Stabilisation Unit (SU) y Center for International Peace Operations (ZIF), 2017. Disponible en: http://www.zif-berlin.org/fileadmin/uploads/experten-einsaetze/Voluntary_Guidelines_on_the_Duty_of_Care_to_Seconded_Civilian_Personnel_Final_170420.pdf [Accedido el 10 de mayo de 2017]

O. Behn y M. Kingston, "Whose Risk Is It Anyway? Linking Operational Risk Thresholds and Organisational Risk Management", *Humanitarian Exchange Magazine*, número 47, junio de 2010. Disponible en: http://odihpn.org/magazine/whose-risk-is-it-anyway-linking-operational-risk-thresholds-and-organisational-risk-management/ [Accedido el 25 de abril de 2017]

O. Behn y M. Kingston, *Risk Thresholds in Humanitarian Assistance*, EISF, 2010.

Organización Internacional de Normalización (ISO), ISO 31000:2009: *Gestión del riesgo. Principios y directrices*, 2009.

P. Buth, *Crisis Management of Critical Incidents*, EISF, 2010.

S. Davidson, *Family First: Liaison and Support during a Crisis*, EISF, 2013.

S. Davidson, *Managing the Message: Communication and Media Management in a Crisis*, EISF 2013.

Saving Lives Together, *Guidelines for the Implementation of the "Saving Lives Together" Framework*, Saving Lives Together, julio de 2016. Disponible en: https://www.eisf.eu/library/guidelines-for-the-implementation-of-the-saving-lives-together-framework/ [Accedido el 10 de mayo de 2017]

Source 8, *Office Opening: A guide for non-governmental organisations*, EISF, 2015.

Anexo. **Marco de gestión de riesgos de seguridad. Guía de referencia rápida**

Gobernanza y rendición de cuentas

- Definir una estructura adecuada para gestionar los riesgos de seguridad de la organización para permitir que se cumplan los objetivos y velar por que se entiendan con claridad las funciones y las responsabilidades.
- Identificar a un referente de seguridad que respalde la elaboración y la puesta en práctica del marco de gestión de riesgos de seguridad.
- Establecer un grupo de trabajo o un comité interdepartamental sobre seguridad que supervise la elaboración y la puesta en práctica del marco de gestión de riesgos de seguridad.
- Asegurarse de que todas las descripciones o términos de referencia de puestos pertinentes detallan las funciones y las responsabilidades en materia de gestión de riesgos de seguridad relativas a dicho puesto o actividad.

Políticas y principios

- Desarrollar una política de seguridad que plasme los principios y el planteamiento sobre seguridad de la organización.
- Velar por que la política describa con claridad la actitud de la organización hacia el riesgo, su estructura para gestionar los riesgos de seguridad y las responsabilidades de seguridad de cada uno de los integrantes del personal y las que corresponden a funciones concretas de seguridad.
- Identificar unos requisitos mínimos de seguridad que sean prácticos y adecuados con los que deba contar cada lugar o actividad, vinculados a un sistema de calificación de riesgos por país.

Operaciones y programas

- Elaborar un proceso sencillo para diagnosticar los riesgos de seguridad que identifique los riesgos clave en un país o lugar específico y que explique las medidas de control presentes para gestionar dichos riesgos.
- Velar por que todos los programas en país realicen diagnósticos de riesgos de seguridad de manera habitual y por que estos se documenten.
- Velar por que los planes de seguridad, que explican las medidas y los procedimientos de seguridad con los que se cuenta para gestionar los riesgos identificados, se establecen en todos los lugares donde la organización tenga una presencia considerable o donde trabaje habitualmente.
- Evaluar la capacidad de seguridad y el apoyo a disposición del personal por parte de colaboradoras u organizaciones de acogida locales. Asegurarse de todas las disposiciones y los acuerdos para apoyar en cuestiones de seguridad manifiesten con claridad las responsabilidades de ambas partes.

Gestión de viajes y apoyo

- Obtener un sistema de calificación de riesgos básico por país o viaje para informar al personal sobre los riesgos relativos a viajar o a trabajar en dichos países. Establecer unos requisitos mínimos sobre medidas, mecanismos y formación de seguridad que se apliquen a cada calificación de riesgos.
- Asegurarse de que se elaboren y se aprueben los diagnósticos de riesgos en viaje cada vez que el personal viaje a destinos de riesgo elevado o si el carácter de la visita plantea preocupaciones sobre seguridad.
- Elaborar unos procedimientos de seguridad en viaje internacional específicos para el personal, los consultores y los visitantes que viajan. En ellos se deberían aclarar las funciones y las responsabilidades, la formación y las reuniones informativas, el seguimiento en viaje, las autorizaciones y los procedimientos de emergencia.
- Velar por que el personal reciba información y pautas detalladas y actualizadas sobre seguridad, protección y riesgos para la salud en su destino antes de que partan de viaje.
- Asegurarse de que todo el personal, los consultores y los visitantes que viajan a contextos de riesgo más elevado asisten a una reunión informativa sobre seguridad específica para el país o la zona a la que van a viajar, antes de su partida y al llegar (si la organización cuenta con una oficina en país).

- Establecer procedimientos de verificación para el personal que viaje, para así controlar sus movimientos y velar por que se pueda ubicar al personal según sus reservas de vuelo.
- Velar por que todo el personal, consultores incluidos, posea la cobertura de seguros adecuada en sus viajes y en su trabajo en terreno, y por que todo el personal cuente con toda la información sobre sus pólizas de seguros.

Sensibilización y capacitación

- Asegurarse de que todo el personal nuevo recibe una iniciación a la seguridad que cubra la política y el planteamiento sobre seguridad de la organización, así como las responsabilidades dentro de la organización.
- Identificar recursos adecuados de formación en línea sobre seguridad que todo el personal debería recibir como parte de su iniciación.
- Revisar distintas opciones de formación en materia de seguridad para diferentes categorías de personal en función de los entornos de riesgos a los que viajen o donde trabajen, así como sus responsabilidades de seguridad.

Monitoreo de incidentes

- Desarrollar procedimientos para informar de incidentes y formatos posibles. Orientar al personal sobre la importancia de informar sobre incidentes, de qué hay que informar y cómo.
- Establecer un sistema de registro de incidentes para almacenar información clave sobre todos los incidentes de seguridad que afecten al personal.
- Revisar periódicamente todos los incidentes que hayan afectado al personal para identificar tendencias y problemas potenciales en incidentes de seguridad.

Gestión de crisis

- Identificar una estructura apropiada de gestión de crisis para coordinar y gestionar la respuesta de la organización ante incidentes críticos.
- Elaborar un plan de gestión de crisis que explique las funciones y las labores del EGC y del EGI, deje clara la autoridad decisoria y destaque los procedimientos clave de respuesta en situaciones de crisis.
- Contemplar incluir el acceso a servicios de apoyo sobre gestión de crisis (médicos y no médicos) como parte de la cobertura de seguros de la organización.

Colaboración y redes en materia de seguridad

- Velar por que el personal participe con regularidad en foros y reuniones en materia de seguridad entre agencias para reforzar la colaboración en seguridad y que se comparta información.

Monitoreo de cumplimiento y eficacia

- Proporcionar a los directores o a los representantes en país con una lista de comprobación para gestionar los riesgos de seguridad que les sirva para evaluar si se están cumpliendo las políticas de seguridad y los requisitos mínimos.
- Asegurarse de que se realizan auditorías habituales de seguridad por país o por programa, sobre todo si las actividades se desarrollan en países de riesgo elevado.
- Emprender una revisión periódica del planteamiento y el marco de gestión de riesgos de seguridad de la organización y desarrollar un plan de acción para mejorar la seguridad y la protección de todo el personal.
- Establecer y hacer cumplir una cultura sólida de disciplina respecto al incumplimiento de políticas de seguridad y los requisitos mínimos de seguridad.

Recursos de apoyo

- Poner a disposición un abanico de pautas, herramientas y plantillas dentro de una biblioteca en materia de seguridad para ayudar a los directores y al personal a gestionar los riesgos de seguridad.

Otras publicaciones de EISF

Si tiene interés en colaborar en futuros proyectos de investigación o desea sugerir temas para futuras investigaciones, por favor póngase en contacto con **eisf-research@eisf.eu**.

Documentos e informes

Duty of Care under Swiss law: how to improve your safety and security risk management processes
October 2018
Fairbanks, A.
cinfo and EISF

Managing the Security of Aid Workers with Diverse Profiles
September 2018
Jones, E. *et al.*

Communications Technology and Humanitarian Delivery: Challenges and Opportunities for Security Risk Management – 2nd edition
December 2016
Vazquez Llorente, R. and Wall, I. (eds.)

Security Risk Management and Religion: Faith and Secularism in Humanitarian Assistance
August 2014
Hodgson, L. *et al.* Edited by Vazquez, R.

The Future of Humanitarian Security in Fragile Contexts
March 2014
Armstrong, J. Supported by the EISF Secretariat

The Cost of Security Risk Management for NGOs
February 2013
Finucane, C. Edited by Zumkehr, H. J. – EISF Secretariat

Security Management and Capacity Development: International Agencies Working with Local Partners
December 2012
Singh, I. and EISF Secretariat

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
September 2012 – *Sp. and Fr. versions available*
Persaud, C. Edited by Zumkehr, H. J. – EISF Secretariat

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011 – *Fr. version available*
Glaser, M. Supported by the EISF Secretariat (eds.)

Risk Thresholds in Humanitarian Assistance
October 2010
Kingston, M. and Behn O.

Abduction Management
May 2010
Buth, P. Supported by the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Buth, P. Supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Ayre, R. Supported by the EISF Secretariat (eds.)

Joint NGO Safety and Security Training
January 2010
Kingston, M. Supported by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Finucane, C. Edited by Kingston, M.

Artículos

Managing security-related information: a closer look at incident reporting systems and software
December 2018
de Palacios, G.

Digital Security for LGBTQI Aid Workers: Awareness and Response
December 2017
Kumar, M.

Demystifying Security Risk Management
February 2017, (in *PEAR Insights Magazine*)
Fairbanks, A.

Duty of Care: A Review of the Dennis v Norwegian Refugee Council Ruling and its Implications
September 2016
Kemp, E. and Merkelbach, M. Edited by Fairbanks, A.

Organisational Risk Management in High-risk Programmes: The Non-medical Response to the Ebola Outbreak
July 2015, (in *Humanitarian Exchange*, Issue 64)
Reilly, L. and Vazquez Llorente, R.

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing Them
March 2012
Van Brabant, K.

Managing Aid Agency Security in an Evolving World: The Larger Challenge
December 2010
Van Brabant, K.

Whose Risk Is it Anyway? Linking Operational Risk Thresholds and Organisational Risk Management
June 2010, (in *Humanitarian Exchange*, Issue 47)
Behn, O. and Kingston, M.

Risk Transfer through Hardening Mentalities?
November 2009
Behn, O. and Kingston, M.

Guías

Managing Sexual Violence against Aid Workers: prevention, preparedness, response and aftercare
March 2019
EISF

Abduction and Kidnap Risk Management
November 2017
EISF

Security Incident Information Management Handbook
September 2017
Insecurity Insight, Redr UK, EISF

Security Risk Management: a basic guide for smaller NGOs
June 2017
Bickley, S.

Security to go: a risk management toolkit for humanitarian aid agencies – 2nd edition
March 2017 – *Fr. and Sp. versions available*
Davis, J. *et al.*

Office Opening
March 2015 – *Fr. version available*
Source8

Security Audits
September 2013 – *Sp. and Fr. versions available*
Finucane C. Edited by French, E. and Vazquez Llorente, R. (Sp. and Fr.) – EISF Secretariat

Managing the Message: Communication and Media Management in a Crisis
September 2013 – *Fr. version available*
Davidson, S. Edited by French, E. – EISF Secretariat

Family First: Liaison and Support During a Crisis
February 2013 – *Fr. version available*
Davidson, S. Edited by French, E. – EISF Secretariat

Office Closure
February 2013
Safer Edge. Edited by French, E. and Reilly, L. – EISF Secretariat

eisf

Dirección del EISF
T: +44 (0) 203 195 1360
M: +44 (0) 77 6099 2239
eisf-director@eisf.eu

Investigación del EISF
T: +44 (0) 203 195 1362
M: +44 (0) 77 6099 2240
eisf-research@eisf.eu

www.eisf.eu

Edición en inglés: Primera publicación en junio de 2017
Edición en español: Primera publicación en mayo 2019

Con apoyo financiero de:

MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN
aecid
cooperación española