eisf

EISF – Coordinación
T: +44 (0) 203 195 1360
M: +44 (0) 77 6099 2239
eisf-coordinator@eisf.eu

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

www.eisf.eu

Primera publicación
Septiembre 2013 (edición en inglés)

Humanitarian Policy

NRC NORWEGIAN REFUGEE COUNCIL

UNA GUÍA DE EISF PARA ORGANIZACIONES NO GUBERNAMENTALES

eisf

Auditorías de seguridad

CHRISTOPHER FINUCANE PARA EUROPEAN INTERAGENCY SECURITY FORUM

European Interagency Security Forum (EISF)

European Interagency Security Forum (EISF) es una plataforma independiente para referentes de seguridad de agencias humanitarias europeas que operan a nivel internacional. Los miembros de EISF tienen el compromiso de mejorar la seguridad de las operaciones de asistencia humanitaria y del personal implicado, para un mejor acceso e impacto en las poblaciones afectadas por situaciones de crisis.

Clave para el trabajo de EISF es el desarrollo de proyectos de investigación y herramientas que promueven el conocimiento, la preparación y las buenas prácticas en el ámbito de la ayuda humanitaria.

EISF es una entidad independiente financiada actualmente por la Oficina de EE.UU para la Ayuda a Desastres en el Exterior (US Office of Foreign Disaster Assistance, OFDA), la Agencia Suiza para el Desarrollo y la Cooperación (Swiss Agency for Development and Cooperation, SDC), el Departamento para el Desarrollo Internacional de Reino Unido (Department for International Development, UK aid) y las contribuciones de sus miembros.

www.eisf.eu

Agradecimientos

Mucha gente ha contribuido al desarrollo de este texto. Los antecedentes comenzaron en 2009 cuando **Maarten Merkelbach**, (Geneva Center for Security Policy) y **Christopher Finucane** (Humanitarian Policy) llevaron a cabo una investigación de los sistemas de seguridad de organizaciones internacionales de ayuda humanitaria, con el objetivo de comprender mejor cómo las ONG estaban respondiendo a los retos crecientes en materia de seguridad. La investigación continuó con el apoyo del Centro de Refugiados y Respuesta al Desastre de la Escuela de Salud Pública John Hopkins Bloomberg (Center for Refugee and Disaster Response at John Hopkins Bloomberg School of Public Health), donde la metodología fue depurada con la dirección del profesor Gilbert Burnham. Es esta metodología de investigación la que conforma la base de esta exhaustiva guía y herramientas.

Esta guía ha sido escrita por **Christopher Finucane** y editada por **Ellie French** en representación de la Secretaría de EISF. La traducción al castellano ha sido realizada por **Javier Martínez Llorca**, de Médicos Sin Fronteras-España, y editada por **Raquel Vázquez Llorente** en representación de la **Secretaría de EISF**.

Esta publicación no habría sido posible sin la participación de trabajadores humanitarios de todo el mundo, en especial de Save the Children, Medair, ZOA, Oxfam y War Child.

Este proyecto ha sido posible con el apoyo financiero de los donantes de EISF y del Consejo Noruego para el Refugiado (Norwegian Refugee Council).

Contenido

Introducción

¿Qué es una auditoría de sistemas de gestión de seguridad?

La gestión de seguridad en las ONG es más efectiva cuando se lleva a cabo de una manera sistemática. Los procesos se deben aplicar en un orden lógico para alcanzar las condiciones y resultados deseados. Para muchas ONG, el propósito primordial de los sistemas de gestión de seguridad es generar unas condiciones que permitan el desarrollo de la misión de ayuda humanitaria dentro de una tolerancia al riesgo que sea aceptable en un contexto operativo dado.

Una auditoría de sistemas de gestión de seguridad (SGS) consiste en una revisión basada en pruebas de la estructura y funciones de un sistema, y en un test sobre el objetivo del mismo. La auditoría proporciona información esencial a los gestores y a su personal a partir de la cual se identifican las fortalezas y debilidades del sistema, permitiendo que los recursos se apliquen ahí donde sean más necesarios. El proceso de auditoría también sirve como herramienta para que las ONG puedan evaluar sus procesos internos de gestión y determinar si el sistema de gestión de seguridad es el adecuado para el objetivo.

¿Por qué una auditoría de sistemas de gestión de la seguridad?

Las organizaciones de ayuda humanitaria auditarán sus sistemas de gestión de seguridad por dos razones fundamentales:

a. Como empleadores, las ONG tienen la obligación moral hacia sus empleados de asegurar que éstos no están en una situación de peligro como consecuencia de su trabajo; y

b. En muchos contextos las ONG están obligadas por ley a ejercer un deber de cuidado hacia los empleados, requiriéndose sistemas y procesos claramente definidos para gestionar los riesgos en el lugar de trabajo[1].

Comprender la estructura de un SGS es esencial para determinar la efectividad del sistema. ¿En qué consiste el sistema? ¿Cómo se puede comunicar el sistema a aquellos responsables de su puesta en marcha?

Esta guía proporciona primero el proceso para contestar a estas dos preguntas clave, y presenta después las herramientas para llevar a cabo una evaluación sobre el diseño del sistema y su eficacia. Determinar la efectividad del sistema es más subjetivo que evaluar su diseño y estructura. En otras palabras, puede resultar más fácil describir el aspecto de algo que ver cómo funciona.

¿Para quién es esta guía?

La guía y las herramientas están destinadas tanto a profesionales de la ayuda humanitaria como a personal directivo. Juntas, ofrecen un método estándar de auditoría acompañado de exhaustivas orientaciones e información de apoyo. Las herramientas son flexibles, por lo que pueden ser aplicadas al conjunto del sistema organizativo o modificarse para abordar las necesidades de una oficina en el terreno.

¿Necesito formación para auditar un sistema de gestión de seguridad?

Siguiendo las orientaciones de esta guía, los trabajadores humanitarios que conocen las estrategias de su organización en relación a la gestión de programas deberían de ser capaces de aplicar las herramientas y auditar el SGS. Esta guía no está concebida para su uso exclusivo por referentes o gestores de seguridad. Mientras que personal en estos puestos puede poseer un mayor conocimiento de los matices que tiene la gestión de seguridad en una organización, empleados con poca o ninguna formación en seguridad podrán analizar el sistema siguiendo las orientaciones y el método de auditoría aquí explicados.

Si las ONG contemplaran llevar a cabo formación interna en el uso de las herramientas que esta guía contiene, los objetivos clave del aprendizaje serían:

- Comprender los conceptos, lógica y procesos que respaldan el sistema de gestión de seguridad antes de intentar analizar el sistema;
- Comprender que los sistemas de gestión de seguridad no son estructuras aisladas, y que a menudo van a estar vinculadas con otros sistemas de gestión dentro de la organización; y
- Comprender que el riesgo es un concepto a menudo subjetivo, dándose, por tanto, actitudes y comportamientos muy diferentes que podrían influir en cómo el sistema se comunica y/o se aplica.

Tomarse el tiempo necesario para leer estas orientaciones antes de emprender una auditoría reducirá considerablemente la necesidad de formación, y mejorará la calidad de los resultados de dicha auditoría.

Cómo usar la guía y las herramientas

Esta guía proporciona información de referencia de utilidad y pone las herramientas en contexto. Las herramientas están divididas en tres partes fundamentales, siguiendo un proceso lógico:

- La Sección A explica la planificación y preparación de la auditoría del sistema;
- La Sección B se ocupa de la realización de la auditoría; y
- La Sección C presenta cómo analizar los resultados y determinar qué aspectos podrían ser mejorados.

Esta guía, aunque genérica, conforma una metodología de auditoría estándar que puede servir de referencia. Las ONG pueden considerar la adaptación de partes del proceso de auditoría para reflejar mejor la estructura de gestión de su organización.

Los conceptos clave y las definiciones están enunciados en el glosario.

Muchas definiciones están adaptadas según la ISO 31000:2009 *Gestión del Riesgo. Principios y Directrices* y la Guía ISO 73 *Vocabulario de Gestión de Riesgos* [2].

A lo largo del texto:

- Los puntos fundamentales están indicados con
- Referencias a otras partes de la guía están indicadas con
- Referencias a publicaciones de EISF, disponibles en www.eisf.eu están indicadas con
- Se facilitan hipervínculos para una navegación sencilla.

Al final de esta guía hay un número de herramientas prácticas. Están referenciadas cuando sea pertinente con el icono de herramienta mostrado abajo:

- Herramienta 1: Sistema de referencia
- Herramienta 2: Plantilla para el registro de documentos
- Herramienta 3: Lista de comprobación para la revisión documentos
- Herramienta 4: Desarrollo de preguntas para las entrevistas
- Herramienta 5: Ejemplo de preguntas para la encuesta *online*
- Herramienta 6: Plantilla para la auditoría del SGS

Las herramientas también están disponibles en formato que puede editarse en www.eisf.eu Las herramientas han de modificarse de acuerdo a cada organización y contexto.

El proceso de auditoría de sistemas de gestión de seguridad

A Planificación y preparación de una auditoría

i. Comprender el proceso de auditoría

Antes de que la auditoría tenga lugar es importante acordar una acepción común de lo que constituye un sistema. Un «sistema» se puede definir como «un conjunto de principios o procedimientos de acuerdo a los cuales se hace algo; o un esquema o método organizado»[3].

En el contexto de la seguridad de las ONG, parte de ese sistema es el marco de referencia de gestión de riesgos de seguridad (SMF, por sus siglas en inglés)[4], que ha conformado una parte central de la estrategia de gestión de riesgos del sector de la ayuda humanitaria. En sí mismo, el SMF no es un sistema integral, sino más bien un subsistema de un conjunto más amplio de principios y procedimientos que las ONG necesitan tomar en consideración al diseñar e implementar sistemas de gestión de seguridad adaptados a sus necesidades.

ii. Establecer un calendario

Es igualmente importante reconocer que llevar a cabo una auditoría del SGS requiere una asignación apropiada de tiempo y esfuerzo. Por lo general no se da el caso de que una auditoría pueda realizarse en un día. En especial, éste es el caso de auditorías institucionales que analizan toda la organización, para las que se recomienda una asignación de tiempo de hasta dos semanas (excluyendo el tiempo dedicado a la formación).

Herramienta 1
Sistema de referencia

Oficinas más pequeñas a nivel nacional podrían precisar menos tiempo si se pretende auditar sus SGS locales sin tomar en cuenta estructuras más amplias del SGS. El tiempo real para llevar a cabo una auditoría variará, y estará determinada sobretodo por la disponibilidad del personal clave y el consiguiente acceso a información primordial.

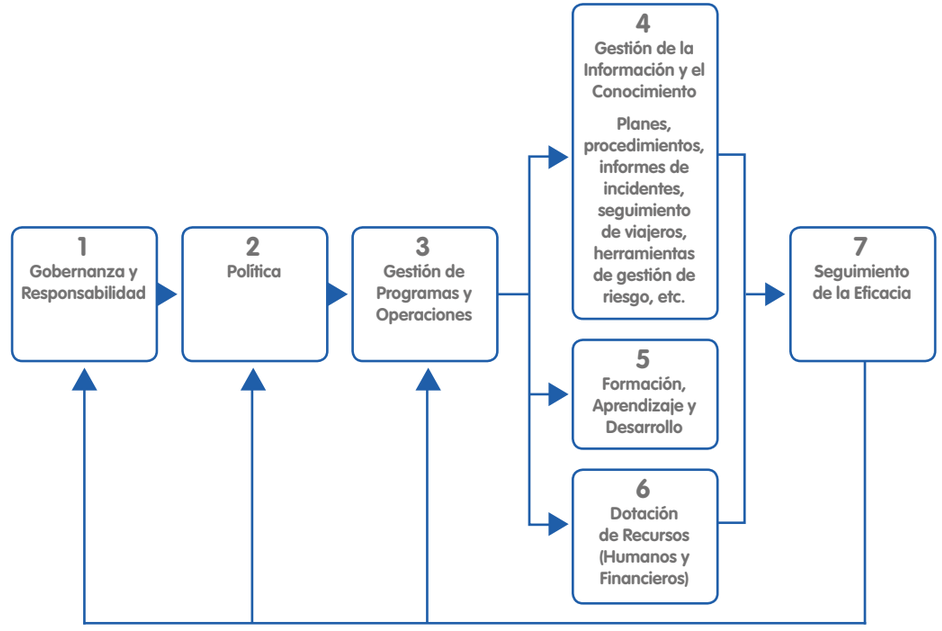
iii. Mapear un sistema de referencia

El primer paso en el proceso de realizar una auditoría es leer esta guía y a continuación fijar un sistema de referencia. Esto conlleva mapear el sistema de base de la manera en que éste se entienda. Un simple diagrama de bloques es una forma útil de generar la referencia.

Esta base de referencia se utilizará a través de la auditoría para planificar, guiar y analizar los resultados.

En la figura 1 se presenta un sistema de referencia genérico como ejemplo. La referencia ilustra siete partes clave, ordenadas lógicamente, consideradas esenciales para el SGS de una ONG. La primera parte da comienzo al sistema, ofreciendo el primer conjunto de resultados que conducen a las partes subsiguientes. Cada parte contribuye a la siguiente. Los indicadores específicos se aplican entonces a las partes del sistema para así llevar a cabo una auditoría basada en pruebas. Esta estrategia permite al examinador escudriñar cada parte del SGS.

Figura 1 **Mapa del sistema de referencia**



Las organizaciones de ayuda humanitaria varían en casi todas las formas concebibles: tamaño presupuestario, plantilla, alcance geográfico, estrategias de programación, etc. Estas diferencias son el resultado de los principios, valores y misión de una organización, y están constantemente moldeados por sus trabajadores. Como resultado de estas variables, y para reflejar las características individuales y los matices operativos de las organizaciones, los sistemas de gestión de seguridad también variarán.

La figura 1 de arriba muestra las siete partes del sistema de gestión de seguridad. Éstas son:

1. Gobernanza y Responsabilidad
2. Política
3. Gestión de Programas y Operaciones
4. Gestión de la Información y el Conocimiento
5. Formación, Aprendizaje y Desarrollo
6. Dotación de Recursos
7. Seguimiento de la Eficacia

El diagrama muestra que la gestión de seguridad es sistemática y lógica. Las estructuras de gobernanza (parte 1) configuran las directrices generales y la tolerancia al riesgo explícita de una organización. Ello guía y moldea las políticas de gestión del riesgo de la organización (parte 2), que a su vez son implementadas a través de la gestión de programas y operaciones (parte 3).

La información y la gestión del conocimiento abarca los procesos de evaluación del riesgo (y aquí es donde tradicionalmente encaja el subsistema marco de referencia gestión de seguridad, SMF) (parte 4). El sistema debe incluir mecanismos para abordar la capacidad y competencia de la plantilla para gestionar riesgos, la cual se adquiere a través de una estrategia de formación, aprendizaje y desarrollo (parte 5).

La dotación de recursos (parte 6) es la parte del sistema donde se fijan y proveen los recursos humanos y financieros. El sistema concluye con una evaluación continua (parte 7) que proporciona la retroalimentación que permite que las cuestiones de política y gobernanza sean adaptadas en respuesta a la evolución de los acontecimientos.

Cada parte del sistema es considerado esencial para el sistema de gestión de seguridad de una organización de ayuda humanitaria, así como el orden de los procesos. Las particularidades dentro de cada proceso serán específicas a la organización y al contexto en el que opera.

El proceso de auditoría debe pasar por el sistema en el mismo orden que la referencia genérica, empezando por la parte 1 y finalizando en la parte 7. A lo largo de esta guía, las referencias a partes del sistema permanecen constantes y se aplica un índice simple para relacionar cada parte del sistema con sus indicadores específicos. Por ejemplo, los indicadores de la parte 1 (Gobernanza y Responsabilidad) están numerados 1.1, 1.2, 1.3 y 1.4. Los indicadores de la parte 2 están numerados 2.1, 2.2, 2.3, 2.4, y así sucesivamente. Esto se muestra con mayor detalle más adelante en la guía.

iv. Propiedad del riesgo

Para algunas partes del SGS la guía facilita dos conjuntos genéricos de indicadores. El primer conjunto se aplica al sistema de gestión de seguridad de la organización (marcado en texto **azul**), y el segundo a una oficina de país o en el terreno (marcado en texto **púrpura**). Las diferencias entre los dos reflejan el nivel de propiedad del riesgo, que es la característica clave que distingue entre la gestión de una oficina central y de una oficina en el terreno.

La «propiedad del riesgo» se define como «la persona o entidad con la responsabilidad y la autoridad para gestionar un riesgo»[5]. Con esta definición en mente, auditar un SGS a nivel institucional permitirá deducir los propietarios del riesgo a nivel de consejo y ejecutivo. A nivel de terreno, los propietarios del riesgo serán los directores regionales y de país, y sus designados delegados.

Los principales propietarios del riesgo serán a menudo miembros del consejo de administración, junta, u otros órganos de supervisión, junto con el órgano ejecutivo de la organización. Éstas son las personas responsables de establecer los sistemas necesarios para impedir que las cosas vayan mal, y son las personas que en última instancia serán responsables si las cosas van mal. El nivel de responsabilidad se delega habitualmente hacia abajo por la línea de gestión, a través de los departamentos de oficinas centrales hacia los gestores en el terreno y el personal.

Un SGS primera y principalmente refleja la actitud[6] y la tolerancia[7] al riesgo de una organización. Su objetivo es la protección de los trabajadores y de la reputación de la organización ante posibles daños por medio de la identificación y gestión de riesgos previsibles.

El análisis del sistema, por consiguiente, pretende mapear y evaluar el sistema en primera instancia a nivel de oficina central o nivel institucional. Cuando un sistema se redimensiona a nivel regional, de país, o de terreno, debe seguir reflejando aquel de la organización como conjunto. Las particularidades del contexto local influirán en cómo se aplica el sistema, pero deberían tener sólo un efecto menor en la estructura del sistema.

v. Identificar indicadores para cada parte del sistema de gestión de seguridad

Para guiar una evaluación de la estructura del sistema, los indicadores se aplican a cada parte del sistema. Los indicadores se comprueban en base a las pruebas disponibles y se evalúan como:

- Presentes dentro del sistema;
- Parcialmente presentes, cuando algunos indicadores se pueden encontrar durante la auditoría, pero no con la suficiente claridad para decir con certeza que la condición se ha cumplido; o
- No presentes, cuando no se puede atribuir ninguna prueba formal a los indicadores.

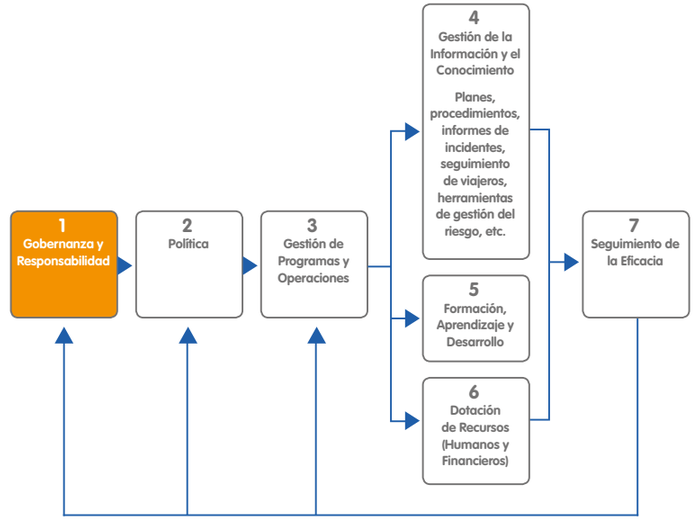
En otras palabras, los indicadores describen aquello que se está buscando entre las pruebas disponibles y/o el conocimiento institucional acerca del SGS.

Esta guía presenta cuatro indicadores genéricos para cada parte del sistema del modelo de referencia. Estos indicadores se han desarrollado a lo largo de años pasados y han sido utilizados con éxito para auditar el SGS de varias ONG internacionales. Los indicadores se adaptan a los diferentes niveles de gestión simplemente ajustando el nivel de la propiedad del riesgo.

Como punto de partida, esta guía recomienda usar los indicadores genéricos antes de crear indicadores específicos para la organización. Naturalmente, algunas matizaciones pueden ser necesarias para adaptar los indicadores genéricos a la organización, pero probablemente estos cambios serán mínimos.

Indicadores para la parte 1: gobernanza y responsabilidad

«Gobernanza y responsabilidad» se define como un proceso de supervisión y rendición de cuentas en el desempeño de la gestión de riesgos de seguridad. Los responsables principales en materia de seguridad establecerán y comunicarán la estructura de gobernanza.



Herramienta 6

Plantilla para las auditoría del SGS

Indicadores:

1.1	Una declaración de responsabilidad y gobernanza en referencia a la gestión de riesgos de seguridad y a la actitud de la organización hacia el riesgo y sus límites es comunicada por el Consejo de Administración[8] / Director de País.
1.2	El Consejo de Administración / Director de País asigna responsabilidades específicas en materia de seguridad y gestión de riesgos a una o más partes funcionales de la organización / oficina de país.
1.3	A alguien dentro del Consejo de Administración / Director de País se le asigna de forma explícita la responsabilidad sobre la supervisión de la gobernanza de los riesgos para la seguridad de la organización / oficina de país.
1.4	Existe un proceso informativo y de rendición de cuentas (con frecuencia y contenido definidos) para informar al Consejo de Administración / Director de País sobre asuntos relacionados con los riesgos de seguridad y el desempeño de la organización / oficina de país.

Ver sección iv: propiedad del riesgo

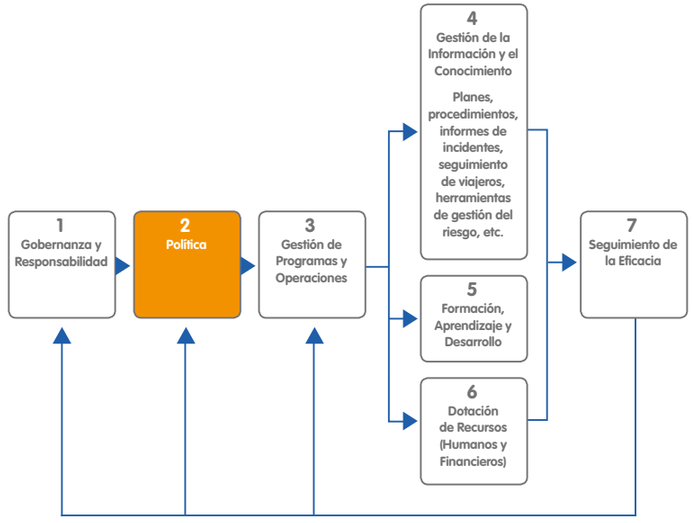
Indicadores para la parte 2: política

Mientras que todas las partes del sistema son esenciales para que éste funcione, la política de la organización es particularmente importante. En el contexto del SGS, «política» se define como la comunicación de la posición que la ONG ha decidido asumir en la gestión de seguridad, así como de sus principios rectores. Ello debería incluir la articulación del papel que juegan los miembros del consejo y los ejecutivos, así como de sus decisiones, y la delegación de responsabilidades en la gestión.

Algunas ONG eligen tener políticas a nivel institucional o de oficina central. Otras ONG con estructuras de gestión más descentralizadas hacen hincapié en políticas a nivel de terreno (por ejemplo, oficinas de país o regionales). Esta guía y la metodología para la auditoría se pueden utilizar para cualquier estructura de gestión ajustando los indicadores de política, con objeto de reflejar cómo la organización establece y comunica su política de seguridad.

Herramienta 6

Plantilla para las auditoría del SGS



Indicadores:

2.1	Las políticas articulan e implementan la posición y decisiones del Consejo de Administración / Director de País en relación a la gestión de riesgos de seguridad, incluyendo las actitudes y límites de la organización respecto al riesgo[9].
2.2	La implementación de las políticas (a través de planes, procedimientos y/o directrices) es apropiada para el contexto local.
2.3	Las políticas especifican las responsabilidades y obligaciones de los empleados en relación a la seguridad, y las comunican a todas las partes relevantes de la organización.
2.4	Los documentos que detallan la política de la organización están a disposición de los empleados en todos los idiomas al uso.

Ver sección iv: propiedad del riesgo

Política versus procedimiento

Es un error común incluir procedimientos detallados en documentos que explican la política de la organización. Aunque estrechamente vinculados, las cuestiones de política organizacional no son lo mismo que los asuntos de procedimiento, y éstos han de ser comunicados a los trabajadores en conformidad. Política es la posición que se toma respecto a cierto asunto. Procedimiento, es cómo se lleva a cabo esa política, teniendo en cuenta las influencias del contexto. En otras palabras, las políticas explican las responsabilidades y obligaciones clave, mientras que los procedimientos muestran los procesos utilizados para implementar esas políticas.

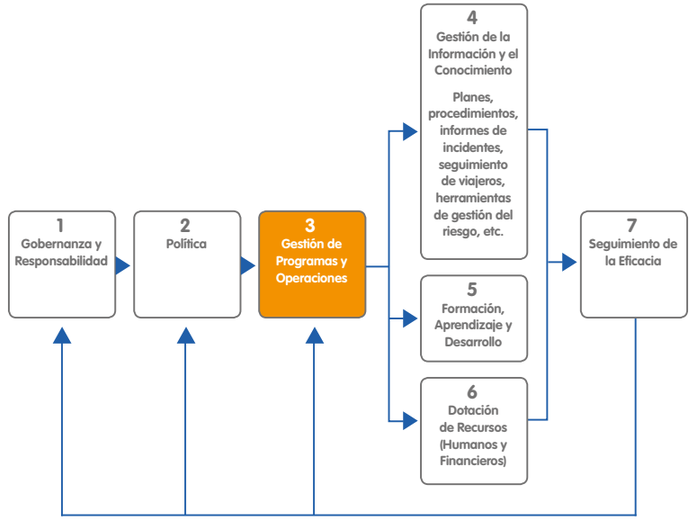
Un ejemplo de esta diferencia sería una ONG que tenga la política de que todas las actividades de programa incluyan en su planificación una evaluación del riesgo de seguridad. Esta política sería relevante para todos los programas en todos los países. Cómo se llevan a cabo estas evaluaciones del riesgo es un asunto procedimental que puede diferir entre países. En un país de bajo riesgo la evaluación del riesgo se podría llevar a cabo por el gestor del programa y revisado anualmente. En un país con riesgo más elevado se podría llevar a cabo por especialistas en la gestión de seguridad, y revisado trimestralmente. En ambos casos, la política permanece inalterada al ser aplicada.

Herramienta 6

Plantilla para las auditoría del SGS

Indicadores para la parte 3: gestión de programas y operaciones

Esta parte del sistema pretende integrar la gestión de seguridad. Es el proceso de introducir la gestión de seguridad dentro de procedimientos operativos y dentro de ciclos de la gestión de programas.

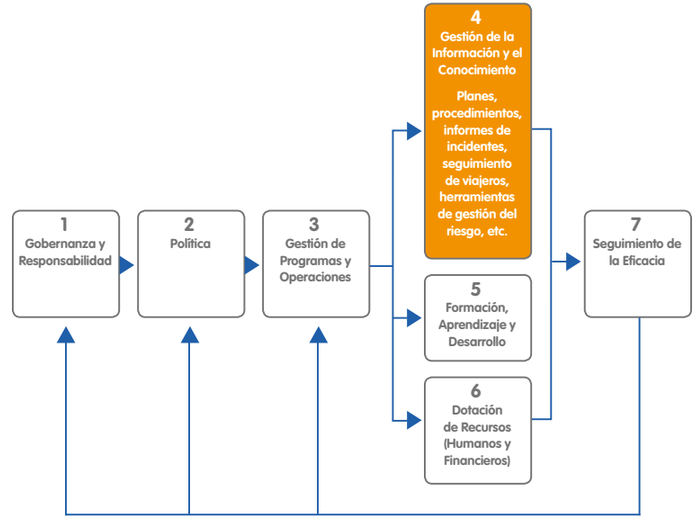


Indicadores:

3.1	La autoridad responsable de la toma de decisiones en cuestiones de seguridad (esto es, la propiedad del riesgo) está claramente documentada en contratos de empleo, descripciones de puestos de trabajo y valoraciones del desempeño del personal.
3.2	La gestión de seguridad es promovida de forma activa a través de la organización por empleados con cargos de gestión, y es demostrable mediante comunicaciones y pruebas documentales, talleres de trabajo y/o otras iniciativas internas.
3.3	Se articulan estrategias o enfoques específicos para el contexto y se comunican a todas las partes relevantes de la organización.
3.4	Los procesos de rendición de cuentas y cumplimiento son documentados, incluyendo procesos explícitos para gestionar incumplimientos de la política de gestión de seguridad de la organización, y de planes y procesos de seguridad.

Indicadores para la parte 4: gestión de la información y el conocimiento

La gestión de la información y el conocimiento es donde normalmente se encuadran los enfoques tradicionales de gestión de seguridad, tales como la aplicación de marcos de gestión de riesgos de seguridad[10]. Esta parte del sistema se describe como un cuerpo de conocimiento institucional (desarrollado por la organización) para registrar y comunicar la implementación de políticas. Esto incluirá herramientas para la seguridad (p. ej. herramientas de evaluación del riesgo), planes y procedimientos adaptados al contexto, y mecanismos de informe de incidentes. Es aquí donde también la aceptación y otras estrategias de seguridad son generalmente descritas.



Herramienta 6

Plantilla para las auditoría del SGS

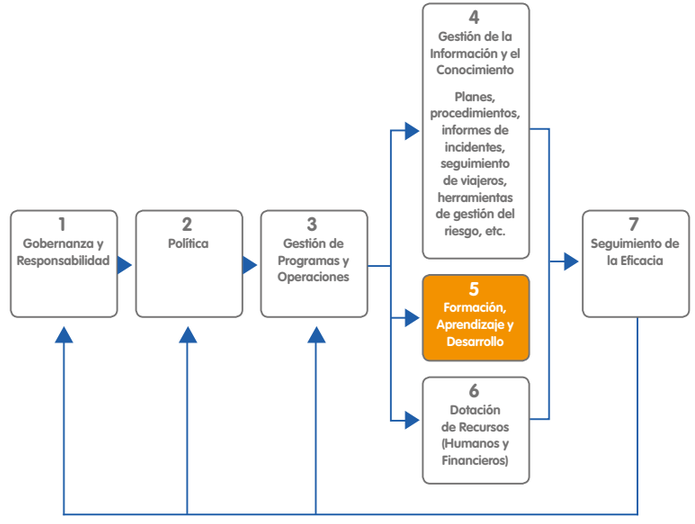
Indicadores:

4.1	Tanto sistemas de gestión de información de seguridad como herramientas para informar sobre incidentes están en funcionamiento y disponibles para todos los empleados.
4.2	La organización participa activamente en foros o consorcios sobre gestión de seguridad y comparte información con otros.
4.3	Se documentan los planes y procedimientos de seguridad adaptados a contextos específicos, y éstos reflejan la política de la organización.
4.4	Los planes y procedimientos de seguridad exponen abiertamente las responsabilidades y obligaciones tanto individuales como de la organización.

Indicadores para la parte 5: formación, aprendizaje y desarrollo

Las organizaciones de ayuda humanitaria reconocen a menudo que su activo más importante son sus trabajadores. Construir una plantilla competente requiere una política de contratación meticulosa, así como la puesta en marcha de estrategias de fomento de capacidad para la mejora de las habilidades y conocimientos que se requieren para cumplir con los objetivos del programa.

Dentro de un SGS deben ser identificables procesos explícitos para la formación, aprendizaje y desarrollo. Esta parte del sistema se define como una estrategia documentada que identifica las necesidades que los trabajadores tienen de formación, aprendizaje y desarrollo, y los recursos que se requieren para asegurar que esas necesidades puedan ser cubiertas. Esta parte del sistema es un indicador importante de la estrategia de una ONG a la hora de ejercer su deber de cuidado, y demuestra un compromiso por parte del empleador en desarrollar una fuerza de trabajo[11] capaz de gestionar riesgos de seguridad. Las estrategias de formación en gestión de seguridad son difíciles de poner en práctica debido a que estas estrategias han de tener en cuenta recursos financieros limitados, ser capaces de alcanzar una fuerza de trabajo dispersa, y hacer frente a cambios de personal.



Herramienta 6

Plantilla para las auditoría del SGS

Indicadores:

5.1	Los estándares de desempeño se determinan y comunican a través de la organización.
5.2	Todos los empleados tienen acceso a una estrategia (y/o plan) documentada de formación, aprendizaje y desarrollo.
5.3	Existe un compromiso manifiesto de la dirección que asegura que todos los empleados tengan acceso a oportunidades de formación, aprendizaje y desarrollo en temas de seguridad.
5.4	Autoridades acreditadas reconocen los cursos de formación (si es factible).

Estándares de desempeño

Las estrategias también necesitan tener la capacidad de alcanzar estándares de desempeño predefinidos. Estandarizar el desempeño es una herramienta de gestión útil que facilita resultados cuantificables, especialmente si se combinan con objetivos SMART (Haughey, 2000).

La estandarización SMART (por sus siglas en inglés) significa que los objetivos de desempeño son específicos (S), mensurables (M), alcanzables (A), realistas (R) y oportunos (T)[12]. Por ejemplo, una organización podría decidir que uno de cada cinco trabajadores en el terreno reciba entrenamiento en primeros auxilios, dentro de un tiempo definido, y por un tiempo determinado.

Otro ejemplo sería el estándar de que uno de cada dos miembros del personal que trabaja en contextos de alto riesgo complete formación especializada, como por ejemplo programas de concienciación en entornos hostiles (comúnmente referido como entrenamiento HEAT, por sus siglas en inglés), de nuevo definido bajo criterios SMART.

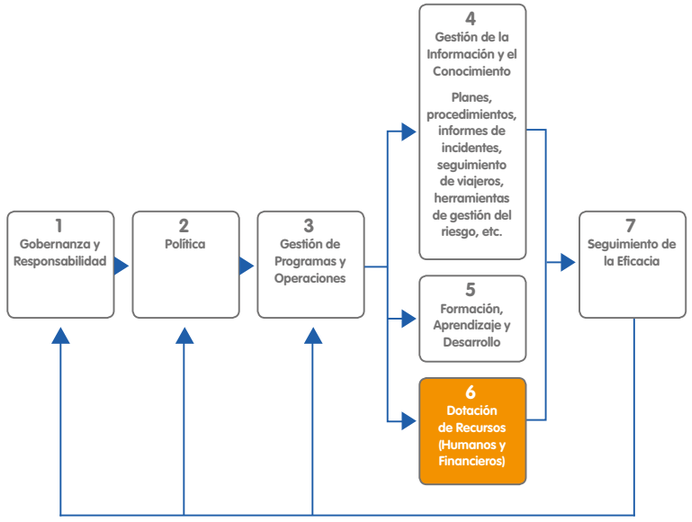
Indicadores para la parte 6: dotación de recursos

Esta parte del SGS garantiza que los recursos para la gestión de seguridad sean incluidos en las propuestas de programa, documentos de planificación y presupuestos.

Un sistema no puede funcionar sin recursos adecuados y prioritarios.

Herramienta 6

Plantilla para las auditoría del SGS



Indicadores:

6.1	Existen líneas presupuestarias específicas para requisitos de seguridad en todos los presupuestos de programas.
6.2	Las solicitudes de subvenciones incluyen líneas presupuestarias específicas para cubrir futuros costes de seguridad y detallan el cálculo de esos costes.
6.3	Las cantidades presupuestadas son consideradas suficientes para afrontar todas las necesidades de recursos, con procesos claros y lógicos para estimar dichos montos.
6.4	Hay pólizas de seguros vigentes (médicos, de viaje, de crisis, etc.) y la cantidad cubierta se considera adecuada para afrontar los potenciales costes por riesgos.

Herramienta de Cartera de Gastos de Gestión de Riesgos (RMEP)

La puesta en práctica de acciones de gestión de riesgos requerirá la contratación y provisión de seguros, equipamiento, formación y servicios de especialistas. Todos ellos han de comunicarse de forma explícita a los donantes y acompañarse de una justificación de gastos convincente. La Cartera de Gastos de Gestión de Riesgos (RMEP, por sus siglas en inglés) es una herramienta útil para asegurar que esta parte del sistema de gestión de seguridad esté presente y funcione.

Informe de EISF: El Coste de Gestión de Riesgos de Seguridad para las ONG (The Cost of Security Risk Management for NGOs)

Herramienta de EISF: La Cartera de Gastos de Gestión de Riesgos (The Risk Management Expense Portfolio)

A. Planificación y preparación

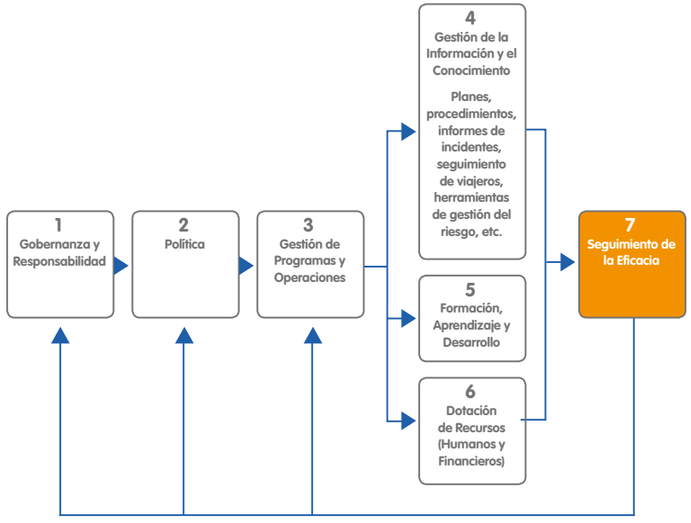
Indicadores para la parte 7: seguimiento de la eficacia

Esta última parte del sistema se describe como un proceso documentado de seguimiento y evaluación que incluye indicadores de desempeño de la gestión; análisis de la respuesta a incidentes, así como registro de lecciones aprendidas; revisión frecuente de políticas y procedimientos; y claras responsabilidades de presentación de informes para la evaluación de la implementación de sistemas de gestión de seguridad.

El sistema de referencia que se presenta en esta guía no es un sistema cíclico. Está diseñado para permitir que los propietarios del riesgo puedan mostrar la lógica del proceso que se da desde la fase de gobernanza hasta la de implementación de programas. El seguimiento del sistema facilita un medio de comprobación interno, abriendo paso a ajustes en los mecanismos de gobierno en respuesta a cambios organizativos o de contexto en el entorno de trabajo.

Herramienta 6

Plantilla para las auditoría del SGS



Indicadores:

7.1	Los sistemas de gestión del desempeño de empleados hacen referencia explícita a las responsabilidades en materia de seguridad, y también al cumplimiento con las políticas de la organización.
7.2	Las personas responsables de llevar a cabo el seguimiento de la implementación y cumplimiento de los sistemas de seguridad tienen esas responsabilidades explícitamente definidas en la descripción de sus puestos de trabajo.
7.3	Los resultados de las lecciones aprendidas, revisiones, análisis de incidentes a posteriori, y auditorías se usan activamente para mejorar el sistema de gestión de seguridad y/o sus subsistemas y procesos.
7.4	La dirección demuestra que los procesos de rendición de cuentas se aplican en caso de incumplimiento.

Este tipo de pruebas pueden ser más subjetivas o anecdóticas[13], y por lo tanto más difíciles de identificar durante una auditoría, pero es igualmente importante examinarlas y documentarlas.

Los usuarios de esta guía pueden considerar cambiar los indicadores aquí propuestos para adaptarlos a las necesidades de su organización. Cuando esto ocurra, se recomienda que el mismo grupo de indicadores se aplique a lo largo de la organización para así permitir una estrategia consistente y un medio válido de comparación entre los sistemas de diferentes programas de país.

Los indicadores deben centrarse en asuntos clave. Por ello, esta guía sólo utiliza cuatro indicadores para cada parte del sistema, con objeto de reflejar los asuntos más importantes que han de examinarse durante una auditoría del sistema.

vi. Preparar la recolección de datos

La preparación de la recogida de datos conllevará:

- Solicitar información a la organización para la revisión de documentos;
- Invitar a personas a participar en entrevistas y/o discusiones de grupo; y
- Desarrollar y publicar una encuesta *online* dirigida al personal en general.

Herramienta 1
Sistema de referencia

La herramienta 1 facilita una referencia de lo que la auditoría está realmente buscando–el diseño y la estructura del sistema. Una vez que el usuario tenga una idea del sistema básico, es tiempo de recoger tanta información como esté disponible con vistas a analizarla durante la auditoría. La primera (pero no la única) fuente de información serán los archivos y comunicaciones de la organización. La información también podrá ser provista por el personal de la organización, y se podrá obtener mediante entrevistas con informantes clave, grupos de discusión y/o encuestas *online*.

¿Qué constituye una prueba?

Los indicadores se diseñan para poder ser evaluados en función de las pruebas, que pueden ser tangibles, anecdóticas o una combinación de ambas. Existen diferentes tipos de pruebas. El término «prueba» se define como «el cuerpo disponible de hechos o información que indican si una creencia o proposición es verdadera o válida; o signos o indicaciones de algo»[14].

En el contexto de las auditorías de SGS, las pruebas fácticas equivalen a los archivos y comunicaciones publicados por la ONG, así como a las normas culturales establecidas dentro de los procesos de gestión; cosas que pueden ser identificadas con claridad y consistencia.

Herramienta 2
Plantilla para el registro de documentos

Sin embargo, también es fundamental explorar el verdadero comportamiento del personal dentro de la organización. Un proceso o comportamiento puede existir y funcionar como parte del SGS sin ser documentado. A través de entrevistas y de grupos de discusión es posible examinar cómo funciona realmente la organización en relación a cuestiones de seguridad, recogiendo así pruebas que de otro modo no estarían disponibles para el análisis.

vii. Preparar la revisión de documentos

Herramienta 3
Lista de comprobación para la revisión documentos

Las fuentes de prueba documentada son a menudo de carácter transversal y proveen información para más de una parte del SGS. Hay que tener en consideración que la cantidad de documentos puede ser enorme, especialmente en ONG grandes y consolidadas. Un registro documental es una herramienta útil para mantener un seguimiento de lo que ha sido solicitado, recibido y revisado. El registro también puede ayudar al contrastar las pruebas en relación a los indicadores del sistema.

viii. Participación de los empleados

Al preparar y planificar una auditoría es crucial contar con la participación de los empleados clave. La plantilla de una organización es a menudo su activo más valioso, y este cuerpo de conocimiento colectivo será esencial al examinar un SGS.

Es muy importante garantizar la participación de los empleados más experimentados, en especial si son propietarios del riesgo. Los directores ejecutivos y otros altos cargos son críticos para el proceso de auditoría. En algunos entornos puede ser un desafío asegurar su participación debido a su carga de trabajo y agendas a menudo apretadas.

ix. Preparar las entrevistas con informantes clave

Las entrevistas con informantes clave buscan:

1. Conocer el nivel de conocimiento y comprensión del sistema de gestión de seguridad de la organización; y
2. Recoger recomendaciones del personal sobre posibles mejoras.

Los informantes clave deben ser seleccionados dentro del espectro más amplio posible entre los trabajadores, con atención particular a los propietarios del riesgo (esto es, aquellos con responsabilidad en la toma de decisiones y en la rendición de cuentas en relación a la gestión de seguridad).

▶ *Ver sección iv: propiedad del riesgo*

Herramienta 4
Desarrollo de preguntas para las entrevistas

Una lista típica para entrevistas con informantes clave en una ONG internacional incluye al/a los:

- Director Ejecutivo (CEO, por sus siglas en inglés) o título equivalente
- Jefes de departamentos o direcciones, incluyendo programas internacionales, recursos humanos, finanzas, auditoría y riesgo, y áreas específicas en función del sector de la organización (p. ej. humanitaria)
- Personal legal
- Consejeros de programa
- Consejeros técnicos
- Directores de país y regionales
- Gestores de programa en el terreno
- Empleados de seguridad (p.ej. directores de seguridad, gestores o referentes de seguridad)

Duración de las entrevistas

El tiempo va a limitar a menudo el número de entrevistas que se pueden realizar como parte de una revisión o auditoría. A modo orientativo, el tiempo disponible para las entrevistas debe ser de un mínimo de 45 minutos. Si la entrevista a un informante clave es particularmente útil se puede acordar más tiempo (en un día diferente). A efectos de planificación, se recomiendan seis entrevistas diarias con informantes clave.

x. Preparar las discusiones de grupo

Herramienta 1
Sistema de referencia

Los grupos de discusión son una forma útil de involucrar a varios empleados al mismo tiempo. Para que esto sea efectivo los grupos deben configurarse con gente que tenga una conexión común. Por ejemplo, un grupo de discusión puede formarse enteramente con personal de una oficina en el terreno, mientras que otro grupo puede ser configurado a partir de referentes de seguridad de un país o región específicos.

Herramienta 4
Desarrollo de preguntas para las entrevistas

Los grupos de discusión seguirán una estructura similar a las entrevistas. Las sesiones pueden comenzar introduciendo el proceso de auditoría y el sistema de referencia generado a partir de la herramienta 1, y a continuación pasar a presentar las preguntas, asegurando que se ajustan al contexto local cuando sea necesario.

xi. Preparar las encuestas *online*

Las encuestas *online* son una herramienta útil para recibir opiniones de los empleados en términos más generales, más allá de los informantes clave y los grupos de discusión. Éstas deben ser relativamente cortas, y deben centrarse en unas pocas cuestiones clave directamente relacionadas con los indicadores del SGS.

Herramienta 5
Ejemplo de preguntas para la encuesta *online*

El propósito de una encuesta es examinar el nivel de comprensión e interpretación del sistema a través de un amplio grupo de muestra. Hay que tener en cuenta que el tiempo es un recurso valioso para todo el personal, en particular para aquellos en el terreno. Completar las encuestas no debería tomar más de 10 ó 15 minutos.

Las encuestas deben desarrollarse y publicarse *online* durante la etapa de preparación y planificación de la auditoría, explicando claramente quién ha de completarlas y cuál es el plazo. Ello permitirá que las respuestas estén disponibles en el tiempo asignado para la realización de la auditoría.

B Realización de la auditoría

Una preparación y planificación cuidadosas permiten que la auditoría se lleve a cabo de la forma más efectiva y eficiente posible. También facilita las condiciones óptimas para obtener resultados precisos. Por ese motivo, aplicar la sección A de esta guía requiere un considerable esfuerzo.

Llevar a cabo la auditoría comprende las siguientes actividades clave:

- Revisión exhaustiva de documentos;
- Realización de entrevistas con informantes clave y grupos de discusión focales;
- Recopilación de respuestas de las encuestas online; y
- Realización de entrevistas de seguimiento (para clarificación, información adicional, etc.)

El objetivo de estas actividades es valorar las pruebas y decidir si los indicadores del SGS están:

- Presentes dentro del sistema;
- Parcialmente presentes, cuando algunos indicadores se pueden encontrar durante la auditoría, pero no con la suficiente claridad para decir con certeza que la condición se ha cumplido; o
- No presentes, cuando no se puede atribuir ninguna prueba formal a los indicadores.

Los evaluadores toman una decisión informada basada en el análisis minucioso de toda la información disponible para identificar pruebas de los indicadores. Tome notas detalladas de todas las actividades, ya que esto facilitará el análisis y asegurará un resultado preciso. La herramienta 6 proporciona un ejemplo de plantilla para la auditoría que permite que las pruebas y notas se comprueben en referencia a indicadores individuales.

Herramienta 2
Plantilla para el registro de documentos

Herramienta 3
Lista de comprobación para la revisión documentos

Herramienta 4
Desarrollo de preguntas para las entrevistas

Herramienta 5
Ejemplo de preguntas para la encuesta *online*

Herramienta 6
Plantilla para la auditoría del SGS

C Mapeo de resultados e identificación de medidas de acción

xii. Mapear el sistema

Interpretar los resultados es relativamente simple si los indicadores se han evaluado como se recomienda anteriormente. Las pruebas sugieren si los indicadores están presentes, parcialmente presentes, o no presentes. Esto se puede registrar mediante el uso del habitual sistema de «luces de semáforo»:

Verde para un indicador que se evalúa como demostrado dentro del sistema de gestión de seguridad de la organización;

Ámbar para aquellos indicadores que demuestran cierta presencia pero cuya prueba es más anecdótica; y

Rojo para indicadores que no se pueden demostrar con ninguna prueba registrada.

Evaluación de las partes del SGS

Esta forma de mapear proporciona una indicación muy útil acerca de la salud general del sistema, ya que cada parte del SGS se puede registrar como una tabla de indicadores con la evaluación del sistema de colores. La figura de abajo muestra un ejemplo de cómo se puede realizar este registro.

Figura 2 Ejemplo de indicador

En este ejemplo de indicadores para la dotación de recursos se muestra una evaluación de no presente en el 6.1 y 6.3, parcialmente presente en el 6.2, y el indicador 6.4 está presente en el SGS.

6.1	Existen líneas presupuestarias específicas para requisitos de seguridad en todos los presupuestos de programas.
6.2	Las solicitudes de subvenciones incluyen líneas presupuestarias específicas para cubrir futuros costes de seguridad y detallan el cálculo de esos costes.
6.3	Las cantidades presupuestadas son consideradas suficientes para afrontar todas las necesidades de recursos, con procesos claros y lógicos para estimar dichos montos.
6.4	Hay pólizas de seguros vigentes (médicos, de viaje, de crisis, etc.) y la cantidad cubierta se considera adecuada para afrontar los potenciales costes por riesgos.

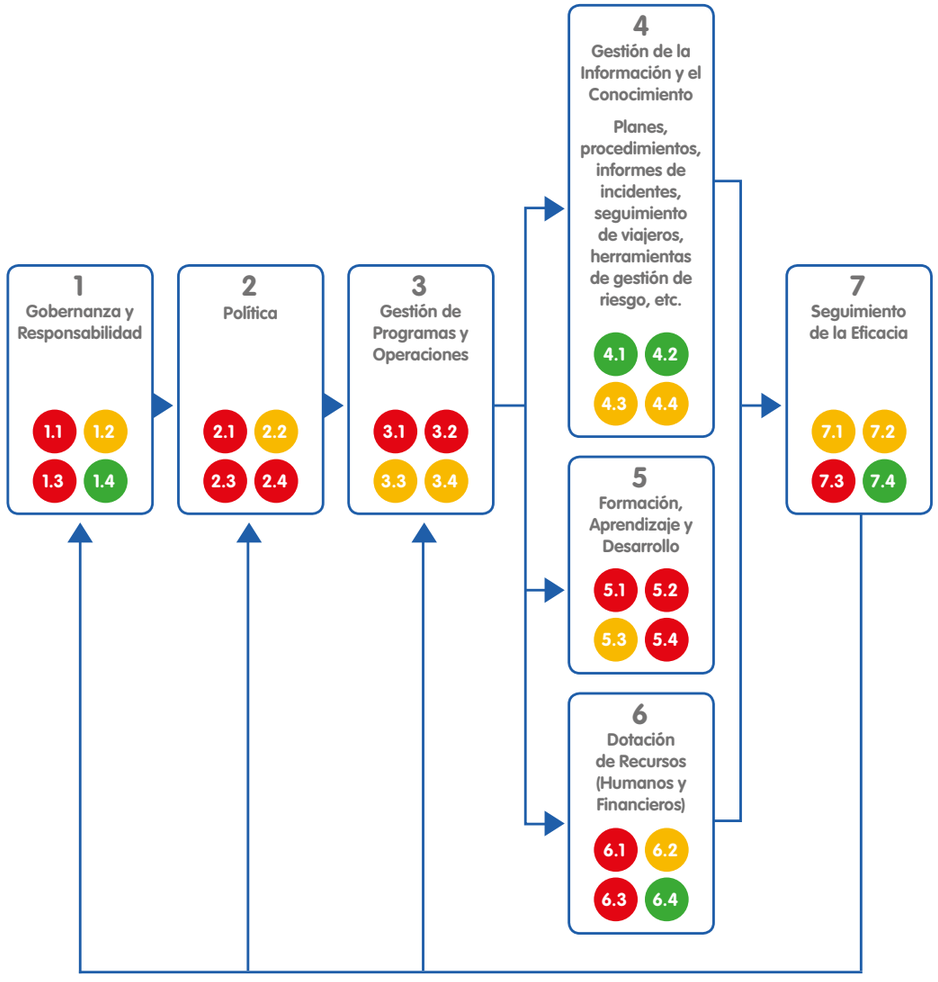
Herramienta 1
Sistema de referencia

Evaluación general del SGS

La salud general del SGS puede ser registrada y comunicada transfiriendo cada evaluación individual de los indicadores al sistema de referencia generado en la herramienta 1.

Figura 3 **Evaluación de indicadores**

Los indicadores y la evaluación de sus resultados pueden superponerse a la correspondiente parte del sistema.



xiii. Identificar fortalezas y debilidades

En términos simples, la salud del sistema se puede ilustrar a través de los resultados de los indicadores. Cuantos más indicadores estén presentes (mostrados en verde en la figura 3 de arriba), más apto para el fin podrá ser considerado el sistema. La auditoría puede llamar la atención sobre partes del SGS que muestran indicadores parciales o no presentes.

Los indicadores evaluados como parciales o no presentes precisarán un examen ulterior. Esto podría indicar que las pruebas no fueron registradas en la recogida de datos inicial o, más comúnmente, que existe una deficiencia en el sistema. Visualizar el sistema de esta manera nos indica la dirección hacia la que enfocar los esfuerzos de una futura revisión o mejora.

Es importante recordar que como cada parte contribuye a la siguiente, si una parte presenta debilidades, ello reducirá la fortaleza de las partes siguientes, deteriorando todo el sistema.

Por ejemplo, la figura 3 muestra un ejemplo donde los indicadores de política son débiles, y el efecto en cadena se puede observar a través del sistema. Mejorar los mecanismos y procesos de gobierno y política debería en teoría fortalecer la totalidad del SGS.

xiv. Tomar medidas

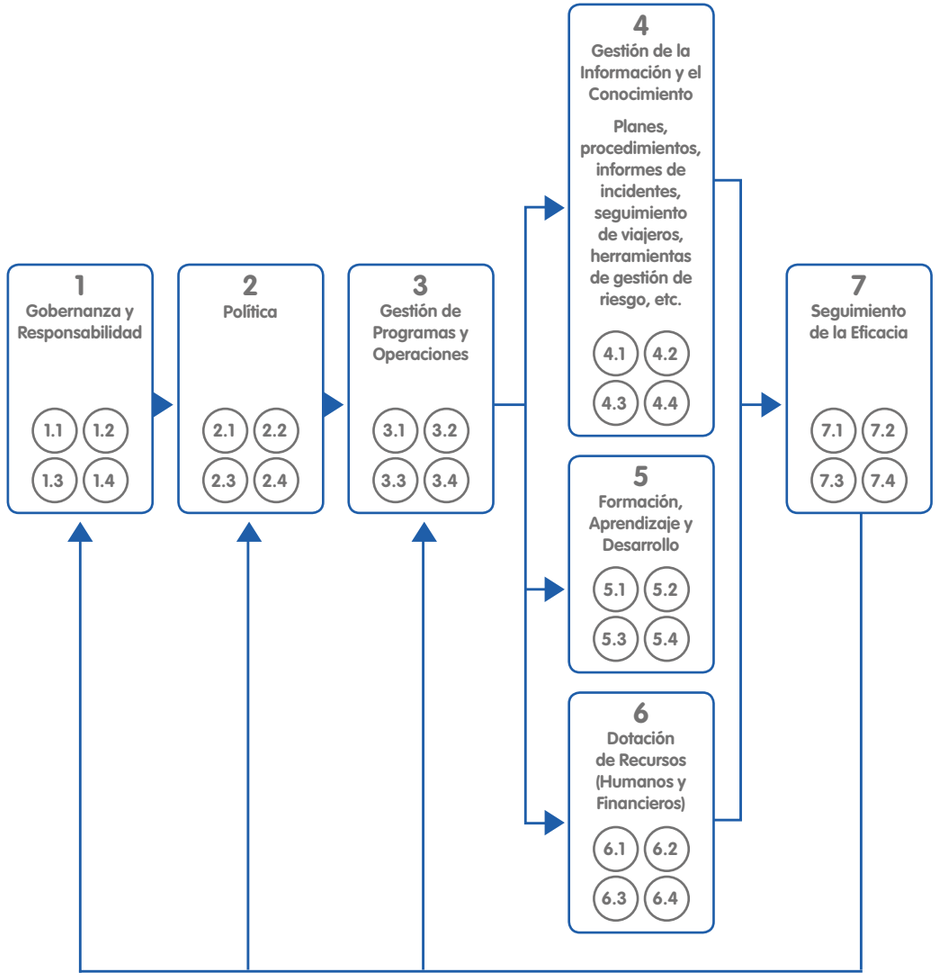
El último escalón en una auditoría de sistemas de gestión de seguridad es asegurar que las medidas de acción han sido registradas y comunicadas a los propietarios del riesgo para su puesta en marcha. Cuando se deseen incorporar mejoras, tales como destinar recursos adicionales para la formación, se debe desarrollar un plan con objetivos y plazos realistas.

Hay que asegurarse de que los resultados de la auditoría se comunican a aquellos que participaron en ella, y también a los empleados en general. Compartir los resultados de la auditoría no sólo mejora la transparencia, sino que también ayuda a los empleados a entender uno de los sistemas de gestión más importantes dentro de su organización.

Herramientas

Disponibles para su descarga y edición en **www.eisf.eu**

Herramienta 1
Sistema de referencia



Herramienta 2
Plantilla para el registro de documentos

Título	Versión/ Fecha de publicación	Referencias a indicadores	Notas

Herramienta 3
Lista de comprobación para la revisión de documentos

En la preparación de una auditoría, los siguientes documentos facilitarán pruebas o información útil acerca del SGS. Esta herramienta separa tipos de documentos de acuerdo con la parte del SGS que es más relevante.

Parte 1: Gobernanza y Responsabilidad

- ◯ Actas de reuniones del Consejo de Administración y/o Dirección, cuando cuestiones de seguridad hayan sido un punto de la agenda para el debate y/o la toma de decisiones
- ◯ Comunicaciones formales del Consejo y/o Directivos a la plantilla en referencia a la gestión de seguridad
- ◯ Comunicaciones formales entre el Consejo y/o Directivos y donantes en referencia a la gestión de seguridad
- ◯ Códigos de conducta para empleados y/o otros
- ◯ Leyes y regulaciones aplicables que rijan la contratación, negligencia (derecho de responsabilidad civil), salud y seguridad, etc.
- ◯ Estándares nacionales y/o internacionales utilizados para informar la gestión de seguridad
- ◯ Estándares de gestión de riesgos (nacionales o internacionales)

Parte 2: Políticas

- ◯ Políticas de gestión de seguridad
- ◯ Políticas de gestión de crisis
- ◯ Otras políticas relacionadas, como políticas sobre denuncia de irregularidades
- ◯ Políticas de personal
- ◯ Políticas de aprovisionamiento y compras
- ◯ Políticas de gestión de programas
- ◯ Otras políticas de gestión de riesgos

Parte 3: Gestión de Programas y Operaciones (planes y procedimientos)

- ◯ Una selección de planes de gestión de seguridad específicos por país y sus asociados procedimientos operativos estándar
- ◯ Directrices de seguridad
- ◯ Otros documentos de procedimiento relacionados, como manuales, etc.

Parte 4: Gestión de la Información y el Conocimiento

- ◯ Informes sobre incidentes (de los últimos 12 meses) incluyendo informes sobre «conatos» de incidentes
- ◯ Comunicaciones a posteriori del incidente (medidas de acción, decisiones en respuesta a los incidentes, etc.)
- ◯ Comunicaciones formales en referencia a cualquier incidente serio o crisis (de principio a fin)
- ◯ Herramientas y directrices de evaluación de riesgos

Parte 5: Formación, Aprendizaje y Desarrollo

- ◯ Estrategia de formación en gestión de seguridad (global)
- ◯ Planes (a nivel regional y de país) de formación en gestión de seguridad
- ◯ Listas o criterios de habilidades y competencias
- ◯ Información acerca del uso de proveedores de formación externos incluyendo ejemplos de licitaciones
- ◯ Programas de formación interna
- ◯ Evaluaciones de formación interna o externa por parte de los empleados

Parte 6: Dotación de Recursos

- ◯ Estrategia de financiación de la gestión de seguridad (global)
- ◯ Presupuesto/s para seguridad (global/es)
- ◯ Planes y presupuestos para la financiación de la gestión de seguridad (a nivel regional y de país)
- ◯ Una selección de presupuestos para programas (a nivel regional y de país)
- ◯ Descripciones de puestos de trabajo, contratos de empleo y términos de referencia para gerentes de seguridad, consejeros de seguridad y referentes de seguridad
- ◯ Descripciones de puestos de trabajo, contratos de empleo, y términos de referencia para directores de programa (regionales y de país) y gestores de programa

Herramienta 3

- ◯ Una selección de propuestas de programa acompañada de presupuestos para programas existentes (para demostrar cómo los requisitos de seguridad se incluyen y se comunican a los donantes)
- ◯ Una lista de donantes actuales, y las propuestas a los donantes y/o las directrices para los informes

Parte 7: Seguimiento

- ◯ Procesos documentados para el control y revisión del desempeño de la gestión de seguridad
- ◯ Informes y/o comunicaciones formales a través de las líneas de gestión en referencia al desempeño de la gestión de seguridad (a nivel de organización)
- ◯ Ejemplos documentados de previas revisiones de seguridad, auditorías o evaluaciones

Herramienta 4
Desarrollo de preguntas para las entrevistas

Las preguntas para las entrevistas con informantes clave y grupos de discusión deben seguir la misma lógica que el sistema de referencia.

Comience las entrevistas presentando el proceso de auditoría y el sistema de referencia generado en la herramienta 1.

Pregunte cuestiones generales primero, y después proceda a preguntas más específicas según la entrevista va progresando. Ejemplos de preguntas clave incluyen:

- **¿Cree que la estrategia de gestión de seguridad de la organización es sistemática y organizada, o ad hoc?**
- **¿Puede describir el sistema de gestión de seguridad de la organización?**
- **¿Cuáles son las partes y procesos fundamentales del sistema?**
- **¿Cuáles considera que son las áreas clave para mejorar?**

Se puede continuar con otras preguntas específicas acerca del rol del informante clave. Por ejemplo, a los gerentes de recursos humanos se les pueden hacer preguntas sobre las responsabilidades de seguridad incluidas en las descripciones de los puestos de trabajo, o a los altos cargos de la ONG preguntas sobre gobernanza.

Las preguntas de la entrevista deben lidiar directamente con los indicadores de cada parte del SGS. Un método útil consiste en pasar por cada parte del sistema de referencia individualmente, preguntando a los informantes clave su opinión sobre si los indicadores están presentes, parcialmente presentes o no presentes.

Cuando se lleva a cabo una auditoría institucional es importante considerar cómo se comunica y se comprende el SGS tanto a nivel de oficina central, como de oficina de país o en el terreno. Esto conllevará preguntar a los propietarios del riesgo a nivel de oficina de país sobre el funcionamiento del sistema y su comprensión del mismo en el contexto más amplio de la organización (esto es, a nivel institucional), y también acerca de cómo este SGS institucional se implementa en la práctica.

Ver sección iv: propiedad del riesgo

Herramienta 5
Ejemplo de preguntas para la encuesta *online*

Recursos para la gestión de seguridad

En su opinión, ¿los indicadores están presentes, parcialmente presentes o no presentes en su organización? Marque su respuesta aquí debajo para cada uno de los indicadores.

6.1 **Existen líneas presupuestarias específicas** para requisitos de seguridad en todos los presupuestos de programas.

Presente	Parcialmente presente	No presente	No sabe

6.2 **Las solicitudes de subvenciones incluyen** líneas presupuestarias específicas para cubrir futuros costes de seguridad y detallan el cálculo de esos costes.

Presente	Parcialmente presente	No presente	No sabe

6.3 **Las cantidades presupuestadas son consideradas suficientes** para afrontar todas las necesidades de recursos, con procesos claros y lógicos para estimar dichos montos.

Presente	Parcialmente presente	No presente	No sabe

6.3 **Hay pólizas de seguros vigentes** (médicos, de viaje, de crisis, etc.) y la cantidad cubierta se considera adecuada para afrontar los potenciales costes por riesgos.

Presente	Parcialmente presente	No presente	No sabe

Herramienta 6
Plantilla para la auditoría del sistema de gestión de seguridad

Ref	Indicadores	Notas de evaluación y pruebas
Parte 1: Gobernanza y Responsabilidad		
1.1	Una declaración de responsabilidad y gobernanza en referencia a la gestión de riesgos de seguridad y a la actitud de la organización hacia el riesgo y sus límites es comunicada por el Consejo de Administración / Director de País.	
1.2	El Consejo de Administración / Director de País asigna responsabilidades específicas en materia de seguridad y gestión de riesgos a una o más partes funcionales de la organización / oficina de país.	
1.3	A alguien dentro del Consejo de Administración / Director de País se le asigna de forma explícita la responsabilidad sobre la supervisión de la gobernanza de los riesgos para la seguridad de la organización / oficina de país.	
1.4	Existe un proceso informativo y de rendición de cuentas (con frecuencia y contenido definidos) para informar al Consejo de Administración / Director de País sobre asuntos relacionados con los riesgos de seguridad y el desempeño de la organización / oficina de país.	

Ref	Indicadores	Notas de Evaluación y Pruebas
Parte 2: Política		
2.1	Las políticas articulan e implementan la posición y decisiones del Consejo de Administración / Director de País en relación a la gestión de riesgos de seguridad, incluyendo las actitudes y límites de la organización respecto al riesgo.	
2.2	La implementación de las políticas (a través de planes, procedimientos y/o directrices) es apropiada para el contexto local.	
2.3	Las políticas especifican las responsabilidades y obligaciones de los empleados en relación a la seguridad, y las comunican a todas las partes relevantes de la organización.	
2.4	Los documentos que detallan la política de la organización están a disposición de los empleados en todos los idiomas al uso.	
Parte 3: Gestión de Operaciones y Programas		
3.1	La autoridad responsable de la toma de decisiones en cuestiones de seguridad (esto es, la propiedad del riesgo) está claramente documentada en contratos de empleo, descripciones de puestos de trabajo y valoraciones del desempeño del personal.	
3.2	La gestión de seguridad es promovida de forma activa a través de la organización por empleados con cargos de gestión, y es demostrable mediante comunicaciones y pruebas documentales, talleres de trabajo y/o otras iniciativas internas.	
3.3	Se articulan estrategias o enfoques específicos para el contexto y se comunican a todas las partes relevantes de la organización.	
3.4	Los procesos de rendición de cuentas y cumplimiento son documentados, incluyendo procesos explícitos para gestionar incumplimientos de la política de gestión de seguridad de la organización, y de planes y procesos de seguridad.	

Ref	Indicadores	Notas de Evaluación y Pruebas
Parte 4: Gestión de la Información y el Conocimiento		
4.1	Tanto sistemas de gestión de información de seguridad como herramientas para informar sobre incidentes están en funcionamiento y disponibles para todos los empleados.	
4.2	La organización participa activamente en foros o consorcios sobre gestión de seguridad y comparte información con otros.	
4.3	Se documentan los planes y procedimientos de seguridad adaptados a contextos específicos, y éstos reflejan la política de la organización.	
4.4	Los planes y procedimientos de seguridad exponen abiertamente las responsabilidades y obligaciones tanto individuales como de la organización.	
Parte 5: Formación, Aprendizaje y Desarrollo		
5.1	Los estándares de desempeño se determinan y comunican a través de la organización.	
5.2	Todos los empleados tienen acceso a una estrategia (y/o plan) documentada de formación, aprendizaje y desarrollo.	
5.3	Existe un compromiso manifiesto de la dirección que asegura que todos los empleados tengan acceso a oportunidades de formación, aprendizaje y desarrollo en temas de seguridad.	
5.4	Autoridades acreditadas reconocen los cursos de formación (si es factible).	

Ref	Indicadores	Notas de Evaluación y Pruebas
Parte 6: Dotación de Recursos		
6.1	Existen líneas presupuestarias específicas para requisitos de seguridad en todos los presupuestos de programas.	
6.2	Las solicitudes de subvenciones incluyen líneas presupuestarias específicas para cubrir futuros costes de seguridad y detallan el cálculo de esos costes.	
6.3	Las cantidades presupuestadas son consideradas suficientes para afrontar todas las necesidades de recursos, con procesos claros y lógicos para estimar dichos montos.	
6.4	Hay pólizas de seguros vigentes (médicos, de viaje, de crisis, etc.) y la cantidad cubierta se considera adecuada para afrontar los potenciales costes por riesgos.	
Parte 7: Seguimiento de la Eficacia		
7.1	Los sistemas de gestión del desempeño de empleados hacen referencia explícita a las responsabilidades en materia de seguridad, y cumplen con las políticas de la organización.	
7.2	Las personas responsables de llevar a cabo el control de la implementación y cumplimiento de los sistemas de seguridad tienen esas responsabilidades explícitamente definidas en la descripción de sus puestos de trabajo.	
7.3	Los resultados de lecciones aprendidas, revisiones, análisis de incidentes a posteriori, y auditorías se usan activamente para mejorar el sistema de gestión de seguridad y/o sus subsistemas y procesos.	
7.4	La gerencia demuestra que los procesos de rendición de cuentas se aplican en caso de incumplimiento.	

Fuentes de información adicional

International Non Governmental Organisations' Accountability Charter, 2005

Stillman, G.B., *NGO Law and Governance: A Resource Book*, ADBI Policy Papers No. 11, 2006

Antares Foundation, *Managing Stress in Humanitarian Work: A Systems Approach to Risk Reduction*, 2008

Center for Safety & Development (CSD), *CSD Matrix & NGO Security Quick Scan*, 2012

K. Micheni, *Christian Aid MOSS Compliance Checklist*

HAP International, *2010 HAP Standard in Accountability and Quality Management*

P. Daudin & M. Merkelbach, *From Security Management to Risk Management – Critical Reflections on Aid Agency Security Management and the ISO Risk Management Guidelines*, Security Management Initiative, 2011

International Standards Organisation, ISO 31000:2009 *Risk Management Principles and Guidelines*, 2009

International Standards Organisation, ISO Guide 73 *Risk Management Vocabulary*, 2009

People in Aid, *Code of Good Practice in the Management and Support of Aid Personnel*, 2003

C. Finucane & M. Merkelbach, *Irish Aid Guidelines for NGO Professional Safety & Security Risk Management*, Dept. of Foreign Affairs and Trade, Government of Ireland, 2013

Glosario

Esta guía utiliza varios términos tomados de la ISO 31000:2009 *Gestión del Riesgo. Principios y Directrices.* Algunas definiciones pueden haber sido modificadas para añadir claridad en el contexto del sector de la ayuda humanitaria.

Objetivos de misión Las metas establecidas y los resultados esperados de una actividad dada.

Riesgo El efecto de la incertidumbre sobre el éxito de los objetivos. Esto incluye la posibilidad de una amenaza que afecte a la organización o a su personal. El riesgo es subjetivo y percibido desde el punto de vista del evaluador.

Actitud hacia el riesgo La estrategia de la organización para evaluar y, en su caso, perseguir, mantener, tomar o apartarse del riesgo.

Gestión de riesgos Las actividades coordinadas para dirigir y controlar una organización en relación al riesgo.

Propietario del riesgo La persona o entidad con la responsabilidad y la autoridad para gestionar un riesgo.

Tratamiento de riesgos El proceso de modificar riesgos. Esto puede incluir actividades para reducir la probabilidad y/o el impacto de una amenaza a través de procedimientos de mitigación de riesgos.

Tolerancia al riesgo La disposición de la organización (o del propietario del riesgo) a soportar (aceptar) el riesgo con el objeto de alcanzar objetivos.

Seguridad (*safety*) La condición de estar protegido ante daños previsibles[15].

Seguridad (*security*) La condición de estar libre de peligros previsibles[16]. La noción de seguridad *(safety and security)* se describe como estar a salvo de, o protegido contra, daños, lesiones, pérdidas o peligros previsibles.

Sistema 1) conjunto de cosas que funcionan juntas como partes de un mecanismo o una red interconectada; (2) conjunto de: principios o procedimientos de acuerdo a los cuales se hace algo; un método o esquema organizado[17].

Referencias bibliográficas

1 Kemp & Merkelbach, SMI Policy Paper, *Can you get sued? Legal liability of international humanitarian aid organisations towards their staff*, 2011.

2 International Standards Organisation, ISO 31000:2009 *Risk Management Principles and Guidelines*, 2009 & ISO Guide 73 Risk Management Vocabulary, 2009.

3 Definición en el texto original en inglés tomada del Oxford Dictionary of English, 2011.

4 Good Practice Review No.8, *Operational Security Management in Violent Environments*, 2010, p.9.

5 International Standards Organisation, ISO 31000:2009 *Risk Management Principles and Guidelines*, 2009 & ISO Guide *73 Risk Management Vocabulary*, 2009.

6 La actitud hacia el riesgo describe la estrategia de la organización para perseguir riesgos o apartarse de ellos (definición extraída de ISO 31000/2009).

7 La tolerancia al riesgo se refiere a la disposición del propietario del riesgo a aceptar riesgos con el objeto de alcanzar un objetivo (definición extraída de ISO 31000/2009).

8 Este texto utiliza el término "Consejo de Administración" para describir el cuerpo de gobierno de una ONG. Algunas ONG pueden utilizar términos diferentes para referirse a este cuerpo de gobierno (p.ej. junta, consejo, comisionados, etc.).

9 Es importante apuntar que las actitudes y los límites hacia el riesgo éstos deben aplicarse con consistencia e igualdad a través de la línea de gestión, ya que éstos son mecanismos de gobernanza institucionales.

10 Good Practice Review No.8, *Operational Security Management in Violent Environments*, 2010, p.9.

11 Para más información sobre el desarrollo de una fuerza de trabajo competente, ver *Irish Aid Guidelines for NGO Professional Safety & Security Risk Management*, Standard 4, p.14 (2013).

12 Duncan Haughey, http://www.projectsmart.co.uk/smart-goals.html último acceso, 5 de agosto de 2013.

13 Las pruebas anecdóticas basadas en testimonios personales en lugar de hechos pueden ser menos fiables.

14 Definición en el texto original en inglés tomada de Oxford Dictionary of English, 2011.

15 Adaptado en el texto original en inglés del New Oxford American Dictionary, 2005.

16 Adaptado en el texto original en inglés del New Oxford American Dictionary, 2005.

17 Definición en el texto original en inglés tomada del Oxford Dictionary of English, 2011.

Otras publicaciones de EISF

Documentos

Security Management and Capacity Development: International agencies working with local partners
December 2012
EISF Secretariat, Iesha Singh

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
September 2012 (English)
September 2013 (Spanish)
Christine Persaud (author), Hye Jin Zumkehr (ed.)

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011
Max Glaser (author), supported by the EISF Secretariat (eds.)

Abduction Management
May 2010
Pete Buth (author), supportedby the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Pete Buth (author), supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Robert Ayre (author), supported by the EISF Secretariat (eds.)

Informes

The Cost of Security Risk Management for NGOs
February 2013
Christopher Finucane (author) Hye Jin Zumkehr (EISF Researcher), EISF Secretariat (eds.)

Risk Thresholds in Humanitarian Assistance
October 2010
Madeleine Kingston and Oliver Behn (EISF)

Joint NGO Safety and Security Training
January 2010
Madeleine Kingston (author), supported by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Christopher Finucane (author), Madeleine Kingston (editor)

Artículos

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing them
March 2012
Koenraad van Brabant (author)

Managing Aid Agency Security in an Evolving World: The Larger Challenge
December 2010
Koenraad Van Brabant (author)

Whose risk is it anyway? Linking Operational Risk Thresholds and Organisational Risk Management (in Humanitarian Exchange 47)
June 2010
Oliver Behn and Madeleine Kingston (authors)

Risk Transfer through Hardening Mentalities?
November 2009
Oliver Behn and Madeleine Kingston (authors)
Also available as a blog at
www.odihpn.org/report.asp?id=3067

Guías

What's the message: Communication and media management in a crisis
September 2013
Sara Davidson (author),
Ellie French, EISF Secretariat (ed.)

Family First: Liaison and support during a crisis
February 2013
Sara Davidson (author),
Ellie French, EISF Secretariat (ed.)

Office Closure
February 2013
Safer Edge (authors), Ellie French and Lisa Reilly, EISF Secretariat (eds).

Próximas publicaciones

Religion and Security
Future of Humanitarian Security

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