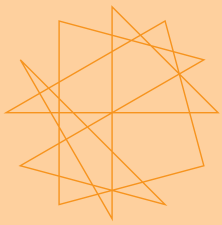
eisf



UNA GUÍA DE EISF PARA ORGANIZACIONES NO GUBERNAMENTALES

Seguridad en práctica:

herramientas de gestión de riesgos para organizaciones de ayuda humanitaria

EUROPEAN INTERAGENCY SECURITY FORUM

El Foro Europeo Interinstitucional para la Seguridad (EISF)

EISF es una plataforma independiente de referentes de seguridad que actualmente representan 90 ONG humanitarias con base en Europa 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.

EISF es una entidad independiente actualmente financiada por la Oficina Estadounidense de Asistencia para Desastres (US Office of Foreign Disaster Assistance, OFDA), la Agencia Suiza para el Desarrollo y la Cooperación (COSUDE) (Swiss Agency for Development and Cooperation, SDC), el Departamento para el Desarrollo Internacional del Reino Unido (Department for International Development, DFID) y las contribuciones de los miembros de EISF.

www.eisf.eu

Agradecimientos

La primera edición de esta guía, publicada en el 2015, fue desarrollada en conjunto por James Davis (Act Alliance) y Lisa Reilly, Directora Ejecutiva de EISF. La Gerente de Proyecto fue Raquel Vázquez Llorente, Investigadora en el EISF.

El Módulo 12 – Gestión de personal fue desarrollado por Christine Williamson. La Gerente de Proyecto fue Adelicia Fairbanks, Investigadora en el EISF.

EISF y los autores desean expresar su agradecimiento a los siguientes individuos por compartir su experiencia con nosotros: Marko Szilveszter Macskovich (Oficina de la ONU para la Coordinación de Asuntos Humanitarios), Michelle Betz (Betz Media Consulting), Veronica Kenny-Macpherson (Cosantóir Group), Jean Michel Emeryk, Peter Wood, Shaun Bickley, William Carter, Rebekka Meissner y Christine Newton.

Traducción y editación por: Translators without Borders, Megan Caine y Susana Carrera (monkeyproof.co.uk), y Yelena Torres López.

Agradecemos especialmente a Gonzalo de Palacios (Humanitarian Access), quien nos apoyó con la revisión de esta edición en español.

Sugerencia para citas

Davis, J. et al. (2017) *Seguridad en práctica: herramientas de gestión de riesgos para organizaciones de ayuda humanitaria*. European Interagency Security Forum (EISF).

Aviso Legal

Diseño e ilustraciones: www.wave.coop

Contenido

Introducción

Acerca de la guía "Seguridad en práctica"

"Seguridad en práctica" intenta proporcionar una guía simple y fácil de usar para personas no expertas en seguridad con el objeto de establecer rápidamente sistemas básicos de gestión de seguridad y riesgos en nuevos contextos o situaciones de respuesta ante emergencias repentinas. Esta guía es aplicable tanto a organizaciones internacionales como a agencias nacionales que se trasladan a nuevas regiones y/o que establecen nuevos programas; es particularmente aplicable a entornos en donde los niveles de riesgo han cambiado debido a causas humanas o naturales.

Esta guía no es un análisis exhaustivo de todos los sistemas de gestión de seguridad y riesgos que pueden ser desarrollados o implementados por organizaciones nacionales e internacionales que trabajan en contextos llenos de desafíos. Por el contrario, "Seguridad en práctica" pretende ser una orientación sobre las necesidades clave que deben abordarse al abrir una nueva oficina, programa o misión. Esta guía emplea listas de verificación y herramientas detalladas para garantizar que las importantes necesidades del deber de cuidado sean identificadas y gestionadas.

El contenido de esta guía es el resultado de la colaboración de una cantidad de diferentes tipos de organizaciones, personas y consultores centrados en temas de seguridad para organizaciones humanitarias internacionales. Los temas seleccionados para ser incluidos en esta guía representan varias áreas clave, pero EISF espera actualizar la guía regularmente para agregar más módulos en el futuro, a medida que organizaciones desarrollen y compartan sus lecciones aprendidas en varios contextos.

Cómo usar la guía "Seguridad en práctica"

Esta guía puede utilizarse de varias maneras. En el nivel más básico, puede guardarse en una llave USB. Asimismo, el personal que implemente esta guía en un nuevo contexto puede imprimirla y llevarla para que sirva de modelo para establecer sistemas y políticas en una etapa temprana y mantener seguro al personal mientras se establece un programa. Idealmente, el documento debería ser considerado por los órganos gestores como parte del proceso de planificación del despliegue, de la planificación del diseño del programa o incluido en la puesta en escala de una organización en respuesta a una emergencia o un cambio significativo en las amenazas del entorno operativo.

Esta guía incluye lo siguiente:

- Actividades cruciales y sugerencias, indicadas con
- Testimonios de expertos, indicadas con
- Referencias cruzadas en la guía, indicadas con
- Glosario de conceptos y definiciones clave.

Para facilitar la comprensión, esta guía está organizada en tres categorías de módulos: **Planificación y preparación, Respuesta** y **Servicios de apoyo**.

Los módulos de planificación, preparación y respuesta corresponden al **proceso de planificación de gestión de riesgos de seguridad** (véase página 7). Al comienzo de cada capítulo, un cuadro de navegación resalta en verde qué etapa del proceso será discutido.

Los módulos correspondientes a servicios de apoyo cubren áreas y procesos que afectan, complementan y alimentan la gestión de riesgos de seguridad de una organización y deben ser considerados a lo largo del proceso de planificación para la gestión de riesgos de seguridad.

Los módulos están estructurados para ayudar al personal a desarrollar contramedidas o estrategias de mitigación de riesgo para contrarrestar las amenazas identificadas en el diagnóstico de riesgos de la organización. Las listas de verificación, los planes y las plantillas deben modificarse para adaptarse a cada organización y contexto.

1 Proceso de planificación de la gestión de riesgos de seguridad

Como con todas las medidas de seguridad, el primer paso crítico es completar un diagnóstico de los riesgos. Los desastres naturales, las hambrunas, los brotes de enfermedades e incluso las elecciones pueden presentar tantos riesgos como los conflictos humanos, el terrorismo u otros tipos de violencia. Esta guía proporciona un formato de diagnóstico de riesgos simple que se puede usar para identificar y medir varios riesgos.

Una buena gestión de seguridad no se trata de tener aversión al riesgo sino de reconocer los riesgos y desarrollar medidas de gestión de riesgos adecuadas para facilitar que los programas se realicen de manera segura. Si las medidas de seguridad impiden que los programas se lleven a cabo, las organizaciones deberían considerar si están equipadas para trabajar en esos contextos.

▶ *Consulte el Módulo 3 – Herramienta de diagnóstico de riesgos.*

▶ *Consulte el glosario.*

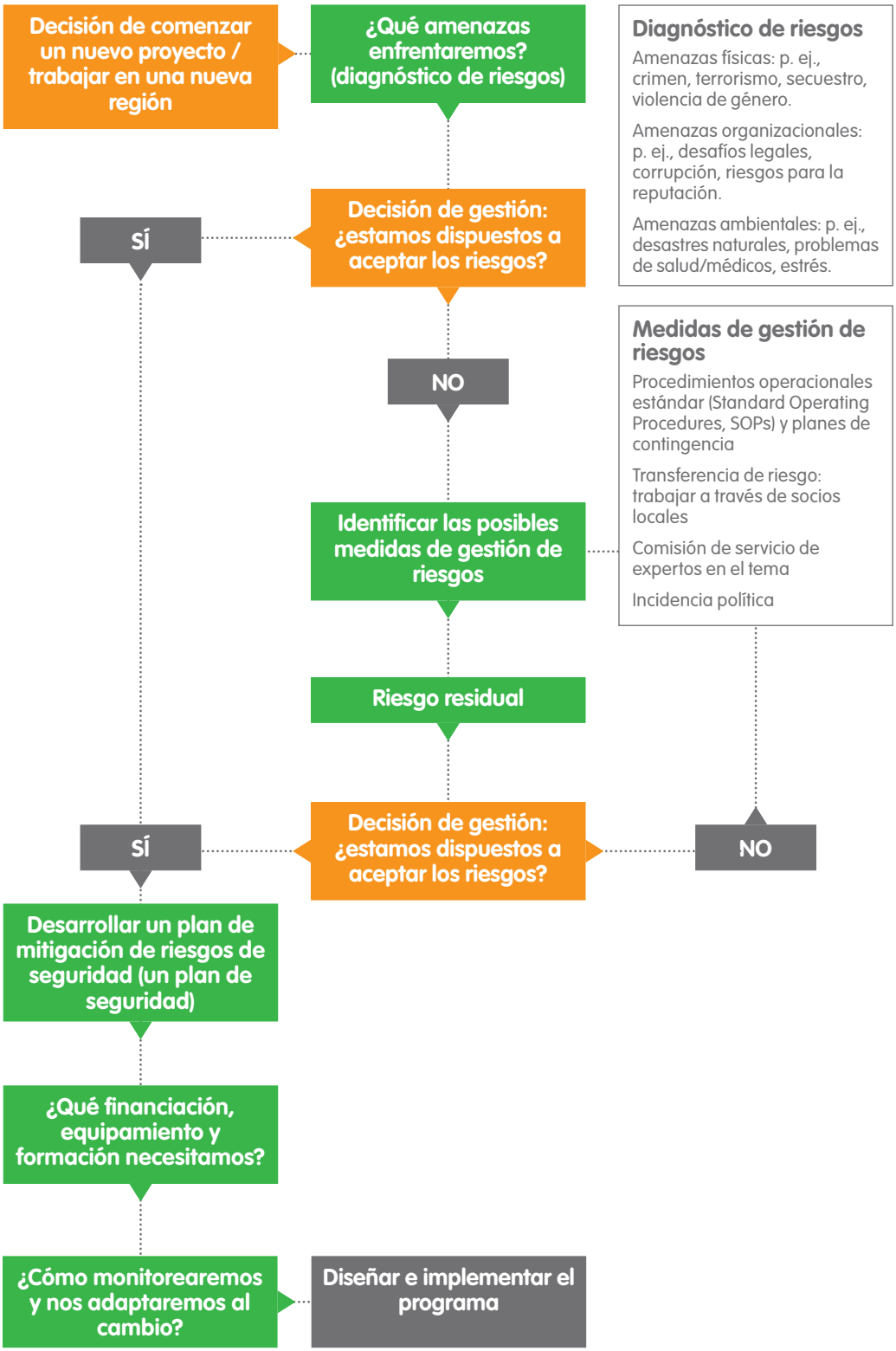
Amenaza

Cualquier reto a la seguridad[1] o de otro tipo al personal, activos, organización, reputación o programación que existe en el contexto en donde opera.

Riesgo

Cómo una amenaza puede afectar al personal, activos, organización, reputación o programación.

1 NdT: en inglés *safety and security*. *Safety* se refiere a hechos accidentales mientras que *security* a hechos en los que hay voluntad de causar daño.


Decisión de comenzar un nuevo proyecto / trabajar en una nueva región
¿Qué amenazas enfrentaremos? (diagnóstico de riesgos)
Diagnóstico de riesgos
Amenazas físicas: p. ej., crimen, terrorismo, secuestro, violencia de género.
Amenazas organizacionales: p. ej., desafíos legales, corrupción, riesgos para la reputación.
Amenazas ambientales: p. ej., desastres naturales, problemas de salud/médicos, estrés.
Decisión de gestión: ¿estamos dispuestos a aceptar los riesgos?
SÍ
NO
Medidas de gestión de riesgos
Procedimientos operacionales estándar (Standard Operating Procedures, SOPs) y planes de contingencia
Transferencia de riesgo: trabajar a través de socios locales
Comisión de servicio de expertos en el tema
Incidencia política
Identificar las posibles medidas de gestión de riesgos
Riesgo residual
Decisión de gestión: ¿estamos dispuestos a aceptar los riesgos?
SÍ
NO
Desarrollar un plan de mitigación de riesgos de seguridad (un plan de seguridad)
¿Qué financiación, equipamiento y formación necesitamos?
¿Cómo monitorearemos y nos adaptaremos al cambio?
Diseñar e implementar el programa

Al responder a una nueva emergencia o al comenzar las operaciones en una nueva región, es esencial incorporar un diagnóstico de los riesgos de seguridad en cualquier proceso de diagnóstico de necesidades. Al hacer esto, cualquier coste de gestión de riesgos de seguridad puede incorporarse al diseño del programa desde el comienzo en lugar de agregarse al final.

El deber de cuidado es un concepto cada vez más importante para las organizaciones que envían personal a entornos llenos de retos. Esencialmente, el deber de cuidado es la obligación legal y moral de una organización de tomar todas las medidas posibles para reducir el riesgo de daño a aquellas personas que trabajan o que operan en nombre de una organización. Esto incluye el personal, los voluntarios, practicantes, contratistas (como los guardias o los conductores) y las organizaciones socias implementadoras (si bien el nivel de deber de cuidado requerido puede ser diferente). Las organizaciones no gubernamentales (ONG), incluidos los gerentes y directores, pueden ser demandados a título individual en muchas jurisdicciones por demostrar negligencia en su deber de cuidado.

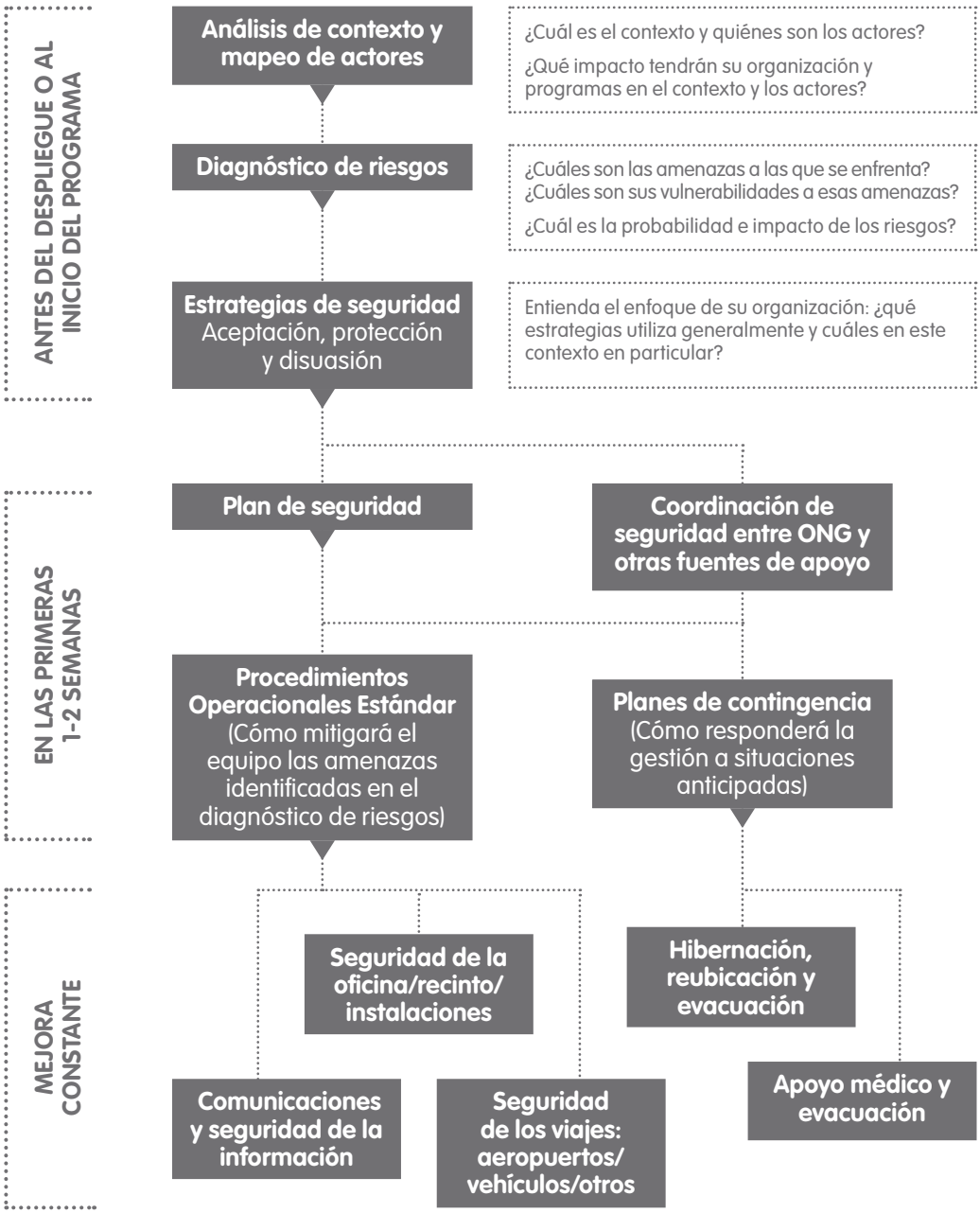
▶ *Consulte el glosario.*

Una buena gestión de riesgos de seguridad no tiene que costar demasiado financieramente. En muchos casos, se trata más de la formación del personal, de crear buenas políticas y controlar constantemente las amenazas del entorno. Mantener un mapa de incidentes, observar una política de control de entrada de comunicaciones, límites de velocidad de vehículos, suministros de emergencia o unirse a otros foros de ONG puede costar muy poco y tener un gran impacto en la seguridad del personal y los activos de la organización. Identificar al personal responsable y priorizar el tiempo para llevar a cabo estas actividades es el desafío clave.

Los donantes tienen cada vez más conocimiento de los costos de gestión de los riesgos de seguridad. Si el diagnóstico de riesgos justifica el gasto, los costes directos se pueden incorporar en el presupuesto de implementación del programa. Los costos necesarios relacionados con la seguridad, como equipamiento (radios, teléfonos satelitales, kits de primeros auxilios, equipamientos/suministros de emergencia, dinero en efectivo de emergencia, mejoras de las instalaciones, seguro o similares), o el tiempo (implementar una estrategia de aceptación proactiva, negociar un acceso sostenible), pueden incorporarse en las propuestas para financiación. Si el diagnóstico de riesgos lo justifica, los donantes frecuentemente están dispuestos a financiar estas partidas presupuestarias de seguridad.

▶ *Consulte el informe del EISF "The Cost of Security Risk Management for NGOs" .*

Proceso de planificación de la gestión de los riesgos de seguridad



Nada en la vida es estático para siempre. Las situaciones mejoran y también se deterioran. Las políticas y los procedimientos de seguridad necesitan ser regularmente actualizados o adaptados para ajustarse a las amenazas cambiantes en el entorno operativo. Es importante definir lo siguiente:

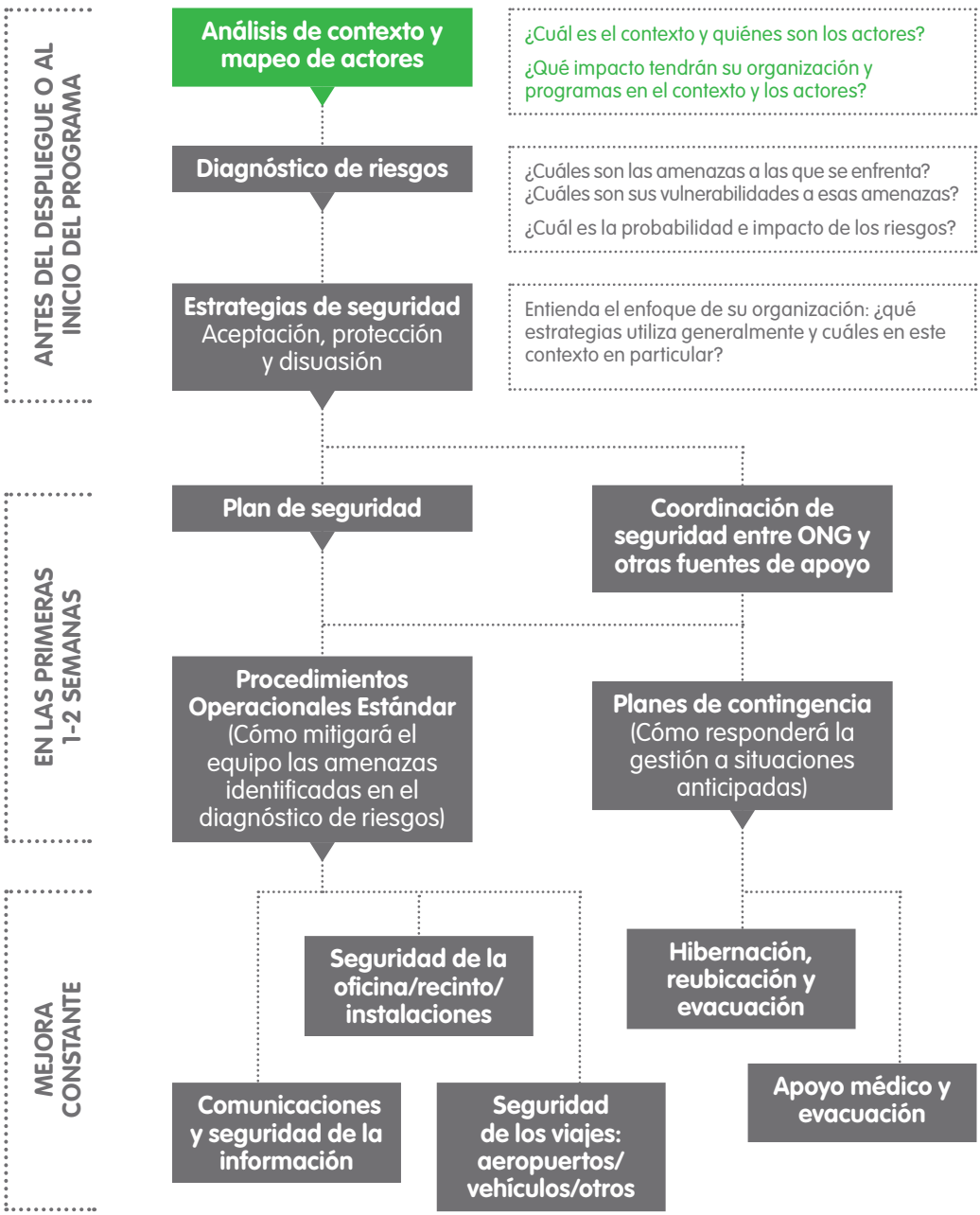
- ¿Quién es responsable de revisar y actualizar el diagnóstico de riesgos y los planes de seguridad?
- ¿Con qué frecuencia se debe llevar a cabo esto (anualmente, trimestralmente, mensualmente)?
- ¿Cómo se informará y formará al personal sobre los cambios de políticas y procedimientos?

Para monitorear la naturaleza cambiante de las amenazas en el entorno operacional, es necesario identificar los factores de cambio, es decir, qué desarrollos del contexto pueden y deberían ser monitoreados para dar una alerta temprana sobre los cambios que pueden impactar los riesgos a los que se enfrenta la organización.

Uno de los mejores y más simples métodos para monitorear el cambio es el mapeo de incidentes, incluyendo "conatos de accidentes" así como los incidentes que han ocurrido dentro de su entorno operacional pero que no han afectado específicamente a su organización.

Al controlar cuándo y dónde ocurren los incidentes, incluyendo el momento del día, quién fue el objetivo y las consecuencias, resulta más fácil ver cuándo la situación mejora o se deteriora. Por ejemplo, puede usar un mapa y marcar con alfileres de diferentes colores para representar cada tipo de incidente y/o quién estuvo involucrado (su organización, otra ONG, la Organización de las Naciones Unidas (ONU), un socio de la organización, una ONG local).

2 Mapeo de actores y análisis de contexto



El mapeo de los diferentes actores en el entorno operacional y el análisis del contexto son, ambas, actividades clave para las organizaciones que se trasladen a nuevos países/áreas/regiones o para comenzar un nuevo programa o proyecto. Estas actividades también son esenciales cuando ha ocurrido una gran alteración del status quo en un contexto operativo conocido.

En los últimos años, se ha ordenado a ONG que se retiren de ciertos países o su personal ha sido condenado y enviado a prisión, a pesar de las necesidades humanitarias urgentes del país, porque alguien cometió un simple error social, ofendió a un gobierno anfitrión o comenzó a trabajar sin haber obtenido la aceptación adecuada de las estructuras de liderazgo formales e informales. Se recomienda altamente iniciar un mapeo de actores y un análisis de contexto tan pronto como sea posible y continuar el proceso durante la duración del programa.

¿Quiénes son los individuos, grupos, organizaciones, instituciones estatales y otros actores clave que pueden afectar su seguridad y operaciones?
¿Cuál es su posición política y/o social, poder, antecedentes y relación con o interés en la organización?

Mapeo de actores

El mapeo de actores es un ejercicio para identificar a todas las personas, partes implicadas u otras organizaciones clave que tendrán un impacto sobre el entorno operacional. Pueden incluir:

- Los ministros del gobierno local, los jefes de departamento o actores similares
- Líderes o grupos de la oposición, o sus simpatizantes clave
- Funcionarios de seguridad del gobierno local (ejército, policía, otros)
- Donantes
- Agencias de la ONU y sus puntos de contacto
- Líderes comunitarios
- Líderes formales e informales en la región en la que se opera
- Otras ONG, tanto nacionales como internacionales
- Empresarios clave que pueden controlar el suministro local y la logística
- Medios de comunicación locales
- Grupos de beneficiarios
- Comunidades anfitrionas
- Otros

Recuerde, cuando se realiza un mapeo de actores, los intereses declarados de una persona o grupo pueden ser muy diferentes de sus intereses reales.

Una vez que se ha identificado a los actores clave, es importante entender cómo se vinculan entre ellos y cuándo la interacción con uno de ellos puede afectar las relaciones con otro. Piense cómo están conectados -qué actores están aliados y cuáles están en conflicto, por ejemplo-, así como también el modo en que estas relaciones pueden verse afectadas por la presencia de la organización y los programas a implementar.

Análisis de contexto

El análisis del contexto se construye sobre el ejercicio del mapeo de actores, mediante el examen de tantos factores relacionados con el contexto como estén disponibles. Pueden incluir:

- Historia, tanto reciente como antigua
- Tradiciones culturales y religiosas que pueden diferir entre las áreas rurales y urbanas
- Alianzas raciales, tribales o políticas
- Factores socioeconómicos
- Condiciones de las infraestructuras
- Niveles de seguridad o inseguridad y factores que los influencian
- Actitudes hacia los extranjeros (occidentales, diáspora o regionales)
- Actitudes hacia agencias de ayuda
- Cuestiones de gobernanza
- Corrupción
- Impacto de las nuevas ONG que llegan, aparte de en la programación, sobre las relaciones sociales, económicas y de poder locales
- Otros factores

Al escribir un análisis de contexto, puede usar el formato PESTLM:

Política

Economía

Social

Tecnología

Legal

Medioambiente

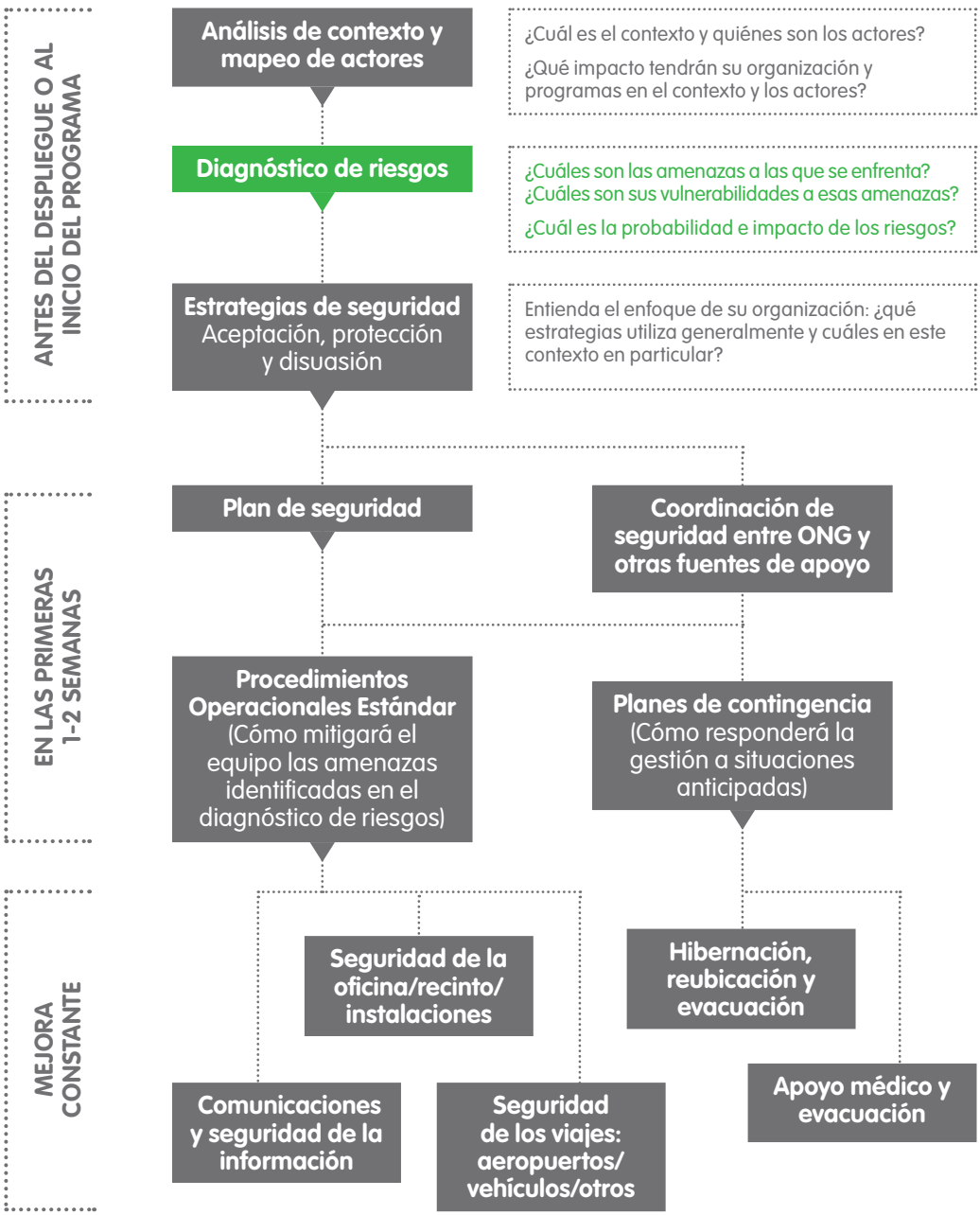
El mapeo de actores y el análisis de contexto pueden ser un reto cuando se responde rápidamente a un nuevo entorno. Identificar a todos los actores y partes interesadas, sin intentar establecer relaciones de poder o motivaciones ocultas, puede ser bastante difícil. Es importante incluir tantas perspectivas como sea posible en el mapeo de actores y en el análisis de contexto. Personas de diferentes etnias, edades y género pueden tener un entendimiento diferente de las relaciones del contexto y lo que las mueven.

Encontrar buenas fuentes de información local, a la vez que se es consciente de los prejuicios, es un buen primer paso, pero también investigue otras organizaciones o individuos que han trabajado recientemente en el contexto y entrevístelos.

En las primeas etapas de una nueva respuesta, el mapeo de actores y el análisis del contexto se deben actualizar regularmente a medida que se conoce más información. Los resultados de este proceso se deben mantener tan confidenciales como sea posible, desde la perspectiva de la gestión, para evitar irritar sensibilidades locales. También, es importante no ser visto como una organización que reúne "inteligencia", por lo que la gestión de la información y el modo en que se emplea y comparte, debería ser monitoreado cuidadosamente.

Consulte el Módulo 8 - Comunicaciones y seguridad de la información.

3 Herramienta de diagnóstico de riesgos



Es muy difícil establecer sistemas de gestión de riesgos de seguridad[2] si no se comprenden claramente las amenazas o riesgos que se enfrentan. Por lo tanto, este debería ser el primer paso crítico en cualquier despliegue o programa, una vez que haya, al menos, una comprensión inicial del contexto.

El propósito de un diagnóstico de riesgos de seguridad es facilitar el desarrollo de medidas de mitigación apropiadas para la implementación de programas seguros y sostenibles.

El proceso de diagnóstico de riesgos debe realizarse como una parte integral del diseño de programas y proyectos. Tanto la exposición al riesgo como las medidas de mitigación están vinculadas a los objetivos y a la implementación de programas.

El entorno en el que se dan los riesgos de seguridad[3] puede cubrir una amplia variedad de amenazas, como la violencia, el conflicto, las amenazas naturales, el terrorismo, los problemas de salud, la interferencia política, el crimen y la corrupción. Esta herramienta está diseñada para permitir a las organizaciones y a las personas sin ninguna experiencia previa de seguridad llevar a cabo un diagnóstico básico de riesgos de seguridad como parte de cualquier proceso de diagnóstico más amplio.

Esta herramienta de evaluación se desglosa en tres pasos:

Identificación de las amenazas → **Evaluar las amenazas y calificar el nivel de riesgo de la organización (vulnerabilidad)** → **Desarrollar estrategias para reducir el riesgo y la vulnerabilidad**

▶ *Consulte el glosario.*

Es importante que todas las organizaciones consideren el "umbral de riesgo" que es aceptable tanto para la organización como para su personal. Algunas organizaciones tienen la experiencia y la capacidad de trabajar en entornos con riesgos moderados y altos, mientras que otras solo tienen la capacidad de trabajar en áreas con riesgos bajos a moderados. Es importante conocer la habilidad de la organización para gestionar el riesgo cuando se determina un umbral para responder a una emergencia humanitaria. El umbral de riesgo aceptable también depende de los tipos de programas que se implementan, es decir, si es crítico para salvar vidas, si es de incidencia política contra estructuras de poder existentes o de desarrollo a largo plazo.

2 NdT: en inglés, *safety* y *security*.
3 NdT: ídem anterior.

Paso 1: Identificar las amenazas

Existen varias metodologías para identificar amenazas, incluyendo el mapeo de actores y el análisis de contexto. Sin embargo, muchas de ellas requieren una gran cantidad de investigación y de tiempo en la región y es posible que no sean prácticas en situaciones de diagnóstico en emergencias. No obstante, las organizaciones deberían completar, al menos, un análisis preliminar como parte de todos los diangósticos iniciales para el diseño y la implementación de un proyecto. Este análisis debe mejorarse a medida que hay más información disponible.

▶ *Consulte el Módulo 2 - Mapeo de actores y análisis de contexto.*

Existe una amplia variedad de amenazas y riesgos que afectan a las organizaciones internacionales y nacionales que entran en un nuevo contexto. A continuación se muestran algunos ejemplos típicos para considerar.

Amenazas violentas

- Ataque armado con un objetivo específico
- Conflicto armado sin objetivo específico
- Secuestro
- Terrorismo
- Violencia con explosivos (minas, artefactos explosivos improvisados (IED), bombardeo)
- Secuestro de vehículos
- Violencia sexual
- Disturbios civiles
- Violencia religiosa
- Crimen
- ¿Otro?

Amenazas organizacionales

- Riesgo a la reputación
- Riesgo financiero (sistema bancario, cambio de moneda, robo, malversación)
- Corrupción
- Riesgo legal (permisos laborales, cumplimiento de legislación local, resistencia a la incidencia)
- Riesgo político
- Violencia en el lugar de trabajo o discriminación
- Desafíos culturales
- ¿Otro?

Amenazas del entorno

- Amenazas naturales (clima, terremotos, inundaciones, etc.)
- Riesgos médicos (acceso a tratamiento médico adecuado para el personal)
- Problemas relacionados con la salud (alimentos, agua, enfermedad, estrés)
- Accidentes de tránsito
- Otros accidentes
- Incendio
- ¿Otro?

Si la organización decide llevar a cabo un programa de respuesta ante una emergencia, se debe realizar un diagnóstico de riesgos más detallado dentro de los primeros 10-15 días del despliegue y se deben incorporar los resultados en la estrategia general.

Paso 2: Evaluar las amenazas y calificar el riesgo

Una vez que la organización ha identificado los tipos de amenazas que enfrentará, necesitará evaluar cada una de ellas y calificar el nivel de riesgo para el personal, para la organización en su conjunto y para sus operaciones.

Una vez que se haya enumerado cada amenaza y todos los riesgos han sido identificados, es importante calificar todos los riesgos. Esto ayuda a aclarar la gravedad (o la falta de ella) del riesgo y qué prioridad se le debe dar.

	Amenaza	Localización	¿Quién/qué estará en riesgo?	¿Cuál será el impacto?
	Enumere las amenazas identificadas en el paso 1 y complete para cada una de ellas.	¿La amenaza está confinada a una o más áreas o en toda la región afectada? Sea específico.	Personal internacional Personal nacional Miembros de la comunidad Vehículos con visibilidad Suministros de ayuda	Pérdida de vida Pérdida de activos Daño a la reputación en la comunidad/con el gobierno Reducción de la capacidad de trabajo
p. ej.	Secuestro de vehículos	Ruta al aeropuerto – Autopista 1	Todo el personal Vehículos con visibilidad Vehículos todoterreno	Pérdida de activos Reducción de la movilidad de los equipos Reducción de la capacidad de trabajo Daño físico a todo el personal Pérdida de vida

La calificación del riesgo viene de una combinación de la probabilidad de que ocurra un incidente y el nivel del impacto que causará.

La mayoría de las ONG y las Naciones Unidas usan un sistema de calificación de riesgo similar al siguiente:

1. Muy bajo

2. Bajo

3. Medio

4. Alto

5. Muy alto

Las amenazas pueden variar de nivel geográficamente. Puede ser necesario evaluar el riesgo por localidad, en lugar de evaluarlo a nivel nacional o regional. Por ejemplo, en una zona fronteriza puede existir la probabilidad de

que haya un conflicto armado, mientras que en provincias más cerca de la capital puede que tal probabilidad sea menor. Dependiendo de la escala de la situación de emergencia puede tener una calificación de riesgo total para una zona, o para varias, dentro de la zona afectada para cada tipo de riesgo.

Las amenazas también pueden variar debido a diferentes niveles de vulnerabilidad del personal. Por ejemplo, algunas veces el personal nacional puede estar en menor riesgo en una zona específica que el personal internacional. La etnia, el sexo, la orientación sexual (así como la identidad y expresión de género) y la experiencia del individuo también pueden afectar la vulnerabilidad del personal.

A continuación encontrará una tabla que puede usar para determinar el nivel de riesgo para cada amenaza que ha sido identificada. Siempre que sea posible, utilice incidentes reportados anteriormente de varios tipos de amenazas para justificar el nivel de calificación de riesgo asignado. Sin embargo, en una nueva situación, en donde no se han presentado respuestas humanitarias recientemente, puede ser necesario usar datos de intervenciones similares junto con información actual de fuentes locales. Las definiciones para cada nivel deben ser consistentes en toda la organización para que se puedan comparar diferentes contextos.

Impacto	Insignificante	Menor	Moderado	Grave	Crítico
	• Lesiones poco serias • Pérdida o daño mínimo a activos • Sin demoras en los programas	• Lesiones menores • Alguna pérdida o daño a activos • Algunas demoras en los programas	• Lesiones sin peligro para la vida • Estrés elevado • Pérdida o daño a activos • Algunas demoras e interrupciones en los programas	• Lesiones serias • Destrucción grave de activos • Interrupción grave de programas	• Muerte o lesión grave • Destrucción grave o total de activos • Pérdida de programas y proyectos
Probabilidad					
Muy poco probable Cada 4 años o más	Muy bajo	Muy bajo	Muy bajo	Bajo	Bajo
Poco probable Cada 2-3 años	Muy bajo	Bajo	Bajo	Medio	Medio
Moderadamente probable Cada año	Muy bajo	Bajo	Medio	Alto	Alto
Probable Una vez por semana	Bajo	Medio	Alto	Alto	Muy alto
Muy probable Diariamente	Bajo	Medio	Alto	Muy alto	Muy alto

Algunas organizaciones pueden tener un sistema de niveles de seguridad que se ha desarrollado en función del nivel de riesgo total de la organización, de los programas y del personal considerando todas las distintas amenazas. El desarrollo de un sistema de niveles de seguridad no está cubierto por esta herramienta.

Paso 3: Desarrollar estrategias para reducir el riesgo y la vulnerabilidad

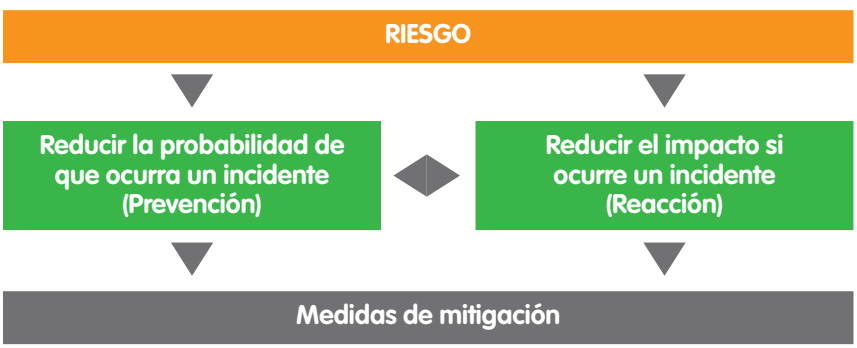
Una vez que se han identificado y evaluado las amenazas que pueden afectar una respuesta humanitaria y se han calificado los riesgos, es importante recomendar medidas de mitigación de los riesgos para abordar estas vulnerabilidades. Si bien no hay dos situaciones idénticas, normalmente existen medidas que se puede seguir para reducir la exposición al riesgo.

El desarrollo de estrategias de seguridad es un paso crítico para asegurar que antes de comprometer personal, recursos y la reputación de una organización en una respuesta, la agencia ha tomado todos los pasos necesarios para minimizar el riesgo.

Este es un componente esencial del deber de cuidado. Las estrategias de mitigación deben reflejar las estrategias de gestión de riesgo preferidas de la organización, como la aceptación, la protección o la disuasión.

- *Consulte el glosario.*
- *Consulte el Módulo 4 - Estrategias de seguridad: aceptación, protección y disuasión.*

En general, hay dos formas de reducir la exposición al riesgo:



Las medidas para reducir el riesgo deben enfocarse tanto en la prevención (reducir la probabilidad) como en la reacción (reducir el impacto). Esto puede reducir el nivel de riesgo residual a partir del nivel originalmente asignado a cada amenaza identificada, lo que mejorará la capacidad para realizar programas de respuesta ante emergencias. Es importante recordar que el objetivo de la gestión de riesgos de seguridad no es colocar barreras para la realización de los programas, sino para favorecer que las organizaciones mantengan su compromiso y capacidad para implementar proyectos a pesar del nivel de riesgo.

Por ejemplo, podríamos reducir la exposición al riesgo de accidentes automovilísticos por medio de:

Reducir la probabilidad

- Garantizar que los vehículos estén bien mantenidos
- Hacer cumplir los límites de velocidad
- Proporcionar capacitación para conductores
- Evitar viajar durante la noche fuera de las ciudades
- Evitar rutas congestionadas de alto riesgo
- Evitar viajar en clima extremo

Reducir el impacto

- Asegurar que siempre se usen los cinturones de seguridad
- Tener equipos de primeros auxilios y capacitar al personal
- Tener un extintor de incendios
- Tener los números de contactos de emergencia
- Colocar triángulos de advertencia de seguridad
- Tener seguro y servicios de asesoramiento

Se pueden reducir algunas amenazas como los incendios en la oficina, los robos y los accidentes automovilísticos mediante buenas estrategias de prevención. Sin embargo, amenazas como los desastres naturales, los fallos de las infraestructuras o el riesgo político son ampliamente impredecibles, y por lo tanto debe enfocarse en la reacción, para reducir el impacto sobre el personal y los programas.

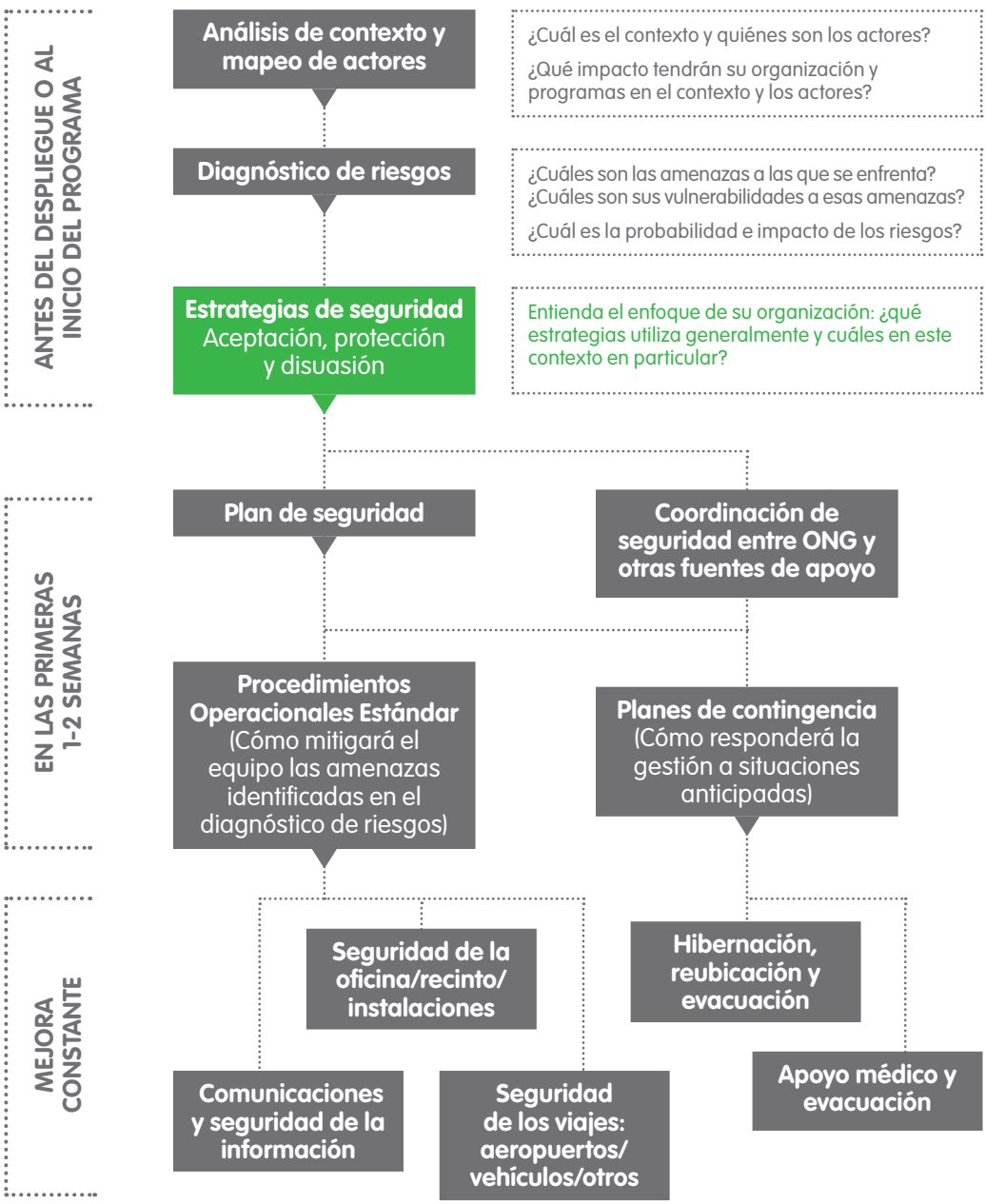
Siempre que sea posible, identifique sistemas confiables de alerta temprana que puedan ayudar su organización a mitigar el riesgo. Pueden implementarse algunas medidas de reacción como parte de la preparación organizacional, como el suministro de equipos de primeros auxilios, la capacitación sobre primeros auxilios, el almacenamiento de suministros de emergencia o la formación sobre seguridad personal.

Las medidas de mitigación deben reflejar el diagnóstico de riesgos. Por ejemplo, si se identifica que una amenaza en particular tiene una baja probabilidad, pero su impacto es crítico, el hecho de implementar medidas solo para reducir la probabilidad tendrá un efecto limitado en la reducción del riesgo.

Cada vez más organizaciones eligen trabajar por medio de socios locales como una forma de reducir su exposición al riesgo, especialmente en contextos llenos de desafíos. Sin embargo, esto transferirá los riesgos a los socios locales. Si bien la amenaza total a la ONG local seguirá siendo la misma, es importante entender que los riesgos resultantes pueden ser muy diferentes y solo porque la organización socia es local, eso no significa que no estará expuesta al riesgo.

▶ *Consulte el documento del EISF "International agencies working with local partners".*

4 Estrategias de seguridad: aceptación, protección y disuasión



Las organizaciones de ayuda humanitaria utilizan típicamente tres estrategias de seguridad en todos los contextos.

Por lo general, las organizaciones internacionales y nacionales de ayuda priorizan la estrategia de aceptación como enfoque predilecto. Sin embargo, esto puede tomar tiempo y las organizaciones que se despliegan en nuevas áreas no pueden asumir que obtendrán la aceptación de la comunidad. Una organización puede enfocarse inicialmente en las medidas de protección y disuasión hasta que se haya logrado la aceptación. Sin embargo, es importante tener en cuenta desde el primer día que cualquier comportamiento tendrá un impacto en los futuros esfuerzos para alcanzar la aceptación.

Aceptación

Después de una emergencia repentina, es un reto para los gobiernos y las comunidades anfitriones distinguir entre las diferentes organizaciones cuando un gran número de nuevas ONG internacionales y nacionales, así como agencias de las Naciones Unidas, se establecen en la zona. Esto puede complicarse por la rápida rotación del personal durante las primeras semanas, cuando los primeros en responder son reemplazados por personal que se quedará más tiempo en la zona. Todo el personal desplegado y los empleados locales -incluyendo gestores, movilizadores comunitarios y conductores- deben ser informados sobre la manera en que la organización aplicará las tres estrategias y sobre cómo la aceptación será construida entre todos los actores interesados.

La construcción de la aceptación no se hace solo en las comunidades con las que trabaja una organización, sino con todos los actores relacionados. Un mapeo de actores ayudará a la organización a identificar los actores relacionados que pueden estar afectados por sus programas, y qué aliados puede tener para así desarrollar la aceptación con ellos. Recuerde que lo que una organización y sus empleados digan en la zona no es la única manera en que las partes interesadas pueden obtener información. Muchas comunidades ahora tienen acceso a Internet, de modo que los mensajes comunicados deben ser coherentes con lo que está en su página web y cuentas de redes sociales.

La aceptación tiene que conseguirse y puede perderse muy fácilmente, y el comportamiento de una persona puede afectar toda la comunidad.

La aceptación se debe abordar proactivamente.

Puntos clave:

- Sea preciso al explicar quién es, los antecedentes y prioridades de su agencia, de dónde proviene su financiación y cómo desarrolla sus programas.
- Si su organización es religiosa o secular, tenga claro cómo esto afecta o no su trabajo, sobre todo en un contexto muy religioso. También sea consciente de cómo será percibido.
- Entienda quiénes son sus socios, cómo son percibidos y el impacto que su relación tendrá en la aceptación del socio y en la propia.
- Asegúrese de que las partes interesadas se hayan comprometido antes de iniciar cualquier trabajo.
- Tenga un sistema de quejas riguroso y sea visto dando seguimiento a los problemas.
- No aísle a su personal de las comunidades. Manténgase visible y accesible.

Protección

Las medidas de protección deben ser desarrolladas en línea con el diagnóstico de riesgos y se debe asegurar que son aplicadas por igual por todo el personal (local e internacional) y a todos los niveles dentro de la agencia. Las organizaciones deben capacitar al personal en medidas de seguridad, orientar a los nuevos empleados, y buscar la coordinación con otras agencias o foros de seguridad.

▶ *Consulte el Módulo 5 - Coordinación de seguridad entre ONG y otras fuentes de apoyo.*

La protección física de los edificios, recintos y/o sitios de distribución no debe hacer pensar que la organización está construyendo un búnker o un fuerte. Los recintos y otras oficinas o espacios de trabajo deben fundirse con los edificios de la vecindad.

▶ *Consulte el Módulo 7 - Seguridad de las instalaciones.*

Es importante enfocarse en los mejores sistemas de comunicación que la organización pueda permitirse, o que estén disponibles, incluyendo radio, Internet, teléfonos móviles, teléfonos fijos, satelitales, fax, correos informales u otros. Los sistemas de comunicaciones deben estar acompañados de políticas para que el personal se reporte (regularmente o en base a un horario) para garantizar la seguridad.

▶ *Consulte el Módulo 8 – Comunicaciones y seguridad de la información.*

Disuasión

La disuasión es generalmente la estrategia de último recurso. Se utiliza cuando la aceptación y la protección no han tenido éxito o han demostrado ser inadecuadas. En algunos contextos, también puede ser requerida por los gobiernos anfitriones (p.ej., Somalia, Chad, Níger).

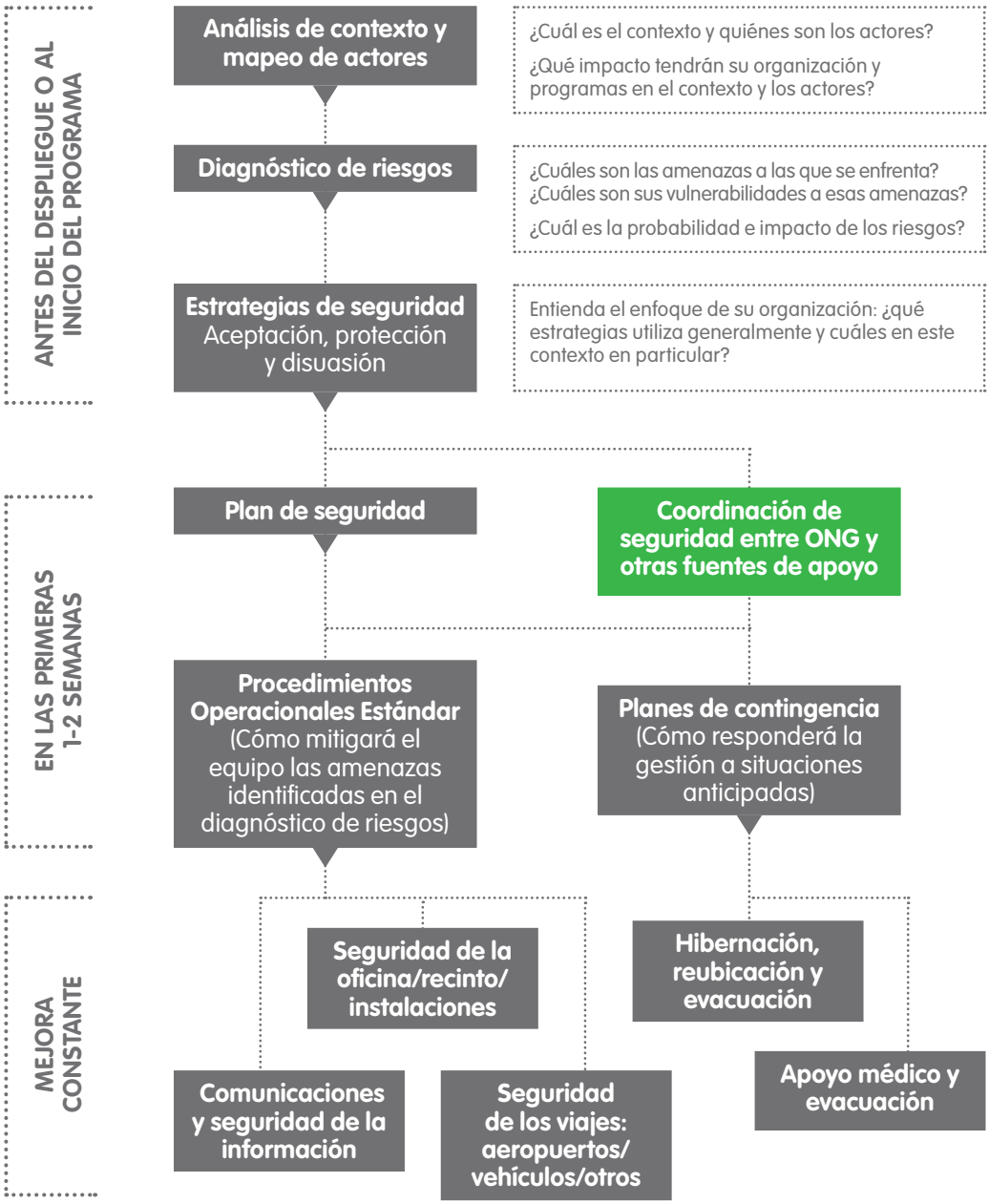
La retirada de los servicios es la principal amenaza que puede ser utilizada en una zona insegura, pero la organización debe asegurarse primero de que los gobiernos locales y los acuerdos con los donantes no se vean comprometidos. No haga amenazas vacías.

Los guardias armados o escoltas militares o de la policía deben evitarse siempre que sea posible ya que a menudo hacen que la aceptación sea imposible o muy difícil -incluso en una fase posterior. Ellos podrían incrementar también el riesgo de lesiones por tiroteos, o el riesgo de extorsión o acoso.

▶ *Consulte el documento informativo del EISF "Engaging private security providers: a guideline for non-governmental organisations".*

A la hora de considerar las diferentes estrategias de seguridad es importante entender la misión, la visión y el mandato de la organización. Todas las organizaciones son diferentes, no sólo en su misión y programas, sino también en sus vulnerabilidades y capacidad para responder ante ellas. Solo porque una organización esté implementando una estrategia particular no significa que vaya a funcionar para otra agencia, incluso si están trabajando en el mismo contexto.

5 Coordinación de seguridad entre ONG y otras fuentes de apoyo



En cualquier país donde las organizaciones de ayuda se congregan en respuesta a una emergencia o crisis ya existente, a menudo se forman diferentes foros y grupos de coordinación. En las regiones donde la inseguridad es un problema, las ONG también pueden hacer foros dedicados a la seguridad. Estos pueden ser parte de un cuerpo de coordinación de ONG más amplio, o de un cuerpo autónomo o un grupo informal para coordinarse y compartir información.

Los foros de seguridad suelen ser presididos por una organización y atienden a ellos los referentes de seguridad de las organizaciones miembro. Estos foros generalmente se utilizan para compartir diagnósticos del contexto e informar sobre incidentes ocurridos. Estos foros pueden compartir los costos de organización de formaciones para personal, proporcionar consejos en respuesta a recomendaciones de las embajadas o gobiernos anfitriones, y actuar como punto central de coordinación con otros actores tales como UNDSS. Si un foro está disponible, se aconseja a las organizaciones unirse tanto para recopilar información sobre el contexto como para identificar las mejores prácticas en ese país en particular.

La pertenencia a un foro de seguridad no es un substituto para que la organización complete su propio diagnóstico de riesgos y desarrolle relaciones de trabajo con actores clave como UNDSS u otras agencias.

Cuando se nombra a un miembro del personal para que asista a estas reuniones de coordinación, asegúrese de que tenga apoyo para dedicar tiempo a esto como prioridad y también que conozca bien las reglas de participación -en particular, la manera cómo la información compartida debe ser manejada. Asegúrese de que ese individuo tenga el apoyo necesario para poder compartir información dentro de la organización para maximizar el beneficio de la pertenencia al foro.

Existen numerosas fuentes adicionales de información a las cuales las organizaciones pueden conectarse para mejorar el flujo de información sobre incidentes, obtener consejos para mitigar los riesgos de varias amenazas y mejorar la capacidad de seguridad. Por ejemplo, "Saving Lives Together" (SLT), es un marco para la colaboración en seguridad entre las ONG y las Naciones Unidas. Comprende un conjunto de recomendaciones tales como intercambio de información y recursos que se basan en las mejores prácticas de gestión de riesgos de seguridad. Aunque la ONU no se hace responsable de evacuación, comunicación u otros servicios de apoyo para ONG, en ciertos contextos pueden coordinar tales servicios.

La última versión del marco SLT fue publicado en 2015 y está acompañada de directrices específicas con respecto a lo que se espera de la colaboración entre las ONG y la ONU. El SLT no es el dominio exclusivo de UNDSS, pero este último

es el que lo lidera dentro del sistema de las Naciones Unidas. Los contactos locales de UNDSS pueden ser identificados a través de los miembros de la sede del SLT, como EISF o InterAction.

Otras fuentes de información de seguridad[4]:

- Los gobiernos nacionales, los gobiernos donantes y sus embajadas.
- Los ministerios de gobiernos anfitriones.
- El Departamento de Ayuda Humanitaria y Protección Civil de la Unión Europea (ECHO) que produce material de seguridad para las organizaciones de ayuda en algunos contextos.
- Las compañías de seguros, ya que a menudo tienen un servicio de asesoramiento de amenazas vinculado con varios países y/o regiones.
- Consultores de seguridad de ONG.
- Los proveedores locales de seguridad (empresas de guardias).
- Los medios de comunicaciones internacionales y nacionales.
- Otras ONG y sus organizaciones socias.
- Comunidades anfitrionas y beneficiarias.
- Personal nacional.
- *Insecurity Insight*.
- *Aid Worker Security Database*.
- *International NGO Safety Organisation* (INSO), si está disponible.
- El Foro Europeo Interinstitucional para la Seguridad (EISF).

Para tomar una buena decisión es necesario contar con información precisa y de confianza. Toda información debe ser tenida en cuenta en base a la fiabilidad de la fuente, el número de individuos/organizaciones que por separado reportan la misma información, y los sesgos locales. Generalmente hay que evitar actuar en base a rumores sin confirmación por una fuente de confianza.

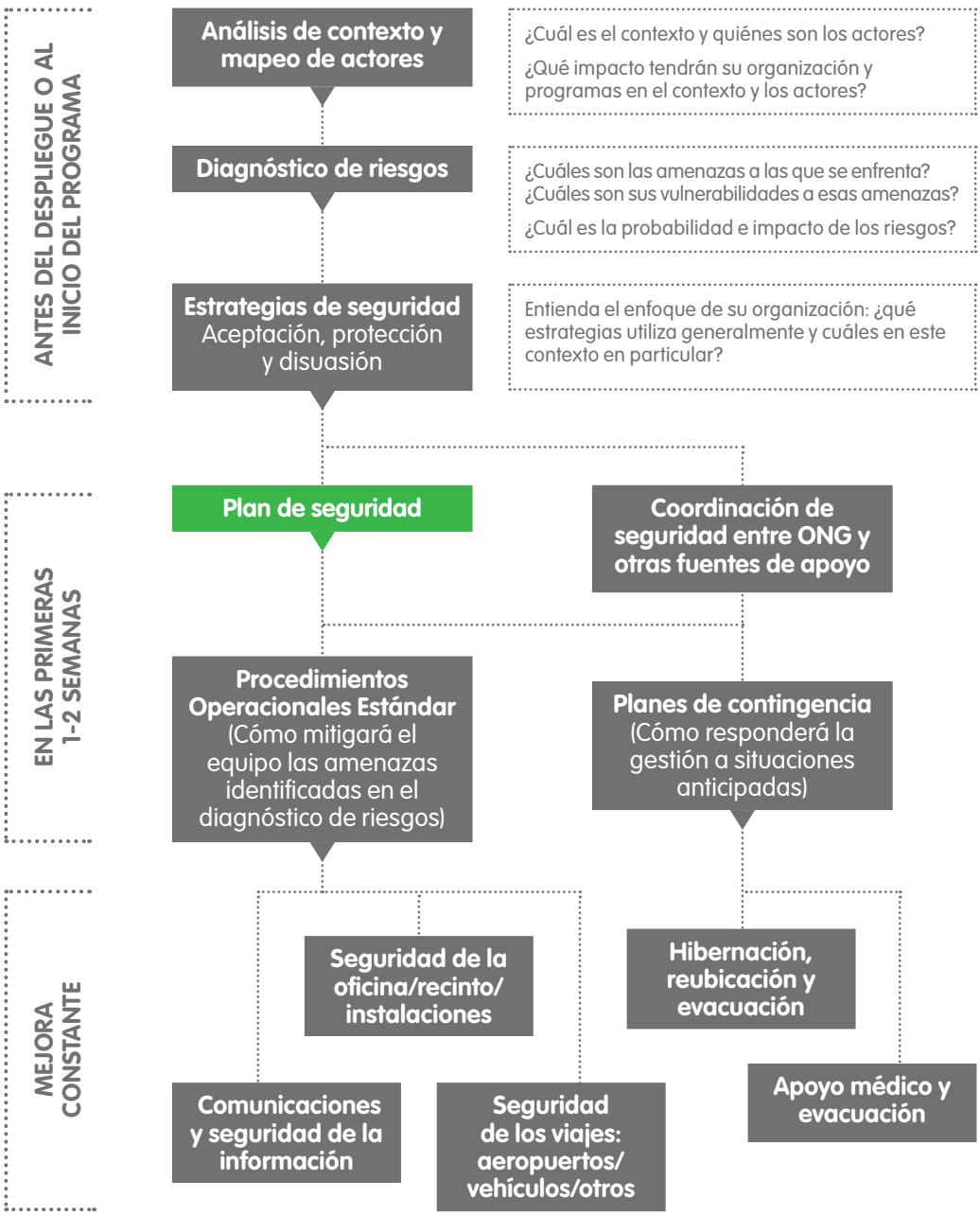
▶ *Consulte el Módulo 8 – Comunicaciones y seguridad de la información.*

En una situación de emergencia o de crisis, la seguridad del personal, su organización y posiblemente también las comunidades beneficiarias dependerán de su capacidad de tomar decisiones y activar planes de contingencia. Hay una serie de sistemas para calificar la calidad de la información. A continuación, se muestra un cuadro sencillo para ayudar a evaluar la información recibida.

4 NdT: en inglés, *safety* y *security*.

	Información detallada y creíble	Información vaga o incompleta
Fuente fiable, de confianza	Buena información para tomar decisiones	Considere la información pero busque confirmación
Fuente desconocida poco fiable	Busque confirmación a través de fuentes conocidas	No ignore pero no tome decisiones antes de consultar otras fuentes

6 Plan de seguridad



Los planes de seguridad no son documentos estratégicos. Deben ser simples, fáciles de usar y proporcionar información en un formato que el personal pueda usar en su trabajo diario; si no, el documento no será leído completamente ni utilizado. Para ser gestionable, los planes de seguridad no deben tener más de 20 páginas o el personal no los leerá, recordará ni usará el documento.

Existen muchas variaciones de planes de seguridad. Sin embargo, la mayoría sigue un formato general y contiene tipos de información similar dependiendo de la organización, el tipo de programa, la cantidad de personal y el tamaño de los activos, la ubicación de los proyectos, el contexto operacional y otros factores localizados.

La mejor manera de hacer planes de seguridad es involucrar una mezcla de personal, incluyendo gerentes, administradores, gestores de programas, el personal de terreno y los conductores, así como una mezcla de diferentes nacionalidades, etnias y sexos. Cada uno de ellos ofrecerá una perspectiva diferente.

Usando una mezcla de personal, nacional e internacional, de la oficina del país y del personal de terreno, puede crear un sentimiento de propiedad e interés colectivo en relación con el plan y así mejorar su cumplimiento. Sin embargo, evite tener un enfoque muy centrado en la gestión ya que el personal de primera línea en el terreno puede enfrentar el mayor riesgo. De manera similar, evite un enfoque excesivo en el personal internacional y considere la exposición al riesgo de todos los empleados, también el personal nacional trabajando en los programas. Si el plan de seguridad incluye diferentes medidas para el personal internacional, nacional reubicado y local, los motivos para estas diferencias deben explicarse claramente a todo el personal. De lo contrario, individuos pueden percibir que la organización solo se ocupa de un grupo en particular dentro del personal.

El plan de seguridad, o al menos las partes relevantes, deben estar disponibles en el idioma de los usuarios. Para el personal no alfabetizado y si la traducción no es posible, considere cómo se divulgará la información dentro del plan de seguridad. Es importante incluir y explicar el plan de seguridad a todo el personal basado en la oficina, incluyendo al personal de limpieza y vigilantes. Los miembros del personal que no están involucrados en la organización como personal de programación o de gestión pueden ser más vulnerables a ofertas de dinero a cambio de información. Ellos saben menos sobre la misión de la organización y pueden tener menos interés en garantizar la seguridad de todo el personal.

Si el diagnóstico de riesgos identifica una amenaza, el plan de seguridad debe aconsejar al equipo cómo gestionar el riesgo de esa amenaza.

Puede usar la plantilla de abajo para garantizar que su plan de seguridad tenga todos los elementos principales.

I. Descripción general del plan de seguridad

- Objetivo del documento

¿Por qué es importante este documento para todo el personal?

- ¿Quién es responsable de preparar el plan, actualizarlo y formar al personal?
- Su umbral de riesgo

¿Qué nivel de riesgo puede manejar su organización? ¿Cuánto es demasiado?

- Su estrategia de seguridad

¿Cómo utiliza su organización las estrategias de aceptación, disuasión y protección? ¿Cómo evalúa los resultados?

▶ *Consulte el Módulo 4 - Estrategias de seguridad: aceptación, protección y disuasión.*

- Fecha del documento/actualización/revisiones

¿Cuándo se redactó el documento? ¿Cuándo se debe actualizar?

II. Contexto actual – su diagnóstico de riesgo

▶ *Consulte el Módulo 3 – Herramienta de diagnóstico de riesgos.*

- El contexto general

Una buena descripción general del país y la región y de los desafíos enfrentados.

- Su sistema de diagnóstico de riesgos

¿Cómo identifica las amenazas y su sistema de calificación?

- Amenazas a las que se enfrenta en su contexto
- Evaluación de amenazas y evaluación del riesgo

III. Procedimientos operacionales estándar (SOP por sus siglas en inglés)

Esta sección debe incluir los SOP para todas las amenazas y riesgos identificados en su diagnóstico de riesgos. Deben ser simples, con instrucciones claras para que el personal sepa cómo prevenir el riesgo (reducir la probabilidad) y/o cómo reaccionar si ocurre un incidente (reducir el impacto). Debe estar en el formato de listas de verificación, procedimientos o acciones.

- Transporte de efectivo
- Comunicaciones, incluyendo planes de redes sociales

Consulte el Módulo 3 – Herramienta de diagnóstico de riesgos.

- Reporte de incidentes
- Viajes a terreno y seguridad de los vehículos

Consulte el Módulo 9 - Seguridad de los viajes: aeropuertos, vehículos y otros medios de transporte.

- Incendio en la oficina o recinto
- Control de acceso a la oficina e instalaciones
- Robo
- Accidente de vehículo
- Incluya otros SOP

IV. Otras secciones clave

- Salud y seguridad[5]

Protección del personal de amenazas a la salud (malaria, VIH, etc.) así como accidentes, estrés, tsíndrome de estrés post traumático (PTSD por sus siglas en inglés).

- Recursos humanos

Políticas relacionadas con la contratación, verificación de antecedentes, contratos, confidencialidad, etc.

- Seguridad administrativa y financiera

Políticas para prevenir robos, fraude, corrupción, así como manipulación de efectivo y aprovisionamiento.

- Incluir otras secciones clave

V. Sección de gestión de crisis

¿Quién forma parte su equipo de gestión de crisis (Crisis Management Team, CMT) y a quién reporta este equipo?

¿Cómo se activará el CMT?

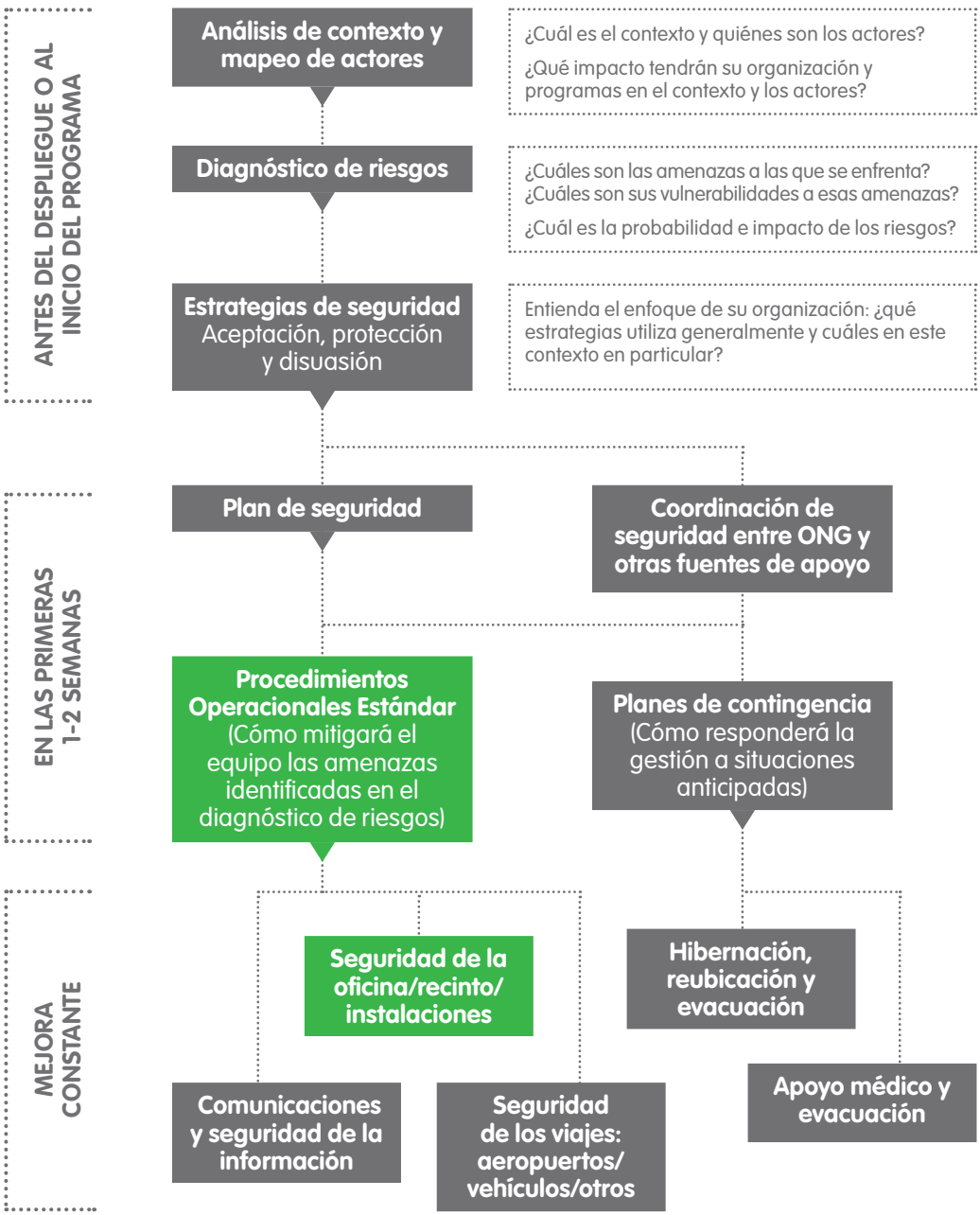
También incluya los planes de contingencia para crisis que se anticipan puedan ocurrir como secuestros, desastres naturales, evacuaciones y conflicto armado. A diferencia de los SOP, los planes de contingencia son herramientas de gestión y no son para distribución general.

Consulte el Módulo 10 – Hibernación, reubicación y evacuación.

Consulte el Módulo 11 – Apoyo médico y evacuación.

5 NdT: en inglés, *health* and *safety*.

7 Seguridad de las instalaciones



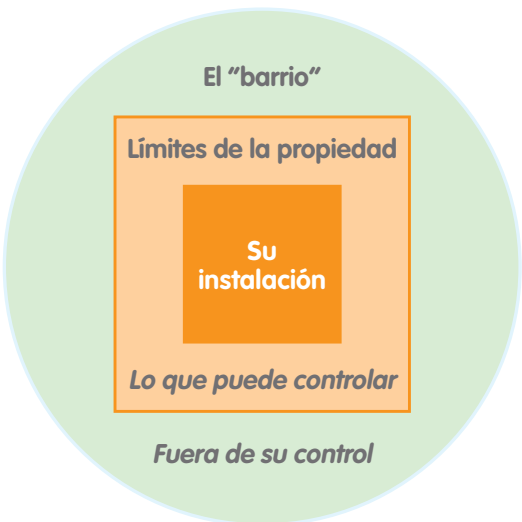
Cuando se considera una nueva oficina, residencia o recinto, primero revise su diagnóstico de riesgos para entender cuáles son los tipos de amenazas, cuál es el nivel de amenaza y cuál es el nivel de protección o disuasión que probablemente necesitará. Esto también aplica si se traslada a una oficina existente con una organización socia. También considere si será posible crear una estrategia de aceptación en la ubicación: esto normalmente es más difícil en áreas más urbanas que en entornos rurales, si bien siempre es recomendable crear un entendimiento mutuo con sus vecinos.

Esto es aplicable a todas las propiedades de la organización, oficinas, residencias, almacenes, clínicas, escuelas, etc.

En una respuesta de emergencia, usualmente es necesario y/o conveniente compartir el espacio. Si este es el caso, es importante acordar quién es responsable de qué, es decir, perímetro de seguridad, servicios de vigilancia, estrategia de aceptación local, etc.

▶ *Consulte la guía del EISF "Office opening: a guide for NGOs".*

Seguridad de oficinas, recintos y otras instalaciones



El anillo exterior: el barrio

Este es el área que bordea la oficina/recinto/instalación/residencia. El diagnóstico de riesgos debe identificar quién en el área puede afectar la seguridad del personal. Necesita entender su barrio y las partes interesadas en él para implementar su estrategia de aceptación. Puede ser más fácil en áreas rurales que en entornos urbanos, pero desarrollar un entendimiento con sus vecinos es esencial en todos los contextos.

Considere:

- Acceso a la calle, tanto el acceso a la oficina y cómo viajará de manera segura a otros lugares. ¿Es un callejón sin salida? Esto puede ser positivo para la identificación de una observación hostil pero limitará las opciones de viaje/rutas de escape.
- Peligros naturales como ríos (inundación), colinas (deslizamientos/avalanchas), pantanos (malaria/dengue) o bosques (incendio, animales salvajes).
- Vecinos como las embajadas, puestos militares/policiales, bancos, oficinas gubernamentales, otras ONG o universidades.
- Distancia a los aeropuertos, hoteles, ubicaciones clave en una emergencia.
- Estructuras de bloqueo/características naturales que interrumpirían las comunicaciones satelitales en una emergencia.
- El propietario, su historia y reputación.
- Acceso confiable a agua limpia.
- Acceso a teléfono, Internet y redes móviles.

El anillo medio: la propiedad

Esta es la primera área que está bajo el control de la organización. El diagnóstico de riesgos debe guiarlo sobre cómo asegurar la propiedad en términos de una pared perimetral, una valla o una cerca, o si la deja abierta, es decir, su estrategia de protección.

Recuerde siempre que, si siente la necesidad de construir un "búnker" para estar seguro, probablemente no debería estar basado en esa área.

Cuando planifica el perímetro debe considerar cómo puede impactar a sus vecinos y a su imagen. Considere el mensaje que envía. Si decide tener un perfil bajo y luego envuelve su recinto con alambre de púas, haciendo que se destaque de sus vecinos, será contraproducente. También debe considerar cómo su presencia puede afectar a sus vecinos:

- ¿Necesita un generador? Si lo necesita, ¿puede ubicarlo lejos de otras propiedades y/o hay posibilidades para aislamiento acústico?
- ¿Hay suficiente espacio de estacionamiento en el recinto y/o en el área sin molestar a los demás?
- ¿Su presencia crea un riesgo de seguridad para sus vecinos?
- Si contrata guardias, ¿dónde se ubicarán?

Es posible crear medidas de protección que no cambien negativamente la apariencia del recinto. Por ejemplo, alambre de púas debajo de la parte superior de la pared, usando jardineras de flores o macetas para disfrazar las barreras de hormigón, etc.

Adentro de su propiedad existen otras cuestiones que necesitará considerar:

- Control de acceso (planificado): ¿cómo acceden el personal, los visitantes, los proveedores o los miembros de la comunidad a su propiedad? Considere entradas para vehículos/personal, controles de identidad, áreas de estacionamiento seguro, tarjetas de identificación, zonas de espera y controles de multitudes (si corresponde).
- Control de acceso (no planificado): ¿qué fácil es para las personas entrar? ¿Existen límites compartidos con los vecinos o hay espacios abiertos? ¿Hay árboles sobresalientes y qué tan cerca están los muros perimetrales a los edificios?
- Los peligros de incendio incluyendo almacenamiento de gasolina y combustible, líneas de energía eléctrica y áreas designadas para fumadores.
- ¿Cómo se recolecta la basura? ¿Se trata de un modo seguro y adecuado para el medioambiente?
- Salidas de emergencia: si su recinto tiene una pared y una entrada central frente a la calle, ¿cómo evacuará de forma inadvertida si hay peligro frente a las instalaciones? ¿A dónde irá? ¿Quizás a un recinto/instalaciones de la ONU/otra ONG/residencias en la vecinidad?

El anillo interno: el/los edificio(s)

La seguridad de los edificios de la organización, sean oficinas, recintos/almacenes o residencias, es esencial dado que contienen sus objetos más valiosos incluyendo a las personas, equipamientos, activos, efectivo, registros y materiales y suministros de ayuda. El diseño del edificio también debe ser apropiado para los peligros naturales, p. ej., resistente a terremotos, aislado contra el calor y/o frío o para el frío y/o calor.

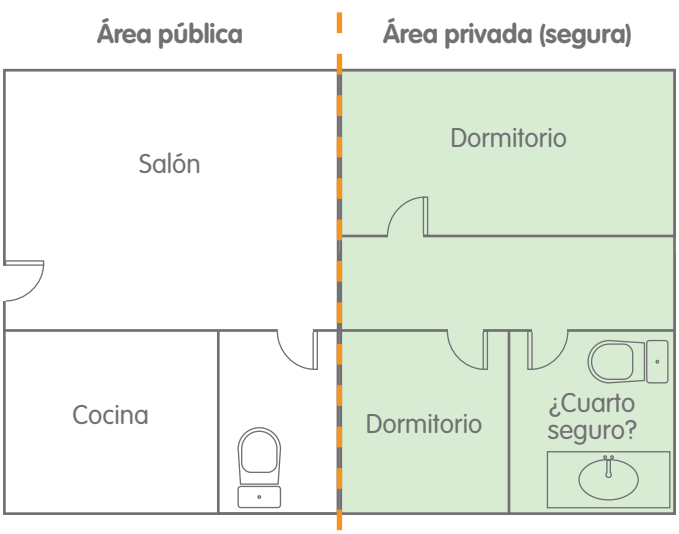
Para que el personal sea efectivo en su trabajo, es importante que se sientan seguros en sus oficinas y alojamientos. Considere:

- La seguridad de puertas/ventanas, asegurándose que impiden el acceso no autorizado pero que no atrapen al personal en caso de un incendio/evacuación.
- La seguridad de los techos (frecuentemente un punto de entrada preferido para robos después de horas de trabajo).
- Una área de recepción que controla el acceso a otras áreas vulnerables.
- Procedimientos de control de acceso para que los visitantes autorizados, al ingresar al edificio, no puedan pasear por la propiedad sin supervisión.
- Inspecciones eléctricas programadas para reducir el riesgo de incendio además de políticas estrictas sobre la prohibición de sobrecarga de enchufes de corriente.
- Almacenamiento seguro de documentos incluyendo cajas fuertes a prueba de incendio fijadas en la pared o el suelo.

- Rutas y procedimientos de evacuación de emergencia claramente señalizados y practicados.
- De ser necesario, un cuarto seguro que pueda alojar a todo el personal que esté en el edificio y equipado con suministros de emergencia (botiquín de primeros auxilios, linternas, mantas, alimentos, dispositivos de comunicación cargados/funcionando, extintor de incendios). Verifique que el equipo de comunicación de emergencia funcione en el cuarto seguro. Los teléfonos satelitales normalmente requieren contacto sin obstáculos, por lo que se pueden necesitar antenas externas.
- Unidades de suministro eléctrico ininterrumpido (Uninterrupted Power Supply, UPS) para proteger computadoras y otros dispositivos eléctricos cuando no se puede confiar en el suministro eléctrico o está sujeto a picos o cortes de energía.
- Alarmas contra incendios o intrusión y acciones a tomar cuando se escuchen, incluyendo simulacros y ejercicios prácticos.

Seguridad de las residencias del personal

Las residencias del personal pueden ser abordadas de manera similar a las otras propiedades, pero con algunas precauciones adicionales para garantizar la seguridad. Mientras que toda la residencia necesita tener seguridad adecuada, objetos de valor (TV, computadoras, electrodomésticos, etc.) normalmente están en las áreas "públicas" de la casa donde los invitados o amigos pueden entretenerse y estos objetos probablemente son la principal atracción de ladrones. Las áreas privadas de la residencia incluyen áreas para dormir, por lo cual necesitarán estándares más altos de seguridad que las áreas públicas.



Considere:

- Una puerta sólida, con cerradura, entre las áreas públicas y privadas de la residencia.
- Mejor seguridad de las ventanas y el techo en áreas privadas, con cerradura desde adentro pero no siendo un obstáculo en el caso de un incendio para la evacuación.
- Un cuarto seguro con botiquines de primeros auxilios, mantas, linternas, extinguidores de incendios y un dispositivo de comunicación cargado y probado regularmente.
- Tela mosquitera en las ventanas para alejar los mosquitos (para la prevención de enfermedades).
- Control estricto de las llaves y cualquier duplicado.
- Luces exteriores, especialmente alrededor de las entradas.

También es importante considerar la cultura local. En un ambiente conservador, puede necesitar considerar una separación entre sectores masculinos y femeninos, así como una separación entre el personal nacional como los guardias y los conductores y el personal internacional -de manera que el personal internacional se pueda relajar sin ofender o dar una impresión equivocada al beber alcohol y bailar, las mujeres llevando pantalones cortos, etc.

Vigilantes y guardias de seguridad

Muchas organizaciones buscan contratar vigilantes y/o guardias de seguridad localmente como un primer paso para desarrollar sus sistemas de seguridad en relación con las instalaciones. Las organizaciones normalmente usan el término "vigilantes" en lugar de "guardias" para respaldar la comprensión de que no se espera que el personal arriesgue su propia seguridad para proteger el recinto y sus activos.

Los guardias usualmente son el primer punto de contacto entre la comunidad anfitriona y una ONG. Cómo se comportan, sus modales, así como su profesionalismo a menudo se reflejarán en su empleador. Por lo tanto, asegure lo siguiente para todos los guardias y vigilantes:

- Que conozcan el mandato y el Código de Conducta de su organización.
- Que reciban instrucciones claras sobre sus tareas y cómo serán supervisados.
- Proporcionar a los guardias tuna lista de "acciones" sobre como responder en caso de visitas, actividades sospechosas, robo, incendio, lesiones u otro incidente que probablemente pueda ocurrir, según haya sido identificado en su diagnóstico de riesgos.
- Asegura que los miembros del personal traten a los guardias con respeto y que entiendan las obligaciones de los guardias. Asegura cumplimiento de esto por parte de los demás empleados.

- Se les debe proporcionar a los guardias una lista de contactos de emergencia y medios para comunicarse si sucede un incidente.

▶ *Consulte el documento informativo del EISF "Engaging private security providers: a guideline for non-governmental organisations".*

Prácticamente todos los guardias de las ONG no están armados. Sin embargo, en entornos de alto riesgo puede ser común que las organizaciones tengan una respuesta armada en caso de emergencia, ya sea activada por botones de pánico o por los guardias existentes. Si este es el caso, la organización debe obtener información sobre quién presta el servicio armado (compañía privada, policía, ejército), cuál es su propósito (proteger al personal y los activos de la organización o arrestar a los atacantes), su nivel de formación y la responsabilidad de la organización si alguien (personal, guardia, peatón) recibe un disparo durante una respuesta armada.

Existen tres categorías principales de guardias de seguridad: guardias comerciales, guardias contratados y voluntarios de la comunidad. Cada uno de ellos tiene ventajas y desventajas.

Servicios de guardias comerciales

Son suministrados por una compañía de servicios de guardias contratados. La compañía de guardias puede rotar el personal haciendo que sea difícil crear un nivel de confianza. Es importante, particularmente en edificios residenciales, que los miembros del personal conozcan al guardia que debe abrir la puerta de entrada. De otra manera, el guardia puede causar sentimientos de inseguridad en lugar de aliviarlos.

Ventajas	Desventajas
El proveedor puede prestar servicios adicionales como un equipo de respuesta rápida (sea claro sobre qué implica), alarmas, redes de radio, patrullas y supervisores nocturnos.	La organización tiene poco o ningún control sobre las instrucciones y obligaciones estándar de los guardias.
Contrataciones, formación, sueldos, recursos humanos, administración y programación son realizadas por el proveedor.	Las compañías de seguridad, en su mayoría, están más preocupadas por los "resultados".
	Los guardias están mal pagados y desmotivados.

Guardias contratados

Están empleados directamente por la organización.

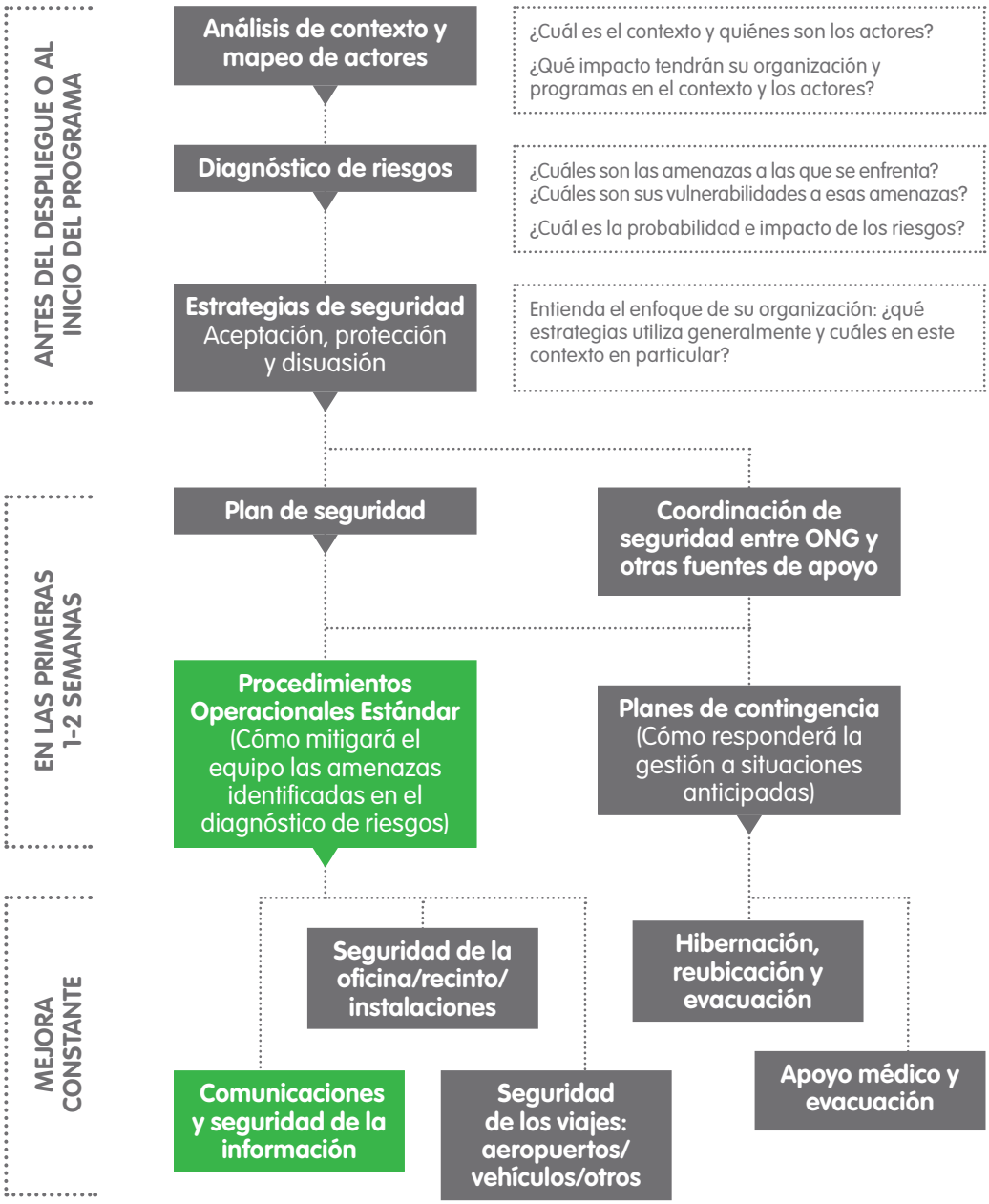
Ventajas	Desventajas
Los guardias pueden estar mejor pagados dado que el dinero de las organizaciones de ayuda no se destina al sistema de beneficio comercial.	La organización debe asumir la responsabilidad de la formación, los uniformes, el equipamiento, la administración y supervisión.
Como miembros del personal, tienen una mayor lealtad y el conocimiento de los estándares, políticas y Código de Conducta de la organización.	No hay un apoyo adicional disponible.

Voluntarios de la comunidad

Normalmente, son guardias proporcionados por la comunidad anfitriona en las áreas del programa. Habitualmente son la única opción en áreas remotas. Normalmente existe un costo por salarios, formación, equipamiento mínimo.

Ventajas	Desventajas
Utiliza el enfoque de "estrategia de aceptación" incorporando a la comunidad en la seguridad.	No hay estándares establecidos para las funciones del trabajo.
	Falta de rendición de cuentas.
	Abierto al abuso.

8 Comunicaciones y seguridad de la información



Al establecer un nuevo despliegue, proyecto o misión, hay que tomar el tiempo para analizar los tipos de comunicaciones que se tendrá a disposición (teléfono fijo, redes de telefonía móvil, teléfonos satelitales, Internet, correo postal, mensajería, etc.) y qué tan confiables se espera que sean. En el mundo moderno, las comunicaciones son una necesidad clave para la "supervivencia", tanto como los alimentos, el agua y el albergue.

Presupuestar fondos con suficiente antelación para contar con sistemas de comunicaciones fiables -incluyendo sistemas de respaldo y alternativos para reemplazar el equipamiento dañado, perdido o robado- es un componente clave tanto de la seguridad del personal como del éxito del programa. Además, es posible que hagan falta licencias para utilizar algunos métodos de comunicación, tales como las radios o los sistemas satelitales. Las Naciones Unidas tal vez puedan ayudar a obtener dichas licencias. La organización debe incluir en el presupuesto el tiempo de uso o la adquisición de las licencias cuando sea necesario.

Sea consciente de las nuevas tecnologías que pueden mejorar sus comunicaciones eficientemente como las tarifas satelitales para teléfonos inteligentes o sistemas de mensajería por satélite frente a teléfonos de voz tradicionales.

Compre lo mejor que se puede permitir finacieramente.

No obstante, las organizaciones tienen que considerar la imagen que da su equipamiento de comunicaciones. Si tener un perfil bajo es parte de la estrategia de seguridad, colocar radios y antenas de alta frecuencia a los vehículos, los hará resaltar tanto como si llevaran un logo.

En las regiones donde hay conflicto o disturbios civiles o donde acaba de ocurrir un desastre natural, nunca asuma que el Internet y las redes móviles funcionarán adecuadamente. Cuando hay emergencias de seguridad o desastres naturales, los gobiernos suelen tomar control de las redes (o incluso cerrarlas), cuando más las necesita. Es importante no depender de un solo sistema, ya sean líneas terrestres, redes de telefonía móvil, teléfonos satelitales, Internet u otros.

Sea creativo. En situaciones de emergencia, las ONG han utilizado repetidores de taxistas para mantener las comunicaciones con el personal cuando los teléfonos o el Internet no han estado operativos, o empleado camellos para llevar mensajes y mantener el contacto con comunidades alejadas.

Procedimientos y seguridad de las comunicaciones

Establecer y mantener una red de comunicaciones amplia es clave para la seguridad y el éxito de las operaciones. Si su organización tiene redes de radio o teléfonos satelitales, enseñe al personal a utilizarlos en el proceso de orientación inicial e indíque dónde pueden usar el equipo de comunicaciones instalado (por ejemplo, ¿hay que estar en el exterior? ¿hay puntos donde el equipamiento no funciona?). Asegúrese de que el personal pueda comunicarse con su familia y amigos durante los despliegues y especialmente en emergencias.

Cada vez son más las organizaciones y los organismos de coordinación que utilizan WhatsApp y otras aplicaciones sociales similares para intercambiar información directamente entre el personal. Esto puede ser muy ventajoso a la hora de compartir información en tiempo real, aunque la información que se transfiere en estas redes no está verificada. Debe haber directrices claras sobre qué información se puede y no se puede compartir y sobre los procedimientos que indiquen cómo actuar al recibir información.

Por lo general, todos los procedimientos y las directrices de comunicación deben ser discutidos con el personal. Los procedimientos escritos, así como la información esencial de contacto en casos de emergencia, incluyendo los números de teléfono, frecuencias y señales de llamada, deben estar publicados en la oficina, en cada vehículo y en una tarjeta que cada empleado lleve consigo.

Es importante comprobar los sistemas regularmente y tener una fuente de energía de respaldo para la radio y para cargar los teléfonos móviles/satelitales.

Buenas prácticas:

- El personal nunca transmite información sensible, por ejemplo, sobre transferencias de efectivo o itinerarios de viaje, en lenguaje claro por radio o redes telefónicas.
- El equipamiento de comunicaciones, que incluye radios, teléfonos móviles y teléfonos satelitales, está aprobado por el gobierno del país anfitrión y tiene las licencias correspondientes previas a su uso.
- Cuando se utilizan las radios, se han obtenido múltiples frecuencias VHF y HF para cada oficina (cuando sea posible).
- Se ha coordinado el uso de redes de radio de otras organizaciones -como las de las Naciones Unidas.
- Se hacen controles periódicos por mensaje de texto, llamadas por teléfono satelital o radio con las oficinas alejadas y el personal en viaje por la zona, según sea necesario. Hay una política vigente en caso de que un miembro del personal o un equipo no pueda responder y no pueda ser contactado. Todo el personal está familiarizado con esta política y se implementa sistemáticamente.
- Se han establecido palabras o frases en código para casos de emergencia comunes como secuestros o intrusiones. Su uso se ha discutido con el personal.
- Las radios y los teléfonos de emergencia se monitorean 24 horas al día, según corresponda.

Seguridad de la información

Independientemente de cómo nos percibamos a nosotros mismos, a menudo, las organizaciones de ayuda internacional ya no son percibidos por actores externos como agencias neutrales o independientes. Estas organizaciones intervienen, obligan a otros rendir cuentas, hacen incidencia política y a veces asumen actividades asociadas normalmente con los gobiernos (como la atención médica, el agua, el saneamiento y el socorro de emergencia) y en muchas ocasiones realizan estas actividades con financiación de gobiernos "occidentales" que tienen sus propias agendas políticas. Esto hace que todo lo que hacen las ONG humanitarias parezca sospechoso a los ojos de mucha gente.

▶ *Consulte el documento informativo del EISF "The future of humanitarian security in fragile contexts: an analysis of transformational factors affecting humanitarian action in the coming decade".*

Por lo general, los gobiernos tienen los medios para monitorear las llamadas telefónicas, la actividad en Internet, las cuentas de Facebook y Twitter y el contenido RSS de las organizaciones, así como de hackear el disco duro de sus computadoras. Las organizaciones criminales también percibirán a las ONG como adineradas, a causa de los vehículos, las computadoras portátiles y los teléfonos satelitales que suelen utilizar, además de los niveles de financiación de los donantes que se anuncian públicamente. Todo esto hace que las organizaciones de ayuda sean vulnerables a los riesgos en materia de seguridad de la información. Sea consciente de que los delincuentes o agentes gubernamentales pueden leer cualquier cosa que usted escriba en un correo electrónico.

▶ *Consulte el documento informativo del EISF "Communications Technology and Humanitarian Delivery: Challenges and Opportunities for Security Risk Management".*

Tenga cuidado con lo que guarda en los discos compartidos. El personal de respuesta de emergencia suele traer sus propias computadoras y copiar todo en un disco compartido cuando se va, para la continuidad. Esto puede incluir fotos inadecuadas, información personal y análisis de contexto que otros actores o miembros del personal pueden considerar ofensivos. Es importante tener presente también qué información -tanto profesional como personal- se guarda en dispositivos móviles tales como teléfonos inteligentes, ya que se puede perder o sustraer con facilidad.

Evalúe el impacto que la información pueda tener si cae en las manos equivocadas -acoso del personal, diseminación de fotos inapropiadas, acceso a correos electrónicos o a la red privada virtual/servidor de la oficina, y así sucesivamente.

Buenas prácticas:

- Periódicamente haga una copia de seguridad de todos los archivos y guarde las copias de seguridad de todos los documentos y registros clave (acuerdos con el gobierno, documentos legales, estados bancarios, registros de recursos humanos) en otro lugar por si ocurre un incendio, una inundación, un robo u otro hecho que destruya los originales.
- Los documentos en papel pueden dar lugar a que se filtre información cuando se dejan en papeleras o se dejan sobre un escritorio, al alcance del personal de limpieza o de otros empleados o visitantes, que pueden verlos/copiarlos/llevárselos. Utilice una trituradora de papel para deshacerse de los archivos que no se guarden en un lugar seguro.
- Mantenga un buen sistema de firewall (sistema de protección) en todos los servidores y reduzca al mínimo el acceso del personal a las redes con

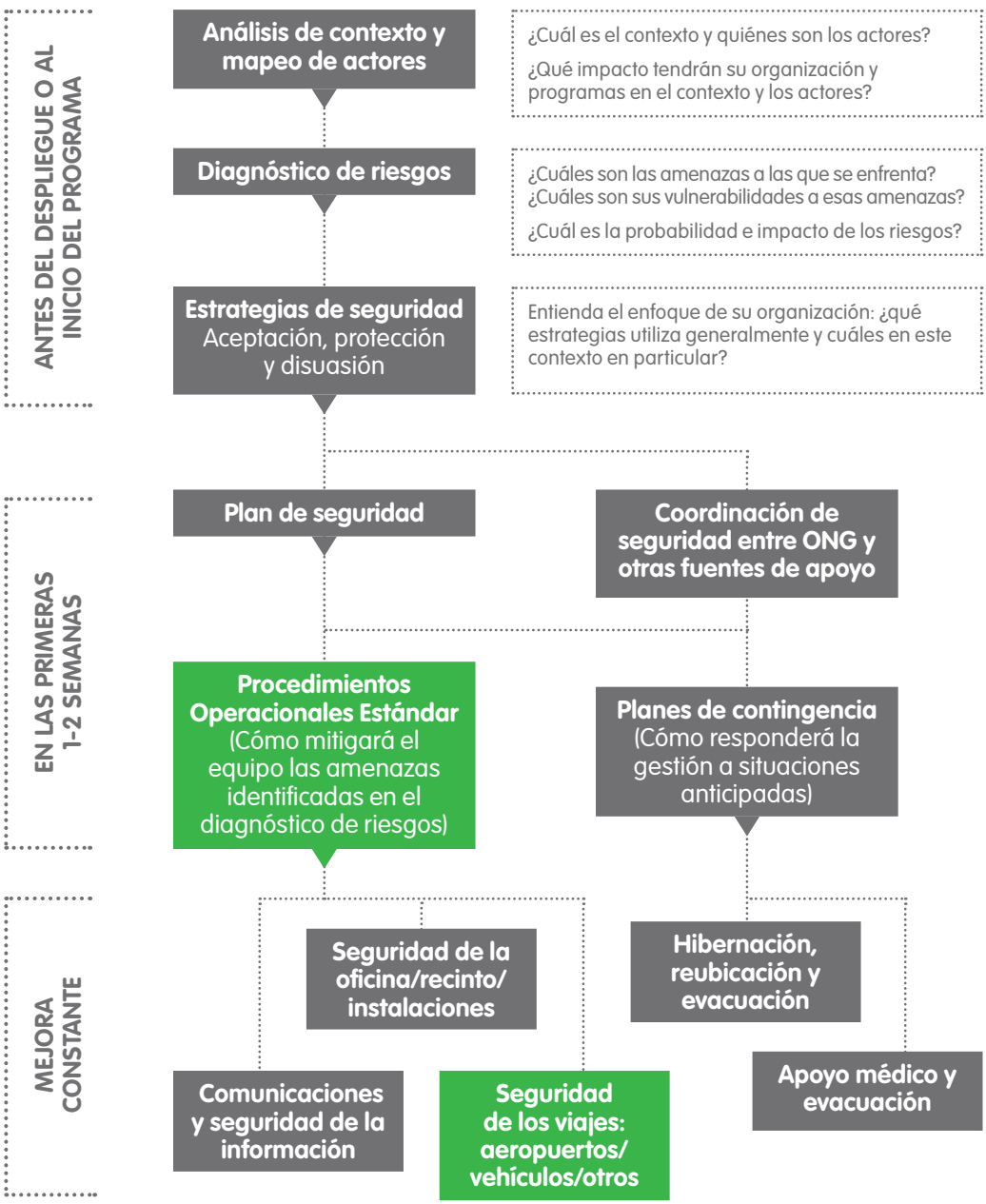
computadoras, tabletas o teléfonos ajenos a la organización para prevenir la propagación de virus.

- Recuerde que Skype no es más seguro al hackeo que cualquier otro método de comunicación.
- Nunca dé la impresión de estar recopilando "inteligencia" ni de estar pasando información militar o de seguridad a gobiernos extranjeros (ni a sus donantes, ni siquiera a la sede de su organización). Asimismo, el hecho de encriptar información puede mandar un mensaje equivocado. Particularmente si su ONG dice ser abierta y rendir cuentas, es posible que le cuestionen por qué es necesario encriptar la documentación.
- De ser posible, no utilice computadoras de escritorio. Aunque las computadoras portátiles son más fáciles de robar, también son más sencillas de trasladar si hay que llevar la oficina o el proyecto a otro lugar.
- Considere la posibilidad de emplear procesos de verificación de la información recibida por WhatsApp y otras aplicaciones sociales que simplifican la transferencia de información directamente entre el personal. También debe haber orientaciones claras sobre lo que se debe y lo que no se debe compartir.
- Asegúrese de contar con una política sobre las redes sociales que deje claro al personal lo que puede y no puede publicar en las redes sociales.

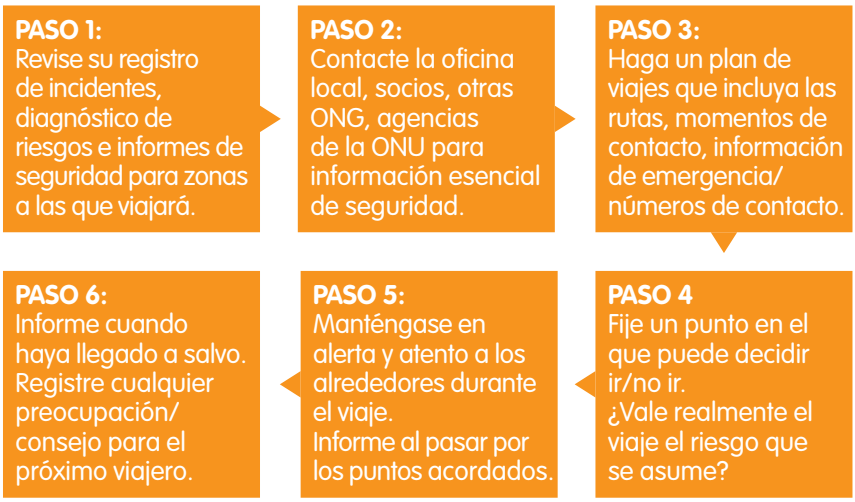
▶ *Consulte la guía del EISF titulada "Managing the Message: Communication and Media Management in a Crisis".*

Para las herramientas técnicas y las directrices, *"Front Line Defenders"* y *"Tactical Technology Collective"* han diseñado una guía sobre la seguridad digital para activistas y defensores de los derechos humanos titulada *"Security in-a-Box"* (Caja de herramientas para la seguridad). La guía cubre los principios básicos, incluyendo consejos sobre cómo utilizar las plataformas de redes sociales y los teléfonos móviles de manera más segura, además de ofrecer instrucciones paso a paso para instalar y utilizar los servicios y programas de seguridad digital más esenciales.

9 Seguridad de los viajes: aeropuertos, vehículos y otros medios de transporte



Según el *Aid Worker Security Annual Report 2014*, de 795 trabajadores humanitarios asesinados entre 2006 y 2013, 263 (33%) fueron asesinados en emboscadas en las carreteras. El momento en el que el personal de las ONG se encuentra más vulnerable a los robos, asaltos, secuestros, corrupción, lesiones o muerte es cuando viaja. Esto incluye el transporte aéreo entre países; el transporte por carretera desde el aeropuerto a la oficina u alojamiento, desde la oficina a la residencia, hacia y desde los proyectos de terreno y las reuniones; y cualquier parte donde el personal se desplace desde un lugar seguro a otro.



Buenas prácticas:

- Cuando viaje, asegúrese de poder ser contactado tanto como sea posible.
- Deje una copia de su itinerario de viaje, documentación importante y detalles de contacto locales por si acaso no se pueda establecer una comunicación directa.
- Antes de partir, confirme tener todos los visados, cartas de invitación, moneda local, direcciones y números de teléfono necesarios.
- Haga copias de todos los documentos importantes que tenga en su poder, tales como pasaporte, visado, tarjetas de seguro y de crédito y déjeselas al punto de contacto en su departamento. En algunos casos puede resultar útil llevar una copia de su pasaporte (incluyendo páginas de visado) y guardar el original en una caja fuerte.
- Envíe a su propio correo electrónico una copia de la documentación importante para que pueda acceder fácilmente a ella en línea desde cualquier computadora.
- Si es necesario, obtenga una licencia de conducir internacional.
- Lleve consigo sus certificados de vacunación.

- Considere si necesita o no contar con seguro médico/de evacuación/de otro tipo.
- Investigue si debe tomar alguna precaución en relación con la salud (tales como medicamentos, botiquín de primeros auxilios, purificador de agua).

Puede resultar útil hacer ejercicios de planificación de escenarios antes de emprender un viaje, especialmente cuando se viaja a zonas nuevas o a lugares inestables con un entorno cambiante. Todo el personal involucrado puede discutir los posibles escenarios y posibles respuestas ante ellos, para estar así mejor preparados por si sucede algo.

Cuando viaje por negocios, sería ideal que se le proporcione una tarjeta de identificación personal de la organización. Con esta tarjeta de identificación, le será más fácil rápidamente demostrar que viaja en nombre de la organización. La tarjeta no es un medio de identificación oficial, pero puede serle muy útil cuando desee dar a conocer la finalidad de su visita y, de ser necesario, dotarlo a usted de un estatus específico para la visita. Siempre lleve consigo su tarjeta de identificación. Si fuera necesario, puede también llevar consigo una carta de compromiso. Esta carta debería resaltar la finalidad de su visita y mencionar a las personas que visitará.

Viajes aéreos

Cuando se recorren largas distancias, suele ser inevitable utilizar el transporte aéreo. Para los viajes por aire, especialmente para los viajes regionales y nacionales, es importante que se considere el registro de seguridad de la compañía aérea seleccionada y se constate si esta compañía está certificada por IATA (International Air Transport Association), UE y FAA (Federal Aviation Administration), de lo contrario, su cobertura de seguro posiblemente no sea válida. Algunas páginas web que se pueden usar para consultar los registros de seguridad son FlightSafe, SkyTrax y AirlineRating.

Buenas prácticas:

- Siempre que sea posible, elija viajar en aviones con más de 30 asientos. Por lo general, estos aviones deben cumplir con normas de seguridad más estrictas y con estándares de fabricación más rigurosos.
- Elija vuelos sin escalas, ya que la mayoría de los accidentes ocurren durante el despegue y el aterrizaje.
- Siéntese cerca de una salida y memorice la ubicación.
- Cuando sea posible, elija los asientos de pasillo para que pueda levantarse y moverse más rápidamente en caso de emergencia. Esto también es bueno para la circulación de la sangre, de manera que pueda levantarse y estirarse cuando sea posible.

- No beba alcohol (o minimice su ingesta) ya que la presurización de la cabina incrementa el efecto del alcohol en el cuerpo.
- Infórmese sobre lo que está y no está permitido transportar en el equipaje de mano y esté preparado para que lo revisen.
- Nunca deje su equipaje de mano o facturado desatendido.
- Guarde en su equipaje de mano todos los elementos clave necesarios para sobrevivir en caso de pérdida, daño o retraso de su equipaje facturado.

Al llegar al aeropuerto, los pasajeros deberían tener una lista de contactos de personas clave y saber qué hacer si no se encuentra al conductor inmediatamente. ¿Dónde espera el pasajero? ¿Debería tomar un taxi o no? Y si lo hace, ¿qué tipo de taxi? Los pasajeros deberían tener una manera de contactar la sede y al personal local si surge algún problema, como un retraso del vuelo o la pérdida de una conexión. Antes de viajar, debería estar acordado como parte de la inducción de seguridad los detalles del punto de encuentro y del transporte desde el aeropuerto.

Según el contexto, a los viajeros se les debería suministrar el nombre y la foto del conductor o alguna forma para poder identificarlo correctamente. Los conductores deberían exhibir una tarjeta con el logotipo de la organización en lugar del nombre del pasajero. Si se exhibe el nombre, otras personas pueden aproximarse fácilmente al pasajero y además puede duplicarse fácilmente el nombre en una tarjeta o cartel falsificados.

Lo antes posible tras su llegada, los viajeros deberían recibir un informe de seguridad actualizado y una tarjeta que contenga los números clave de teléfono y ubicaciones.

Viajes por carretera

Si va a comprar o a alquilar su propio vehículo, asegúrese que dicho vehículo sea del tipo adecuado para el trabajo que desempeñará. Considere su diagnóstico de riesgos con respecto a la marca, la visibilidad, las tasas de robo por tipo de vehículo, el estado de la carretera y del terreno, la disponibilidad de repuestos y otros problemas logísticos.

Cuando alquile algún vehículo, debería considerar si lo va a alquilar con un conductor o si por el contrario utilizará a los propios conductores de la organización. En este último caso, todos los miembros de la plantilla que operen un vehículo deben poder realizar tareas de mantenimiento básico, tales como cambio de neumáticos y verificación del motor, los frenos, la batería y los líquidos del radiador. Si planea viajar en los vehículos de un socio local, asegúrese de comprobar las políticas de formación y supervisión de los conductores, los registros de mantenimiento de los vehículos y los procedimientos de seguridad para viajes. Los conductores deben respetar

las leyes y normas de tránsito locales y conducir a una velocidad que se ajuste a la situación en que se encuentran. Los pasajeros también son responsables de garantizar que esto se cumpla.

Todo el personal -tanto nacional como internacional- también debería ser informado de la política concerniente a pasajeros no autorizados, particularmente soldados y milicias armadas. De manera similar, debería instituirse una política clara concerniente a la utilización de los vehículos para uso personal durante y después de la jornada laboral, fines de semana y días feriados y debería comunicarse a todo el personal. El personal nacional e internacional debería tener la documentación de viaje apropiada, incluyendo las licencias para conducir.

Al viajar, todos los ocupantes del vehículo (incluído el conductor) deberían conocer la misma información básica sobre la organización en caso de que se les pare y sean cuestionados por separado. Adicionalmente, asegúrese de que se ha identificado un portavoz antes de la salida.

Cuando sea posible, el personal debería viajar acompañado por al menos otra persona. Los viajeros deben informar a otras personas sobre la hora y el destino del viaje conforme a los procedimientos establecidos. Un plan de comunicaciones detalla los horarios de contacto y las acciones tras las llamadas perdidas y también existen procedimientos para los accidentes de tránsito, de cuyo contenido todo el personal está informado. Si el personal no llega al destino en el horario planificado, se debería implementar consecuentemente la política de comunicación acordada.

▶ *Consulte el Módulo 8 – Comunicaciones y seguridad de la información.*

Para garantizar los contactos en el tiempo acordado durante el viaje, es clave que todos los teléfonos celulares estén cargados al máximo y que funcionen en la zona donde se llevará a cabo la misión. Si eso no se cumple, deberían considerarse protocolos y equipamientos de comunicación alternativos. Cuando se evalúan distintos protocolos y sistemas, debería tenerse presente que estos pueden variar dependiendo de la ruta elegida. Si existen opciones de rutas, elija las rutas de viaje primarias y alternativas a fin de evitar las zonas peligrosas y adaptarse a las condiciones de seguridad cambiantes. Es útil tener en la oficina un mapa actualizado con las rutas del país o de la región en el que se hayan marcado tanto las zonas peligrosas como las zonas que no tienen señal disponible para teléfonos celulares.

Buenas prácticas:

- Los vehículos deben estar equipados con herramientas básicas, neumático de recambio, equipamiento para cambio de neumáticos,

botiquín de primeros auxilios, mantas, agua potable de emergencia (2 litros por persona, por día), triángulos de emergencia, linterna, extintor de incendios y cualquier otro elemento que sea necesario para las condiciones geográficas/climáticas locales.

- Los cinturones de seguridad deben estar instalados y funcionar y deben ser utilizados siempre, tanto en los asientos delanteros como en los traseros.
- Los vehículos se revisan diariamente. Se ha designado a una persona como responsable del mantenimiento y de la corrección de discrepancias.
- Cada vehículo debe tener el registro y la documentación esencial del mismo.
- Cualquiera que utilice una moto en cualquier momento llevará un casco.
- Los tanques de combustible de los vehículos se mantienen por encima de la mitad, en la medida de lo posible.
- Las llaves de repuesto de los vehículos se guardan bajo un control estricto en cada oficina.
- Mientras se conduce, se mantienen las puertas del vehículo cerradas con el seguro y la menor cantidad de ventanas abiertas.
- Los vehículos no tienen ventanas polarizadas ni oscurecidas que puedan dificultar la visibilidad.
- Se cuenta con el uso de formularios de viaje, comprobantes de viaje o de un sistema de rastreo de vehículos que ayude a rastrear el movimiento de los vehículos.
- Cada vehículo cuenta con los datos de contacto de emergencia de individuos, organizaciones, hospitales y puestos policiales relevantes de la zona.

También constituye una buena práctica mantener libros de registro para cada vehículo y guardar en el vehículo una copia del programa de mantenimiento, lista de verificación, comprobantes de viaje, procedimientos de comunicación, mapas, etc. No obstante, piense cómo será tratada esta información si es descubierta cuando se inspecciona un vehículo en los puestos de control.

Otros medios de transporte

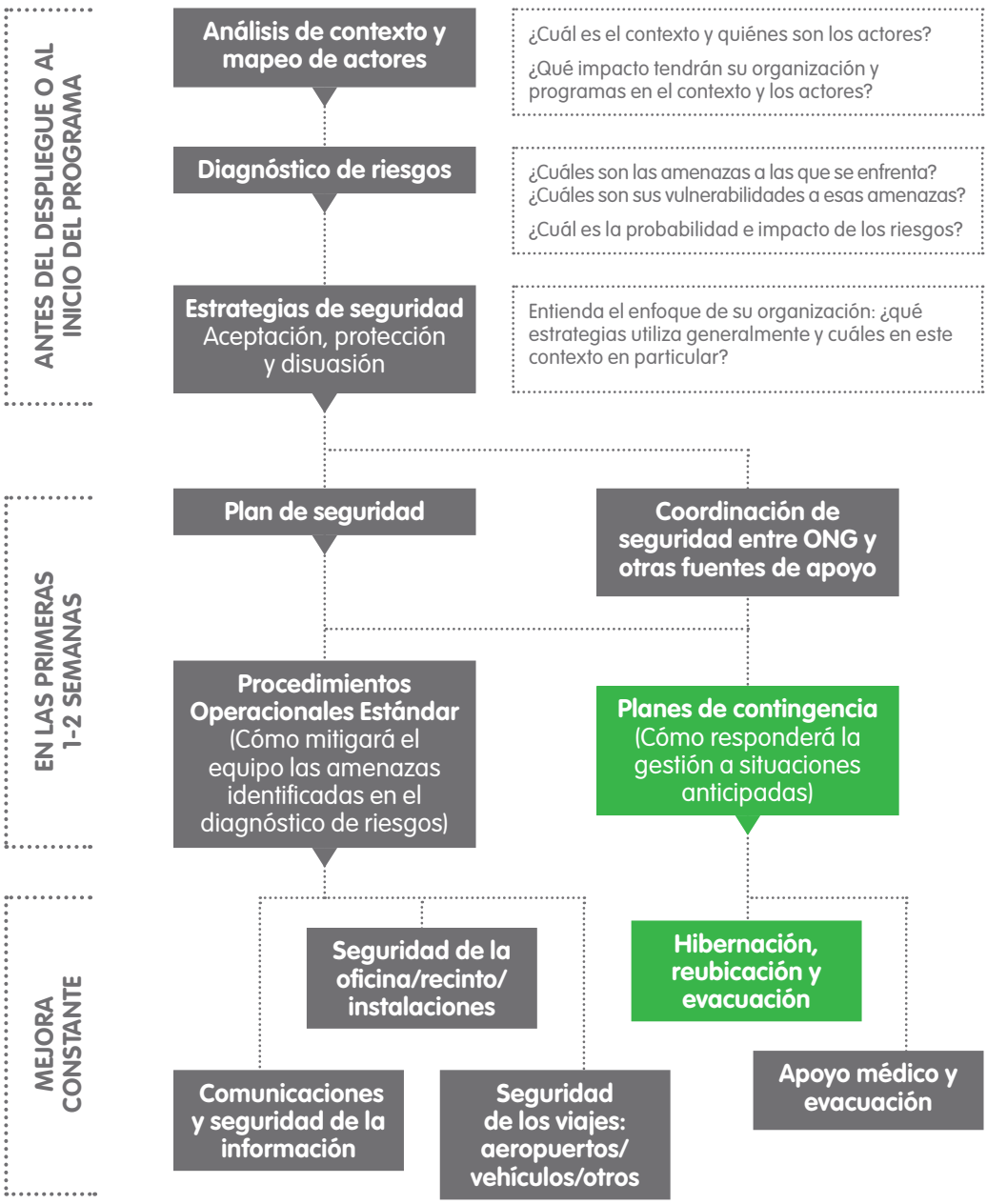
En algunos contextos será necesario, o más económico, utilizar otras formas de desplazamiento alternativas. Estas pueden incluir barcos, trenes, helicópteros, transporte público y taxis. Para cada medio de transporte, realice un breve diagnóstico del riesgo, que incluya investigar los riesgos y desarrollar estrategias de mitigación para cada uno de ellos.

Es posible que las organizaciones deban tomar precauciones adicionales para los viajes en barco en particular. Es importante asegurarse que el operador del barco o la organización suministre elementos de seguridad,

tales como salvavidas y radiobalizas de emergencia (Emergency Position Indicating Radio Beacon units - EPIRB). También puede ser necesario que la organización provea entrenamientos de natación o salvamento.

Para el transporte público tenga en cuenta las necesidades tanto del personal nacional como del personal internacional para trasladarse desde y hacia la oficina, durante y después de las horas de trabajo y para el descanso y la recuperación, y/o ausencias/vacaciones.

10 Hibernación, reubicación y evacuación

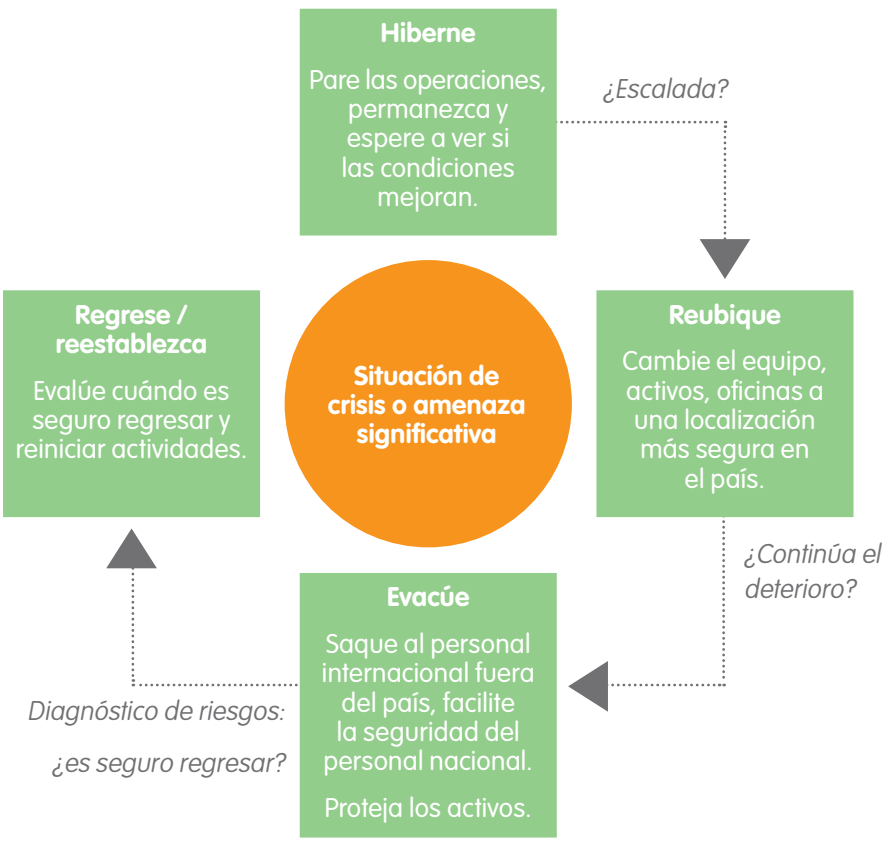


Las organizaciones de ayuda a menudo trabajan en regiones en las que se producen desastres naturales o en las que los conflictos amenazan al medio humano. Por lo tanto, es importante reflexionar sobre el modo en que reaccionará su organización ante una situación que se vuelve insegura durante un período breve o prolongado. Generalmente existen tres niveles de reacción ante un cambio significativo en un contexto amenazante:

Hibernación: El personal se queda en la casa y se detienen temporalmente los programas durante un período de crisis. En algunas circunstancias, es posible que el personal deba refugiarse en la oficina o en un recinto.

Reubicación: Cambio de oficina y/o de actividades de una zona insegura a una zona más segura, generalmente de modo temporal y dentro del mismo país.

Evacuación: Suspensión de las operaciones en un país, con la evacuación de extranjeros a otro estado y del personal nacional de las zonas de despliegue a sus hogares. Es posible que continúen unos programas de manera limitada usando gestión remota, dependiendo de la situación.



Es importante identificar "factores desencadenantes" que el personal dentro del país y de la sede central puedan acordar conjuntamente para determinar cuándo deberían activarse los diferentes planes de contingencia. Por ejemplo, para las inundaciones, cuando los niveles de precipitaciones alcanzan un nivel histórico que generalmente tiene como consecuencia una inundación, pueden activarse los planes de contingencia de hibernación o de reubicación. Si un conflicto armado en otra parte del país supera una línea o una zona acordada, pueden activarse los planes de contingencia de reubicación.

▶ *Consulte el glosario.*

Al estar de acuerdo previamente sobre estos factores desencadenantes, todo el personal en el país, el gobierno anfitrión, la sede y los donantes entenderán su decisión. Sin embargo, tal vez no convenga compartir los factores desencadenantes o las acciones resultantes con ciertos actores. Por ejemplo, al considerar dónde reubicar las actividades si el conflicto armado se acercara demasiado al lugar donde se encuentra actualmente, tal vez no sea apropiado compartir esta información con actores parte del conflicto en caso que afecte sus decisiones o incremente su vulnerabilidad como objetivo.

Es importante que, mientras sea posible, los factores desencadenantes se desarrollen cuando la situación está tranquila. Si se toman decisiones cuando la crisis está más caliente, la percepción del riesgo de las personas afectará el proceso de toma de decisiones.

Aunque no hay dos crisis iguales, generalmente hay algún tipo de advertencia de que la situación está empeorando o de que un desastre natural es inminente. Si bien algunos desastres naturales ocurren sin aviso (como es el caso de muchos terremotos), en otros, como las tormentas tropicales, las inundaciones o el deterioro de un conflicto, generalmente hay algún tipo de aviso o indicador. Cada plan de contingencia debería tener tres fases:

- Fase de advertencia: alerta a todas las partes concernidas de que es momento de prepararse.
- Fase de activación: activa el plan de contingencia.
- Fase de recuperación: detalla cómo la organización resumirá las operaciones de modo seguro.

La reubicación y la evacuación del personal pueden realizarse en fases, con la aplicación de diferentes factores desencadenantes para los diferentes tipos de personal. Por ejemplo, en un área propensa a las inundaciones, los

factores desencadenantes pueden ser: lluvias torrenciales durante seis días con posibilidad de inundaciones, se reubica al personal no esencial; lluvias torrenciales durante ocho días con ríos que alcanzan un nivel acordado, reubicación de todo el personal.

La definición de personal esencial puede variar entre las diferentes organizaciones y contextos, y también puede variar según los diferentes riesgos. Para identificar quién es el personal esencial, la función, el programa, la experiencia y la voluntad de asumir riesgos jugarán su papel. También deberían considerarse la etnia y la nacionalidad en riesgos relacionados con conflictos.

La mayoría de las organizaciones tienen una política de "libertad" para los individuos que da derecho a ser reubicados o evacuados si se supera su percepción del riesgo. Los individuos deberían conocer las políticas de las organizaciones en contextos en los que pueden ser necesarias la reubicación y/o la evacuación.

Hibernación

Buenas prácticas:

- Asegurarse que las oficinas tengan stock de emergencia de comida, agua y suministros de primeros auxilios para la cantidad de personas anticipada y el periodo de tiempo acordado.
- Los suministros almacenados deberán ser adecuados: no perecederos, transportables y nada congelado, ya que pueden echarse a perder si el generador se rompe.
- Los suministros deben almacenarse en lugares accesibles (p.ej., en lugares con peligro de terremotos, no almacene los suministros en una zona protegida contra robos pero que impida que el personal pueda acceder a los suministros en caso de que una emergencia -en este caso, un terremoto- ocurra).
- Tenga un equipo de comunicación adecuado en el lugar de hibernación (por ejemplo, si se traslada a un cuarto seguro cerrado, un teléfono satelital no funcionará).
- Tenga un generador de respaldo y combustible, si fuera necesario.
- Pague al personal el salario de 2-3 semanas en efectivo para que puedan sobrevivir.
- Póngase en contacto con los proveedores y los bancos y comuníqueles sus planes.
- Permita que el personal trabaje desde su casa, pero contáctelos diariamente y conozca su situación y sus observaciones.
- Minimice las actividades en la oficina, archive documentos importantes

fuera del lugar e inhabilite vehículos si existiera amenaza de robo durante períodos de caos.

- Manténgase en contacto con otras ONG en situaciones similares.
- Mantenga el contacto con las comunidades para obtener información y hacerles saber que no han sido olvidadas.

Reubicación

Buenas prácticas:

- Identifique con anticipación los lugares en los que puede reubicarse temporalmente si el centro de operaciones o una región específica se vuelve insegura para trabajar. Estos pueden incluir:
  - Oficinas de terreno existentes
  - Recintos de otras ONG
  - Casas de huéspedes
  - Otros lugares seguros
- Asegúrese de que el lugar temporal tenga un teléfono y acceso a Internet adecuados.
- Mantenga buenas comunicaciones con las comunidades, de modo que no se sientan abandonadas, y no se dañe como consecuencia su estrategia de aceptación.

▶ *Consulte el Módulo 4 – Estrategias de seguridad: aceptación, protección y disuasión.*

- Si los miembros del personal han sido reubicados, asegúrese de que cualquier plan de evacuación de contingencia se actualice consecuentemente, en caso de que la situación empeore. Si el personal está registrado en las Naciones Unidas, la embajada o una empresa aseguradora en un lugar específico, asegúrese de que la información esté actualizada.
- Asegúrese de que también se tenga en cuenta al personal nacional y sus familias, de modo que no se le pida al personal que deje a sus familias en zonas peligrosas mientras van a trabajar en condiciones de seguridad.

▶ *Consulte la guía del EISF "Office Closure".*

Evacuación

Buenas prácticas:

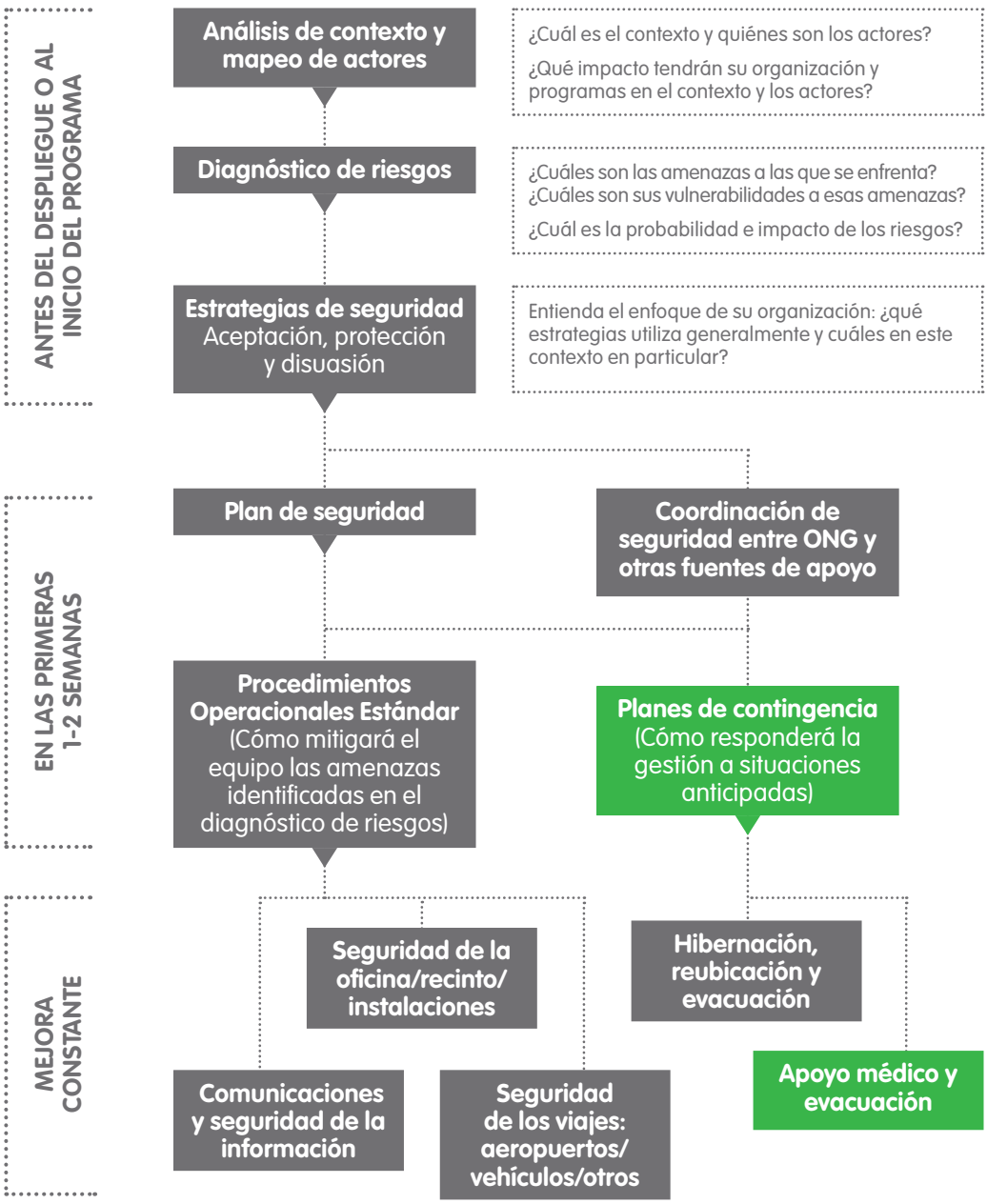
- No se concentre exclusivamente en el personal internacional. El personal nacional que se contrata en una zona y trabaja en otra (personal reubicado) a menudo corre mucho más riesgo que el personal

internacional. Asegúrese de que el personal nacional se evacue internamente a sus zonas de origen antes de retirarse.

- No prometa evacuar al personal nacional. No es función de las ONG crear refugiados ni es legal emplear personal en un país tercero.
- Pague al personal un mes de salario en efectivo antes de la evacuación.
- Establezca canales de comunicación con el personal nacional que se quede y con las comunidades para que ayuden a determinar cuándo es seguro regresar.
- Planifique el modo en que se garantizará la seguridad de los activos en el país, como vehículos y equipamiento informático o los procedimientos legales para trasladarlos a un estado vecino.
- No dependa de las Naciones Unidas para evacuar a su personal internacional. Establezca sus propios arreglos.
- No cuente con las promesas de embajadas para evacuar a todo su personal, especialmente si el personal internacional no es ciudadano de ese país.
- Si tiene un seguro, infórmese sobre los detalles de la cobertura. Tal vez especifique, por ejemplo, un estándar específico de pista de aterrizaje que solo está disponible en la capital.

Una vez que el personal ha sido evacuado, puede ser muy difícil volver al mismo lugar. Al elaborar el plan de contingencia para la evacuación, considere indicadores de regreso, así como el modo de mantener las relaciones establecidas anteriormente con las diferentes partes implicadas. Las evacuaciones deberían considerarse siempre como medidas de último recurso.

11 Apoyo médico y evacuación



Riesgos médicos y diagnóstico de las necesidades

Cuando las organizaciones se desplazan a un país nuevo, u otra región dentro de un país, es importante que evalúen qué riesgos a la salud – tanto física y mental, incluido el estrés– pueden enfrentar el personal. Esta amenaza médica o diagnóstico de los peligros instruirán sus preparativos. Más allá de las condiciones médicas universales, las amenazas médicas pueden agruparse en los siguientes tipos:

- Trauma balístico
- Violencia sexual
- Accidentes de tránsito
- Enfermedades (endémicas y epidémicas)
- Higiene
- Psicosocial
- Ambiental (vida silvestre, calor, altura)
- Nuclear, biológico, químico, radiológico

Es igualmente importante evaluar la asistencia médica disponible y su capacidad de respuesta -incluida la infraestructura- así como considerar los problemas con respecto al seguro y específicos de género que puedan surgir.

Asistencia médica y capacidad de respuesta

- ¿Qué nivel de servicios están disponibles? (p.ej., atención de emergencia, cirugía o cuidados paliativos)
- ¿Hay fármacos disponibles? ¿Los pacientes necesitan sus propias agujas, jeringas o antibióticos?
- ¿Las instalaciones médicas son capaces de ocuparse de afecciones comunes serias como infartos, insuficiencia de otro órgano o emergencias médicas similares?
- ¿Hay ONG médicas en el área? ¿Qué servicios médicos tienen capacidad y/o voluntad de proporcionar a su personal?
- ¿Hay ambulancias? ¿Se puede confiar en ellas? ¿Pueden llegar a lugares remotos?
- Si no hay servicio de ambulancias en su área de operaciones, o si este no es confiable, ¿cómo se evacuará al personal herido?
- Si tiene que considerar autoevacuaciones, se recomienda que se capacite al personal en cómo hacerlo de manera segura.

Infraestructura

Si la evacuación aérea dentro del país es una opción, establezca una relación anticipadamente y entienda los requisitos del servicio:

- ¿Cómo provee las ubicaciones para las solicitudes de evacuación médica (usando la latitud y longitud del GPS, MPRS, otros)?
- ¿Existen ya ubicaciones de evacuación preregistradas en el área?
- ¿Qué tipo de aeronave usa el servicio y necesita pista pavimentada/de tierra o espacio abierto (¿un área de qué tamaño?) para un helicóptero?
- ¿De qué manera estabiliza/protege a las víctimas para su evacuación?
- ¿Cómo se comunica con la aeronave?
- ¿Cómo registra/protege los documentos de identidad y la información de tratamiento para la víctima?
- ¿A dónde se llevará una víctima normalmente?

Seguro

Normalmente, las organizaciones tendrán seguro médico. Este seguro podría ser una póliza estándar para el personal nacional y posiblemente incluya evacuaciones médicas para el personal internacional. Es importante

que todo el personal esté informado sobre estas pólizas antes del despliegue y conocer su número de póliza y detalles de contacto del asegurador. Algunas organizaciones requieren que los consultores proporcionen su propio seguro médico.

Asegúrese de que el personal administrativo en el país esté al tanto de los arreglos acordados con el proveedor de seguros y en cuanto a la cobertura para todo el personal –incluidos consultores, personal adscrito y voluntarios– particularmente si el personal internacional y/o los visitantes de la sede tienen otros proveedores de seguro médico.

Mantenga registros de las pólizas de seguro en caso de emergencia y establezca un sistema para compartir información específica con el personal en el país, por ejemplo, un formulario registrando datos de emergencia (Record of Emergency Data - RED). Si el proveedor del seguro tiene hospitales y/o médicos aprobados de antemano, es recomendable visitar estos lugares y establecer una relación y canales de comunicación locales. Es importante entender los procedimientos de admisión en el hospital aprobado -solo porque el hospital haya sido aprobado por la empresa aseguradora, no significa que el personal será admitido automáticamente.

Tras la explosión de una bomba (…) varios extranjeros de dos agencias distintas resultaron heridos. Todo el personal fue trasladado a la misma ubicación para el triaje y tenían el mismo proveedor de seguro médico. Una agencia ya había visitado la administración del hospital y había establecido una relación con ellos; su personal fue ingresado al hospital en aproximadamente una hora. La otra agencia siguió los procedimientos que identificó su asegurador médico y tardó más de tres horas para que su personal fuera admitido en el mismo hospital.

Otros puntos a considerar son:

- ¿El seguro médico aprueba hospitales y/o médicos para el área?
- ¿Hay alguna restricción a la cobertura (p.ej., enfermedades contagiosas)?
- ¿Todo el personal está cubierto por la misma póliza (nacional, internacional, personal adscrito, consultores y voluntarios)?
- ¿Hay restricciones con respecto al tipo de evacuación médica que puede cubrir el seguro? ¿Dónde están disponibles en relación con los riesgos enfrentados? Por ejemplo, si requieren un tipo particular de pista para las evacuaciones aéreas.
- ¿El proveedor de seguro tiene puntos de evacuación específicos dentro del país? ¿Dónde están ubicados y cómo llegará el personal a estos puntos?
- ¿Los efectos del estrés están cubiertos?
- ¿Hay terapia disponible para quienes sufran de trauma mental/ psicológico?

Consideraciones específicas al género

- ¿Hay restricciones culturales motivadas por el género con respecto a quien puede proveer primeros auxilios, ya sea entre su personal o dentro de la población local?
- ¿Se prestan servicios ginecológicos u obstétricos? ¿Hay anticonceptivos disponibles?
- ¿El embarazo se considera una condición de alto riesgo en el país anfitrión?
- ¿Hay profilácticos post exposición disponibles?

Preparaciones previas al despliegue

Una vez que se ha llevado a cabo un diagnóstico de los riesgos médicos y se ha tomado en cuenta las consideraciones mencionadas anteriormente, las preparaciones y verificaciones típicas previas al despliegue pueden incluir:

- Informes médicos, exámenes (incluso de salud mental), chequeos y vacunas.
- Información médica personal (p.ej., signos vitales iniciales, tipo de sangre, afecciones, medicamentos, contacto del médico generalista).
- Suministros médicos personales y botiquines de primeros auxilios (fecha, cantidad y si los suministros se pueden importar al país anfitrión).
- Equipamiento o suministros disponibles y que se adquieren en el país.
- Formación requerida (incluyendo actualizaciones) en primeros auxilios o habilidades médicas avanzadas.

Los planes de contingencia médica son fáciles en teoría, pero a menudo pueden fallar, agregando estrés a un incidente y empeorando el resultado. Las asunciones que hacemos acerca de la logística pueden ser poco realistas, los planes pueden ser inadecuados, la información se vuelve obsoleta. Invierta su energía lo más pronto posible en la planificación de contingencia médica, antes de salir y cuando llegue, y ponga a prueba y actualice los planes de forma regular, de modo que los incidentes médicos no se conviertan en crisis.

Los líderes del equipo deben también discutir específicamente con los puntos de contacto dentro de la ONG la ayuda, los procesos, y los requisitos que la organización tiene o que ofrece. Esto podría incluir:

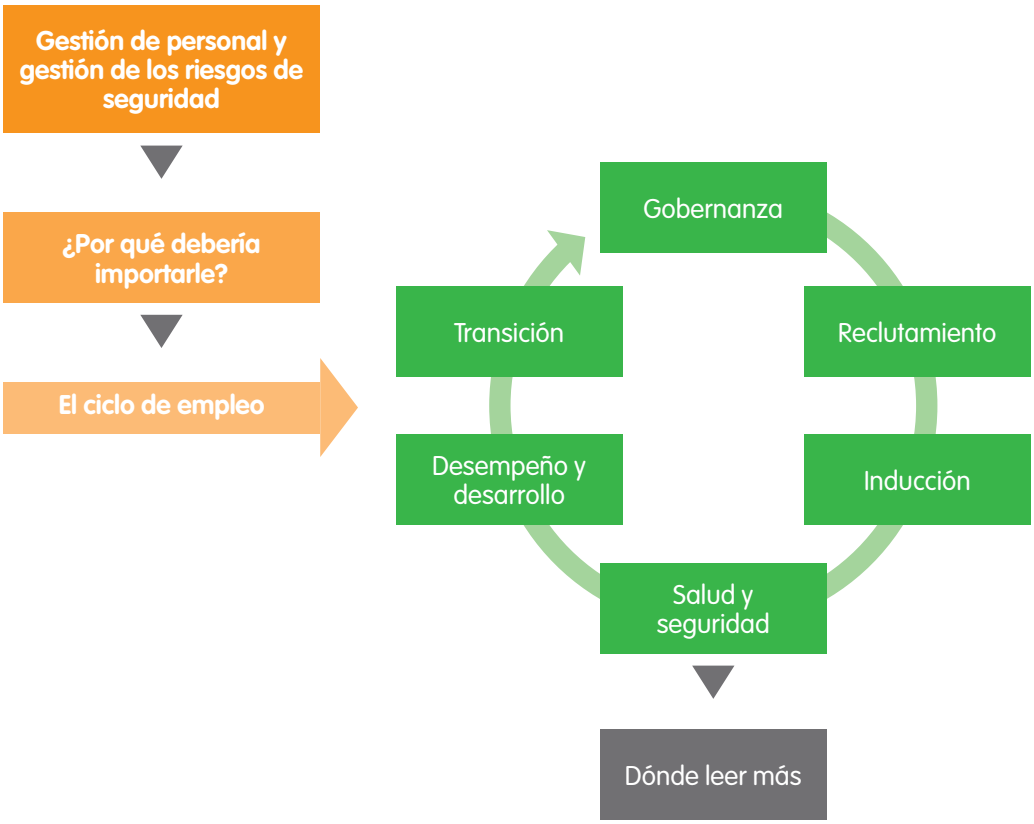
- Plan de gestión de crisis y planes de contingencia para emergencias médicas.
- Detalles de la cobertura de seguro (quién está cubierto, qué está cubierto, cuál es la respuesta y sus limitaciones, dónde existen fallos, qué información se requiere y cuándo, detalles de contacto).

- Experiencias organizacionales previas en el manejo de incidentes médicos.
- "Gobernanza clínica" (quién está autorizado para tratar a quién, a qué nivel, incluidos los medicamentos).

Cuando se despliega como un equipo, se debe designar a un miembro para que sea responsable de emprender un diagnóstico de riesgos médicos más detallado. Para los individuos que van a ser desplegados, identifique el punto de contacto local para el apoyo médico y obtenga información previa completa. Esto debe incluir:

- ¿Quién está entrenado, equipado y disponible para proporcionar los primeros auxilios a todo el personal en todo momento?
- ¿Quién puede proporcionar atención en terreno para estabilizar casos críticos, dónde se les localiza/cómo se les contacta?
- ¿Quién puede transportar apropiadamente a los heridos para el cuidado de emergencia, dónde y cómo?
- ¿Quién es el responsable general de controlar y coordinar a nivel de país (organización, aseguradora, otro)?
- ¿Quién comunicará qué, a quién, cuándo, y cómo?
- ¿Qué información es requerida por los proveedores del seguro médico? ¿Por quién y para qué propósito? Por ejemplo, ¿se necesita el informe de un médico para iniciar una evacuación médica?
- ¿Tienen las Naciones Unidas u otros, por ejemplo, el CICR, la capacidad logística para realizar evacuaciones médicas dentro del país? ¿Está este servicio disponible para las ONG y, si es así, cómo se accede a él?

12 Gestión de personal



Gestión de personal y gestión de los riesgos de seguridad

Una buena gestión de personal podría describirse como lograr un desempeño óptimo por parte de los empleados de manera segura y saludable. El personal constituye nuestro recurso más valioso y, si creemos que empleados contentos, seguros y motivados son más propensos a involucrarse, comprometerse y ser productivos, tiene sentido, empresarialmente hablando, brindarles un apoyo adecuado y ofrecerles un entorno laboral saludable y seguro.

La gestión de personal es un campo amplio y complejo, que conlleva responsabilidades legales y éticas para una organización en el sentido de garantizar la salud física y psicológica de sus empleados antes, durante y después de su período de empleo. Las organizaciones tienen múltiples obligaciones legales y éticas en materia del deber de cuidado y se espera

que vayan más allá de las provisiones legales mínimas cuando el trabajo se ejecuta en entornos de alto riesgo.

El personal en posiciones de liderazgo – fideicomisarios, directores y gerentes – debe invertir tiempo y recursos en prácticas de gestión de personal, y cerciorarse de que especialistas técnicos de Recursos Humanos y Seguridad provean la asesoría necesaria de la forma adecuada y en el momento preciso.

Gestión de personal y de los riesgos de seguridad – ¿por qué debería importarle?

La gestión de personal tiene un impacto directo en la gestión de los riesgos de seguridad. Por ejemplo:

1. **Contratación** – contratar a las personas equivocadas puede generar riesgos de seguridad. La falta de habilidades y competencias puede llevar a un desempeño y una toma de decisiones deficientes; las conductas inadecuadas pueden generar riesgos tanto personales como programáticos; y omitir considerar las implicaciones de la composición étnica en algunas regiones puede generar conflictos entre el personal y percepciones negativas en la comunidad local.
2. **Inducción** – preparar adecuadamente al personal tiene un impacto directo en la facilidad y rapidez con que este se adapta a su nueva posición, la vida en equipo y el entorno, reduciendo con ello el riesgo de incidentes de seguridad.
3. **Cierre de oficina y rescisión de contratos** – un proceso claro y transparente de cierre de oficina, y de rescisión de contratos, debe ser implementado con cierta antelación, antes de que inicie el período de notificación. La omisión de hacer esto puede tener implicaciones graves en materia de seguridad.
4. **Manejo del estrés** – las situaciones de riesgo y de grandes presiones son más propensas a producir una fuerza laboral altamente estresada, lo cual puede impactar en las conductas, las relaciones y la capacidad para tomar buenas decisiones en materia de seguridad.
5. **Políticas y prácticas laborales** – el personal tiende a sentirse más valorado y protegido cuando las políticas laborales (por ejemplo, en materia de incentivos, desempeño y conducta) son claras y se aplican de manera consistente. Un personal decepcionado e insatisfecho representa una eventual fuente de amenazas de seguridad para la organización, el personal y los programas.

Al leer este módulo, mantenga presente que:

- El empleado debe poseer las competencias y herramientas necesarias para desempeñar sus funciones adecuadamente.
- El entorno laboral debe ser tal que el empleado se sienta saludable y protegido.
- El personal debe estar informado acerca de sus propias responsabilidades en materia de salud y seguridad, entender los riesgos y aceptar cualquier riesgo residual que exista durante el desempeño de sus funciones, a sabiendas de que la organización ha realizado un análisis apropiado y ha tomado las precauciones necesarias.
- El personal debe tener la opción de negarse si le preocupan los riesgos que se le pide asumir en el desempeño de sus funciones.

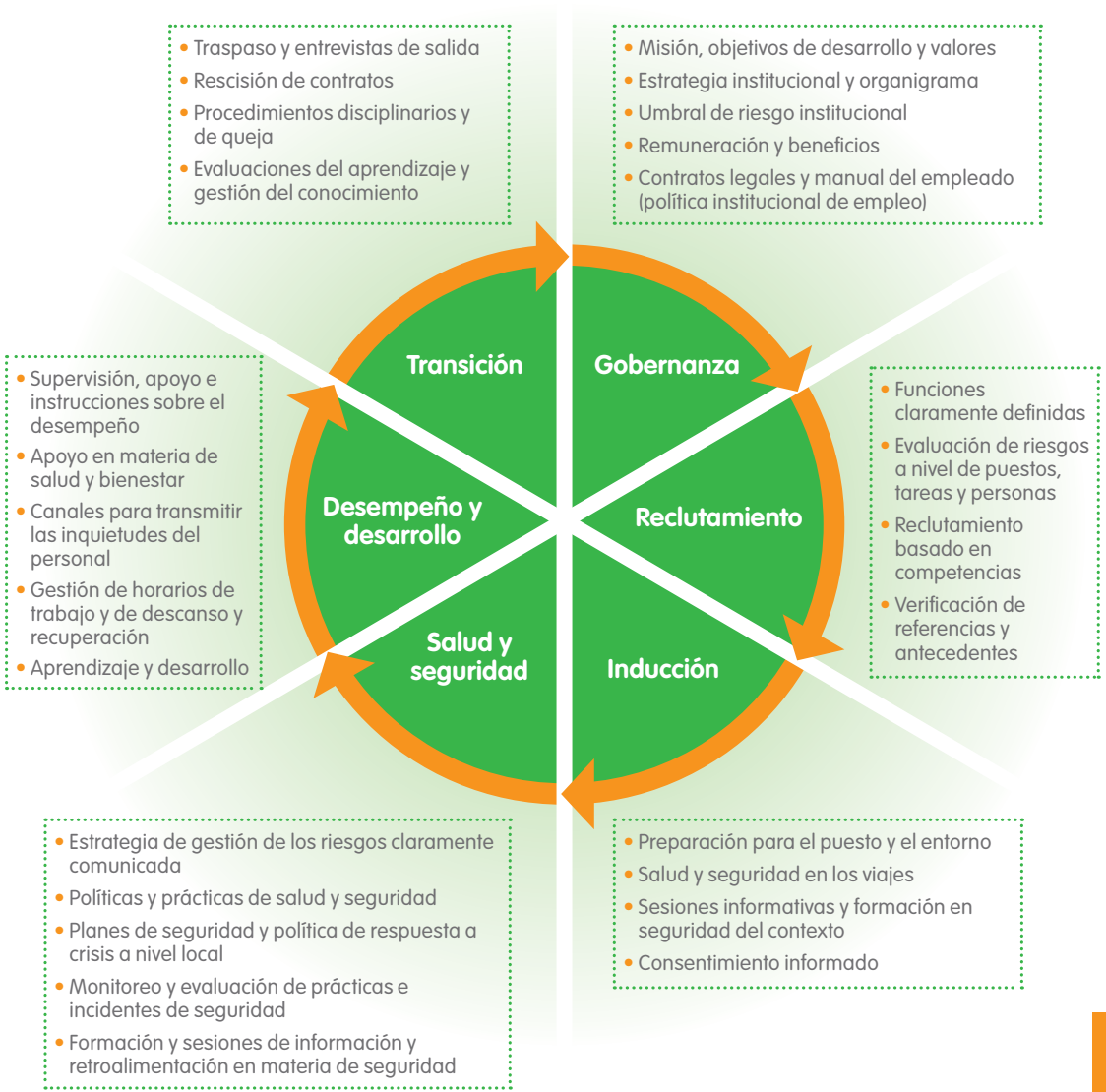
El ciclo de empleo y una buena gestión de personal

Para garantizar que su nivel de gestión de personal se mantenga elevado y cumpla las obligaciones de deber de cuidado se requiere el involucramiento de todo el personal de la organización, empezando por los empleados que ocupan los puestos más altos e incluyendo a todos los niveles de personal.

El ciclo de empleo constituye un buen sistema para identificar las prácticas de gestión de personal que poseen una obligación o un riesgo. Una gestión de personal óptima integra la gestión de los riesgos de seguridad en todas las etapas del ciclo de empleo.

Utilizar el enfoque del ciclo de empleo puede ayudar a entender asimismo quién es el titular o responsable de las diferentes prácticas de la organización. En la mayoría de los casos se trata de más de una persona, o bien de un colectivo o grupo de personas responsables, por ejemplo, un grupo de gestión de riesgos (en ocasiones conocido como comité de salud y seguridad).

Ciclo de empleo y principios de la gestión de personal



Gobernanza

La primera etapa del ciclo de empleo es la gobernanza, es decir, las estructuras y políticas en las cuales se sostiene su organización. La cultura de salud y seguridad de una organización depende en gran medida de la robustez de sus sistemas y prácticas, los más importantes de los cuales a menudo son los más elementales. El personal tiende a sentirse valorado cuando las políticas y prácticas institucionales son claras y se aplican de manera uniforme. Si las prácticas se encuentran mal alineadas entre sí, o son implementadas de manera deficiente, tendrán un impacto negativo en el

personal y elevarán el riesgo para la salud y la seguridad del mismo. El cuadro descrito a continuación revela las prácticas más importantes y las provisiones mínimas que debe ofrecer la organización.

Prácticas robustas son aquellas que se centran en valores, se guían por parámetros altos y son sostenibles, accesibles, pertinentes, conocidas, utilizadas, monitoreadas y evaluadas.

Práctica	Previsiones mínimas
Misión, objetivos de desarrollo, valores	La claridad de la misión, los objetivos de desarrollo y los valores institucionales asegura la claridad de la visión y las expectativas de la organización. La misión revela por qué existe la organización y cómo desearía mejorar el mundo. La misión se requiere para motivar al personal. Los objetivos de desarrollo aseguran que los empleados estén trabajando en pro de un propósito común. Los valores revelan cómo hará su trabajo la organización y qué tipo de personal se requiere para ello. Todo debe vincularse a ese panorama más amplio.
Umbral de riesgo institucional	El umbral de riesgo representa lo que el directorio y/o la alta gerencia considera como un nivel de riesgo aceptable para la organización. El umbral puede ser diferente para distintos tipos de actividades (por ejemplo, salvar vidas o ejecutar actividades de desarrollo). El umbral de riesgo constituye la base de todas las políticas y planes de gestión de los riesgos de seguridad a nivel de toda la organización. Además, permite que cada miembro del personal constate cuál es su propio umbral de riesgo aceptable frente a aquel que establece la organización.
Estrategia y organigrama institucionales	Una estrategia proporciona dirección, al proveer una explicación del trabajo que debe ser realizado, por quién, dónde y en qué plazo. El organigrama institucional describe quién es quién en la organización. Se utiliza para las descripciones de puestos, los grados y la denominación de los mismos, y revela las líneas de mando jerárquicas. Ayuda con los procesos de reclutamiento, inducción, gestión y comunicación a todos los niveles de la organización.
Contrato de trabajo y manual del empleado	Los contratos y manuales legales, claros y accesibles, con principios consistentes con las prácticas laborales, son necesarios para todas las categorías de personal definidas, incluso los contratos a corto plazo que a menudo se utilizan en la etapa de respuesta humanitaria temprana. Para los contratos nacionales, asegúrense de buscar asesoría legal en el país en cuestión. El manual del empleado es una herramienta referencial para gerentes y empleados, que contiene información útil acerca de la organización, de los términos y condiciones de empleo y establece las políticas institucionales.

Práctica	Previsiones mínimas
Remuneración y beneficios	La remuneración y los beneficios (incluyendo asignaciones especiales) deben aplicarse utilizando principios consistentes, alineados con las prácticas locales y adaptables a la etapa de respuesta humanitaria temprana. Los empleados deben ser consultados con relación a cualquier cambio en su remuneración y beneficios. Las variaciones que rigen los diferentes tipos de personal – internacional, reubicado, nacional, voluntarios, etc. – deben estar claramente definidas. Las acciones a tomar con relación a los beneficios incluyen: **Descansos y licencias** – monitorear lo siguiente: vacaciones anuales y acumulación de vacaciones, días festivos nacionales, descanso y recuperación, permiso por enfermedad y permiso de maternidad o paternidad. Apoyar apropiadamente las licencias por enfermedad y llevar a cabo entrevistas de reincorporación al trabajo. **Jubilación** – facilitar información sobre los planes de retiro opcionales. **Seguros** – entregar un resumen de las coberturas de seguros médicos, de viaje y por fallecimiento en servicio, con revisiones anuales y registros de casos.
Horas de trabajo	Horarios de trabajo y compensación por horas extras, con patrones laborales adaptables a la respuesta inicial de una emergencia repentina.

Implicaciones de seguridad

Las organizaciones humanitarias deben apuntar a enlazar sus valores institucionales con los principios humanitarios fundamentales. Dichos principios, especialmente neutralidad e imparcialidad, pueden ayudar a las organizaciones a obtener aceptación local y acceso seguro a ambientes inseguros. Los empleados que no sigan estos principios o los valores de su organización pueden ponerse en riesgo tanto a sí mismos como a la organización.

Un organigrama débil puede generar falta de claridad acerca de dónde reside la responsabilidad por la seguridad dentro de la organización, incluyendo cuál es la jerarquía para la toma de decisiones durante un incidente crítico, por ejemplo, el secuestro de un miembro del personal.

La transparencia en la definición de grados, remuneraciones y asignaciones especiales para todas las categorías de personal reduce el número de inquietudes y quejas. La falta de claridad en torno a estipulaciones contractuales como, por ejemplo, la rescisión anticipada de contratos, puede llevar a empleados disgustados a tomar represalias, comprometiendo con ello la seguridad de otros empleados, la organización y los programas. La organización debe contar con procedimientos disciplinarios claramente establecidos para lidiar con los empleados que se conviertan en una amenaza para sus colegas.

Reclutamiento

Los entornos peligrosos requieren empleados con capacidades específicas y experiencia. Una organización nunca debe subestimar la importancia del proceso de reclutamiento ni los riesgos que conlleva contratar al personal inadecuado. Contratar al personal inadecuado puede ser muy costoso e improductivo, y los empleados que no cumplan con las características del puesto tenderán a estar descontentos y a rendir por debajo de las expectativas, lo cual tendrá repercusiones directas en la ejecución del programa, en el tiempo disponible de su gerente, en la moral del equipo y en la seguridad. Antes de iniciar el proceso de reclutamiento debe realizarse un diagnóstico de riesgos con relación al puesto, a fin de dilucidar los requisitos esenciales del mismo y cerciorarse de atraer a los candidatos adecuados.

Los gerentes deben participar de lleno en el reclutamiento de sus equipos.

Identificar las fortalezas y las áreas que requieren desarrollo de un candidato, y evaluarlas en función de valores, capacidades y competencias esenciales, constituye un elemento fundamental del proceso. El gerente, en coordinación con Recursos Humanos y Seguridad, debe llevar a cabo un diagnóstico de riesgos con el fin de determinar los riesgos que necesitan mitigarse para el postulante y para el puesto en cuestión. Para puestos de alto riesgo o en contextos de alto riesgo, deben identificarse intervenciones obligatorias de salud y seguridad. El proceso de reclutamiento debe servir de insumo para el contenido de la inducción.

Consulte el Módulo 3 – Herramienta de diagnóstico de riesgos.

Práctica	Previsiones mínimas
Reclutamiento	Términos de referencia claros y un proceso de reclutamiento bien manejado, utilizando técnicas basadas en competencias que tengan muy en cuenta el aspecto de la diversidad. Las referencias y certificados de antecedentes deben ser verificados, y deben efectuarse diagnósticos de riesgos con relación tanto al puesto como al postulante, incluyendo análisis de salud y resiliencia. Los gerentes deben estar plenamente capacitados para participar en el proceso de reclutamiento. Si el gerente no domina el idioma local, deben tomarse medidas para que los postulantes al cargo no sean "preseleccionados" por el personal local, a fin de evitar el riesgo de que un sector de la comunidad local se vea favorecido indebidamente.
Igualdad y diversidad	La organización debe contar con una política institucional de igualdad y diversidad y el personal debe entender sus principios y aplicarlos en su trabajo y comportamiento. La política debe describir las características de la discriminación y debe establecer fuertes sanciones para eventuales infracciones. Si bien es cierto que la discriminación en la contratación por razones de etnicidad, género o sexualidad es moralmente y legalmente inaceptable, en muchos contextos la capacidad operativa de una organización puede verse afectada por las características particulares de una persona, de modo tal que estos riesgos deben ser considerados como parte del diagnóstico de riesgos relacionados con el puesto.

Implicaciones de seguridad

El gerente, en coordinación con Seguridad y Recursos Humanos, debe llevar a cabo un diagnóstico de riesgos robusto para todos los puestos durante la fase de reclutamiento. El objetivo es informarse sobre los riesgos inherentes al puesto y ayudar a definir el perfil de los candidatos a ser contratados.

Una vez que los postulantes hayan sido identificados, deberá efectuarse un diagnóstico de riesgos para cada uno de ellos en el puesto en cuestión. El objetivo es evaluar las repercusiones que podrían tener las capacidades, experiencia, edad, género, identidad sexual, discapacidad u origen étnico del postulante en términos de su seguridad y protección personal, cerciorándose al mismo tiempo de cumplir la normativa legal sobre igualdad de oportunidades.

El origen étnico en particular, tanto del personal nacional como internacional, puede tener implicaciones serias para la imagen de su organización y para los riesgos incurridos por el personal y la organización.

El objetivo del gerente es contratar a las personas más calificadas y cerciorarse de establecer medidas de mitigación para que puedan trabajar en un entorno con el menor riesgo posible en materia de seguridad. Entender la diversidad de su personal lo ayudará a desarrollar mejores sistemas de seguridad y recursos confidenciales y accesibles para apuntalar su seguridad.

Es extremadamente importante dedicar tiempo a verificar los certificados de antecedentes y las referencias del personal nuevo durante la fase de reclutamiento, especialmente en organizaciones que trabajan con poblaciones vulnerables, por ejemplo, niños, y donde las infracciones del código de conducta pueden acarrear graves riesgos para la reputación y la seguridad tanto del empleado como de la organización.

Inducción

Preparar a un empleado para desempeñar su trabajo es una de las cosas más importantes que una organización puede hacer. No es razonable enviar a un empleado a un entorno de alto riesgo sin darle antes una preparación exhaustiva. Dejar en manos de un empleado mal preparado la toma de decisiones que podrían poner en peligro su seguridad personal (y la de otros) equivale a abdicar la propia responsabilidad y el propio deber de cuidado. Tres áreas en particular requieren atención en este sentido:

1. Los empleados deben ser informados de las políticas y procedimientos institucionales de seguridad:
   - Deben saber cuál es el nivel de riesgo aceptable para la organización y estar familiarizados con las políticas que rigen la cultura institucional de seguridad.
   - Deben tener confianza en los sistemas con que cuenta la organización para gestionar su seguridad y bienestar.
2. El personal debe estar informado acerca de los riesgos para su seguridad personal:
   - Debe estar plenamente familiarizado con el contexto en el que está trabajando (cómo funciona y se comunica la sociedad que lo rodea) y ser consciente de la forma en que su propio comportamiento puede afectar su vulnerabilidad personal.
   - Deben saber qué se espera de ellos (por ejemplo, medidas de mitigación), tanto en horas de trabajo regulares como fuera de ellas, y comportarse en concordancia con ello.

3. El personal debe ser consciente de cómo el estrés afecta su conducta personal:
   - Las personas a menudo pueden descargar tensiones de maneras nocivas, por ejemplo, bebiendo en exceso o promiscuidad.
   - Las organizaciones deben proporcionar el entrenamiento requerido para que gerentes y empleados sean conscientes de y manejen su propio estrés, y deben implementar sanciones de manera consistente contra los empleados que se pongan en riesgo tanto a sí mismos como a terceros.

Práctica	Previsiones mínimas
Inducción	Un programa de inducción dirigido por el gerente de cada empleado, que incluya información y formación sobre: la misión, los objetivos de desarrollo, las conductas, el organigrama y las líneas de mando jerárquicas; la estrategia del programa; el mandato del equipo y/o programa; las relaciones centrales; el puesto; el traspaso de las funciones y responsabilidades; la situación de salud y seguridad en el contexto; los objetivos del período de prueba; políticas y prácticas institucionales clave.
Consentimiento informado	Consentimiento informado significa que el miembro del personal ha aceptado y firmado un documento que establece que los riesgos de seguridad que entrañan tanto el puesto como el contexto le han sido explicados a cabalidad y los entiende; que entiende las previsiones que la organización está tomando para gestionar los riesgos en el contexto; que entiende lo que se espera de él o ella; y que está de acuerdo con el riesgo residual que enfrenta una vez que la organización ha puesto en práctica medidas de mitigación. El proceso de consentimiento informado debe incluir asimismo una discusión de vulnerabilidades individuales.

El consentimiento informado es un proceso encaminado a garantizar el compromiso y la comprensión del personal – NO constituye una exoneración de responsabilidad legal.

Implicaciones de seguridad

Un empleado mal preparado puede tomar decisiones de seguridad equivocadas sobre la base de una interpretación insuficientemente informada del contexto local en materia de seguridad. Un miembro del personal que haya aceptado ser asignado a un puesto sin estar informado acerca de las restricciones operativas o personales (por ejemplo, la imposición del toque de queda desde horas tempranas de la noche) será más propenso a infringir los procedimientos de seguridad, ponerse en riesgo tanto a sí mismo como al programa y estar desmotivado y descontento con la organización. Esto contribuye a una mayor rotación de personal.

El traspaso de funciones y responsabilidades y una buena inducción, con apoyo apropiado de la gerencia de línea, es fundamental para todo miembro nuevo del personal, y más aún cuando el puesto conlleva responsabilidad decisoria con respecto a la salud y la seguridad del personal en entornos de alto riesgo. Por ejemplo, uno de los aspectos más preocupantes de un proceso judicial en Noruega en el 2015 (Dennis vs Norwegian Refugee Council) fue la falta de conocimiento del contexto local de seguridad por parte de la nueva directora de país.

Salud y seguridad[6]

La medida en que las organizaciones consideran al personal como una pieza central de su misión a menudo se ve reflejada en las políticas y prácticas relativas a la salud, seguridad[7] y bienestar del mismo. La salud y la seguridad del personal constituyen una responsabilidad primordial de cualquier organización y deben ser gestionadas apropiadamente a todo nivel. Los empleadores deben tomar todas las "medidas razonables" para prevenir que sus empleados sufran daños físicos y psicológicos "razonablemente previsibles".

La preparación para el puesto, entre otras cosas formación en autoprotección, primeros auxilios psicológicos, entornos hostiles y manejo de la seguridad y el estrés, ayuda mucho para mantener al personal en buen estado físico y mental, en condiciones de responder a una crisis o un incidente de seguridad. La formación y el desarrollo de capacidades no deben ser dejados de lado, ya que son prioritarios.

Las preguntas clave que mencionamos a continuación le ayudarán a determinar la robustez de las políticas y prácticas de salud y seguridad de su organización.

Salud

- ¿Cuenta el personal con la resiliencia física y mental suficiente como para desempeñar sus funciones? ¿Está informado sobre los factores desencadenantes del estrés?
- ¿Cuenta la organización con procedimientos establecidos para enfrentar incidentes críticos, así como con una política institucional sobre violencia sexual y un equipo calificado para responder a los incidentes de esta naturaleza?
- ¿Ofrece la organización servicios de asesoría confidenciales, con posibilidad de derivar al personal involucrado a servicios apropiados de consejería o tratamiento?

6 NdT: en inglés, *health, safety and security*. En esta sección se refiere simultáneamente a seguridad, derivada de un acto no intencionado, así como seguridad derivada de un acto intencionado.
7 NdT: en inglés, *safety* y *security*.

A menudo se formulan suposiciones acerca de la resiliencia mental del personal. Los profesionales internacionales experimentados con frecuencia constituyen la primera opción para ocupar los puestos de alto riesgo. ¿Evalúan constantemente los niveles de resiliencia del personal y saben cómo apoyarlo adecuadamente? Es importante recordar asimismo que los empleados de la comunidad local son tan susceptibles de quedar traumatizados por eventos graves como cualquier otro miembro de la población local a la que están asistiendo.

▶ *Consulte el Módulo 11 – Apoyo médico y evacuación.*

Seguridad (derivada de un acto no intencionado)[8]

- ¿Se ha llevado a cabo un diagnóstico de salud y seguridad para cada ubicación y se actualiza este regularmente?
- ¿Se reportan los accidentes y existe apoyo médico disponible, entre otras cosas apoyo psicosocial?
- ¿Cuenta la oficina con personal formado en el tema de primeros auxilios, y saben los empleados cómo contactarlo?

El empleador debe cerciorarse de que el lugar de trabajo sea lo más seguro posible y proveer un sistema de trabajo confiable. Si el lugar de trabajo se torna inseguro provisionalmente, el empleador deberá considerar tomar medidas razonables adicionales para reducir el peligro, entre ellas la opción de cancelar permanentemente la actividad laboral.

▶ *Consulte el Módulo 9 – Seguridad de los viajes: aeropuertos, vehículos y otros medios de transporte.*

▶ *Consulte la guía del EISF "Office Opening: A Guide for Non-Governmental Organisations".*

▶ *Consulte la guía del EISF "Office Closure".*

Seguridad (derivada de un acto intencionado)[9]

- ¿Cuenta la organización con un marco normativo de gestión de los riesgos de seguridad y con un plan de seguridad local para identificar, mitigar y gestionar los riesgos en materia de seguridad y responder a los incidentes de seguridad en caso de que ocurran?
- ¿Posee su organización una cultura de seguridad positiva, en el sentido que todo el personal entiende y se compromete a seguir los lineamientos

8 NdT: en inglés *safety*.
9 NdT: en inglés *security*.

institucionales en materia de seguridad con el fin de mantenerse a sí mismo, a sus colegas y operaciones a salvo?

- *Consulte el Módulo 1 – Proceso de planificación de la gestión de riesgos de seguridad.*
- *Consulte el Módulo 6 – Plan de seguridad.*

Práctica	Previsiones mínimas
Salud y seguridad[10]	Cada ubicación debe contar con una política y formación sobre cómo mantenerse saludable y seguro, las mismas que deben estar estrechamente alineadas con las prácticas de manejo del estrés, resiliencia personal, salud física y psicológica, y gestión de los riesgos de seguridad – intencionados, así como no intencionados. Reportar claramente los accidentes, enfermedades o incidentes críticos es fundamental. Los gerentes reciben formación en cómo realizar un seguimiento estrecho de la salud de sus equipos, utilizando conversaciones de aliento, reuniones informales para informar y recibir información sobre el trabajo y la detección de señales tempranas de estrés con la finalidad de prevenir la acumulación de tensión y el agotamiento nervioso de los miembros de sus equipos. Para los altos gerentes gestionados a distancia debería considerarse un sistema de apoyo de pares. La organización debe revisar permanentemente sus prácticas de salud y seguridad, para cerciorarse de que se mantengan relevantes y provean las medidas apropiadas para la seguridad del personal. Las principales partes interesadas deben extraer aprendizajes de las situaciones que suponen un riesgo para el personal, los programas y la organización.

Implicaciones de seguridad

El conocimiento, las conductas y las actitudes de una persona tienen un impacto en su vulnerabilidad y su exposición al riesgo. Cuanto mejor entiendan los empleados por qué existen procedimientos de salud y seguridad, más propensos serán a ceñirse a ellos. Por ejemplo, el personal se inclinará menos a recibir las vacunas recomendadas si no sabe o no entiende los riesgos que implica contraer enfermedades en el transcurso de un viaje.

Los accidentes de tránsito constituyen una de las mayores amenazas para la seguridad del trabajador humanitario sobre el terreno. Cerciorarse de que los conductores cuenten con formación en manejo seguro y que los viajeros utilicen el cinturón de seguridad, puede reducir sustancialmente las probabilidades y consecuencias de los accidentes de tránsito.

10 NdT: en inglés *health, safety and security.*

El personal que trabaja en respuesta humanitaria, especialmente en emergencias de ocurrencia rápida, es más susceptible a padecer altos niveles de estrés debido a las largas horas de trabajo en un entorno sometido a grandes presiones. Establecer medidas para prevenir y manejar el estrés del personal, y formar al personal para que sepa cómo identificar y manejar el estrés, redunda en el bienestar del personal, así como en su capacidad para tomar decisiones. El trabajo excesivo y los altos niveles de estrés hacen que las personas sean más propensas a tomar decisiones de seguridad deficientes.

Toda medida de reducción del estrés, por ejemplo, descanso y recuperación, debe ser aplicada de manera consistente; de no ser así, el personal puede sentirse presionado por sus pares a ignorarlas, incluso cuando son necesarias.

▶ *Consulte la guía del EISF "Auditorías de seguridad".*

Desempeño y desarrollo

La capacidad para realizar el trabajo especificado en la estrategia institucional descansa sobre las posibilidades del personal de desempeñar sus funciones en un entorno saludable y seguro. El personal debe recibir supervisión e instrucción adecuadas. Definir expectativas claras con énfasis en el impacto y proporcionar el apoyo necesario ayudará al personal a llevar a cabo sus funciones de manera adecuada. Por medio de comunicaciones frecuentes en ambos sentidos, tanto formales como informales, el gerente puede escuchar las inquietudes del personal y determinar si tiene un buen desempeño y, de no ser así, desplegar las políticas y prácticas pertinentes de manera consistente para gestionar un desempeño defectuoso, quejas y conductas inapropiadas.

"No poder" versus "no querer": existen dos formas de encarar el mal desempeño – utilizar una política de desarrollo de capacidades cuando el empleado no posee las habilidades o competencias necesarias para poder llevar a cabo el trabajo, y aplicar la política disciplinaria de la organización cuando el empleado no quiere hacer el trabajo.

La comunicación frecuente entre el gerente y el empleado debe incluir conversaciones sobre desarrollo personal con relación a las responsabilidades actuales y futuras del empleado. Apoyar activamente al personal en sus actividades actuales y en sus objetivos profesionales tenderá a motivarlo y mejorar su rendimiento y eficacia.

Práctica	Previsiones mínimas
Gestión del desempeño	El personal debe recibir supervisión e instrucción apropiadas. Los términos de referencia y los objetivos de los puestos deben ser claros. La comunicación con y la retroalimentación del gerente deben ser frecuentes, recompensando el buen desempeño y gestionando el desempeño deficiente, ya sea por medio de políticas de desarrollo de capacidades o por medio de medidas disciplinarias. El seguimiento de la gestión de los riesgos de seguridad debe ser específicamente incluido en el proceso de evaluación del desempeño para todo el personal que tiene responsabilidades en materia de seguridad.
Procedimientos de queja y procedimientos disciplinarios	La organización debe contar con un canal confiable para comunicar las inquietudes y presentar las quejas formales e informales. Las políticas institucionales de quejas y medidas disciplinarias deben especificar un procedimiento imparcial y consistente para gestionar, monitorear y aprender de los casos.
Denuncia de irregularidades	La denuncia de irregularidades es una opción para reportar de manera anónima una queja o inquietud grave y hacer que las que sean legítimas se investiguen de manera reservada.
Aprendizaje y desarrollo para el personal	Es necesario llevar a cabo discusiones periódicas sobre las conductas, oportunidades de desarrollo y objetivos profesionales del personal.

La seguridad debe formar parte del proceso de evaluación del desempeño de cada empleado.

Implicaciones de seguridad

Una de las mayores amenazas que enfrentan las organizaciones son los miembros del personal descontentos. Los empleados que sienten que han sido tratados injustamente pueden reaccionar de diversas formas: robo, abuso y maltrato físico y verbal, amenazas de muerte y hablar mal ya sea de personas individuales o de la organización en general ante partes interesadas externas tales como beneficiarios, notables de la comunidad y funcionarios estatales, así como los medios. Estas reacciones pueden tener graves implicaciones de seguridad para el personal, los programas y la organización.

La gestión del desempeño se sustenta en una buena relación empleado-gerente. Una mala relación puede erosionar la confianza y tener graves consecuencias para la seguridad si, por ejemplo, las recomendaciones de seguridad de un gerente son ignoradas o un empleado toma decisiones que podrían ponerlo en peligro, tanto a sí mismo como a sus colegas, sin haber consultado antes con su gerente.

Sin un canal confiable para transmitir sus preocupaciones, el personal puede sentirse obligado a aceptar todas las decisiones que adoptan sus gerentes, incluso si no se siente cómodo con los riesgos que conllevan. El personal que está más en contacto con la población local es más propenso a tener una mejor percepción del contexto de seguridad, pero la falta de canales de comunicación puede impedir que la información ascienda a través de la cadena de mando, incrementando el riesgo de ocurrencia de un incidente de seguridad.

Transición

Todos los empleados abandonan una organización en algún momento. La forma en que un empleado se despide puede tener consecuencias para el bienestar de dicha persona, sus colegas y la reputación de la organización. Un empleado que "se despide bien" puede convertirse en un embajador de la organización. Cuanto mayor tiempo e información tenga una persona a su disposición para prepararse para su alejamiento, mejor. Siempre que sea posible, los gerentes deben emprender conversaciones acerca de la partida de un miembro del personal antes de la fecha de inicio del período de notificación. Asimismo, es importante entender las razones por las cuales el personal decide renunciar por iniciativa propia.

▶ *Consulte la guía del EISF "Office Closure".*

Práctica	Previsiones mínimas
Medidas previas a la partida	Las conversaciones francas y transparentes con el personal, especialmente el personal nacional, sobre el futuro del proyecto o de la oficina, pueden hacer que los empleados estén mejor preparados para la transición y garantizar un buen traspaso de las funciones y responsabilidades del puesto. Las organizaciones deben establecer medidas para apoyar la transición de los empleados, especialmente cuando se ven obligadas a dejar ir al personal debido a la pérdida de financiamiento u otras razones fuera de su control.
Entrevistas de salida	Se debe recabar información y conocimiento del personal saliente, con base en preguntas sobre, entre otros temas, lo siguiente: equilibrio trabajo-vida personal, valores, desarrollo profesional, calidad de las reuniones informativas y de retroalimentación y razones de la renuncia. La renuncia por parte de varias personas de un mismo equipo puede ser un indicativo de algo más serio y deben tomarse medidas al respecto.
Aprendizaje institucional	Aprender de un miembro del personal saliente constituye una buena forma en que una organización puede generar y gestionar su conocimiento institucional.

Implicaciones de seguridad

Un empleado saliente descontento puede comportar un riesgo para la seguridad. Los despidos en razón de procedimientos disciplinarios, falta de financiamiento, cierre de la oficina y escalada de la seguridad pueden llevar a diferentes tipos de riesgos.

Un empleado decepcionado puede perturbar el desempeño y las relaciones del proyecto, y crear un ambiente tóxico. En un entorno de alto riesgo, gestionar la salida de un miembro del personal en circunstancias difíciles es una de las cosas más importantes y complicadas que un gerente puede tener que hacer.

Compartir información con otros empleadores, permitir horarios de trabajo más flexibles para la búsqueda de empleo y ofrecer oportunidades de formación (por ejemplo, cursos de computación e inglés) pueden ayudar al personal a tener una buena transición y en consecuencia reducir los riesgos de seguridad.

Si no se recaba información de un empleado saliente (generalmente mediante el traspaso de funciones y responsabilidades y las entrevistas de salida), es probable que lo aprendido no se transmita y se repitan los errores. Sin un buen traspaso de responsabilidades y funciones, existe un mayor riesgo de que un miembro nuevo del personal fracase en el desempeño de sus tareas y represente un riesgo para la salud y seguridad tanto propias como de terceros.

Para poder aprender y adaptarse, las organizaciones deben llevar a cabo diagnósticos de seguridad periódicamente y poner en práctica lo aprendido. Los ejercicios de gestión de crisis también son esenciales para la alta gerencia.

Cuando un programa poco exitoso estaba cerrando su oficina en Indonesia, la organización no les comunicó la noticia a sus empleados hasta dos días antes de la fecha de vencimiento de sus contratos. Los rumores ya habían circulado y los empleados estaban muy afectados. El día anterior a la fecha final de pago de salarios se produjo un asalto para robar dinero en efectivo de la caja fuerte y sustraer artículos de valor de la oficina. Los gerentes creían que era mejor no informar al personal de la fecha exacta de cierre por motivos de seguridad. Sin embargo, la falta de transparencia condujo a represalias más agresivas y comprometió la seguridad del personal. Un enfoque más honesto y solidario con el personal del programa probablemente hubiera generado menos incidentes y garantizado una mayor seguridad.

Dónde leer más

El portal web de *CHS Alliance* (http://www.chsalliance.org) aloja recursos para apoyar a las organizaciones con la salud, seguridad y bienestar de su personal. La Norma 8 en "La Norma Humanitaria Esencial en materia de calidad y rendición de cuentas" establece las políticas que deberían desarrollarse para la seguridad y el bienestar del personal.

Duty of Care International (http://dutyofcareinternational.co.uk/) aloja varios recursos (la mayoría en inglés), entre ellos los siguientes:

- La guía "Gestión de recursos humanos (ROOTS 12)" publicada por Tearfund. Se trata de una valiosa herramienta de gestión de personal para gerentes, especialmente si no existe personal especializado en recursos humanos en el país. Consulte la versión en español aquí: http://tilz.tearfund.org/~/media/Files/TILZ/Publications/ROOTS/Spanish/HRM/ROOTS_12_S_-_Full_Doc.pdf?la=es-ES
- "The Importance of HR Management in Supporting Staff Working in Hazardous Environments", por Roger Darby y Christine Williamson.
- "Can you get sued? Legal liability of international humanitarian aid organisations towards their staff", por Edward Kemp y Maarten Merkelbach.

La Fundación SOS Internacional (http://www.internationalsosfoundation.org) ofrece una serie de recursos útiles, en inglés, entre ellos, "Managing the safety, health and security of mobile workers: an occupational safety and health practitioner's guide", coproducida por la Fundación SOS Internacional y la organización IOSH.

El portal web del EISF (www.eisf.eu) aloja una serie de publicaciones propias (algunas también en español y/o francés) para apoyar a las organizaciones con el cuidado del personal, así como una biblioteca de recursos adicionales sobre salud y seguridad del personal.

Glosario

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

Amenaza: cualquier desafío/peligro enfrentado por la organización que afecte su personal, sus activos, su reputación o programas que existan en el contexto donde opera.

Deber de cuidado: obligación legal y moral de una organización de tomar todas las medidas posibles para reducir el riesgo de daño a aquellos que trabajan para una organización o están operando en su nombre.

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

Evacuación: suspensión de operaciones en un país, evacuación del personal internacional a otro estado y al personal nacional de las áreas de despliegue a sus áreas de residencia habitual. Dependiendo de la situación, ciertos programas podrían continuar de manera limitada usando gestión remota.

Factor desencadenante: factores acordados entre el personal del país y la sede para determinar el momento en que deben activarse los diferentes planes de contingencia.

Hibernación: permanencia del personal en casa e interrupción temporal de los programas durante un período de crisis. En algunas circunstancias, puede ser necesario que el personal busque refugio en la oficina o el recinto.

Protección: reducción del riesgo, pero no de la amenaza, a través de la reducción de la vulnerabilidad de la organización (p.ej., cercas, guardias, muros).

Reubicación: traslado de las oficinas y/o actividades de un área insegura a una localización más segura, generalmente de modo temporal y dentro del mismo país.

Riesgo: cómo una amenaza podría afectar la organización, su personal, sus activos, su reputación o sus programas.

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

Otras publicaciones de EISF

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

Documentos e informes

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

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

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 – *Sp. version 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

Edicion en inglés: Primera publicación septiembre 2015 / Actualizado marzo 2017
Edición en español: Primera publicación diciembre 2017