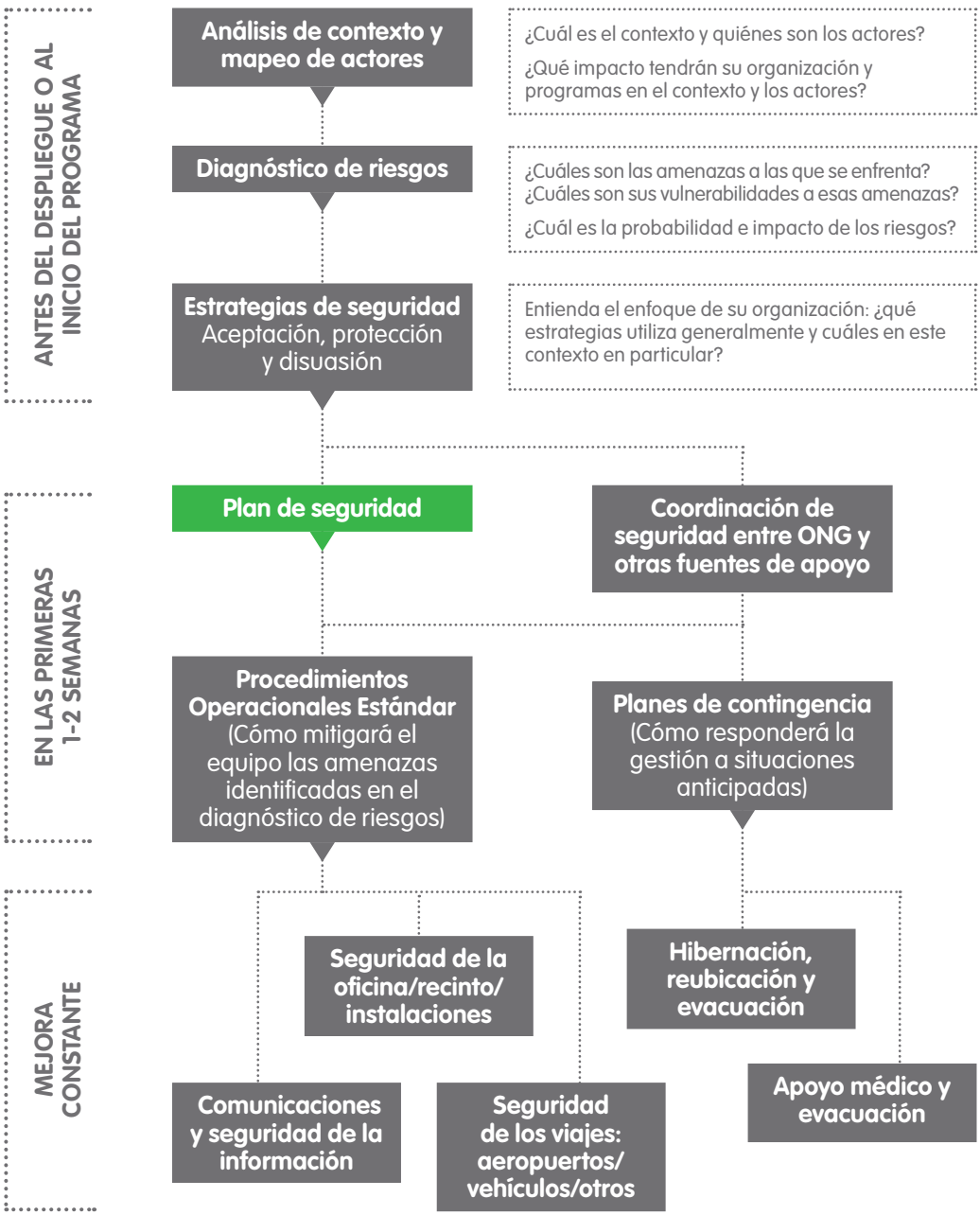
6 Plan de seguridad



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*.

Contenido

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