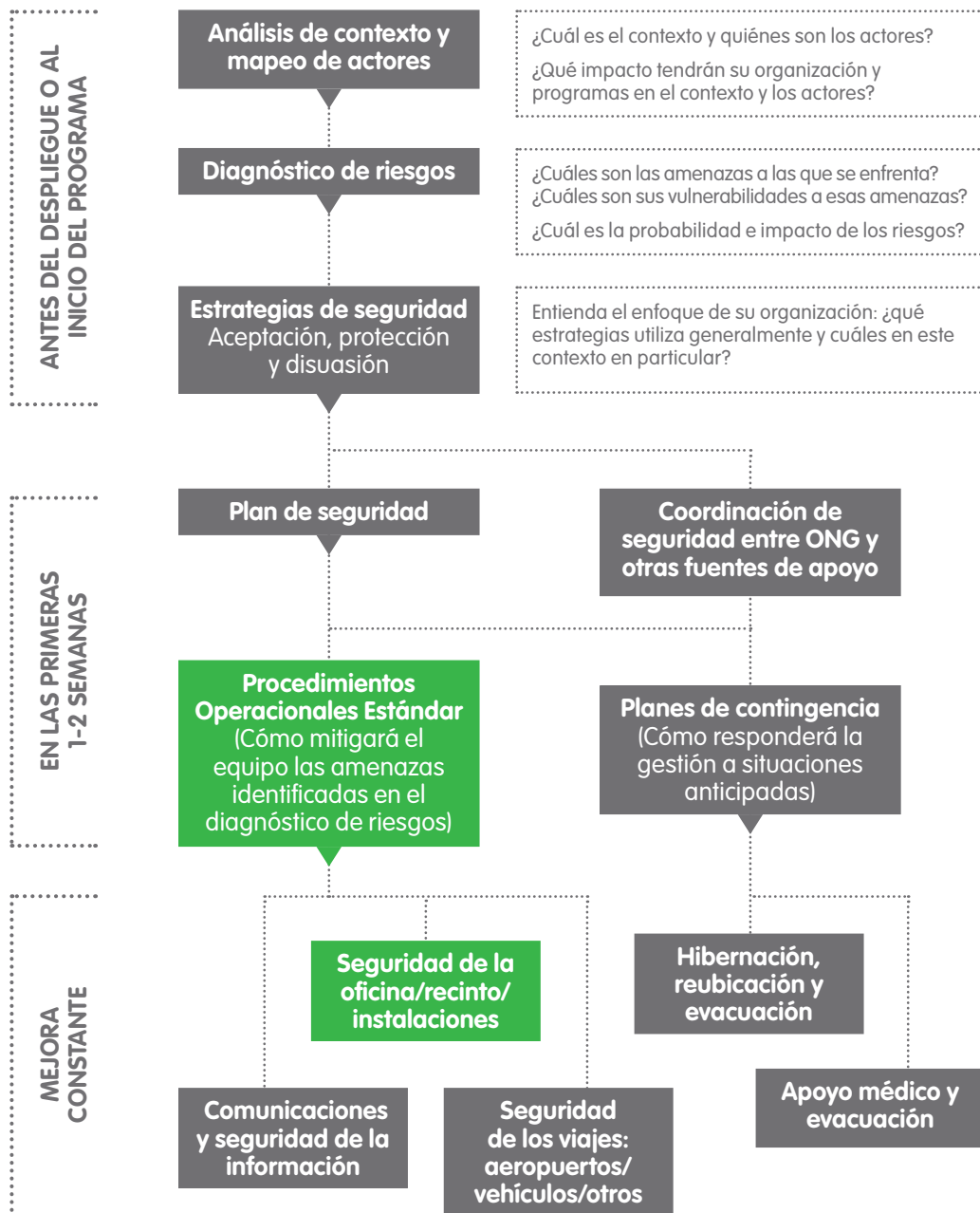


7

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.

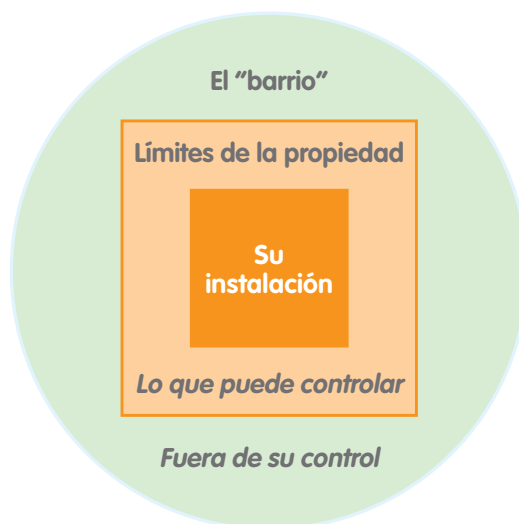


Esto es aplicable a todas las propiedades de la organización, oficinas, residencias, almacenes, clínicas, escuelas, etc.

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.

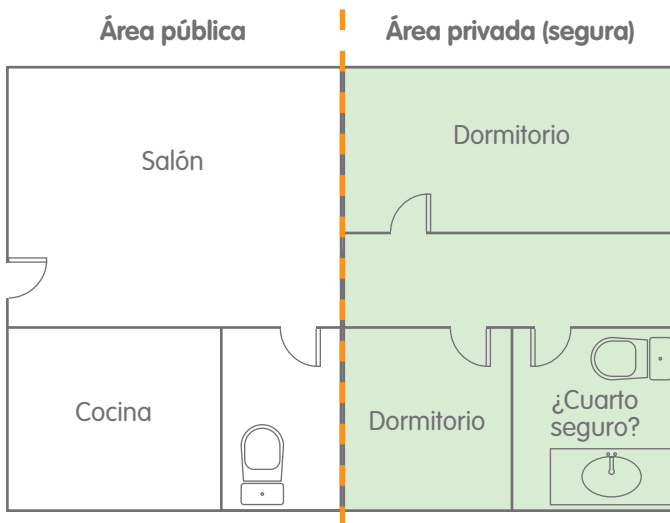
Para que el personal sea efectivo en su trabajo, es importante que se sientan seguros en sus oficinas y alojamientos. Considere:

- 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 una 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.



Contenido

Introducción	02
---------------------	-----------

Módulos	04
----------------	-----------

Planificación y preparación

Módulo 1	04
-----------------	-----------

Proceso de planificación de la gestión de riesgos de seguridad

Módulo 2	09
-----------------	-----------

Mapeo de actores y análisis de contexto

Módulo 3	14
-----------------	-----------

Herramienta de diagnóstico de riesgos

Módulo 4	22
-----------------	-----------

Estrategias de seguridad: aceptación, protección y disuasión

Módulo 5	26
-----------------	-----------

Coordinación de seguridad entre ONG y otras fuentes de apoyo

Módulo 6	30
-----------------	-----------

Plan de seguridad

Módulo 7	34
-----------------	-----------

Seguridad de las instalaciones

Módulo 8	42
-----------------	-----------

Comunicaciones y seguridad de la información

Módulo 9	48
-----------------	-----------

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

Respuesta

Módulo 10	55
------------------	-----------

Hibernación, reubicación y evacuación

Módulo 11	61
------------------	-----------

Apoyo médico y evacuación

Servicios de apoyo

Módulo 12	67
------------------	-----------

Gestión de personal

Glosario	85
-----------------	-----------

Otras publicaciones de EISF	86
------------------------------------	-----------

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 edición 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

EISF es una agrupación dirigida por sus miembros y no posee una identidad legal independiente bajo la Ley de Inglaterra y Gales o cualquier otra jurisdicción. Las referencias a "EISF" en este aviso legal incluirán a las organizaciones miembros, observadores y secretaría de EISF.

El contenido de este documento no pretende constituir un asesoramiento en el que debe confiar. Debe obtener asesoramiento profesional o especializado antes de tomar, o abstenerse de, cualquier acción tomada en base al contenido de este documento.

Aunque EISF trata de asegurar la veracidad de la información de este documento, no garantiza su exactitud ni su exhaustividad. La información de este documento es proporcionada 'tal cual' sin condiciones, garantías u otros términos, y la confianza depositada en la información contenida en el presente documento será responsabilidad total del lector. Por consiguiente, y hasta donde permita la ley, EISF excluye todas las representaciones, garantías, condiciones y otros términos que de no ser por este aviso legal podrían tener efecto en relación con la información del presente documento. EISF no será responsable de ningún tipo de pérdida o daño de cualquier tipo causado al lector o a una tercera parte derivado de la confianza depositada en la información de este documento.

© 2017 European Interagency Security Forum