GUÍA DEL GISF PARA ORGANIZACIONES NO GUBERNAMENTALES

gisf

Partenariados y gestión de riesgos de seguridad:

Guía de acción conjunta para organizaciones de ayuda locales e internacionales

Global Interagency Security Forum

Contexto

La presente guía del GISF parte de investigaciones previas que ha realizado la organización, en concreto del documento de investigación *Partenariados y gestión de riesgos de seguridad: desde la perspectiva de la coparte local*. Las conclusiones de las entrevistas con personas expertas también sirvieron de apoyo en su elaboración, así como los resultados de una fase de prueba en la que ocho organizaciones no gubernamentales internacionales y nacionales/locales probaron partes del borrador de la guía con sus organizaciones copartes.

La autora y el GISF quieren agradecer a las personas y a las organizaciones que dedicaron su tiempo a compartir recursos y conocimientos, así como a probar el borrador de la guía. Dichas contribuciones fueron fundamentales para elaborar el presente documento. En los agradecimientos que aparecen a continuación se menciona a las personas y las organizaciones que han contribuido.

Sugerencia para citas

GISF. (2022) *Partenariados y gestión de riesgos de seguridad: guía de acción conjunta para organizaciones de ayuda locales e internacionales*. Global Interagency Security Forum (GISF).

Descargo de responsabilidades

El GISF es una agrupación dirigida por sus miembros y no posee una personalidad jurídica independiente según la legislación de Inglaterra y Gales o cualquier otra jurisdicción. Las referencias al "GISF" o al "EISF" en este aviso legal incluirán a las organizaciones miembro, observadoras y secretariado del GISF.

El contenido de este documento no pretende asesorarle con fidelidad. Debe obtener asesoramiento profesional o especializado antes de emprender cualquier acción basándose en este documento o de abstenerse de ello. Aunque el GISF trata de asegurar la veracidad de la información de este documento, no garantiza su exactitud ni su exhaustividad.

La información de este documento se proporciona "tal cual" sin condiciones, garantías u otros términos, y la confianza depositada en la información contenida en el presente documento será responsabilidad total de quien lo lee. Por consiguiente, y hasta donde permita la legislación vigente, el GISF se exime de 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. El GISF no será responsable de ningún tipo de daño o perjuicio causado a usted o a terceros derivado de la confianza depositada en la información de este documento.

Agradecimientos y autoría

Coordinadora de proyecto: Léa Moutard

Autora: Adelicia Fairbanks

Traducción al español: María José Castro, con el apoyo de Gonzalo de Palacios (Oxfam)

Personas expertas que han contribuido:

Antigua coparte de CAFOD en Afganistán

CAFOD: Jamie Monteith, Katy Nembe Katonda

Caritas Goma - Marie Muhemedi

Caritas Ukraine: Maksym Skrypal

Concern Worldwide: Peter Doyle

GISF: Lisa Reilly, Heather Hughes

HAI: Sudhanshu Sekhar Singh

Heizmannconsultancy: Franziska Heizmann

ICRC: Roberto Christensen, Jean-Philippe Kiehl, Hugo Van Den Eertwegh, Robert Whelan

ICVA: Eman Ismail, Alon Plato, Jeremy Rempel, Jeremy Wellard

Keen & Care Initiative: Josephine Alabbi

Kvinna till Kvinna: Joana Costa

LWF: Susan Muis

MAG: David Adam

Ohaha Family Foundation: John Ede

Oxfam: Jan Bouwman

Coparte en Myanmar: Tuja

Plan International: Elodie Leroy-Lemoigne

RICE WN: Jackson Olema, Pax Sakari

SARD: Fares Alsaleh

Saferworld: Dorcas Akello, Euan Mackenzie, Ramzy Magambo, Wilfred Opobo, Sara Torrelles

Titi Foundation South Sudan: Gloria Modong Morris Soma

Trócaire: Win Naing, Peter Ott, Ashley Proud, Doi San

WACSOF: Komlan Messie

Señales

puntos clave y consejos

testimonios expertos

referencias cruzadas

recursos adicionales

las seis herramientas en esta guía (desde la página 88) y disponibles para descarga en formato editable en www.gisf.ngo

Las palabras en marrón están en el glosario (página 122)

Definiciones clave

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

Organización no gubernamental nacional/local (ONGN/L): ONG local o nacional cuyas operaciones tienen lugar en su país de origen.

Organización no gubernamental internacional (ONGI): ONG cuyas operaciones tienen alcance más allá de un país o de una subregión.

Partenariado: relación formalizada (contractual) entre organizaciones de ayuda, que suelen ser internacionales-locales/nacionales. Los partenariados en el sector de la ayuda pueden tener diversa forma, duración, ámbito y grado de colaboración.

Transferencia de riesgos: formación o transformación de riesgos (que aumentan o disminuyen) para una parte causada por la presencia o acción de otra parte, ya sea de forma intencionada o no.

Compartir riesgos: las organizaciones comparten la responsabilidad por los riesgos de seguridad que les afectan.

▶ Véase **el glosario** para consultar más definiciones

Índice

Introducción

La presente guía es el tercer elemento de un proyecto del GISF que consta de varias fases y que está encaminado a mejorar **la gestión de riesgos de seguridad (GRS)** en los acuerdos de partenariado entre organizaciones no gubernamentales internacionales (ONGI) y organizaciones no gubernamentales nacionales y locales (ONGN/L) en el sector de la ayuda.

¿Qué es un partenariado?

En esta guía, **partenariado** designa la relación formalizada (contractual) entre una ONGI y una ONGN/L. Los partenariados en el sector de la ayuda pueden tener diversa forma, duración, ámbito y grado de colaboración. Por ejemplo, pueden ser estratégicos y a largo plazo, o por proyecto y a corto plazo.

- La primera fase de este proyecto conllevó analizar la relación entre ONG internacionales y sus copartes locales. Dicho análisis se centró en las perspectivas de las ONGI y en su desarrollo de capacidades.

  Véase *Security Management and Capacity Development: International agencies working with local partners* (2012)

- La segunda fase se centró en las perspectivas y en las experiencias del personal que trabaja en ONGN/L. La investigación descubrió que el traslado de responsabilidades en la prestación de ayuda a las partes locales (dentro de la agenda de **localización**) no ha ido acompañada de unas conversaciones sinceras y abiertas sobre la transferencia de **riesgos de seguridad**.

  Véase *Partenariados y gestión de riesgos de seguridad: desde la perspectiva de la coparte local* (2022)

- Esta guía constituye la tercera fase del proyecto y parte de los hallazgos de la investigación previa para abordar los desafíos, destacar las oportunidades y ofrecer orientación para unos partenariados más equitativos, sostenibles, transparentes, de confianza y de beneficio mutuo desde el punto de vista de la gestión de riesgos de seguridad.

Cabe percatarse de que esta no es una guía de formación.

¿A quién va dirigida esta guía?

La presente guía va dirigida a ONGI y ONGN/L que estén en proceso de constituir un partenariado o que ya estén trabajando en partenariado.

- Para las organizaciones que estén contemplando unos acuerdos de partenariado -o que estén en sus primeras etapas-, esta guía puede encaminar las conversaciones iniciales sobre gestión de riesgos de seguridad.
- Para las organizaciones que ya estén en un partenariado, esta guía puede servir de apoyo a las copartes para revisar las disposiciones de gestión de riesgos de seguridad existentes.

Si ya mantienen un partenariado, las organizaciones deberían utilizar la presente guía y sus herramientas para revisar y modificar los procesos existentes como corresponda, en lugar de empezar de nuevo.

La presente guía va dirigida al personal con responsabilidades relativas a operaciones, seguridad o partenariados dentro de ONGI y de ONGN/L. También es pertinente para personas expertas en ámbitos que no sean el de seguridad. La gestión de riesgos de seguridad no puede ser eficaz si se compartimenta.

Se anima a las personas a consultar y a trabajar con todo el personal pertinente de su organización para fortalecer la gestión de riesgos de seguridad en el partenariado.

¿Cómo utilizar esta guía y sus herramientas?

El presente documento sirve como guía de acción para que las organizaciones de ayuda adopten un enfoque más equitativo hacia la gestión de riesgos de seguridad en un partenariado.

Esta guía se divide en cinco partes:

- **Parte 1:** conversaciones iniciales para establecer los cimientos de un partenariado equitativo;
- **Parte 2:** los pasos de una "revisión conjunta de la gestión de riesgos de seguridad";
- **Parte 3:** cómo identificar y abordar las necesidades, las lagunas y los desafíos respecto a la gestión de riesgos de seguridad;

- **Parte 4:** cómo realizar incidencia para mejorar la gestión de riesgos de seguridad dentro del sector de la ayuda;
- **Parte 5:** herramientas que respalden la gestión de riesgos de seguridad en partenariados.

El gráfico 1 refleja la estructura de la presente guía.

En los inicios del partenariado, es crucial tratar determinadas cuestiones y adoptar formas equitativas de trabajar. Eso incluye aplicar los principios del partenariado, una buena comunicación, así como hablar con sinceridad sobre la transferencia de riesgos y la actitud hacia el riesgo dentro del partenariado.

Gráfico 1.
Gestión de riesgos de seguridad en partenariados

A partir de estos cimientos, la presente guía propone una **revisión conjunta de la gestión de riesgos de seguridad** (o la "revisión conjunta de la GRS") que acompaña a las copartes mediante una serie de preguntas e indicadores que sirven de apoyo para entender mejor la postura de cada una de las copartes respecto a la gestión de riesgos de seguridad. La revisión concluye con la elaboración y la puesta en práctica de un **plan de acción para la revisión conjunta de la gestión de riesgos de seguridad** (o el "plan de acción para la revisión conjunta de la GRS") para supervisar los esfuerzos dirigidos a fortalecer la gestión de riesgos de seguridad dentro del partenariado.

La revisión conjunta de la gestión de riesgos de seguridad debería formar parte de todo diagnóstico de riesgos más amplio del partenariado y no ser un proceso separado o en paralelo.

Luego, esta guía comparte orientaciones sobre cómo las copartes pueden identificar y abordar las necesidades, las lagunas y los desafíos respecto a la gestión de riesgos de seguridad, en concreto sobre cómo llevar a cabo un diagnóstico conjunto de riesgos de seguridad y satisfacer las necesidades de financiación y de fortalecimiento de capacidades. Por último, se habla en la guía de las oportunidades de utilizar la incidencia para reforzar la gestión de riesgos de seguridad de las copartes.

Los acuerdos de partenariado pueden tener distintas manifestaciones, en función del carácter y de la duración de la relación, de los tipos y tamaños de las ONG que participan, así como del contexto. Las organizaciones pueden adaptar las pautas que se ofrecen aquí para que reflejen la estructura y el contexto operativo de su partenariado.

¿Qué es la gestión de riesgos de seguridad?

Las organizaciones copartes deberían tener un entendimiento común sobre "riesgos de seguridad" y "gestión de riesgos de seguridad".

En esta guía, **riesgo** es cómo puede afectar una **amenaza** a una organización, su personal, sus activos, su reputación o a sus programas. Una amenaza es algo que puede causar daños o lesiones al personal, o daños o perjuicios a la organización. La **vulnerabilidad** se refiere a en qué medida la organización, su personal, activos o programas están expuestos a una amenaza.

Los riesgos por eventos no deliberados, como colisiones de tráfico

rodado, se suelen describir como “riesgos de **seguridad (safety)**”.

Los riesgos que surgen por actos intencionados, como actos violentos o secuestros, se suelen describir como “riesgos de **seguridad (safety)**”.

Cabe percatarse de que en esta guía se utiliza en término “seguridad” como paraguas que incluye “security” y “safety”, y que el término “personal” o “plantilla” también incluye a las personas voluntarias en una organización.

La **gestión de riesgos de seguridad** utiliza un conjunto de planteamientos y de herramientas para ayudar a reducir los riesgos que pueden surgir por actos deliberados o no deliberados. La gestión de riesgos de seguridad es un instrumento para un fin, no un fin en sí misma; se trata de disponer de prácticas que permitan a las organizaciones llegar a quienes más lo necesitan al tiempo que protegen a su personal.

Descubra más sobre la gestión de riesgos de seguridad

La presente guía no es una guía introductoria a la gestión de riesgos de seguridad ni una guía del proceso de auditoría de la gestión de riesgos de seguridad.

Si quiere saber más sobre la gestión de riesgos de seguridad, consulte:

- *EISF – Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*
- *GISF – Seguridad en práctica*
- *ODI-Informe de buenas prácticas 8 – Gestión de la seguridad de las operaciones en entornos violentos*

Si busca orientaciones sobre cómo llevar a cabo una auditoría general de la gestión de riesgos de seguridad en la organización, consulte:

- *EISF – Auditorías de seguridad*
- *EISF – The Cost of Security Risk Management for NGOs*

1 Establecer los cimientos de un partenariado equitativo en la gestión de riesgos de seguridad

1.1. ¿Por qué es importante un enfoque equitativo y conjunto sobre seguridad en los partenariados?

“La gestión de riesgos de seguridad propicia de forma crucial la acción humanitaria y es fundamental para unos partenariados justos. Las ONGN/L, al responsabilizarse y encabezar la prestación de ayuda humanitaria, también asumen riesgos de seguridad, incluso cuando la transferencia de riesgos no es deliberada”

GISF – *Partenariados y gestión de riesgos de seguridad: desde la perspectiva de la coparte local*

En las colaboraciones, las ONG locales o nacionales suelen soportar la mayor carga de riesgos de seguridad, sobre todo en las operaciones cotidianas en contextos de riesgo elevado. Cuando se trata la gestión de riesgos de seguridad en los acuerdos de partenariado, las ONG suelen encontrarse problemas por:

- La carencia de diálogo y análisis sobre la **transferencia de riesgos** y las **actitudes hacia el riesgo**.
- Las dificultades en llegar a una comprensión compartida del contexto y los riesgos asociados.
- La falta de financiación apropiada para la gestión de riesgos de seguridad, sobre todo en los presupuestos de ONG locales o nacionales, pero también en los de ONGI.
- Un apoyo y un tiempo inadecuados e insuficientes para fortalecer la capacidad de gestión de riesgos de seguridad de ambas copartes, incluso cuando se identifican las lagunas de forma conjunta.
- Malentendidos a causa de barreras lingüísticas, una interacción física limitada entre copartes, y la falta de un vocabulario común sobre riesgos de seguridad y su gestión.
- Obstáculos a una comunicación abierta y sincera, en lo que influyen

las diferencias en culturas comunicativas, las disparidades de poder, la presión por ser competitivas y el temor a perder financiación.

- Los desafíos para acceder a información pertinente en materia de seguridad y para compartirla (un reto al que a menudo se enfrentan ambas copartes).

Una carencia clave en los partenariados entre ONGI y ONGN/L es una conversación en igualdad de condiciones y conjunta para explorar los desafíos que se mencionan anteriormente. Cuando se abre el diálogo, se suele centrar en que la ONGI verifique con qué cuenta la ONGN/L y si se adecúa a los estándares de la ONGI.

Si bien dichas conversaciones pueden ser de utilidad, ponen a la ONGN/L bajo lupa y pueden relegar a la coparte local a la posición de una entidad que precisa "ser evaluada". Dicha "evaluación desde arriba" da por hecho que el enfoque de la ONGI hacia la gestión de riesgos de seguridad es mejor que el de la ONGN/L, algo que no tiene por qué ser así.

Es necesario que las conversaciones sobre la gestión de riesgos de seguridad dejen de ser, más que nada, una evaluación desde arriba de la capacidad de seguridad de las ONGN/L para dar lugar a conversación conjunta sobre riesgos, recursos, necesidades y oportunidades de colaborar y de fortalecer capacidades.

Un enfoque equitativo de la GRS en los partenariados se aleja de la conversación sobre los desafíos de la "transferencia de riesgos" para hablar de cómo "compartir riesgos".

Para compartir la responsabilidad sobre los riesgos de seguridad, las organizaciones deberían adoptar un planteamiento que fomente una relación más equitativa entre copartes. Eso significa:

- llevar a cabo una revisión conjunta de qué dispone cada coparte en materia de **gestión de riesgos de seguridad**;
- identificar carencias y retos, y cómo pueden trabajar juntas las copartes para abordarlos;
- velar por que las voces y las experiencias del personal en ambas organizaciones copartes se escuchan y se valoran de igual manera;
- estudiar los riesgos de seguridad y las medidas de mitigación que saquen partido de las fortalezas del personal de la ONGN/L;
- reconocer que los planteamientos de seguridad más eficaces son adaptables y específicos para el contexto (lo que puede implicar que

los planteamientos convencionales de seguridad de las ONGI pueden no ser siempre los adecuados).

Qué significa acción "conjunta" en la práctica

FAVORECER:

- Mantener conversaciones abiertas y sinceras sobre qué funciona y qué no
- Impulsarse mutuamente a mejorar las formas de trabajar
- Hacer juntas una lluvia de ideas sobre soluciones
- Compartir información y prácticas de manera habitual
- Consultarse mutuamente para fundamentar nuevas políticas y prácticas
- Adaptar los recursos existentes para que cubran las realidades y las necesidades de ambas copartes

EVITAR:

- Tomar en solitario decisiones que puedan afectar a la organización coparte
- Ignorar preocupaciones o ideas
- Rendirse al primer intento (el partenariado lleva trabajo)
- Eludir conversaciones difíciles o situaciones complicadas

A fin de establecer unos cimientos sólidos para un partenariado equitativo en materia de GRS, las organizaciones deberían hablar de forma abierta sobre la **transferencia de riesgos**, adoptar unos principios del partenariado, interactuar con una buena comunicación y explorar de manera conjunta las **actitudes hacia el riesgo** de cada coparte. Estos temas fundacionales se tratan en más profundidad en los apartados siguientes.

Más información

- *GISF – Partenariados y gestión de riesgos de seguridad: desde la perspectiva de la coparte local*
- *Humanitarian Outcomes – NGOs and Risk: Managing Uncertainty in Local-International Partnerships*

1.2. Entender y abordar la transferencia de riesgos de seguridad entre copartes

Al constituir un partenariado, las organizaciones se transfieren riesgos de forma automática, tanto de forma deliberada como no. Es importante que las copartes desentrañen lo que esa transferencia de riesgos implica para ambas organizaciones y que encuentren maneras de abordar en conjunto cualquier desafío que puedan identificar.

Desequilibrios de poder en los partenariados

Un desafío clave en los partenariados es que, a menudo, una de las organizaciones tiene más poder que la otra. Entre las fuentes de poder están:

- **El acceso a recursos o su uso**: personal, dinero, equipos, herramientas de comunicación.
- **El acceso a información**: entre otras, la capacidad de controlar esa información y cómo se comparte y se comunica.
- **Las conexiones y las redes**: relaciones con otras personas, agencias o grupos con poder (por ejemplo, donantes).
- **La autoridad y la legitimidad**: un reconocimiento formal o uno que parta de la reputación de la organización, que proporciona a la organización la capacidad de tomar decisiones y emprender acciones que tengan una aceptación generalizada.
- **Personalidad jurídica o de registro**: diferencias en la personalidad jurídica o de registro; por ejemplo, la nacionalidad o el tipo de pasaporte, oportunidades de evacuación frente a reubicación, "neutralidad" percibida o implícita.

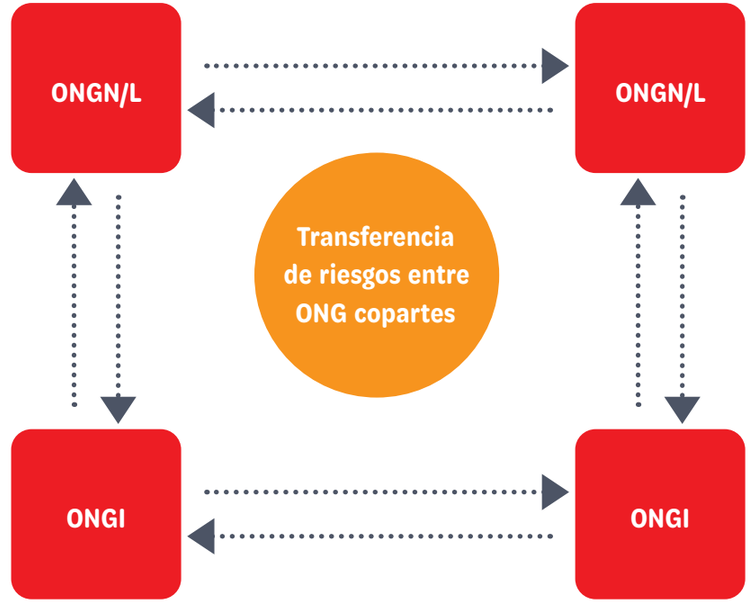
Una organización con menos poder puede sentirse obligada a aceptar las decisiones o las expectativas de una coparte más poderosa. Por ejemplo, una organización local que depende de la financiación que recibe a través de un partenariado con una ONGI puede sentirse incapaz de plantear preocupaciones por miedo a perder la financiación o a perjudicar el partenariado. Las organizaciones más poderosas tienen la responsabilidad de tener en cuenta la presión coyuntural que pesa sobre los hombros de sus copartes y deberían ser proactivas para velar por que sus copartes se sientan capaces de verbalizar sus opiniones y preocupaciones sin temer las consecuencias.

¿Qué es la transferencia de riesgos?

Transferencia de riesgos es la formación o la transformación de riesgos (que aumentan o descienden) para una parte provocadas por la presencia o las acciones de otra.

Los riesgos de seguridad no solo se transmiten del ámbito global al local. Pueden transferirlos las ONGN/L a las ONGI, y se pueden transferir entre actores que operen al mismo nivel (véase el Gráfico 2). Por ejemplo, para una ONGN/L, que la relacionen con una ONGI puede aumentar los riesgos a los que se expone en sus operaciones al repercutir en cómo las comunidades y las autoridades locales perciben y responden a la ONGN/L. Y, al contrario: los acuerdos de partenariado con ONGN/L pueden repercutir en la seguridad y la aceptación de una ONGI en contextos concretos a causa de las percepciones que existan sobre la ONGN/L. También puede darse una transferencia de riesgos dentro de las organizaciones, por ejemplo, del personal en la capital al personal en las oficinas en terreno.

Gráfico 2. Las distintas direcciones en las que se transfieren riesgos



Adaptado de GISF – Partenariados y gestión de riesgos de seguridad: desde la perspectiva de la coparte local

La identidad de una organización –o su identidad percibida– puede influir en cómo son recibidas sus copartes, lo que puede afectar a la transferencia de riesgos y generar riesgos de seguridad para el personal de ambas copartes. La identidad de una organización tiene que ver con su mandato, su misión y sus principales actividades programáticas. Por ejemplo, el carácter religioso de algunas organizaciones, u organizaciones con un foco programático concreto, como proporcionar acceso a servicios y derechos de salud reproductiva. Los perfiles personales de la plantilla también pueden afectar al riesgo al que se exponen las copartes (*véase el cuadro más abajo*).

Recuerden tener en cuenta las amenazas tanto internas como externas al evaluar percepciones y riesgos relacionados con la identidad y cómo se forman o transforman a causa del partenariado.

Las copartes deberían entender y abordar juntas las cuestiones que surjan a raíz de la transferencia de riesgos de seguridad dentro del partenariado; y eso lo pueden hacer planteándose preguntas clave de manera recíproca al principio del partenariado e incorporando los riesgos que puedan surgir del partenariado a un proceso de diagnóstico de riesgos de seguridad y al plan de gestión de seguridad.

▶ *Véase el apartado 2.3.2. para consultar preguntas clave que exploran los riesgos de seguridad que pueden surgir a raíz de los partenariados*

HERRAMIENTA 5. Plantilla de plan de diagnóstico conjunto de riesgos de seguridad y su gestión

Perfiles personales y riesgos relacionados

Las personas que integran la plantilla tienen distintos perfiles de riesgo, que están relacionados con sus rasgos personales, tanto visibles como ocultos, como su género, nacionalidad, grupo étnico, etc. Dichos rasgos interactúan entre ellos, con el contexto y también con la función y la organización de dicha persona, y con la organización coparte.

En consecuencia, los riesgos pueden ser distintos para cada individuo. El perfil de cada una de las personas que integran la plantilla desempeña un rol en a qué amenazas se enfrenta y cuán **vulnerable** es a dichas amenazas. Es importante tener en cuenta los riesgos diversos a los que se enfrenta el personal durante todo el partenariado.

Las copartes también deberían recordar que algunas veces las amenazas provienen de la propia organización o del partenariado. Por ejemplo, el personal de una ONGN/L que pertenece a determinados grupos éticos puede estar especialmente expuesto a amenazas internas, que no siempre son visibles para el personal de una ONGI o este puede no entenderlas.

Los perfiles personales de la plantilla en una organización pueden ser muy distintos de los de otra, y así también su exposición a amenazas. Las organizaciones no deberían confiar en los diagnósticos de riesgos de seguridad y las medidas de mitigación de sus copartes, sino contemplar los riesgos específicos a los que se enfrenta su plantilla a causa de sus perfiles personales.

▶ *Véase el apartado 2.3.4. con preguntas que las copartes se pueden plantear recíprocamente para abordar estos tipos de riesgos*

Más información

- *GISF – Partenariados y gestión de riesgos de seguridad: desde la perspectiva de la coparte local*
- *Humanitarian Outcomes – NGOs and Risk: Managing Uncertainty in Local-International Partnerships*

1.3. Adoptar unos principios de partenariado

Se anima a las copartes a reflexionar sobre los siguientes principios durante todo el partenariado y a actuar de manera proactiva para respaldarlos.

Equidad	Transparencia y confianza	Beneficio mutuo	Complementariedad	Enfoque hacia resultados	Responsabilidad
Pueden darse desequilibrios de poder entre organizaciones locales e internacionales, pero el principio de equidad vela por que, a pesar de dichos desequilibrios, ambas copartes tengan el mismo derecho a ser escuchadas y que se valoren sus contribuciones en la misma medida. Esta equidad ha de tener como base el respeto y la justicia. En lo que respecta a la gestión de riesgos de seguridad, eso implica, por ejemplo, que las preocupaciones en materia de seguridad de ambas copartes se escuchen, entiendan y traten en la misma medida.	Los cimientos de una relación de confianza son interacciones sinceras y abiertas -que se producen en una situación de igualdad- entre las copartes. Las organizaciones copartes deben mantener conversaciones abiertas y sinceras sobre cuáles son las necesidades de seguridad y cuál es la manera más realista de abordarlas. Eso significa escuchar y confiar en quienes están más en riesgo, que a menudo es el personal de las ONGN/L.	Los resultados positivos del partenariado deberían ir más allá de la mera consecución de los objetivos del partenariado. Para lograrlo, las copartes han de velar por que exista una buena comunicación y que se entiendan con claridad los intereses, las motivaciones y las metas en sentido más amplio de cada una de las copartes. Al fortalecer de manera proactiva la capacidad del personal y al abordar las necesidades de seguridad a largo plazo de ambas copartes, las organizaciones no solo están velando por la seguridad de los programas del partenariado, sino que también generan unos planteamientos sobre la gestión de riesgos de seguridad que pueden perdurar más que el partenariado.	Las copartes deberían reconocer que la diversidad es un valor. Las actividades de ambas copartes deberían partir de la base del conocimiento y la pericia que cada una aporta al partenariado, evitar duplicaciones y abordar de forma proactiva las barreras, tales como las lingüísticas y las culturales. La capacidad y el conocimiento locales son herramientas fundamentales para gestionar con eficacia los riesgos de seguridad. Todo planteamiento de gestión de riesgos de seguridad dentro del partenariado debería aprovechar las ventajas comparativas entre ambas copartes y sus contribuciones.	Las acciones de las copartes deberían centrarse en los resultados y tener un alcance realista. En la gestión de riesgos de seguridad, eso implica que ambas copartes se coordinen para elaborar y poner en práctica acciones realistas respecto a la seguridad. Las actividades deberían servir como apoyo directo para que mejoren la seguridad y los resultados del programa para ambas copartes.	Las copartes deberían tener la obligación ética de asumir su responsabilidad laboral con integridad y de manera adecuada. Las copartes solo deberían comprometerse al trabajo que puedan emprender con sus competencias, destrezas, capacidades y recursos. Cuando las copartes sientan que no pueden llevar a cabo su trabajo de una manera responsable por problemas de seguridad, estos se deben tratar abiertamente entre ambas partes, y abordarse.

Adaptado de los Principios de asociación aprobados por la Plataforma Humanitaria Mundial y los principios que presentó The Partnering Initiative

Más información

- *Plataforma Humanitaria Mundial – Principios de asociación*
- *Global Mentoring Initiative – Partnerships: Pre-conditions, principles and practices*
- *The Partnering Initiative – The Partnering Cycle and Partnering Principles*

1.4. Comunicar y generar confianza en los partenariados

La comunicación es un desafío primordial para constituir un partenariado equitativo. La complejidad y la sensibilidad de los riesgos de seguridad no son excusa para la ambigüedad ni para fiarse de las suposiciones.

Las copartes deberían alentarse entre sí a preguntar y a sentirse empoderadas para buscar información y así mejorar el entendimiento mutuo. A modo de apoyo y para generar confianza, el personal que tenga tareas de enlace entre las copartes debería:

1. **Demostrar un cuidado auténtico:** cuestionar los posibles prejuicios y sesgos que puede tener antes de empezar a conversar.
2. **Escuchar para entender, no para responder**.
3. **Buscar los puntos en común para construir la relación:** identificar objetivos e intereses comunes a partir de los cuales poder construir.
4. **Asumir la diferencia hasta que se demuestren los puntos en común:** asegúrese de no dar por supuesto un entendimiento común. Tenga siempre en cuenta la cultura y las tradiciones de cada coparte para reforzar los mensajes.
5. **Expresar empatía:** diga la verdad con consideración y tenga en cuenta las circunstancias de la coparte que puedan afectar a su interacción con ustedes (p. ej., situación personal, antecedentes, necesidades).
6. **Ser transparente y establecer las expectativas correctas:** sea sincero/a sobre las limitaciones y restricciones con las que trabaja y no prometa más de lo que pueda cumplir.
7. **Mostrar positividad y respeto:** céntrese en los objetivos comunes para crear cohesión entre ustedes y su coparte.
8. **Separar a las personas del problema:** enfoque las dificultades con su coparte, en lugar de achacarle responsabilidades.
9. **Elegir el momento, el lugar y el método adecuados para comunicarse:** tenga en cuenta la cultura de la coparte (p.ej., las tradiciones

orales frente a las escritas) y asegúrese de que las comunicaciones importantes son accesibles con facilidad. Vele por que la vía de comunicación sea segura y que ambas copartes se sientan cómodas utilizándola.

10. **Diga lo que piensa, piense lo que dice:** responsabilícese de las acciones y las palabras, lo que incluye asumir errores y malentendidos.
11. **Pedir y recibir comentarios de una forma que empodere:** de manera tanto anónima como directa que genere confianza en el personal para dar su opinión.
12. **Claridad y concreción en las comunicaciones:** exprese con claridad qué se espera de la coparte a través de la comunicación.
13. **Comunicarse con frecuencia**, sobre todo en periodos de incertidumbre.

Las organizaciones deberían asegurarse siempre de que el enfoque comunicativo es el adecuado para la coyuntura y para las personas involucradas.

"En algunos contextos no podemos usar el término 'seguridad' porque se relaciona con la inteligencia y puede poner a la coparte local en riesgos adicionales por parte de las autoridades estatales".

Integrante del personal de una ONGN/L

Las copartes deberían tener a una persona interlocutora que esté presente en esas conversaciones y que no solo conozca el idioma de ambas organizaciones, sino también su cultura, y que pueda servir como intérprete.

Asegúrese de que las personas correctas forman parte de la conversación. Además, tenga en cuenta a qué nivel deberían celebrarse dichas conversaciones: ¿debería estar solo presente el personal de la sede y de la oficina principal en país de la organización, o también el personal de la oficina en terreno o en primera línea?

"A veces en la sede establecemos todas estas medidas para mejorar los acuerdos de partenariado, pero se pueden desmoronar en terreno cuando el personal nacional se comunica de manera deficiente con las copartes locales y perpetúa una estructura de poder vertical".

Integrante del personal de una ONGI

Las organizaciones deberían contemplar que una buena comunicación sea parte de la formación al personal o un aspecto de su evaluación de desempeño.

HERRAMIENTA 1. Una buena comunicación en los partenariados

Los acuerdos de partenariado y los métodos de comunicación también han de construirse entendiendo que los sesgos siguen siendo generalizados entre las copartes, y dentro del sector de la ayuda en un sentido más amplio. **Los sesgos**, en este contexto, se entienden como una inclinación injusta o un prejuicio hacia (o contra) un grupo determinado por motivos de raza, grupo étnico y otros aspectos identitarios, incluida la nacionalidad.

▶ *Véase el glosario para saber más sobre los distintos tipos de sesgos*

Los sesgos de cualquiera de las copartes pueden afectar gravemente a las relaciones y a la comunicación en el partenariado, sobre todo cuando ya se den unos desequilibrios de poder y una falta de confianza que supongan dificultades. Ambas copartes deberían considerar qué sesgos conscientes e inconscientes pueden tener.

Ejemplos de sesgos

En el sector de la ayuda, los sesgos se suelen ver en forma de los distintos estándares de seguridad que se aplican a diferentes grupos del personal. En un ejemplo de una investigación previa del GISF, el personal de la ONGN/L recibía menos efectivo que sus compañeros de la ONGI para financiar su viaje, lo que derivaba en que el personal de la ONGN/L tuviera que comprometer su alojamiento nocturno, algo que no tenían que hacer sus copartes de ONGI.

Más información

- *GISF – Partenariados y gestión de riesgos de seguridad: desde la perspectiva de la coparte local*
- *The Partnering Initiative – Talking the Walk: A Communication Manual for Partnership Practitioners*
- *Global Mentoring Initiatives Resources*

Parte 1

- *Aid Reimagined*
- *Race Forward*

1.5. Explorar las actitudes hacia los riesgos de seguridad dentro del partenariado

Los riesgos pueden mitigarse (reducirse) de diversas maneras. Por ejemplo, el riesgo de accidentes de tráfico rodado se puede atenuar con el mantenimiento de los vehículos y al formar a quienes conducen en una conducción adecuada y los procedimientos de emergencia. Sin embargo, incluso si se establece una mitigación, el riesgo de que se produzca un accidente de tráfico rodado sigue existiendo. Se trata del **riesgo residual**. La actitud concreta hacia el riesgo de una organización determinará si acepta los riegos residuales (que se denomina "aceptación del riesgo" o alcanzar el "umbral de riesgo" de una organización).

La decisión de "aceptar" riesgos de seguridad no siempre se toma en igualdad de condiciones entre ONGI y ONGN/L.

Aceptación del riesgo, actitud hacia el riesgo y umbral de riesgo

Aceptación del riesgo, **actitud hacia el riesgo** y **umbral de riesgo** son todos términos que se utilizan para describir la cantidad de riesgo que una organización desea asumir (o tiene obligación de hacerlo) para cumplir sus objetivos.

Es imprescindible que las copartes entiendan, desentrañen y hablen de las actitudes hacia el riesgo de ambas organizaciones. Eso es clave para un partenariado equitativo. Las copartes deberían respetar las preocupaciones de la otra y ser conscientes de la posibilidad de **habituarse al riesgo** o de que las organizaciones se sientan presionadas para superar su umbral de riesgo para seguir operando.

Los siguientes principios éticos pueden servir de apoyo a las organizaciones a la hora de evaluar su propia actitud hacia el riesgo en los acuerdos de partenariado:

1. **Criticidad:** ¿cuán crítico es el programa?
2. **Acción sin daño:** ¿qué daños pueden derivar de un incidente de seguridad?
3. **Autonomía**: ¿el personal de ambas copartes –en particular, las personas más en riesgo– ha dado su consentimiento libre e informado para asumir los riesgos de seguridad o el partenariado ha desempeñado un papel en esta decisión?
4. **Custodia:** ¿la organización usa los recursos de una manera responsable y de la que rinda cuentas?
5. **Justicia:** ¿las copartes se tratan recíprocamente de una manera justa?
6. **Fidelidad:** ¿son las copartes leales a la visión y las funciones institucionales y profesionales?

La **actitud hacia el riesgo** de cada una de las copartes debería ser un tema central de conversación cuando comience el partenariado y volver a revisitarse de forma periódica durante todo el ciclo de vida del partenariado.

HERRAMIENTA 2. Actitud hacia el riesgo en partenariados

Más información

- *GISF – Partenariados y gestión de riesgos de seguridad: desde la perspectiva de la coparte local*
- *EISF – Security Risk Management and Capacity Development: International agencies working with local partners (particularly, 'Figure 3: Framework for ethical decision-making')*
- *EISF – Risk Thresholds in Humanitarian Assistance*

2 Llevar a cabo una revisión conjunta de los procesos de gestión de riesgos de seguridad dentro del partenariado

2.1. Revisión conjunta de la GRS

Para compartir de manera equitativa la responsabilidad en materia de seguridad, las copartes deberían apoyarse mutuamente en la gestión de los riesgos de seguridad. Para eso, un primer paso es mantener conversaciones abiertas, sinceras y constructivas sobre cómo cada coparte entiende y gestiona los riesgos de seguridad, y sobre cómo pueden colaborar las copartes para apoyar sus enfoques respectivos sobre la gestión de riesgos de seguridad. La presente guía ofrece una revisión conjunta de la gestión de riesgos de seguridad para respaldar dichas conversaciones. La "**revisión conjunta de la GRS**" es un proceso con dos acciones generales:

1. Revisar la comprensión y el enfoque que cada organización tiene sobre la gestión de los riesgos de seguridad e identificar las carencias y los desafíos; y
2. Abordar de manera conjunta las carencias y los desafíos a los que se enfrenta cada coparte en la gestión de seguridad mediante la elaboración y la puesta en práctica del "**plan de acción de la revisión conjunta de la GRS**".

La revisión conjunta de la GRS empieza con un cuestionario. Las respuestas a las preguntas fundamentan la elaboración de los indicadores clave. Luego, las copartes evalúan dichos indicadores para identificar qué existe ya y qué lagunas quedan. Esa evaluación puede servir para fundamentar la elaboración de un plan de acción con una lista de comprobación de tareas que mejore la coordinación de ambas copartes para gestionar los riesgos de seguridad. Después, ambas copartes supervisan periódicamente ese "plan de acción de la revisión conjunta de la GRS". Véase el Gráfico 3 para visualizar las distintas partes del proceso de revisión conjunta de la GRS. La presente guía incluye herramientas de apoyo a los distintos pasos de proceso, que se destacan también en el Gráfico 3.

Gráfico 3. Pasos de la revisión conjunta de la GRS

El siguiente **marco de gestión de riesgos de seguridad** se usa en la presente guía para enmarcar las distintas partes de la revisión conjunta de la GRS (*véase el Gráfico 4*). Se anima encarecidamente a las copartes a utilizarlo como mapa de referencia para sus conversaciones.

Gráfico 4. Marco de gestión de riesgos de seguridad

Fuente: EISF - Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas

Parte 2

Gestionar riesgos de seguridad efectivos

La revisión conjunta de la GRS consiste en explorar enfoques sobre la gestión de los riesgos de seguridad dentro de los acuerdos de partenariado. Por lo tanto, la revisión es una "herramienta de gestión del partenariado", no una "herramienta de gestión de los riesgos de seguridad".

Tras llevar a cabo dicha revisión, las copartes deberían contemplar los riesgos de seguridad efectivos que suponen una amenaza para su personal, las organizaciones y el partenariado, como los accidentes de tráfico o las agresiones a su personal. Eso se puede realizar llevando a cabo un **diagnóstico conjunto de riesgos de seguridad** y elaborando un **plan conjunto de gestión de riesgos de seguridad**. Dichas "herramientas de gestión de riesgos de seguridad" se tratan con más profundidad en la Parte 3 de la presente guía.

▶ *Véase el apartado 3.1. Identificar y abordar conjuntamente los riesgos de seguridad*

2.2. Planificar el enfoque

Para empezar, las copartes deberían planificar el enfoque. Eso implica:

- convenir en que el objetivo de la revisión es mejorar la gestión de los riesgos de seguridad;
- establecer fechas y horas que sean aceptables para ambas copartes para celebrar las conversaciones;
- acordar cómo se va a realizar la revisión.

La revisión conjunta de la GRS habrá de adaptarse a las circunstancias de las organizaciones copartes y tener en cuenta los factores pertinentes. Por ejemplo, la relación entre cada una de las copartes con las comunidades y otras partes con las que trabajan, sus actitudes hacia el riesgo y su capacidad para responder a desafíos en materia de riesgos de seguridad, pero también sus ubicaciones, tipo de trabajo, etc.

En los partenariados a largo plazo, lo idóneo sería que las revisiones conjuntas de la gestión de riesgos de seguridad en el partenariado se realizasen cada dos años; y en contextos delicados, con más frecuencia, a ser posible. Puede que resulte útil para las copartes llevar a cabo la revisión si se producen cambios significativos en el contexto operativo que afecten a la realización de los programas de alguna manera o cambios en la relación entre las copartes (p. ej., una ampliación de las

operaciones). Las copartes deberían identificar y acordar juntas qué desencadenantes consideran que darían pie a dichas conversaciones.

Lo idóneo sería que la mayor parte de las conversaciones en torno a la gestión de riesgos de seguridad se produzcan antes de formalizar un partenariado. Sin embargo, cuando eso no sea factible, las organizaciones han de dialogar sobre seguridad lo antes posible y durante todo el partenariado.

También es importante tener en cuenta otras evaluaciones que se puedan estar produciendo al mismo tiempo dentro del partenariado. Las organizaciones locales a menudo han de hacer malabares con las expectativas de varias copartes ONGI así como de los múltiples departamentos de la misma ONGI, no solo respecto a seguridad, sino a la gestión de riesgos en sentido más amplio y, en concreto, del riesgo fiduciario.

A causa de las susceptibilidades en torno a las cuestiones de seguridad, el personal de las ONGN/L puede sentirse más cómodo al tratar sus desafíos y preocupaciones en reuniones presenciales en lugar de mediante comunicaciones por escrito.

Las copartes deberían preguntarse con un espíritu crítico qué personas han de participar. Por ejemplo, podría ser la dirección senior, el personal con responsabilidades en seguridad, y el de referencia del partenariado. No obstante, otras personas de la plantilla pueden aportar perspectivas útiles; p. ej., el personal de programas que esté en mayor riesgo y el personal con responsabilidades en finanzas o incidencia.

▶ *Véase la Parte 4 para saber más sobre la función de la incidencia*

Adaptar el enfoque a causa de factores externos

Las organizaciones copartes habrán de adaptar el enfoque que refleja esta guía para que corresponda con las oportunidades y las limitaciones presentes por el carácter del partenariado, el contexto y otras circunstancias, tales como dificultades del entorno (p. ej., epidemias e inseguridad). Entre las adaptaciones pueden estar:

- llevar a cabo talleres en remoto por teléfono o en línea, velando por que todas las partes interesadas necesarias puedan acceder al canal de comunicación o a la plataforma que se use;
- mostrar flexibilidad ante circunstancias que cambian con rapidez, relacionadas con el entorno y la **seguridad**;

continuación

Adaptar el enfoque a causa de factores externos *continuación*

- asegurarse de que todas las partes interesadas son conscientes de los riesgos que pueden repercutir en cómo se desarrolla este enfoque y de que están preparadas para abordar dichos riesgos o adaptarse para admitir la **vulnerabilidad** de las personas involucradas en el proceso;
- velar por una comunicación habitual y adecuada con todas las partes interesadas, así como mantener abiertos los canales de comunicación para fomentar la capacidad de ser flexibles y de adaptación.

Como medida proactiva, las organizaciones deberían tener en cuenta las necesidades a largo plazo de ambas copartes y establecer unas estructuras de colaboración sólidas y unas relaciones de confianza para así generar resiliencia contra conmociones y crisis en un futuro.

2.3. Cumplimentar el cuestionario y evaluar los indicadores

Antes de nada, las copartes deberían acordar las preguntas clave que van a plantearse para entender mejor qué gestión de riesgos de seguridad implica cada una de las organizaciones y en el partenariado en su conjunto.

Las respuestas a las preguntas pueden servir para desarrollar indicadores clave para el partenariado en su conjunto o, si procede, para cada una de las organizaciones copartes. Los indicadores se pueden considerar: presentes, presentes en parte o no presentes. Las copartes deberían convenir en qué significa cada una de las "categorías de evaluación" antes de examinar los indicadores. Por ejemplo, ¿"presente" significa que está documentado de alguna manera, que la dirección responsable confirma su presencia o que varias personas de la plantilla están de acuerdo en que está presente?

Las preguntas y los indicadores de ejemplo que se muestran en el apartado siguiente están categorizados conforme a los distintos elementos del **marco de gestión de riesgos de seguridad** que aparece previamente en el apartado 2.1. Sin embargo, las preguntas y los indicadores son solo a efectos orientativos y se pueden modificar según las circunstancias de cada partenariado.

HERRAMIENTA 3. Cuestionario y plantilla de trabajo para la revisión conjunta de la GRS para responder a las preguntas y evaluar los indicadores. La herramienta también se puede descargar en formato editable en www.gisf.ngo

El capítulo siguiente trata el cuestionario para la revisión conjunta de la GRS apartado por apartado, con explicaciones y algunas preguntas adicionales que las organizaciones pueden decidir abordar.

Preguntas preliminares para las copartes sobre la gestión de riesgos de seguridad

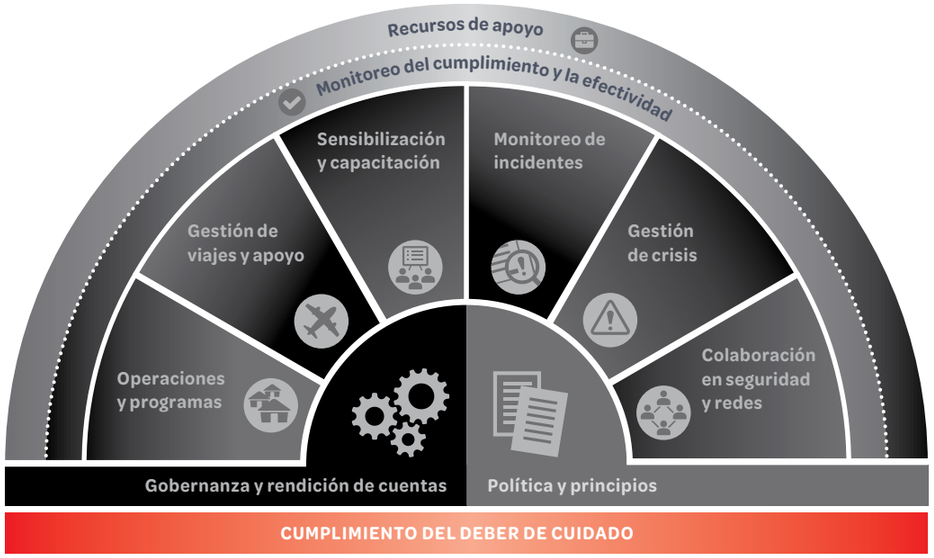
Puede que las copartes no estén en posición de cumplimentar la revisión completa; quizás, si se encuentran todavía en las primeras etapas del partenariado, prefieran hacer una exploración inicial mediante las siguientes preguntas preliminares.

Preguntas preliminares para las copartes sobre gestión de riesgos de seguridad	
Deber de cuidado	• ¿Cuáles son las obligaciones jurídicas y morales del deber de cuidado de cada coparte respecto a la otra?
Gobernanza y rendición de cuentas	• ¿Han contribuido ambas copartes en las oportunidades clave de toma de decisiones (p. ej., reuniones) sobre el programa, el proyecto, el partenariado o la seguridad? • ¿Cuentan ambas copartes con estructuras apropiadas de gestión de riesgos de seguridad (incluso las funciones y las responsabilidades) que permitan cumplir los objetivos del partenariado? • ¿Se mencionan los riesgos de seguridad y su gestión en el contrato de partenariado?
Transferencia de riesgos	• ¿Cómo perciben a las copartes las partes interesadas con las que cada una de ellas suele interactuar con frecuencia y de las que depende para operar? • ¿Cómo varía la vulnerabilidad de cada organización y de su personal ante las amenazas existentes a consecuencia del partenariado? ¿Es un factor la identidad que se percibe de una organización? • ¿Surgen nuevas amenazas a consecuencia del partenariado? • ¿El partenariado cambia la probabilidad o el impacto de una amenaza concreta? De ser así, ¿es positivo o negativo?
Políticas y principios	• ¿Ambas copartes entienden el mandato, la misión, los valores y los principios de cada una de las organizaciones? ¿Están ambas organizaciones cómodas con la labor y el planteamiento de operaciones de la otra (p. ej., ¿están de acuerdo ambas copartes en sus posturas respectivas en lo que se refiere a adherirse a los principios humanitarios)?

Preguntas preliminares para las copartes sobre gestión de riesgos de seguridad *continuación*	
Operaciones y programas	• ¿Cuáles son las necesidades y las expectativas en materia de seguridad de cada una de las copartes? • ¿Cuentan las copartes con un sistema que hayan acordado para identificar y monitorear los riesgos de seguridad a los que se enfrenta el personal? • ¿Las copartes han convenido en quién es la responsable de gestionar los riesgos identificados, y en cómo ha de hacerse y financiarse? • ¿Hay un sistema para que ambas copartes sepan si se dan cambios en el entorno de riesgos? • ¿Cada una de las copartes cuenta con recursos suficientes (financiación, tiempo y personal) para gestionar los riesgos de seguridad?
Enfoques de una gestión inclusiva de riesgos de seguridad	• ¿El planteamiento sobre gestión de riesgos de seguridad de ambas organizaciones tiene en cuenta cómo la identidad de las personas que integran la plantilla puede afectar a su vulnerabilidad ante las amenazas? • ¿Cómo deberían hablar las copartes sobre temas de identidad sensibles, como las amenazas internas y externas por motivos de orientación sexual o género? ¿Cuáles son los niveles de confort (sin perder de vista las sensibilidades culturales)? • ¿Cómo se pueden apoyar las copartes entre ellas para salir de sus niveles de confort para asegurar una gestión de riesgos de seguridad efectiva para todo el personal?
Amenazas internas y salvaguardia	• ¿Cómo gestionarán las organizaciones las amenazas de seguridad que pueden surgir dentro de las propias copartes (p. ej., el personal)? • ¿Cómo se abordan las preocupaciones sobre salvaguardia dentro del partenariado? ¿Existen mecanismos adecuados para plantear cuestiones de salvaguardia a disposición del personal, la población beneficiaria y la comunidad de ambas copartes?
Viajes	• ¿Cómo deberían gestionarse los riesgos de seguridad que son consecuencia de viajes relacionados con el partenariado?
Fortalecimiento de la sensibilización y la capacitación	• ¿Cómo identificarán las copartes las necesidades de sensibilización y de refuerzo de capacidades, y cómo las cubrirán de manera conjunta (tanto en términos de seguridad personal como de gestión de riesgos de seguridad)?
Monitoreo de incidentes	• ¿Cómo deberían compartir las copartes información sobre incidentes entre ellas, de hacerlo?
Gestión de crisis	• ¿Cómo colaborarán/se coordinarán las copartes si se produce una crisis o un incidente crítico que afecte a alguna de las organizaciones en la ubicación donde el partenariado tiene actividad?
Colaboración y redes en materia seguridad	• ¿Existen plataformas en el contexto pertinente que traten temas de seguridad? • Si la respuesta es afirmativa, ¿tienen ambas copartes acceso y una voz igual en esas redes y plataformas de coordinación en sus zonas operativas, incluso en las plataformas para compartir información sobre seguridad?
Monitoreo de cumplimiento y eficacia	• ¿Cómo deberían revisar ambas copartes con regularidad la gestión de riesgos de seguridad dentro del partenariado?
Recursos	• ¿Las copartes han compartido entre ellas sus recursos respectivos sobre gestión de riesgos de seguridad?
Final del partenariado	• ¿La finalización del partenariado conforme al contrato (y al calendario financiero) repercute en la seguridad de alguna de las copartes? De ser así, ¿cómo se debería abordar eso?

Recordatorio: Al ir consultando la revisión en los apartados siguientes, siga el diagrama que aparece a continuación.

2.3.1. Deber de cuidado



El **deber de cuidado** es un elemento clave que hay que abordar en los partenariados para entender con claridad las responsabilidades y las expectativas de cada una de las copartes en lo que respecta al cuidado del personal. También es importante verificar que ambas copartes entienden de una forma parecida el deber de cuidado, ya que no todas las organizaciones estarán familiarizadas con el término.

El deber de cuidado de una organización

El deber de cuidado es la obligación jurídica y moral de una organización de adoptar todas las medidas posibles y razonables para reducir el riesgo de daños a quienes trabajan para una organización o actúan en su nombre. Se aplica a los contextos de riesgo elevado y a los de riesgo bajo. Si bien el deber de cuidado se suele centrar mucho en las obligaciones jurídicas, las copartes deberían también examinar su deber de cuidado moral, que se suele referir a cada una de las acciones (u omisiones) que van más allá de las obligaciones jurídicas de una organización, y va encaminado a velar por el bienestar de toda persona a quien afecten las actividades de la organización.

El deber de cuidado básico suele implicar:

- Conocer los riesgos a los que se enfrentan las personas de las que es responsable la organización.

continuación

El deber de cuidado de una organización *continuación*

- Establecer medidas de mitigación para gestionar los riesgos identificados.
- Elaborar planes de emergencia.
- Asegurarse de que el personal entiende los riesgos a los que se enfrenta y las medidas de las que dispone para gestionarlos.
- Velar por que el personal toma decisiones fundamentadas sobre los riesgos que implica su puesto.
- Proporcionar el apoyo adecuado en caso de que se produzca un incidente de seguridad.

Preguntas de ejemplo

1.1. ¿Cuáles son las obligaciones jurídicas y morales del deber de cuidado de cada coparte respecto a la otra, de haberlas?

1.2. ¿Cuáles son las obligaciones jurídicas y morales del deber de cuidado de cada coparte hacia su personal, población beneficiaria y comunidades afectadas respectivas?

1.3. ¿Se tienen en cuenta las necesidades psicosociales de todo el personal y se abordan? ¿Hay alguna acción que puedan emprender las copartes para perfeccionar su deber de cuidado hacia el personal que implementa (p. ej., cobertura del seguro, bienestar psicosocial)? ¿Cuál?

1.4. ¿Entiende cada una de las coparte el deber de cuidado –tanto jurídico como moral– y coincide lo que ambas entienden?

1.5. ¿La finalización del partenariado conforme al contrato (y el calendario económico) tendrá repercusiones en la seguridad de alguna de las copartes? Si fuera así, ¿cómo debería abordarse esto?

Indicadores de ejemplo

1.1. Ambas copartes entienden y cumplen las obligaciones jurídicas del deber de cuidado.

1.2. Ambas copartes han hablado y acordado las obligaciones morales del deber de cuidado.

Siguientes pasos en el **deber de cuidado** y más información

Para respaldar este proceso, las copartes también pueden considerar:

- Compartir sus políticas respectivas de deber de cuidado y añadir un párrafo sobre los partenariados a dicha política (si la tuvieran).
- Poner en común una lista de proveedores de servicios que proporcionen apoyo psicosocial adecuado en términos culturales y lingüísticos que luego compartan con el personal de ambas organizaciones.

Más información:

- *cinfo – Duty of Care Maturity Model Tool*
- *EISF – Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*
- *EISF – Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications*
- *EISF y cinfo – Duty of care under Swiss law and Duty of Care Maturity Model*
- *GISF – Partenariados y gestión de riesgos de seguridad: desde la perspectiva de la coparte local*

2.3.2. Gobernanza y rendición de cuentas

Unas buenas estructuras de gobernanza y rendición de cuentas son fundamentales para una gestión de riesgos de seguridad eficaz. Dentro de los acuerdos de partenariado es importante asegurarse de que ambas copartes cuentan con estructuras de gestión de riesgos de seguridad, sin perder de vista la diversidad de prácticas y de capacidades entre una organización y otra.

Es mejor para las organizaciones determinar en los inicios del partenariado la **propiedad del riesgo** y las responsabilidades de cada una de las copartes para asegurarse de que sus expectativas sobre la otra no están desencaminadas. Se pueden compartir responsabilidades sobre los riesgos de seguridad de una manera estratégica, que consistiría en evaluar los perfiles de riesgo de las copartes y velar por la complementariedad.

Las disposiciones para gestionar los riesgos de seguridad tendrán que adaptarse para que coincidan con el tipo de partenariado.

Preguntas de ejemplo

2.1. ¿Cuentan ambas copartes con estructuras apropiadas de gestión de riesgos de seguridad que permitan cumplir los objetivos del partenariado?

2.2. ¿Entienden con claridad ambas copartes las funciones y las

responsabilidades relativas a la gestión de riesgos de seguridad en lo referente al partenariado y a la realización de los programas? Por ejemplo, ¿tienen ambas organizaciones una persona que sea referente de seguridad y que pueda ser el contacto para las copartes en cuestiones de seguridad?

2.3. ¿Cómo percibe cada una de las copartes la **transferencia de riesgos** en el partenariado (si lo hace)? ¿Qué acciones considera cada coparte que puede emprender para pasar de la transferencia de riesgos a **compartir riesgos**? (*Véase el cuadro más adelante con preguntas específicas sobre la transferencia de riesgos*.)

2.4. ¿Se ha acordado un procedimiento para informar de problemas y para que cada una de las copartes rinda cuentas si no consigue cubrir las necesidades en materia de gestión de riesgos de seguridad dentro del partenariado?

2.5. ¿Qué pueden hacer ambas copartes para que mejore la **cultura de seguridad** de su personal, sobre todo en términos de conversaciones y sensibilización dentro de los acuerdos de partenariado?

2.6. ¿Queda claro cómo están vinculados los riesgos de seguridad a otros riesgos (p. ej., riesgos fiduciarios, problemas jurídicos, barreras administrativas)? ¿Quienes trabajan sobre estos otros tipos de riesgos son conscientes de los enfoques sobre gestión de riesgos de seguridad que están aplicando las copartes?

2.7. ¿Han contribuido ambas copartes en las oportunidades clave de toma de decisiones (p. ej., reuniones) respecto al programa, el proyecto, el partenariado o la seguridad?

2.8. ¿Se mencionan los riesgos de seguridad y su gestión en el contrato de partenariado?

Preguntas clave para comprender los riesgos de seguridad que pueden surgir a raíz de los partenariados

Para desentrañar qué riesgos pueden derivar de los partenariados, las organizaciones han de preguntarse a sí mismas y entre ellas:

- ¿Cómo perciben a las copartes las partes interesadas con las que suele interactuar con frecuencia cada una de las organizaciones y de la que depende para operar?
- ¿Repercuten las características identitarias organizacionales en la vulnerabilidad de la organización y de su personal ante amenazas?
- ¿Existe alguna nueva amenaza que surja a consecuencia del partenariado?
- ¿El partenariado cambia la probabilidad o el impacto de una amenaza concreta? De ser así, ¿es positivo o negativo?
- Al explorar medidas de mitigación y estrategias de seguridad, ¿puede una de las organizaciones actuar de una manera determinada para reducir los riesgos a los que se enfrenta su coparte?

▶ *Véase el apartado 1.2. Entender y abordar la transferencia de riesgos de seguridad entre copartes*

Indicadores de ejemplo

2.1. Existe una declaración de rendición de cuentas y de gobernanza respecto a la gestión de riesgos de seguridad dentro del partenariado.

2.2. Existe un proceso de información y de rendición de cuentas (con un contenido y una frecuencia establecidos) para advertir a cada una de las copartes sobre cuestiones de riesgos de seguridad, que arroja claridad sobre las responsabilidades de ambas copartes en lo respectivo a la gestión de los riesgos de seguridad dentro del partenariado.

2.3. Ambas copartes han designado explícitamente a una persona referente con responsabilidades en el ámbito de la gobernanza de los riesgos de seguridad tanto de la organización como del partenariado.

Siguientes pasos en la **gobernanza y en la rendición de cuentas** y más información

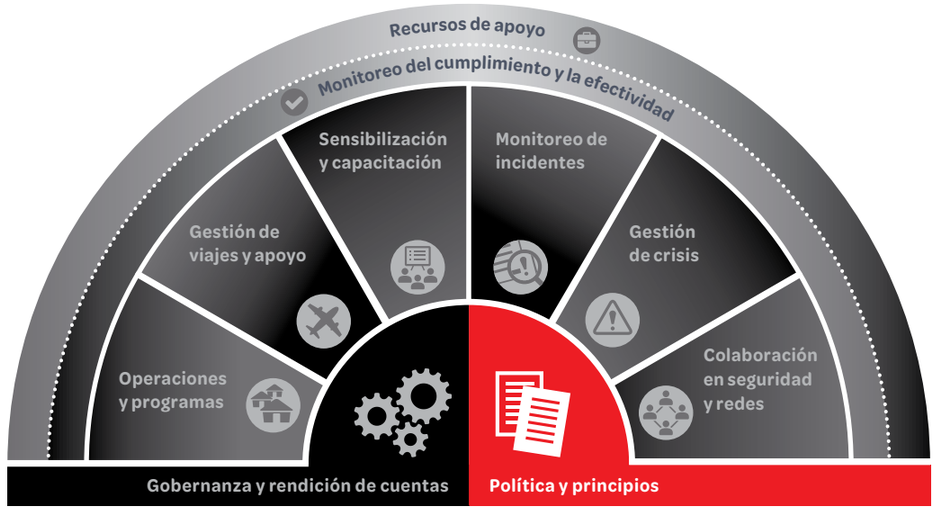
Para respaldar este proceso, las copartes también pueden considerar:

- Crear un organigrama (con el nombre, el contacto, las responsabilidades) del personal que tenga responsabilidades de seguridad dentro del partenariado.
- Actuar para respaldar una cultura de seguridad positiva entre su personal (véase, por ejemplo, "11 pasos hacia una cultura positiva de seguridad" en EISF – *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas* (p. 14-15)).
- Establecer reuniones habituales con personal de ambas organizaciones que se dedique a distintos tipos de riesgos para realizar un mapeo frecuente de las intersecciones y los efectos de los distintos tipos de riesgos a los que se enfrentan ambas organizaciones.

Más información:

- *EISF – Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*
- *GISF – Seguridad en práctica*
- *Humanitarian Outcomes – NGOs and Risk: Managing Uncertainty in Local-International Partnerships*

2.3.3. Política y principios



Ambas copartes deberían enfocar la gestión de riesgos de seguridad desde su política de seguridad organizacional. Dicha política ayuda a comunicar al personal los principios y enfoques que adopta la organización para gestionar los riesgos de seguridad y proporciona información sobre las responsabilidades del personal en la gestión de riesgos de seguridad. Las copartes deberían comparar sus respectivos principios y enfoques sobre la gestión de riesgos de seguridad. Cabe destacar la importancia de hablar sobre la **actitud hacia el riesgo, la habituación al riesgo** y el enfoque global sobre seguridad, incluso los principios humanitarios, de cada una de las copartes.

▶ *Véase el apartado 1.5. Explorar las actitudes hacia el riesgo dentro del partenariado*

HERRAMIENTA 2. Actitud hacia el riesgo en partenariados

Preguntas de ejemplo

3.1. ¿Ambas copartes entienden el mandato, la misión, los valores y los principios de cada una de las organizaciones? ¿Están ambas organizaciones cómodas con la labor y el enfoque sobre operaciones y seguridad de la otra (p. ej., ¿están de acuerdo ambas copartes en sus posturas respectivas en lo que se refiere a adherirse a los principios humanitarios)?

Parte 2

3.2. ¿Existe acuerdo entre las copartes sobre los requisitos mínimos prácticos de seguridad que debe haber en cada lugar o actividad? (Percátese de que, si bien estos deberían aplicarse a ambas copartes, también han de ser realistas y adaptarse a la capacidad de cada organización).

3.3. ¿Cómo definen y plantean la actitud hacia el riesgo las copartes? ¿Y existe un acuerdo entre las copartes sobre lo que es un **umbral de riesgos** aceptable para el partenariado y los programas incluidos en este?

3.4. ¿Cómo perciben las copartes la habituación al riesgo? ¿Y existen formas en las que las copartes se pueden apoyar entre sí para abordarla?

3.5. ¿Cuáles son los vínculos entre la actitud hacia el riesgo, la criticidad del programa y la capacidad de gestión de riesgos de seguridad dentro del partenariado?

3.6. ¿Han acordado las copartes cuáles serán los principios y los objetivos fundamentales del partenariado y los entienden?

Indicadores de ejemplo

3.1. Las políticas de gestión de seguridad y su puesta en práctica (mediante planes, procedimientos o directrices) son adecuadas para el contexto local y las circunstancias del partenariado, y son accesibles para todo el personal (es decir, están disponibles en los idiomas y en los formatos pertinentes).

3.2. El contrato de partenariado incluye una declaración relativa a que se ha entendido y acordado conjuntamente el umbral de riesgos para las actividades del partenariado.

3.3. El contrato de partenariado no contradice –sino que refuerza, cuando sea posible– las políticas de seguridad de ambas copartes (p. ej., disposiciones sobre el uso de escoltas armadas).

Siguientes pasos en **política y principios** y más información

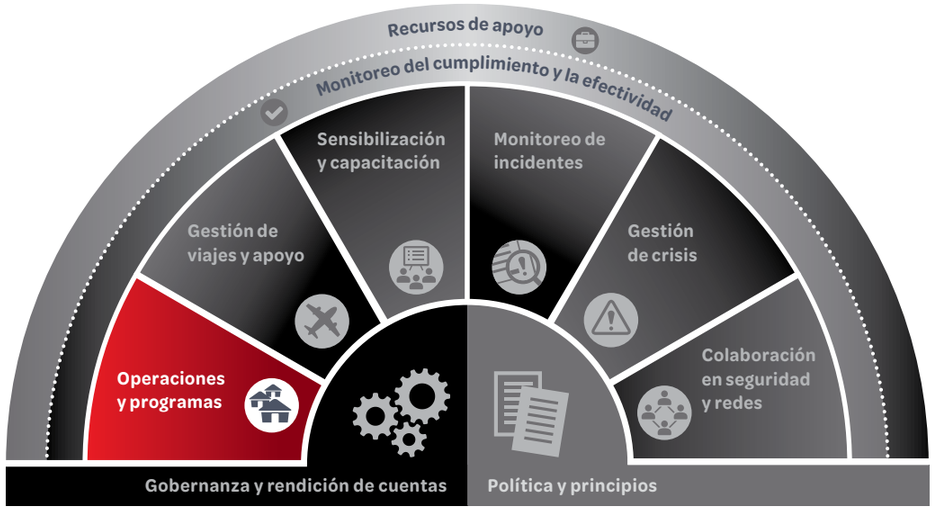
Para respaldar este proceso, las copartes también pueden considerar:

- Compartir el mandato, la misión, los valores, los principios y las políticas de seguridad de cada organización, y hablar de cuál es su comparación entre las copartes (p. ej., ¿están armonizadas o existen tensiones graves?).
- Crear una lista de alarmas respecto a los riesgos de seguridad y las medidas de mitigación que deberían tratarse antes de ponerse en práctica, sobre todo si se refieren a principios y políticas (por ejemplo, el uso de escoltas armadas).
- Comentar las actitudes hacia el riesgo y determinar formas de informar de inquietudes cuando se alcanza el umbral de unas de las copartes.
- Organizar actividades de sensibilización para velar por que todo el personal comprende los conceptos de habituación al riesgo y de aceptación del riesgo, y que pueda plantear preocupaciones.

Más información:

- *EISF – Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*
- *EISF – Risk Thresholds in Humanitarian Assistance*

2.3.4. Operaciones y programas



El elemento central de muchos partenariados es realizar programas de manera efectiva. Las copartes deberían acordar cuál es la mejor manera de gestionar los riesgos de seguridad que surjan de llevar a cabo las actividades. Debería haber unos planes, procedimientos y recursos realistas que respalden el análisis del entorno operativo y la identificación de riesgos de seguridad para el personal y para las operaciones.

Eso servirá para determinar los planteamientos y las medidas más eficaces para gestionar los riesgos de seguridad en el contexto operativo.

Cuando sea posible, contemplen la posibilidad de realizar un diagnóstico conjunto de riesgos de seguridad para cada contexto operativo.

Véase el apartado 3.1. Identificar y abordar conjuntamente los riesgos de seguridad

HERRAMIENTA 5. Plantilla de plan de diagnóstico conjunto de riesgos de seguridad y su gestión

Gestionar con eficacia los riesgos de seguridad implica colaborar con un abanico diverso de compañeras y compañeros. El personal de programas y finanzas debería participar, cuando proceda, en la conversación en torno a la identificación y la mitigación de riesgos, y velar porque se incluye la gestión de riesgos de seguridad en los presupuestos del partenariado y del proyecto.

Véase el apartado 3.2. Financiación de la gestión de riesgos de seguridad en los partenariados

HERRAMIENTA 6. Plantilla de presupuesto de gestión de riesgos de seguridad en partenariados

Preguntas de ejemplo

4.1. ¿Cuáles son las necesidades y las expectativas en materia de seguridad de cada una de las copartes?

4.2. ¿Cuentan las copartes con un sistema que hayan acordado para identificar y monitorear los riesgos de seguridad a los que se enfrenta el personal? (¿Están armonizados los **diagnósticos de riesgos de seguridad** y los planes de seguridad de ambas organizaciones para las ubicaciones en las que opera la coparte que implementa? ¿Cuáles son las divergencias y por qué?)

4.3. ¿Las copartes han convenido en quién es la responsable de gestionar los riesgos identificados, y cómo ha de hacerse y financiarse?

4.4. ¿Hay un sistema para que ambas copartes sepan si se dan cambios en el entorno de riesgo?

4.5. ¿Cada una de las copartes cuenta con recursos suficientes (financiación, tiempo y personal) para gestionar los riesgos de seguridad?

4.6. ¿El presupuesto del partenariado/proyecto incluye partidas referentes a la seguridad y es bastante para cubrir las necesidades de seguridad de ambas copartes? ¿Dicha financiación es lo suficientemente flexible como para cubrir los gastos generales, para adaptarse si se producen cambios en el contexto y en los riesgos de seguridad, o para utilizarla para actividades de capacitación?

4.7. ¿Quién controla lo que se incluye en los presupuestos del partenariado? ¿Puede haber un traslado del control para que sea compartido a partes iguales entre las copartes?

4.8. ¿Cómo se abordan las preocupaciones sobre salvaguardia dentro del

partenariado? ¿Existen mecanismos adecuados para plantear cuestiones de salvaguardia a disposición del personal, la población beneficiaria y las comunidades de ambas copartes?

4.9. ¿Cómo gestionarán las copartes las **amenazas de seguridad** que pueden surgir dentro de las propias organizaciones asociadas (p. ej., el personal)?

Preguntas clave para una gestión inclusiva de riesgos de seguridad

Para desentrañar los riesgos que pueden ser consecuencia de los partenariados, las organizaciones han de preguntarse a sí mismas y entre ellas:

- ¿El planteamiento sobre gestión de riesgos de seguridad de ambas organizaciones tiene en cuenta cómo puede afectar la identidad de las personas que integran la plantilla a su vulnerabilidad ante las amenazas?
- ¿Cómo deberían hablar las copartes sobre temas de identidad sensibles, como las amenazas internas y externas por motivos de orientación sexual o género? ¿Cuáles son los niveles de confort (sin perder de vista las sensibilidades culturales)?
- ¿Cómo se pueden apoyar las copartes entre ellas para salir de sus niveles de confort para asegurar una gestión de riesgos de seguridad efectiva para todo el personal?

Indicadores de ejemplo

4.1. Se ha realizado un **diagnóstico conjunto de riesgos de seguridad** de las operaciones, los riesgos asociados y las repercusiones sobre cada coparte, y existe un proceso claro para ir actualizando el análisis con regularidad. El diagnóstico incluye un análisis de los riesgos internos y de los que puedan surgir a consecuencia del propio partenariado.

4.2. En el presupuesto del partenariado hay partidas explícitas para cumplir los requisitos de seguridad, incluso actividades de refuerzo de capacidades, y ambas copartes consideran que son suficientes para satisfacer todas sus necesidades de recursos.

4.3. Ambas copartes han convenido en las estrategias o los enfoques sobre seguridad específicos para el contexto y están articulados y se han comunicado a todas las partes pertinentes de cada organización.

4.4. Las personas responsables en toda la organización fomentan y apoyan de manera activa la gestión de riesgos de seguridad y eso se demuestra en las comunicaciones y en los informes, con talleres y otras iniciativas.

4.5. Las copartes están de acuerdo en cómo prevenir, prepararse y responder ante incidentes de explotación, abuso y acoso sexuales que afecten a su personal y a su población beneficiaria dentro de sus organizaciones y del partenariado.

Siguientes pasos en **operaciones y programas** y más información

Para respaldar este proceso, las copartes también pueden considerar:

- Hacer un mapeo juntas de un día cotidiano en las ubicaciones del proyecto. Este ejercicio puede servir para que salgan preguntas sobre cuestiones de seguridad.
- Llevar a cabo un diagnóstico conjunto de riesgos de seguridad.
  Véase **HERRAMIENTA 5**
- Crear de manera conjunta una lista de necesidades en materia de seguridad precisas para llevar a cabo el programa, y establecer prioridades y calcular sus costes.
  Véase **HERRAMIENTA 6**
- Revisar el presupuesto del programa/el partenariado y añadir los gastos de seguridad que puedan faltar.
- Compartir o, si es pertinente, crear de manera conjunta un plan de gestión de riesgos de seguridad.
  Véase **HERRAMIENTA 5**

Más información:

- *GISF – Seguridad en práctica*
- *EISF – The Cost of Security Risk Management for NGOs*
- *EISF – Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*
- *EISF – Gestión de la seguridad del personal humanitario con perfiles diversos*
- *EISF – Género y Seguridad. Directrices para la transversalización del género en la gestión de riesgos de seguridad*
- *ODI-Informe de buenas prácticas 8 – Gestión de la seguridad de las operaciones en entornos violentos*

2.3.5. Gestión de viajes y apoyo

"El personal de las ONGN/L a menudo viaja a ubicaciones con más riesgos y tiene acceso a vehículos o medios de transporte menos seguros en comparación con el personal de una ONGI. Hay que tener esto en cuenta y abordarlo".

Referente de seguridad de una ONGI

A fin de llevar a cabo los programas, el personal puede tener que viajar para visitar las ubicaciones del proyecto y para asistir a reuniones y a eventos, por ejemplo. En los acuerdos de partenariado, las organizaciones copartes pueden elegir visitar las ubicaciones de la otra o sus oficinas de proyecto. Por lo tanto, ambas copartes deberían convenir en la mejor manera de gestionar los riesgos que surjan por viajar, incluso en desplazamientos en las ubicaciones del proyecto cuando estos sean pertinentes para el partenariado o en viajes que deriven del propio partenariado. Eso incluye velar por que las comunicaciones y las normas en viaje tienen en cuenta los conocimientos y el idioma locales.

El sector de la ayuda debería avanzar hacia una cultura de mismo apoyo por el mismo trabajo. Las distinciones en el apoyo que se presta al personal internacional, nacional y local, ya sea en ONGI o en ONGN/L, han de justificarse adecuadamente (p. ej., si existe una diferenciación clara en los perfiles de riesgo que se base en diagnósticos de riesgo de seguridad).

HERRAMIENTA 5. Plantilla de plan de diagnóstico conjunto de riesgos de seguridad y su gestión

Preguntas de ejemplo

5.1. ¿Cómo deberían gestionarse los riesgos de seguridad que son consecuencia del partenariado? ¿Cuáles deberían ser los requisitos mínimos para la gestión de viajes y las disposiciones de apoyo (para las visitas de campo, la estancia nocturna, los procedimientos de comunicación en viaje y otros apoyos)?

5.2. ¿El personal de ambas organizaciones recibe un apoyo equitativo en viajes y estancias en las ubicaciones del proyecto?

5.3. ¿Están de acuerdo las copartes en la política de seguridad y los procedimientos que deberían seguirse durante las visitas de las copartes y en quién mantiene el **deber de cuidado** hacia el personal visitante?

5.4. ¿El presupuesto del partenariado incluye el seguro para el personal que viaje de ambas organizaciones copartes?

5.5. ¿Se contemplan las diversas necesidades del personal que viaja en los procedimientos de viajes? Por ejemplo, un riesgo agudizado a causa de rasgos personales (género, grupo ético, capacidades, etc.).

Indicadores de ejemplo

5.1. Las copartes convienen en las disposiciones y las responsabilidades en materia de seguridad en las visitas del personal de ambas organizaciones a las oficinas y las ubicaciones de programa de la otra.

5.2. Las copartes comparten entre sí sus procedimientos de seguridad para el personal que viaja a ubicaciones pertinentes para el partenariado (p. ej., dichos procedimientos pueden incluir información sobre funciones y responsabilidades, formación y sesiones informativas, procedimientos de verificación, monitoreo de viajes, autorizaciones de viaje y procedimientos de emergencia).

5.3. Se contemplan las diversas necesidades del personal que viaja en los procedimientos de viajes, p. ej., un riesgo agudizado a causa de rasgos personales (género, grupo ético, capacidades, etc.).

Siguientes pasos en **gestión de viajes y apoyo** y más información

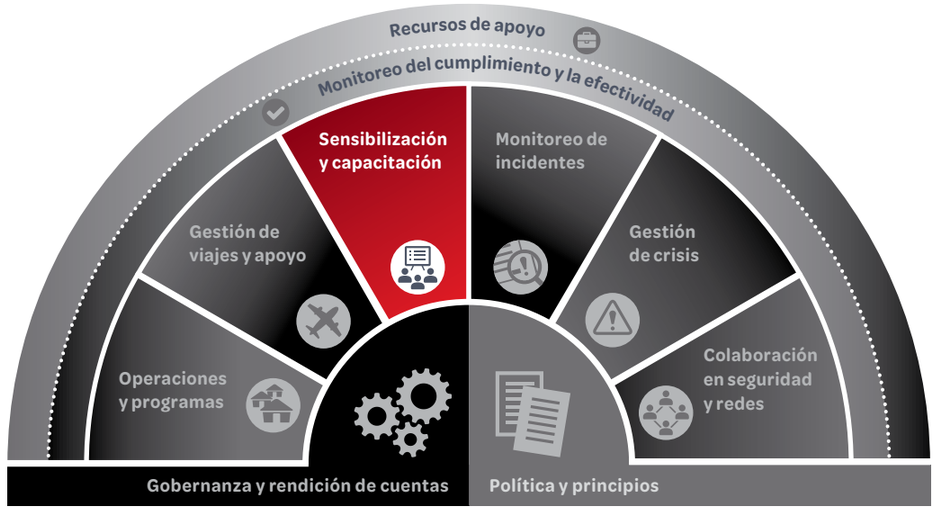
Para respaldar este proceso, las copartes también pueden considerar:

- Imaginar un escenario en el que el personal de una organización visita las oficinas o la ubicación del proyecto de una organización coparte y evaluar qué organización tiene la responsabilidad de planificar el viaje, velar por que estén activadas todas las medidas de seguridad durante el viaje, y responder en caso de que se produzca un incidente.
- Hablar de qué viajes serán necesarios para ambas copartes a fin de llevar a cabo los programas pertinentes y elaborar procedimientos/requisitos de seguridad para cada ubicación (ya sea de forma conjunta o independiente, como decidan ambas copartes).
- Consultar a la plantilla con perfiles personales diversos sobre sus experiencias al viajar y los riesgos que ambas copartes deberían contemplar para reducir los riesgos a los que se enfrenta la plantilla a causa de sus perfiles personales (Véase el apartado 5.7. Viajes, en el documento de investigación del EISF *Gestión de la seguridad del personal humanitario con perfiles diversos*).
- Tratar las medidas mínimas de seguridad para viajes, tales como sesiones informativas de seguridad, procedimientos de verificación, mantenimiento de vehículos, diagnósticos de riesgos en viaje, formación en conducción y gestión de información confidencial sobre viajes.

Más información:

- *EISF – Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*
- *EISF – Gestión de la seguridad del personal humanitario con perfiles diversos (en concreto, el Apartado 5.7. Viaje y el Capítulo 2. Deber de cuidado y contra la discriminación en el ámbito jurídico)*

2.3.6. Sensibilización y refuerzo de capacidades



Un elemento central que suele salir en los acuerdos de partenariado es el refuerzo de capacidades. Mejorar la sensibilización del personal sobre los riesgos de seguridad y su capacidad para gestionar dichos riesgos es fundamental tanto para las ONGI como para las ONGN/L, ya que asegura que el personal en cada una de las organizaciones copartes se siente empoderado para sentir como propias las decisiones y las herramientas en materia de seguridad.

Aprender es un proceso bidireccional.

Al celebrar partenariados, las organizaciones deberían tener en cuenta los puntos fuertes y los puntos débiles de cada una, y estudiar de manera conjunta cómo mejorar la sensibilización del personal sobre los riesgos de seguridad y su capacidad para gestionarlos.

No deben confundirse las diferencias en el planteamiento con la falta de capacidad.

Las copartes deberían acordar qué capacidades es más necesario fortalecer y qué formato es el mejor para sensibilizar (p. ej., formación en remoto frente a presencial, comunicaciones con el personal, etc.). Todo

fortalecimiento de capacidades debería ser lo más sostenible posible para que sea un apoyo a largo plazo de las capacidades del personal y de las organizaciones. Las copartes también pueden considerar la opción de contratar formaciones privadas o consultoras externas para que instruyan al personal, cuando proceda.

▶ *Véase el apartado 3.3. Reforzar la capacidad de gestión de riesgos de seguridad en los partenariados*

Preguntas de ejemplo

6.1. ¿Cómo identificarán las copartes las necesidades de sensibilización y de refuerzo de capacidades, y cómo las cubrirán de manera conjunta (tanto en términos de seguridad personal como de gestión de riesgos de seguridad)?

6.2. ¿Hay un acuerdo respecto a qué lagunas existen en la capacidad de gestionar riesgos de seguridad de ambas copartes y qué puede hacer cada organización para abordarlas?

6.3. ¿El presupuesto del partenariado incluye financiación para respaldar las actividades de fortalecimiento de capacidades a largo plazo?

6.4. ¿Se comparten los acuerdos de partenariado, en concreto los relativos a la gestión de riesgos de seguridad, con el personal pertinente (tanto de nueva incorporación como con antigüedad) en ambas organizaciones copartes?

6.5. ¿El personal que implementa tiene acceso a formación sobre seguridad personal, sobre todo quienes trabajan en los lugares de riesgo más elevado?

6.6. ¿El personal que implementa recibe la formación sobre seguridad en el formato correcto para satisfacer sus necesidades (p. ej., en remoto frente a presencial)?

6.7. ¿La formación cubre las necesidades a largo plazo del personal dado que se nutre de los conocimientos y las destrezas existentes y es lo más sostenible posible?

6.8. ¿El planteamiento sobre gestión de riesgos de seguridad en el partenariado está concebido para que ambas organizaciones se empoderen para abordar las necesidades de seguridad de forma independiente?

6.9. ¿Existen posibilidades de hacer mentoría a largo plazo de quienes sean referentes de seguridad dentro del partenariado?

Indicadores de ejemplo

6.1. Las copartes convienen en las necesidades relativas a la capacidad para gestionar los riesgos de seguridad.

6.2. Se cuenta con una estrategia para fortalecer, aprender y desarrollar capacidades, con un plan claro de puesta en práctica, y su finalidad es mejorar la capacidad a largo plazo de las copartes.

6.3. La organización comparte con regularidad recursos y respalda el acceso a oportunidades adecuadas y específicas del contexto para fortalecer, aprender y desarrollar capacidades en la gestión de los riesgos de seguridad con las organizaciones copartes.

Siguientes pasos en **sensibilización y refuerzo de capacidades** y más información

Para respaldar este proceso, las copartes también pueden considerar:

- Identificar a qué oportunidades de formación y de capacitación tiene acceso cada una de las copartes y cómo las pueden compartir entre ellas.
- Elaborar una lista de las necesidades de formación a largo plazo y de las maneras en las que puede abordarlas cada organización.
- Compartir recursos entre sí con regularidad (por ejemplo, páginas web, herramientas, documentos, listas de proveedores de formación, contactos locales, etc., que sean útiles).

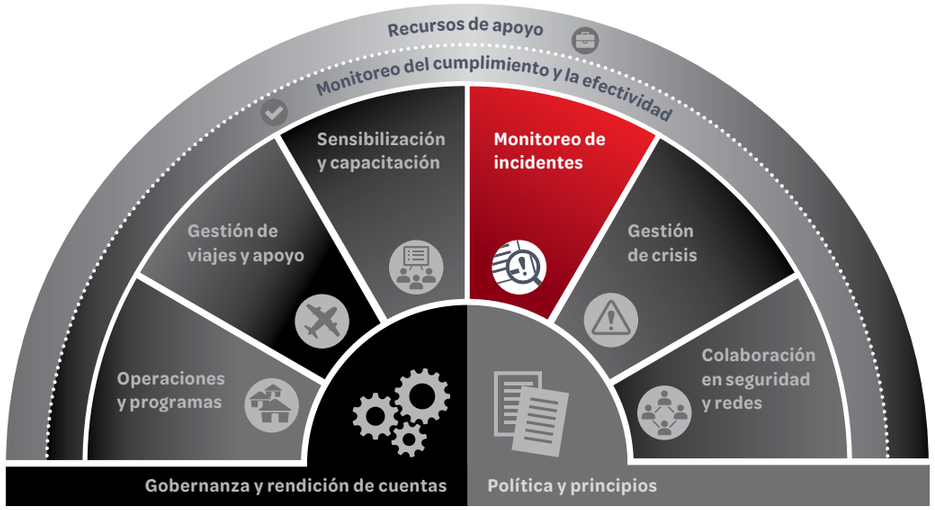
Las organizaciones y las plataformas siguientes ofrecen formación sobre seguridad personal y gestión de riesgos de seguridad:

- página web de la INSSA
- DisasterReady Platform
- UNDSS
- formación Manténgase a salvo (Stay Safe) de la FICR
- Kaya Connect

Más información:

- *EISF – Security Management and Capacity Development: International agencies working with local partners*
- *EISF – Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*

2.3.7. Monitoreo de incidentes



Informar de los incidentes y monitorearlos es un elemento fundamental de la gestión de riesgos de seguridad ya que permite entender mejor el contexto operativo y los riesgos de seguridad a los que se enfrentan las organizaciones y su personal. Dicho conocimiento puede servir para fundamentar la toma de decisiones en toda una organización, lo que incluye operaciones, programas, finanzas, incidencia y gestión de riesgos de seguridad.

Todas las organizaciones experimentan incidentes de seguridad. Las copartes que tengan mejores sistemas de información entenderán mejor los riesgos de seguridad a los que se enfrenta su personal y a través de ello podrán reducir la posibilidad de incidentes futuros.

Los partenariados se fortalecen cuando las organizaciones comparten información sobre incidentes que puedan afectarles y afectar al partenariado en su conjunto. Un desafío clave para informar de incidentes y compartirlos es la falta de confianza, ya sea dentro de una organización con personal que teme informar de incidentes o entre organizaciones copartes que temen que compartir información sobre incidentes pueda afectar al partenariado, a su reputación y a la financiación. Para que haya una mejor información internamente en las organizaciones y entre las copartes, deben establecerse mecanismos de información sólidos y confidenciales que aborden las preocupaciones en torno a la privacidad y las sanciones.

Las copartes deberían mostrar transparencia recíproca y con su personal sobre cómo se utilizará la información que se reciba sobre incidentes y cómo se mantendrá su confidencialidad.

▶ *Véase el apartado 1.4. Comunicar y generar confianza en los partenariados*

Preguntas de ejemplo

7.1. ¿Cómo deberían compartir las copartes información sobre incidentes entre ellas?

7.2. ¿Cómo pueden respaldarse mutuamente las copartes en la gestión de información sobre incidentes de seguridad? Por ejemplo, con procedimientos para informar de incidentes, sistemas para registrarlos y herramientas para analizar los datos sobre incidentes y utilizarlos para fundamentar las decisiones sobre seguridad, programas, operaciones, incidencia, finanzas, etc.

7.3. ¿A qué datos sobre incidentes de seguridad en la ubicación pertinente tiene acceso cada organización, ya sea por sus propias operaciones o a través de sus redes, que pueda compartir con su coparte de manera periódica?

7.4. ¿Cómo pueden abordar ambas copartes el problema de que no se informe de todo lo debido?

7.5. ¿Existe un acuerdo sobre qué tipos de incidentes reportar?

7.6. ¿Cómo se pueden respaldar las copartes para fortalecer la confidencialidad de los mecanismos de información para proteger al personal y también para evitar que la información caiga en manos de partes o autoridades hostiles (p. ej., soluciones tecnológicas y orientaciones sobre buenas prácticas)?

Indicadores de ejemplo

7.1. Se dispone de un proceso para gestionar y compartir información relativa a seguridad para el contexto operativo, incluso datos sobre incidentes, entre las copartes, y ambas lo respetan.

7.2. Existe un acuerdo sobre cómo se utilizan los datos sobre incidentes para fundamentar la toma de decisiones, donde se incluye una política

clara sobre si han de adoptarse medidas disciplinarias a raíz de que se informe o se deje de informar de incidentes.

7.3. La organización revisa de manera periódica los incidentes que afectan a su personal para identificar las tendencias y las preocupaciones respecto a incidentes de seguridad, y lo comparte con las organizaciones copartes.

Siguientes pasos en **monitoreo de incidentes** y más información

Para respaldar este proceso, las copartes también pueden considerar:

- Compartir y revisar de forma conjunta los procedimientos existentes y los mecanismos internos para informar de incidentes.
- Nombrar a una persona referente para la información sobre incidentes.
- Establecer una forma de compartir información sobre incidentes entre ellas.
- Formar al personal sobre cómo informar de incidentes, gestión de información y confidencialidad (véase, por ejemplo, las guías móviles de DisasterReady que aparecen en la lista más abajo).
- Analizar de qué tipos de incidentes ha de informarse y qué repercusiones podrían tener sobre el partenariado determinados tipos de incidentes.

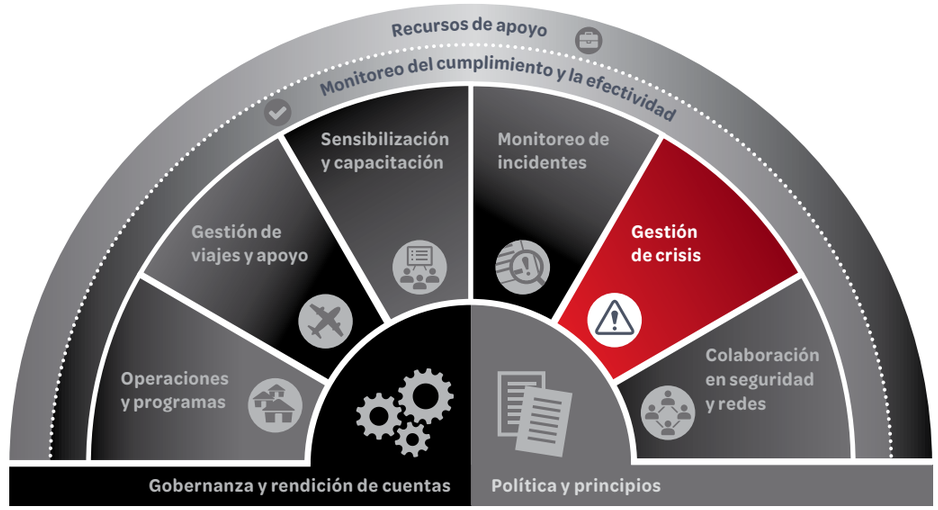
Las plataformas siguientes recopilan y comparten datos en abierto sobre incidentes de múltiples organizaciones:

- Aid Worker Security Database – Humanitarian Outcomes
- Proyecto Aid in Danger project – Insecurity Insight
- INSO Key Data Dashboard

Más información y recursos:

- *RedR UK, Insecurity Insight y EISF – Manual de gestión de la información sobre incidentes de seguridad*
- *DisasterReady Safety and Security Incident Information Management (SIIM) mobile guide for organisations*
- *DisasterReady Safety and Security Incident Information Management (SIIM) mobile guide for staff*

2.3.8. Gestión de crisis



Las organizaciones que operan en contextos de riesgo elevado tienen más probabilidades de experimentar un incidente grave que no se puede gestionar mediante procedimientos organizacionales normales. Este tipo de incidentes (que se suelen designar como "crisis" o "incidente crítico") podrían ser, por ejemplo, el fallecimiento, el secuestro o la detención de alguien del personal (a consecuencia de **amenazas** tanto externas como internas). Una crisis también podría ser un acontecimiento que, por su gravedad, tenga consecuencias importantes para la organización. Las organizaciones con sistemas maduros de gestión de riesgos de seguridad tendrán una forma especializada de responder a una crisis (a veces denominada "estructura de gestión de crisis").

Si bien las crisis son excepcionales, las copartes deberían estar preparadas, de todas maneras, para esa eventualidad y convenir de antemano en la mejor manera de gestionar un incidente así de grave. Las copartes deberían contemplar qué organización estaría en mejor lugar para responder en caso de que se produzca una crisis que afecte al partenariado (p. ej., en términos de logística, acceso y pericia).

La gestión de crisis es un tema complejo que en esta guía se trata de una manera muy breve. Se alienta a las copartes a consultar recursos adicionales sobre cómo gestionar una crisis (véase la parte de "Más información" al final del apartado).

Preguntas de ejemplo

8.1. ¿Cómo colaborarán/se coordinarán las copartes si se produce una crisis o un incidente crítico que afecte a alguna de las organizaciones en la ubicación pertinente?

8.2. Si se produce una crisis o un incidente crítico y afecta a ambas copartes, ¿quién debería encabezar la respuesta de gestión de crisis? ¿Cuáles son las responsabilidades y quién tiene autoridad para tomar decisiones?

8.3. ¿Qué apoyo puede proporcionar cada coparte a la otra si alguna de las organizaciones experimenta un incidente crítico en la ubicación del partenariado?

8.4. ¿Las copartes deberían incluir a personal de cada una de las organizaciones en un sistema rápido para compartir información sobre seguridad para velar por que el personal en la ubicación afectada esté bien y que se cuente con él en caso de crisis o incidente crítico?

8.5. ¿Se dispone de procedimientos para evaluar tras el incidente y para analizar dentro del partenariado a fin de entender qué ha sucedido y posiblemente mitigar que se vuelva a producir?

8.6. ¿Qué acceso a seguros tienen ambas copartes si se produce una crisis o un incidente crítico?

Sistema rápido para compartir información sobre seguridad

En caso de un incidente de seguridad o de un cambio repentino en el contexto de seguridad, las organizaciones deben contar con un proceso para comunicar rápidamente las noticias a toda la organización –y, si hay acuerdo de partenariado, entre organizaciones– sin sobrecargar a ninguna persona en concreto. Ese proceso a veces se denomina **árbol de seguridad**, que consiste en asignar a cada integrante del personal un número reducido de personas a las que es responsable de llamar en caso de emergencia. Como alternativa, las organizaciones pueden utilizar plataformas de mensajería masiva, como WhatsApp, para compartir información de seguridad con un gran número de personas de forma rápida (cualquier método de este tipo debe tener en cuenta las cuestiones de seguridad digital).

Indicadores de ejemplo

8.1. Se han acordado las responsabilidades y la autoridad para tomar decisiones en caso de crisis o de incidente crítico que afecte a ambas copartes. Lo idóneo sería que eso constase por escrito o estuviera plasmado de una forma visual (p. ej., en un diagrama de flujo).

8.2. Las copartes disponen de una estructura y de un plan de gestión de crisis.

8.3. Las copartes tienen acceso a servicios de apoyo de emergencia (tanto médicos como no médicos) dentro de la cobertura del seguro de cada una de las organizaciones.

Siguientes pasos en **gestión de crisis** y más información

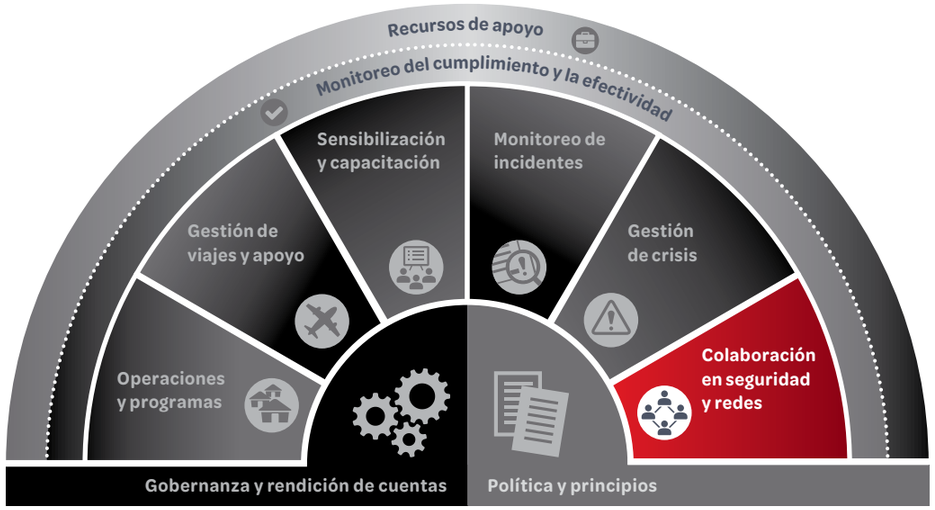
Para respaldar este proceso, las copartes también pueden considerar:

- Convenir en un sistema de comunicaciones en caso de crisis.
- Crear un equipo de gestión de crisis que incluya a personal de ambas organizaciones y que se pueda activar en caso de crisis.
- Realizar simulacros de crisis.
- Analizar las opciones de seguros para prepararse para una crisis o un incidente crítico.
- Prepararse para una crisis al consultar y compartir recursos sobre cómo gestionar de manera eficaz crisis e incidentes críticos (véase la lista de recursos más abajo).

Más información:

- *EISF – Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*
- *EISF – Crisis Management of Critical Incidents*
- *EISF – Gestión de la violencia sexual contra el personal humanitario*

2.3.9. Colaboración y redes en materia de seguridad



Colaborar en cuestiones de seguridad con otras organizaciones que operan en el mismo contexto no solo refuerza la gestión de riesgos de seguridad de una organización, sino que mejora la seguridad colectiva de todas. Las colaboraciones deberían ir más allá de las organizaciones copartes e incluir la interacción activa con redes y foros para compartir información en distintos ámbitos, entre ellos, el local o comunitario, nacional, regional e internacional.

Ambas copartes deberían contemplar cómo pueden respaldar las redes donde se tratan cuestiones de seguridad.

Ejemplo de colaboración en materia de seguridad

El Grupo de Trabajo sobre Acceso Humanitario liderado por la OCHA para el noroeste de Siria está formado por varias ONGN/L, ONGI y agencias internacionales, y es un buen ejemplo de un partenariado exitoso en gestión de riesgos de seguridad, con efectos positivos sobre la situación de riesgos de seguridad de organizaciones que operan en el contexto. Por ejemplo, la plataforma ha permitido que las ONGN/L planteen cuestiones comunes que les preocupan sin tener que exponer

continuación

Ejemplo de colaboración en materia de seguridad *continuación*

sus **vulnerabilidades** como organizaciones individuales ante donantes u organizaciones copartes, lo que fomenta que se hable de una manera más abierta y sincera al tiempo que se protege a las ONGN/L de toda repercusión negativa que dichas conversaciones pudieran tener sobre su reputación o sus oportunidades de financiación.

Las copartes deberían apoyarse mutuamente para acceder a las colaboraciones y a las redes necesarias en materia de seguridad que les ayudarán a mejorar la seguridad de su personal. A veces para eso es necesario hacer incidencia con otras organizaciones.

▶ *Véase la Parte 4 para saber más sobre incidencia en cuestiones de gestión de riesgos de seguridad*

Preguntas de ejemplo

9.1. ¿Existen plataformas que traten temas de seguridad en el contexto pertinente? Si la respuesta es afirmativa, ¿tienen acceso ambas copartes y una voz igual en esas redes y plataformas de coordinación en sus áreas operativas, incluso en las plataformas para compartir información sobre seguridad?

9.2. ¿Cuáles son los obstáculos y los desafíos que impiden la participación activa de ambas copartes en los foros, las reuniones y las conversaciones interinstitucionales sobre seguridad en los ámbitos local, nacional, regional e internacional?

9.3. ¿Qué acciones puede emprender cada una de las organizaciones que faciliten la inclusión de su coparte en esas conversaciones?

9.4. ¿Qué acciones puede emprender cada una de las copartes de manera individual y colectiva para mejorar la colaboración en materia de seguridad con otras organizaciones –tanto nacionales como internacionales– en la zona operativa?

Indicadores de ejemplo

9.1. Ambas copartes participan activamente en foros, plataformas, reuniones y consorcios sobre gestión de riesgos de seguridad, y comparten información sobre seguridad con otras en los ámbitos local, nacional, regional o internacional.

9.2. Ambas organizaciones promueven y facilitan que participen sus copartes, cuando sea posible, en foros, plataformas, reuniones y

conversaciones interinstitucionales para fortalecer que se comparta información y la colaboración en materia de seguridad. Eso incluye compartir con las copartes los datos de contacto de partes pertinentes que puedan proporcionar apoyo en la gestión de riesgos de seguridad.

Ejemplos de plataformas de coordinación donde se habla de seguridad

- *Saving Lives Together (SLT)*
- *International NGO Safety Organisation (INSO)*
- *MENA Region Humanitarian Safety and Security Forum*
- *South Sudan NGO Forum*

Siguientes pasos en **colaboración y redes en materia de seguridad** y más información

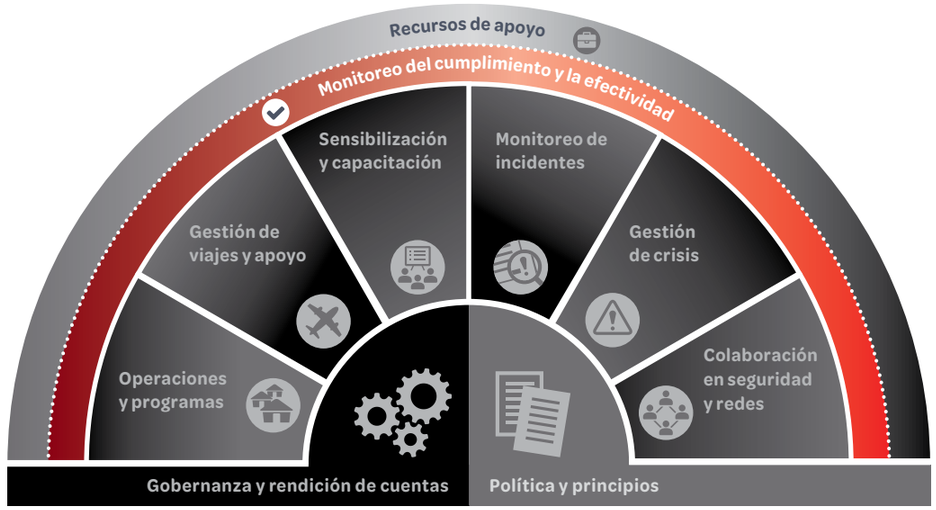
Para respaldar este proceso, las copartes también pueden considerar:

- Introducir a sus copartes en las plataformas de colaboración en materia de seguridad pertinentes.
- Tratar y abordar los obstáculos a que ambas copartes participen de manera activa en las plataformas existentes.
- Ponerse en contacto con las plataformas de colaboración en materia de seguridad e identificar a una persona referente dentro de la organización que se encargue de interactuar con regularidad con dichas plataformas.
- Crear redes de colaboración en materia de seguridad donde no existan e invitar a participar a un abanico de organizaciones distintas.

Más información:

- *RedR UK, Insecurity Insight y EISF – Manual de gestión de la información sobre incidentes de seguridad*
- *EISF – Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*
- *GISF – Partenariados y gestión de riesgos de seguridad: desde la perspectiva de la coparte local*

2.3.10. Monitoreo de cumplimiento y eficacia



"El cumplimiento tiene que ver con mantener el planteamiento sobre seguridad de la organización (lo que vela por sus viabilidad y sostenibilidad a largo plazo), así como con supervisar dicho planteamiento".

Referente de seguridad de una ONGI

Las organizaciones deberían supervisar y revisar su **marco de gestión de riesgos de seguridad** para asegurarse de que el personal está cumpliendo los procedimientos y de que el enfoque de la organización sobre seguridad sigue siendo el adecuado para cumplir su propósito. En los acuerdos de partenariado, eso también implica velar por que cada una de las copartes está cumpliendo las responsabilidades en las que ha convenido respecto a la gestión de riesgos de seguridad en el partenariado.

Preguntas de ejemplo

10.1. ¿Cómo deberían revisar ambas copartes con regularidad la gestión de riesgos de seguridad dentro del partenariado?

10.2. ¿Qué grado de supervisión del cumplimiento y de la eficacia en lo respectivo a la gestión de riesgos de seguridad dentro de cada organización o en el partenariado es aceptable para ambas copartes?

10.3. ¿Cuánta información quieren compartir entre sí las copartes respecto a lecciones aprendidas, revisiones, auditorías de seguridad y análisis tras el incidente que haga referencia al contexto, al partenariado o a un proyecto concreto?

10.4. ¿El proceso de cumplimiento supone una sobrecarga irrazonable para alguna de las copartes?

10.5. ¿Las expectativas sobre cumplimiento y eficacia son coherentes con la capacidad? ¿Este monitoreo complementa un monitoreo relativo al partenariado que llevan a cabo otros departamentos, como el financiero?

10.6. ¿Existen ya procesos de gestión con la finalidad de supervisar y revisar en el partenariado donde se pueda integrar la gestión de riesgos de seguridad?

10.7. ¿Qué acciones pueden emprender ambas copartes para establecer y hacer cumplir una cultura disciplinaria sólida dentro de sus organizaciones hacia el incumplimiento de las políticas y los requisitos mínimos de seguridad?

Indicadores de ejemplo

10.1. Ambas copartes comparten y hablan de las conclusiones de las lecciones aprendidas, las revisiones, los análisis tras incidentes y las auditorías de seguridad relativas al contexto, al partenariado o al proyecto/programa.

10.2. Las personas responsables de supervisar la puesta en práctica del sistema de seguridad y su cumplimiento (tanto dentro de cada organización como dentro del partenariado) tienen la formación adecuada, participaron en la **revisión conjunta de la GRS**, y dichas responsabilidades constaban de manera expresa en la descripción de su puesto.

10.3. Los sistemas de gestión de desempeño del personal hacen mención explícita de las responsabilidades de seguridad y del cumplimiento de las políticas de la organización.

Siguientes pasos en **monitoreo de cumplimiento y eficacia** y más información

Para respaldar este proceso, las copartes también pueden considerar:

- Crear una lista de comprobación (por ejemplo, Herramienta 3 – Lista de comprobación para la revisión de documentos, en la guía Auditorías de seguridad de EISF).
- Utilizar los mecanismos de cumplimiento existentes que las copartes puedan estar usando ya para otros partenariados a fin de evitar duplicar esfuerzos/información.

Más información:

- *EISF – Auditorías de seguridad*
- *EISF – Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*

2.3.11. Recursos de apoyo

"Las ONGI tienen la responsabilidad de respaldar a sus copartes ONGN/L en la gestión de riesgos de seguridad".

Referente de seguridad de una ONGN/L

Todo el personal debería tener acceso a orientaciones, herramientas y otros recursos que respalden sus esfuerzos para gestionar riesgos de seguridad como parte de su trabajo. La mayoría de los recursos sobre gestión de riesgos de seguridad están disponibles en línea de manera gratuita y en diversos idiomas (*véase más adelante en este apartado el cuadro de Más información*).

Ambas copartes deberían compartir de manera proactiva recursos sobre gestión de riesgos de seguridad dentro del partenariado.

Las copartes deberían aumentar el acceso de todo su personal a recursos de apoyo al ponerlos a disposición sin conexión, en otros formatos que el escrito y traducidos a los idiomas pertinentes.

Preguntas de ejemplo

11.1. ¿Los recursos de apoyo sobre gestión de riesgos de seguridad están disponibles y son accesibles para todo el personal? Y, si no es así, ¿qué acciones se pueden emprender para mejorar la accesibilidad?

11.2. ¿Las copartes han compartido entre ellas sus recursos respectivos sobre gestión de riesgos de seguridad?

11.3. ¿Qué otros recursos podrían aprovechar las copartes para gestionar riesgos de seguridad?

Indicadores de ejemplo

11.1. Se comparten periódicamente recursos sobre gestión de riesgos de seguridad que satisfacen las necesidades de todo el personal pertinente de las copartes y en un formato accesible.

11.2. Las copartes ponen a disposición una serie de orientaciones, herramientas y plantillas como parte de una biblioteca de seguridad que les sirva mutuamente para gestionar los riesgos de seguridad.

Siguientes pasos en **recursos de apoyo** y más información

Para respaldar este proceso, las copartes también pueden considerar:

- Compartir entre sí recursos de seguridad y tratarlos para velar por que se entienden.
- Adaptar los recursos para que sean más accesibles (p. ej., visualización de los procesos de toma de decisiones, traducciones a los idiomas pertinentes, etc.).

Más información:

- *EISF – Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas (disponible también en inglés, francés y árabe)*
- *página web de GISF Library*
- *GISF Training hub*
- *Recursos y formación de DisasterReady (disponibles en varios idiomas)*

2.4. Elaborar y poner en práctica un plan de acción de revisión conjunta de la GRS

Después de rellenar el cuestionario y evaluar los indicadores, el último paso en la **revisión conjunta de la GRS** es abordar los indicadores

parciales o ausentes, lo que puede hacerse mediante la elaboración y la puesta en práctica de un **plan de acción de revisión conjunta de la GRS**. Ambas organizaciones deben llevar a cabo el plan de acción conjunto y acordar un calendario de seguimiento periódico.

El objetivo de este plan de acción es mejorar la coordinación entre las copartes en torno al sistema de gestión de riesgos de seguridad dentro del partenariado (es, por tanto, una "herramienta de gestión del partenariado", no una "herramienta de gestión de riesgos de seguridad".

Los indicadores que se consideren presentes en el ejercicio de evaluación no es necesario incluirlos en el plan de acción.

Esta guía presenta una **plantilla de plan de acción para la revisión conjunta de la GRS** que puede ayudar a las copartes a registrar la situación de cada indicador, las funciones y responsabilidades, los objetivos clave y el calendario de aplicación. Las copartes pueden adaptar la plantilla para que les sirva para conversar y monitorear las acciones que emprendan como parte de la revisión conjunta de la GRS.

HERRAMIENTA 4. Plantilla de plan de acción para la revisión conjunta de la GRS

El plan de acción de la revisión conjunta de la GRS frente a un plan de gestión de riesgos de seguridad

El "**plan de acción para la revisión conjunta de la GRS**" que se presenta en esta guía se refiere específicamente a una lista de comprobación de tareas que ambas copartes acuerdan poner en práctica como parte del proceso de revisión conjunta de la GRS que se propone en esta guía.

Dentro de cada organización puede haber un "plan de gestión de riesgos" separado (a veces denominado "plan de gestión de riesgos de seguridad", "plan de gestión de la seguridad" o "plan de seguridad"), que se refiera específicamente a las medidas que debe adoptar una organización para gestionar los riesgos de seguridad identificados (por ejemplo, cómo gestionar el riesgo de robo o de detención).

▶ *Véase el apartado 3.1. Identificar y abordar conjuntamente los riesgos de seguridad*

3 Identificar y abordar conjuntamente las necesidades, las lagunas y los desafíos de la GRS

3.1. Identificar y abordar conjuntamente los riesgos de seguridad

Compartir la responsabilidad de los riesgos de seguridad implica que las copartes exploren juntas los diferentes tipos de riesgos de seguridad a los que están expuestas y el impacto que pueden tener en ambas organizaciones y en su personal. También significa que identifican y llevan a cabo de manera conjunta acciones para gestionar los riesgos de seguridad.

Compartir la responsabilidad de los riesgos de seguridad es la base de un enfoque equitativo de la gestión de los riesgos de seguridad dentro de un partenariado.

Para compartir los riesgos, las copartes deben primero tener un entendimiento común de los riesgos que les afectan a ellas y al partenariado. Para ello deben conversar y estudiar las percepciones de cada coparte sobre los riesgos de seguridad a los que se enfrentan y su actitud al respecto. La conversación debe permitir a ambas organizaciones explicar lo que entienden por "probabilidad" e "impacto" en la práctica, para asegurarse de que tienen una comprensión similar de cómo describir los grados de riesgo a los que se enfrentan. Una vez hecho esto, las copartes pueden hablar desde una base común de lo que perciben como un grado aceptable de riesgos.

HERRAMIENTA 2. Actitud hacia el riesgo en partenariados

Las copartes también deberían comprender y abordar juntas las cuestiones derivadas de la transferencia de riesgos de seguridad dentro

del partenariado. Un riesgo de seguridad al que se enfrenta una coparte puede afectar con facilidad a la otra coparte y al partenariado en su conjunto. Al identificar conjuntamente los riesgos y acordar cómo abordarlos, las copartes combinan su capacidad y conocimientos para reducir la probabilidad de que se produzca un incidente y mejorar la capacidad de la otra para gestionar un incidente en caso de que se produzca.

Por ejemplo, durante la realización de un proyecto en el marco del partenariado, la ONGN/L que implementa puede enfrentarse al riesgo de un accidente de tráfico. Un incidente de este tipo no solo afectará directamente al personal de la ONGN/L, sino que también afectará al presupuesto del partenariado, a la capacidad de ambas copartes para cumplir los objetivos de su programa y a la reputación de ambas. Para mitigar el riesgo de un accidente de tráfico, la ONGN/L puede, por ejemplo, ayudar a su coparte ONGI a entender la probabilidad de que ocurra un incidente de tráfico y por qué el riesgo puede ser elevado (por ejemplo, carreteras inseguras, vehículos no seguros). A su vez, la ONGI puede, por ejemplo, apoyar a los conductores de la ONGN/L para que accedan a formación sobre conducción segura o proporcionar financiación adicional para que la ONGN/L compre vehículos más seguros.

Es fundamental llevar a cabo un diagnóstico conjunto de riesgos de seguridad para comprender el apoyo que necesitan las copartes y elaborar medidas de mitigación adecuadas. El diagnóstico conjunto de riesgos de seguridad puede realizarse en el ámbito global para considerar los riesgos generales derivados del partenariado o en el ámbito nacional para considerar los riesgos específicos del contexto. Dicho diagnóstico puede utilizarse para elaborar un plan de gestión de riesgos de seguridad en común para mitigar los riesgos identificados. Esta guía presenta una plantilla de diagnóstico conjunto de riesgos de seguridad y su gestión para ayudar a las copartes a realizar este ejercicio.

HERRAMIENTA 5. Plantilla de plan de diagnóstico conjunto de riesgos de seguridad y su gestión

Un diagnóstico común de los riesgos de seguridad y la "revisión conjunta de la GRS" más amplia pueden, además, poner de manifiesto otras necesidades, lagunas y desafíos en la GRS, como los relacionados con la financiación y la capacidad. Estos desafíos se analizan en mayor profundidad en los apartados siguientes.

Más información

- *EISF – Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*
- *GISF – Seguridad en práctica*

3.2. Financiación de la gestión de riesgos de seguridad en los partenariados

Los costes de la gestión de los riesgos de seguridad deben contemplarse lo antes posible; sería idóneo hacerlo antes de que comiencen las actividades del programa, para garantizar que ambas copartes disponen de la financiación necesaria para llevar a cabo las actividades del proyecto de forma segura.

La financiación de la gestión de riesgos de seguridad es esencial para que el personal pueda llegar con seguridad a las comunidades a las que pretende ayudar. Por desgracia, el personal de las ONGN/L se enfrenta a menudo a obstáculos que le dificulta pedir financiación adicional en los acuerdos de partenariado, y las partidas presupuestarias relacionadas con la seguridad son las más propensas a quedar fuera cuando hay presiones para recortar costes. Las copartes ONGI pueden abordar algunos de estos retos iniciando conversaciones sobre la financiación de la gestión de los riesgos de seguridad con las ONGN/L, en lugar de esperar a que les llegue una solicitud de financiación.

Las copartes deben apoyarse mutuamente para identificar, solicitar y hablar con sinceridad sobre las necesidades de financiación para la GRS, ya que es una condición para programar y cumplir bien el deber de cuidado de las organizaciones.

Los costes de la gestión de riesgos de seguridad incluyen cualquier gasto relacionado con reducir el potencial de daños y perjuicios para la organización y su personal, o con indemnizar por daños y perjuicios efectivos. Entre los ejemplos de costes pueden estar:

- la elaboración y la puesta en práctica de políticas y procedimientos;
- los salarios de las personas que sean referentes de seguridad;
- las actividades de formación y sensibilización en materia de seguridad;
- la realización de **diagnósticos de riesgos de seguridad**;
- la respuesta a incidentes, incluida la suspensión o el cierre del programa;

- los seguros;
- los equipos de apoyo a la seguridad, incluidas las comunicaciones;
- proporcionar elementos físicos de seguridad, incluso puertas, cerraduras, etc.;
- los servicios de bienestar y apoyo psicosocial para el personal.

HERRAMIENTAS 3 Y 4. La plantilla de trabajo y el cuestionario de revisión conjunta de la GRS, y la plantilla de plan de acción para la revisión conjunta de la GRS pueden ayudar a las copartes a considerar las lagunas de financiación y a identificar formas de cubrir los costes de la GRS de forma más amplia dentro del partenariado

HERRAMIENTA 5. La plantilla de plan de diagnóstico conjunto de riesgos de seguridad y su gestión puede utilizarse como base para calcular el coste de la gestión de los riesgos de seguridad dentro de un partenariado respecto a los riesgos de seguridad identificados

Si la financiación es insuficiente para gestionar adecuadamente los riesgos de seguridad a los que el personal está expuesto, las copartes deben reconsiderar el proyecto o programa en función del umbral de riesgo que hayan acordado.

Investigaciones anteriores del GISF han revelado que la mayoría de los donantes internacionales están abiertos a que se incluyan los costes de gestión de los riesgos de seguridad en los presupuestos de los proyectos. Es imprescindible que las propuestas de proyectos del partenariado incluyan el presupuesto necesario para gestionar los riesgos de seguridad, lo que se demostrará mediante **diagnósticos de riesgos de seguridad** específicos para el contexto. Quienes redacten las propuestas deben conocer la postura del donante correspondiente en materia de políticas sobre la financiación de la gestión de los riesgos de seguridad, así como las necesidades de su propia organización y de las copartes en lo que respecta a eso, de modo que las actividades de gestión de los riesgos de seguridad diagnosticadas cuenten con los recursos adecuados.

HERRAMIENTA 6. Plantilla de presupuesto de gestión de riesgos de seguridad en partenariados

Si resulta problemático incluir los costes de seguridad en las propuestas, quienes gestionen las subvenciones, el personal de programas y las personas que lideren las organizaciones deberían abogar ante los donantes para que se incluyan los costes de seguridad.

Véase el apartado 4.2.3. Incidencia y financiación relativas a la gestión de riesgos de seguridad

Más información

- *EISF – The Cost of Security Risk Management for NGOs*
- *GISF – Partenariados y gestión de riesgos de seguridad: desde la perspectiva de la coparte local*

3.3. Reforzar la capacidad de gestión de riesgos de seguridad en los partenariados

"Todo el personal debe saber cómo debe gestionar riesgos de seguridad como parte de su puesto".

Referente de seguridad

Las investigaciones del GISF han mostrado que existe una percepción errónea generalizada de que los conocimientos y la pericia sobre gestión de riesgos de seguridad —y sobre muchos otros aspectos de la prestación de ayuda— residen en las ONGI. A menudo se percibe la "capacitación" del personal de las ONGN/L como una necesidad por defecto y puede seguir el modelo de formaciones o sesiones informativas sobre seguridad de uno o dos días. Si bien cada ONGN/L será diferente, esa visión no representa las capacidades de muchas ONGN/L en el sector de la ayuda.

Las investigaciones han indicado que las ONGN/L/ demuestran amplias competencias en:

- establecer y mantener la aceptación, por ejemplo, preservando la calidad y las relaciones a largo plazo con la población beneficiaria;
- coordinación y negociación;
- analizar y comprender el contexto local (incluida la dinámica de la comunidad, los conflictos y la política locales);
- interactuar con las personas afectadas y comprenderlas, así como sus necesidades y aspiraciones.

Las copartes internacionales no deben suponer que una ONGN/L carece de ideas y de acciones en materia de seguridad solo porque no tenga normas escritas o el mismo enfoque de gestión de riesgos de seguridad. Del mismo modo, solo porque las ONGN/L conozcan bien el contexto local, no se puede asumir que no experimentan riesgos de seguridad o que tienen la capacidad necesaria para gestionarlos. Y, por otro lado, las ONGN/L no deben dar por sentado que las ONGI tienen toda la capacidad, los conocimientos o los recursos necesarios para gestionar con eficacia los riesgos de seguridad. Las ONGI a menudo dependen de los conocimientos y de las formas de trabajo locales para operar con seguridad en contextos de riesgo elevado.

Las copartes deben comenzar por identificar las capacidades que existen dentro del partenariado y acordar las áreas de capacidades que necesitan refuerzo. Se puede obtener una panorámica de las necesidades y las carencias mediante la **revisión conjunta de la GRS**.

▶ *Véase la Parte 2. Llevar a cabo una revisión conjunta de la gestión de riesgos de seguridad*

En el caso de partenariados a largo plazo, se recomienda adoptar enfoques más detallados para fortalecer la capacidad de gestión de riesgos de seguridad. Existen varias herramientas que pueden apoyar esa iniciativa.

Más información

- La herramienta *Duty of Care Maturity Model Tool* de cinfo puede ayudar a las organizaciones a medir su madurez con respecto a las áreas clave relacionadas con el cumplimiento del **deber de cuidado** y la mejora de la gestión de riesgos de seguridad.
- En el anexo 1 de *Security Management and Capacity Development: International agencies working with local partners* del EISF se ofrece una herramienta simplificada para diagnosticar el grado de seguridad de las copartes.

En las conversaciones sobre fortalecimiento de capacidades, las copartes deben buscar la complementariedad de los distintos enfoques de gestión de riesgos de seguridad y aprovechar lo que ya existe y es eficaz para gestionar los riesgos de seguridad. Parte de esta conversación implica debatir qué oportunidades de desarrollo existen ya.

"Algunas de nuestras copartes... ya están recibiendo capacitación de otros agentes; hablar de esto ayuda a evitar que se dupliquen recursos. También puede indicar dónde podría haber intereses compartidos entre un grupo de partes para trabajar juntas en una labor específica (por ejemplo, formación colectiva)".

Referente de seguridad de una ONGI

Los esfuerzos por fortalecer las capacidades de gestión de riesgos de seguridad deben ser lo más sostenibles posible y perdurar más allá del propio partenariado.

Entre las actividades para fortalecer capacidades pueden estar:

- Proporcionar información y recursos sobre seguridad, y asegurarse de que son accesibles para el personal que los necesita (por ejemplo, considerar si es necesario traducirlos u ofrecerlos en un formato no escrito).
- Impartir formación en materia de seguridad que satisfaga las necesidades del personal, ya sea formación por parte de las ONGN/L para sus copartes internacionales sobre el contexto local y las estrategias de seguridad eficaces, o que las ONGI proporcionen al personal de las ONGN/L formación en materia de seguridad adecuada al contexto (incluido el apoyo para que el personal de las ONGN/L acceda a los cursos de formación en materia de seguridad personal interinstitucionales regionales o nacionales).
- Adoptar un "enfoque de formación de formadores" para garantizar que el personal formado tenga la capacidad de transmitir los conocimientos y recursos adquiridos.
- Integrar la experiencia en las organizaciones copartes. Por ejemplo, al enviar a personal de una organización coparte a la otra, para fomentar un intercambio en profundidad de información, conocimientos y formas de trabajo.
- Desarrollar programas formales de mentoría entre las personas que sean referentes de seguridad de ambas organizaciones o con mentores externos al partenariado (véase la INSSA, por ejemplo, en otros recursos más adelante).
- Colaborar con otras organizaciones, tanto internacionales como locales, para compartir recursos que apoyen el fortalecimiento de las capacidades de seguridad, incluido impartir formación interinstitucional en materia de seguridad directamente o a través

de terceras partes, por ejemplo, consultoras independientes o quienes proporcionen formación sobre seguridad.

Cabe destacar la importancia de que las copartes supervisen y evalúen las iniciativas para fortalecer capacidades a corto y largo plazo. Eso puede realizarse mediante la revisión periódica del plan de acción para la revisión conjunta de la GRS.

HERRAMIENTA 4. Plantilla de plan de acción para la revisión conjunta de la GRS

Adaptar las actividades de fortalecimiento de capacidades a causa de factores externos

Los factores ambientales y de seguridad pueden dificultar que se realicen las actividades para fortalecer capacidades. Los planteamientos han ser flexibles y adaptarse a unas circunstancias que cambian con rapidez. Las organizaciones deben ser creativas y atender las necesidades del personal más vulnerable.

El problema de que "te roben" el personal

Un desagradable efecto secundario de las iniciativas para fortalecer capacidades puede ser que el personal local se vuelva más atractivo para otras organizaciones, generalmente ONGI, que pueden ofrecer un salario más alto. Para las ONGN/L puede ser un desafío competir con las ONGI como empleadoras, especialmente si carecen de financiación estructural, y eso puede afectar a su capacidad para retener a un equipo central fuerte.

Esta cuestión ha de hablarse entre las copartes y es un tema dentro de la agenda de **localización** más amplia. La Charter4Change, que ha sido respaldada por varios centenares de organizaciones, espera que las firmantes identifiquen y apliquen una compensación justa (como el pago de una cuota de captación) a una organización local si contratan a su personal en un entorno humanitario.

Más información

- *EISF – Security Management and Capacity Development: International agencies working with local partners (en concreto, el anexo 1)*
- *EISF – Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*
- *ODI – From the Ground Up*
- *GISF – Partenariados y gestión de riesgos de seguridad: desde la perspectiva de la coparte local*
- *GISF – Developing a 'COVID-19 Secure' HEAT course*
- *página web del GISF – training hub*
- *ICRC – Safer Access Framework*

Las plataformas siguientes proporcionan de manera gratuita formación personal sobre gestión de riesgos de seguridad:

- *página web de la INSSA*
- *DisasterReady Platform*
- *UNDSS*
- *formacion Mantengase a salvo (Stay Safe) de la FICR*
- *Kaya Connect*

Para medir la madurez de una organización en la gestión de riesgos de seguridad desde la perspectiva del deber de cuidado, véase:

- *EISF y cinfo – Duty of Care Maturity Model*
- *cinfo – Duty of Care Maturity Model Tool*

4 Incidencia para el cambio: reforzar la seguridad en el sector de la ayuda mediante partenariados

4.1. Incidencia conjunta

"Una voz que representa a muchas partes, de la que se hacen eco muchas, y que es clara y está basada en pruebas, es una voz poderosa que puede influir con eficacia en terceros y en los objetivos".

Manual de Incidencia de Foros de ONG del ICVA

La incidencia consiste en influir en el cambio. Al trabajar en partenariado, las organizaciones pueden identificar cuestiones relacionadas con la seguridad que están más allá de su capacidad para abordarlas como organizaciones individuales o dentro del partenariado. Para este tipo de dificultades, las copartes deben considerar la posibilidad de participar en iniciativas colectivas de incidencia para influir en el cambio dentro del sector de la ayuda en general.

Algunos de los objetivos de incidencia relativa a la seguridad pueden ser:

- posicionar la gestión de riesgos de seguridad como una consideración central en todas las conversaciones programáticas, en lugar de tratarla como un "complemento";
- velar por que se incluya a referentes de seguridad en los debates estratégicos y de alto nivel;
- garantizar una mayor inclusión de la gestión de riesgos de seguridad en los debates de la agenda de **localización**;
- asegurarse de que los donantes satisfagan las necesidades de financiación de la gestión de riesgos de seguridad de ambas organizaciones copartes;
- garantizar un mayor acceso de ambas copartes a recursos, colaboraciones y redes en materia de seguridad.

Las organizaciones copartes están especialmente bien situadas para participar en los esfuerzos de incidencia, ya que pueden abordar estos retos conjuntamente y aprovechar los puntos fuertes de cada una para influir en el cambio.

Las copartes pueden elaborar una estrategia conjunta de incidencia en la que identifiquen metas, objetivos, destinatarios, mensajes, alianzas y oportunidades comunes. Eso puede hacerse de manera formal (siguiendo las pautas que se comparten más adelante en el Gráfico 5) o de manera más informal al:

1. identificar de manera conjunta qué cambios desean ver las copartes;
2. trabar alianzas, dentro de cada organización, dentro del partenariado y fuera de él;
3. unir sus voces en función de los conocimientos y las pruebas obtenidas.

Es imprescindible que el personal de incidencia y quienes sean referentes de seguridad trabajen mano a mano en ambas organizaciones copartes para que cualquier esfuerzo de incidencia se base en los conocimientos y la experiencia de personas expertas en seguridad.

Iniciativas de incidencia por separado

Si bien los partenariados ofrecen a las organizaciones una oportunidad única para emprender una incidencia conjunta, puede ser beneficioso para las copartes participar también en actividades de incidencia por separado.

Las ONGI, por ejemplo, suelen estar mejor posicionadas ante donantes y como integrantes de grupos internacionales de incidencia para hacer incidencia en representación de las ONGN/L. Las ONGI deberían utilizar su influencia para promover una mejor seguridad para las ONGN/L, por ejemplo, realizando incidencia con donantes para unos presupuestos de seguridad adecuados para las organizaciones locales y nacionales.

Las ONGI tienen la responsabilidad de utilizar su posición para hacer incidencia en representación de las ONGN/L.

Por su parte, las ONGN/L pueden emprender sus propios esfuerzos de incidencia, por ejemplo, para cambiar sus relaciones con sus copartes internacionales cuando estas no responden a las necesidades de las ONGN/L.

Las ONGN/L deberían elaborar un programa de incidencia independiente o con otras ONGN/L para abogar por el cambio cuando las partes internacionales, incluidas sus copartes ONGI, no son receptivas a sus necesidades

Gráfico 5. Estrategia de incidencia: pasos y preguntas fundamentales

Adaptado del Manual de Incidencia de Foros de ONG de ICVA

4.2. Gestión de riesgos de seguridad y esfuerzos de incidencia

Este apartado proporciona ejemplos de cómo las organizaciones pueden realizar incidencia en materia de seguridad y destaca los retos que podrían abordarse a través de la incidencia relativa a seguridad.

4.2.1. Proteger al personal humanitario contra los ataques selectivos

Al trabajar juntas, las organizaciones de ayuda pueden llamar la atención sobre los riesgos de seguridad a los que se enfrenta su plantilla y pedir una mayor protección del personal humanitario. El movimiento "**Not A Target**" es un ejemplo de este tipo de iniciativas (las actividades relacionadas con este movimiento en las redes sociales utilizan el hashtag #NotATarget).

Es esencial la colaboración entre las organizaciones humanitarias –y en concreto, entre partes internacionales y locales– en estos esfuerzos. Gran parte de la labor para poner de manifiesto los ataques a los que se enfrenta el personal sanitario se fundamenta en pruebas procedentes de fuentes locales. Los informes de la Red Siria de Derechos Humanos, por ejemplo, documentan los ataques contra civiles, profesionales sanitarios y otros. Estas pruebas permiten a la organización y a sus copartes abogar por una mayor protección de la población civil y otros no combatientes, incluido el personal sanitario, en Siria.

Las evidencias de riesgos de seguridad pueden desempeñar una función importante en los mensajes y ayudar a cumplir los objetivos de incidencia.

La recopilación de información sobre incidentes de seguridad que afecten al personal de varias organizaciones, aunque no esté pensada originalmente para fines de incidencia, también puede ayudar a las organizaciones a identificar tendencias y a presentar pruebas de los retos relacionados con la seguridad, lo que puede conducir a iniciativas de incidencia colectiva. Por ejemplo, la Coalición para preservar la salud en los conflictos utiliza datos sobre incidentes de seguridad de los que han informado múltiples organizaciones para abogar por una mayor protección del personal sanitario en entornos de conflicto. Para este tipo de iniciativas, es importante reunir los datos de incidentes de múltiples organizaciones.

Las copartes también pueden realizar incidencia juntas en caso de incidente grave. Por ejemplo, en agosto de 2020, 7 integrantes del personal de la ONG ACTED fueron trágicamente asesinados en Níger. Este incidente llevó a ACTED a lanzar un llamamiento mundial a la acción para mejorar la protección del personal humanitario. Al llamamiento a la acción se unieron otras 63 organizaciones y dio lugar a conversaciones de alto nivel en el Gobierno francés y en Naciones Unidas sobre el cumplimiento del derecho internacional humanitario y la necesidad de mejorar la protección del personal humanitario.

4.2.2. Incidencia sobre gestión de riesgos de seguridad y la agenda de localización

Las organizaciones internacionales y locales también pueden contemplar la posibilidad de realizar incidencia para mejorar la comprensión y los esfuerzos para abordar los desafíos relacionados con la seguridad en el marco de los partenariados. El Gran Pacto (Grand Bargain) y la agenda de **localización** se han centrado en gran medida en trasladar el poder de toma de decisiones a las ONGN/L dentro del espacio humanitario, lo que ha recibido el apoyo de iniciativas notables como la Charter4Change y la Alliance for Empowering Partnership (A4EP). Sin embargo, este cambio no se ha traducido en un mayor diálogo sobre las necesidades de seguridad de las ONGN/L en la agenda de localización o en el sector de la ayuda en general. Se trata de una laguna importante y reveladora.

Los equipos de incidencia que trabajan en la agenda de localización en las dos organizaciones copartes deberían colaborar con sus referentes de seguridad para abogar por una mayor consideración y diálogo en torno a los riesgos de seguridad a los que se enfrentan las ONGN/L. Por ejemplo, una mayor inclusión de la gestión de los riesgos de seguridad en las herramientas centradas en la localización, como el marco para medir el desempeño de la localización elaborado por NEAR (Network for Empowered Aid Response), sería un paso positivo.

4.2.3. Incidencia y financiación relativas a la gestión de riesgos de seguridad

Las organizaciones necesitan suficiente financiación específica para gestionar los riesgos de seguridad. Sin embargo, la financiación para las organizaciones está cada vez más disputada, sobre todo para las ONGN/L, y a menudo puede ser inferior a lo que realidad se necesita. Para obtener suficiente financiación para seguridad, las organizaciones pueden tener que emprender iniciativas de incidencia dirigidas a sus copartes o donantes, ya sea como organizaciones individuales o mediante incidencia colectiva.

Las organizaciones que temen plantear a las donantes y copartes sus preocupaciones sobre las lagunas de financiación para la gestión de riesgos de seguridad pueden encontrar más fácil participar en campañas de incidencia colectiva con otras ONG. Las ONGN/L, por ejemplo, podrían utilizar plataformas como NEAR para abogar por que sus ONGI copartes se aseguren de que cuentan con una financiación adecuada para seguridad.

Cuando las propias ONGI tengan problemas con la financiación de la seguridad, deberían tratar de incluir el apoyo a la gestión de los riesgos de seguridad para ellas mismas y para sus copartes ONGN/L en cualquier estrategia de incidencia que tengan hacia donantes.

Un elemento clave de una estrategia eficaz de incidencia de este tipo es tener claras las necesidades y las carencias de financiación de la seguridad de ambas copartes. Quienes sean referentes de seguridad pueden desempeñar una función importante en este tipo de incidencia, al proporcionar ejemplos a sus colegas de incidencia sobre los problemas de seguridad que pueden surgir debido a las lagunas existentes en la financiación de la seguridad.

Véase el apartado 3.2. Financiación de la gestión de riesgos de seguridad en los partenariados

Ejemplo:
La campaña "At What Cost?" ("¿A qué precio?")

En julio de 2019, el GISF (entonces, EISF) lanzó una campaña llamada "¿A qué precio?" para sensibilizar sobre la financiación inadecuada de la seguridad dentro del sector de la ayuda. La carta abierta de la campaña cuestionaba la práctica dentro del sector de la ayuda de asignar un porcentaje arbitrario para los costes de seguridad en los presupuestos, una práctica que no reconoce la diversidad de contextos, operaciones, organizaciones y riesgos a los que se enfrentan las organizaciones de ayuda. La carta aboga por que se incluyan partidas presupuestarias específicas y explícitas para la seguridad del personal, con mensajes clave dirigidos a diferentes grupos:

"El EISF... hace un llamamiento al sector de la ayuda para que reanude el debate sobre la financiación de la gestión de riesgos de seguridad, de modo que la seguridad del personal no quede relegada en los presupuestos. Al personal humanitario de todos los

Ejemplo: **La campaña "At What Cost?" ("¿A qué precio?")** *continuación*

ámbitos, le pedimos que se cuestione cómo se incluye el verdadero coste de su seguridad en los presupuestos de los programas. A las personas responsables de seguridad, les pedimos que presionen a sus organizaciones para que incluyan la seguridad como una partida presupuestaria directa. A la comunidad de donantes, les pedimos que se coordinen con las organizaciones no gubernamentales para reformar los procesos de financiación de la gestión de riesgos de seguridad".

Carta abierta del EISF a las organizaciones no gubernamentales y donantes

Esta carta abierta ha sido firmada por casi 200 partes interesadas que trabajan en 38 países de todo el mundo. Al pedir a la comunidad de donantes, a las personas responsables de seguridad y a todo el personal humanitario que sean más conscientes y presionen para conseguir una financiación adecuada para la seguridad, la carta consiguió concienciar y provocar un cambio concreto. Tras la campaña, el Departamento de Desarrollo Internacional de Reino Unido (que fue reemplazado en septiembre de 2020 por el Ministerio de Asuntos Exteriores, de la Commonwealth y de Desarrollo) anunció que actualizaría la plantilla y las orientaciones de su mecanismo de respuesta rápida para incluir una partida específica para la gestión de riesgos de seguridad.

Más información

- *Oxfam y la Open University – curso Make Change Happen*
- *ICVA – Manual de Incidencia de Foros de ONG*
- *Working Group on Protection of Humanitarian Action – Toolkit: Responding to Violence against Humanitarian Action on the Policy Level*
- *Call for Action for Safeguarding of Humanitarian Space and Ending Impunity for Attacks against Humanitarians*
- *GISF – How to effectively advocate for aid workers' protection?*
- *RedR UK, Insecurity Insight y EISF – Manual de gestión de la información sobre incidentes de seguridad (en concreto el apartado 4.5 Usar la información sobre incidentes de seguridad para incidencia estratégica)*
- *NEAR – Localisation Performance Measurement Framework*
- *Syrian Network for Human Rights*
- *Safeguarding Health in Conflict Coalition*
- *Reflections on GISF's 'At What Cost?' Campaign*
- *An open letter to non-governmental and donor organisations from the European Interagency Security Forum*

Algunas organizaciones e iniciativas que se dedican a labores de localización:

- *NEAR*
- *Charter4Change resources*
- *A4EP*

5 Herramientas

Herramienta 1
Una buena comunicación en los partenariados

La presente herramienta sirve como orientación en cómo evaluar la calidad de la comunicación dentro de los acuerdos de partenariado.

A menudo se producen malentendidos entre copartes en torno a los riesgos y los contextos de seguridad. Las diferencias comunicativas culturales y las barreras lingüísticas son un especial desafío para tratar en profundidad y de manera significativa los riesgos de seguridad (p. ej., culturas orales frente a las escritas o falta de interacción presencial). El personal que se dedica a la seguridad también usa muchas veces una jerga con muchos conceptos que cuesta traducir a distintos idiomas.

Las copartes deberían revisar con regularidad la calidad de su comunicación e identificar los principales obstáculos a sus intercambios. Las copartes pueden usar esta herramienta como ejercicio individual para mejorar su comunicación o como herramienta de evaluación conjunta para comparar distintos enfoques de comunicación y abordar cualquier malentendido.

Ejercicio – Evalúe la calidad de su comunicación (por ejemplo, correos electrónicos, cartas, llamadas, reuniones presenciales)	**Evaluación** – Revise la comunicación dentro del partenariado en términos más generales
1. ¿La comunicación es clara? 2. ¿Se evita el uso de jerga y de acrónimos en la comunicación? 3. ¿La comunicación es transparente sobre los motivos y propósitos que tiene? Es decir, ¿queda claro por qué se está comunicando y qué espera obtener de la comunicación? 4. ¿El canal y el método de comunicación son adecuados para quien la va a recibir? 5. ¿La comunicación muestra sensibilidad cultural, es positiva, respetuosa y parte de la noción de equidad (es decir, evita el uso de un lenguaje negativo, vertical y exigente)?	1. ¿Es palpable la confianza en la comunicación entre las copartes? 2. ¿Comparten las copartes información de manera proactiva? 3. ¿Las copartes solicitan las observaciones de la otra organización de manera habitual, tanto formal como informalmente, incluso sobre cuán eficaz ha sido la comunicación entre ellas? 4. ¿La comunicación que existe es necesaria o es excesiva? 5. ¿Las copartes asumen la responsabilidad de lo que se ha dicho o se ha hecho? 6. ¿La comunicación es coherente? (En su frecuencia, carácter y con las expectativas de cada coparte). 7. ¿La comunicación la reciben las personas correctas? Si no es así, ¿por qué? Aborde toda barrera cultural o lingüística.

continuación

continuación

Ejercicio – Evalúe la calidad de su comunicación (por ejemplo, correos electrónicos, cartas, llamadas, reuniones presenciales)	**Evaluación – Revise la comunicación dentro del partenariado en términos más generales**
6. ¿Muestra la comunicación consideración por las circunstancias específicas de la persona y de organización en su conjunto que la van a recibir? **7.** ¿La comunicación es pertinente para todas aquellas que la van a recibir? Y, si no es así, ¿cómo se puede lidiar con eso (p. ej., parte del personal puede considerar que es innecesario que se le involucre en conversaciones sobre seguridad cuando no posee responsabilidades en materia de seguridad u opera en zonas de riesgo bajo)?	**8.** ¿Se puede incorporar a un interlocutor para que fortalezca la comunicación entre las copartes? **9.** ¿Pueden abordar las copartes de manera conjunta las preocupaciones sobre seguridad digital que puedan provocar que el personal evite utilizar determinadas plataformas de comunicación (es decir, en algunos contextos, los correos electrónicos y las llamadas de teléfono pueden ser interceptados por agentes gubernamentales)? **10.** Donde existe preocupación sobre la seguridad de determinados tipos de comunicación, ¿se ofrecen alternativas de comunicación (como la presencial) a todo el personal?

Véase el apartado 1.4. para consultar otras orientaciones sobre una buena comunicación

Herramienta 2
Actitud hacia el riesgo en partenariados

La presente herramienta permite a las copartes explorar y elaborar un entendimiento mutuo sobre la actitud hacia el riesgo y su aceptación. Debería usarse la herramienta para establecer un diálogo continuado entre las copartes y se debería revisar de manera habitual.

Paso 1: Definir qué significan probabilidad e impacto

La gravedad de un riesgo dependerá de su probabilidad de producirse y, de ser así, de la gravedad de su impacto. Las copartes deberían hablar de qué entienden por "probabilidad" e "impacto" en la práctica mediante la definición de cada una de las categorías de impacto y probabilidad que aparecen a continuación. Ese diálogo permitirá que ambas copartes comparen los riesgos a partir de una comprensión parecida; p. ej., una coparte puede considerar que "improbable" es una vez al mes, mientras que la otra lo define como una vez al año. Al definir qué significa cada una de las categorías de "impacto", las copartes deberían tener en cuenta al personal, los equipos y el/los programa/s pertinente/s.

Probabilidad		**Definiciones**
1	**Muy improbable**	Por ejemplo, más de: una vez cada diez años menos de: una vez al año
2	**Improbable**	
3	**De probabilidad moderada**	
4	**Probable**	
5	**Muy probable**	
Impacto		**Definiciones**
1	**Insignificante**	Por ejemplo, Personal: lesiones menores a una persona de la plantilla Equipo: pérdida de equipo no esencial Programa: pérdida temporal de acceso a causa de dificultades del clima en esa estación
2	**Menor**	
3	**Moderado**	
4	**Grave**	
5	**Crítico**	

Paso 2: Elaborar una matriz para convenir en los grados de riesgo aceptables

Las copartes pueden utilizar una matriz que compare la probabilidad de un incidente con su impacto (lo que a veces se calcula en términos numérico como Probabilidad x Impacto), para identificar dónde reside el grado de riesgo aceptable dentro del partenariado para cada una de las copartes. Los grados de riesgo aceptables deberían ir subrayados en verde. A continuación, se muestra una matriz solo como ejemplo y cada organización/partenariado tendrá distintos grados de aceptación del riesgo y, por lo tanto, debería adaptar el diagnóstico de aceptación del riesgo para que cumpla sus necesidades.

	IMPACTO				
PROBABILIDAD	**Insignificante = 1**	**Menor = 2**	**Moderado = 3**	**Grave = 4**	**Crítico = 5**
Muy probable = 5	(1x5) = 5	(5x2) = 10	15	20	25
Probable = 4	4	8	12	16	20
De probabilidad moderada = 3	3	6	9	12	15
Improbable = 2	2	4	6	8	10
Muy improbable = 1	1	2	3	4	5

Más allá de centrarse en el número resultante, se anima a las copartes a pensar si el riesgo es bajo/medio/elevado y a realizar un diagnóstico sobre esa base.

Herramienta 3
Plantilla de trabajo y cuestionario de revisión conjunta de la GRS

La presente plantilla proporciona una serie de preguntas de ejemplo y a continuación indicadores de ejemplo que las copartes pueden responder y evaluar juntas. Los indicadores se pueden evaluar para el partenariado en su conjunto o, cuando sea pertinente, los pueden evaluar cada una de las organizaciones copartes mediante un sistema de evaluación en tres niveles: presente, presente en parte y no presente. La finalidad de esta herramienta es alentar una conversación sincera y abierta entre las copartes sobre las capacidades, los recursos, las lagunas y las necesidades en materia de gestión de riesgos de seguridad dentro de cada organización y en el partenariado en su conjunto. En esta herramienta se incluyen algunas de las preguntas y los indicadores que constan en la Parte 2 de la presente guía

NO se trata de una "herramienta de gestión de riesgos de seguridad", sino de una "herramienta de gestión del partenariado". TAMPOCO se trata de una herramienta para evaluar los puntos fuertes y débiles del sistema de gestión de riesgos de seguridad de una organización coparte.

Cabe percatarse de que esta es una lista de preguntas y de indicadores de ejemplo, y de que las copartes deberían adaptar esta plantilla para que incluya preguntas e indicadores pertinentes para sus necesidades y su situación específicas.

Consulte la Parte 2 de la presente guía para ver preguntas e indicadores adicionales

Parte 1. Deber de cuidado

N.º de ref.	Pregunta	Respuesta		Notas
1.1.	¿Cuáles son las obligaciones jurídicas y morales del deber de cuidado de cada coparte respecto a la otra, de haberlas?	ONGN/L		
		ONGI		
1.2.	¿Cuáles son las obligaciones jurídicas y morales del deber de cuidado de cada coparte hacia su personal, población beneficiaria y comunidades afectadas respectivas?	ONGN/L		
		ONGI		
1.3.	¿Se tienen en cuenta las necesidades psicosociales de todo el personal y se abordan? ¿Hay alguna acción que puedan emprender las socias para perfeccionar su deber de cuidado hacia el personal que implementa (p. ej., cobertura del seguro, bienestar psicosocial)? ¿Cuál?	ONGN/L		
		ONGI		

N.º de ref.	Indicador que evaluar	Partenariado	ONGN/L	ONGI	Notas y evidencias
1.1.	Ambas copartes entienden y cumplen las obligaciones jurídicas del deber de cuidado.	*No se cumple*	*Se cumple*	*Se cumple en parte*	
1.2.	Ambas copartes han hablado y acordado las obligaciones morales del deber de cuidado.				

Parte 2. Gobernanza y rendición de cuentas

N.º de ref.	Pregunta	Respuesta		Notas
2.1.	¿Cuentan ambas copartes con estructuras apropiadas de gestión de riesgos de seguridad que permitan cumplir los objetivos del partenariado?	ONGN/L		
		ONGI		
2.2.	¿Entienden con claridad ambas copartes las funciones y las responsabilidades relativas a la gestión de riesgos de seguridad en lo referente al partenariado y a la realización de los programas? Por ejemplo, ¿tienen ambas organizaciones un referente de seguridad y que pueda ser el contacto para las copartes en cuestiones de seguridad?	ONGN/L		
		ONGI		
2.3.	¿Cómo percibe cada una de las copartes la transferencia de riesgos en el partenariado (si lo hace)? ¿Qué acciones considera cada coparte que puede emprender para pasar de la transferencia de riesgos a compartir riesgos?	ONGN/L		
		ONGI		

N.º de ref.	Indicador que evaluar	Partenariado	ONGN/L	ONGI	Notas y evidencias
2.1.	Existe una declaración de rendición de cuentas y de gobernanza respecto a la gestión de riesgos de seguridad dentro del partenariado.	*No se cumple*	*Se cumple*	*Se cumple en parte*	
2.2.	Existe un proceso de información y de rendición de cuentas (con un contenido y una frecuencia establecidos) para advertir a cada una de las copartes sobre cuestiones de riesgos de seguridad, que arroja claridad sobre las responsabilidades de ambas copartes en lo respectivo a la gestión de los riesgos de seguridad dentro del partenariado.				
2.3.	Ambas copartes han designado explícitamente a una persona referente con responsabilidades en el ámbito de la gobernanza de los riesgos de seguridad tanto de la organización como del partenariado.				

Parte 3. Política y principios				
N.º de ref.	**Pregunta**	**Respuesta**		**Notas**
3.1.	¿Ambas copartes entienden el mandato, la misión, los valores y los principios de cada una de las organizaciones? ¿Están ambas organizaciones cómodas con la labor y el planteamiento de operaciones de la otra (p. ej., ¿están de acuerdo ambas copartes en sus posturas respectivas en lo que se refiere a adherirse a los principios humanitarios)?	ONGN/L		
		ONGI		
3.2.	¿Existe acuerdo entre las copartes sobre los requisitos mínimos prácticos de seguridad que debe haber en cada lugar o actividad? (Percátese de que, si bien estos deberían aplicarse a ambas copartes, también han de ser realistas y adaptarse a la capacidad de cada organización).	ONGN/L		
		ONGI		
3.3.	¿Cómo definen y plantean la actitud hacia el riesgo las copartes? ¿Y existe un acuerdo entre las copartes sobre lo que es un umbral de riesgos aceptable para el partenariado y los programas incluidos en este?	ONGN/L		
		ONGI		

continuación

Parte 3. Política y principios *continuación*					
N.º de ref.	**Indicador que evaluar**	**Partenariado**	**ONGN/L**	**ONGI**	**Notas y evidencias**
3.1.	Las políticas de gestión de seguridad y su puesta en práctica (mediante planes, procedimientos o pautas) son adecuadas para el contexto local y las circunstancias del partenariado, y son accesibles para todo el personal (es decir, están disponibles en los idiomas y en los formatos pertinentes).	*No se cumple*	*Se cumple*	*Se cumple en parte*	
3.2.	El contrato de partenariado incluye una declaración relativa a que se ha entendido y acordado conjuntamente el umbral de riesgo para las actividades del partenariado.				
3.3.	El contrato de partenariado no contradice –sino que refuerza, cuando sea posible- las políticas de seguridad de ambas copartes (p. ej., disposiciones sobre el uso de escoltas armadas).				

Parte 4. Operaciones y programas				
N.º de ref.	**Pregunta**	**Respuesta**		**Notas**
4.1.	¿Cuáles son las necesidades y las expectativas en materia de seguridad de cada una de las copartes?	ONGN/L		
		ONGI		
4.2.	¿Cuentan las copartes con un sistema que hayan acordado para identificar y monitorear los riesgos de seguridad a los que se enfrenta el personal? (¿Están armonizados los diagnósticos de riesgos de seguridad y los planes de seguridad de ambas organizaciones para las ubicaciones en las que opera la coparte que implementa? ¿Cuáles son las divergencias y por qué?).	ONGN/L		
		ONGI		
4.3.	¿Las copartes han convenido en quién es la responsable de gestionar los riesgos identificados, y cómo ha de hacerse y financiarse?	ONGN/L		
		ONGI		

continuación

Parte 4. Operaciones y programas *continuación*					
N.º de ref.	**Indicador que evaluar**	**Partenariado**	**ONGN/L**	**ONGI**	**Notas y evidencias**
4.1.	Se ha realizado un diagnóstico conjunto de riesgos de seguridad de las operaciones, los riesgos asociados y las repercusiones sobre cada coparte y existe un proceso claro para ir actualizando el análisis con regularidad. El diagnóstico incluye un análisis de los riesgos internos y los que puedan surgir a consecuencia del propio partenariado.	*No se cumple*	*Se cumple*	*Se cumple en parte*	
4.2.	En el presupuesto del partenariado hay partidas explícitas para cumplir los requisitos de seguridad, incluso actividades de refuerzo de capacidades, y ambas copartes consideran que son suficientes para satisfacer todas sus necesidades de recursos.				
4.3.	Ambas copartes han convenido en las estrategias o los enfoques sobre seguridad específicos para el contexto y están articulados y se han comunicado a todas las partes pertinentes de cada organización.				

Parte 5. Gestión de viajes y apoyo					
N.º de ref.	**Pregunta**	**Respuesta**			**Notas**
5.1.	¿Cómo deberían gestionarse los riesgos de seguridad que son consecuencia del partenariado? ¿Cuáles deberían ser los requisitos mínimos para la gestión de viajes y las disposiciones de apoyo (para las visitas de campo, la estancia nocturna, los procedimientos de comunicación en viaje y otros apoyos)?	ONGN/L			
		ONGI			
5.2.	¿El personal de ambas organizaciones recibe un apoyo equitativo en viajes y estancias en las ubicaciones del proyecto?	ONGN/L			
		ONGI			
5.3.	¿Están de acuerdo las copartes en la política de seguridad y los procedimientos que deberían seguirse durante las visitas de las copartes y en quién mantiene el deber de cuidado hacia el personal visitante?	ONGN/L			
		ONGI			

continuación

Parte 5. Gestión de viajes y apoyo *continuación*					
N.º de ref.	**Indicador que evaluar**	**Partenariado**	**ONGN/L**	**ONGI**	**Notas y evidencias**
5.1.	Las copartes convienen en las disposiciones y las responsabilidades en materia de seguridad en las visitas del personal de ambas organizaciones a las oficinas y las ubicaciones de programa de la otra.	*No se cumple*	*Se cumple*	*Se cumple en parte*	
5.2.	Las copartes comparten entre sí sus procedimientos de seguridad para el personal que viaja a ubicaciones pertinentes para el partenariado (p. ej., dichos procedimientos pueden incluir información sobre funciones y responsabilidades, formación y sesiones informativas, procedimientos de verificación, monitoreo de viajes, autorizaciones de viaje y procedimientos de emergencia).				
5.3.	Se contemplan las diversas necesidades del personal que viaja en los procedimientos de viajes, p. ej., un riesgo agudizado a causa de rasgos personales (género, grupo ético, capacidades, etc.).				

Parte 6. Sensibilización y fortalecimiento de capacidades

N.º de ref.	Pregunta	Respuesta			Notas
6.1.	¿Cómo identificarán las copartes las necesidades de sensibilización y de refuerzo de capacidades, y cómo las cubrirán de manera conjunta (tanto en términos de seguridad personal como de gestión de riesgos de seguridad)?	ONGN/L			
		ONGI			
6.2.	¿Hay un acuerdo respecto a qué lagunas existen en la capacidad de gestionar riesgos de seguridad de ambas copartes y qué puede hacer cada organización para abordarlas?	ONGN/L			
		ONGI			
6.3.	¿El presupuesto del partenariado incluye financiación para respaldar las actividades de fortalecimiento de capacidades a largo plazo?	ONGN/L			
		ONGI			
N.º de ref.	**Indicador que evaluar**	**Partenariado**	**ONGN/L**	**ONGI**	**Notas y evidencias**
6.1.	Las copartes convienen en las necesidades en materia de capacidad para gestionar los riesgos de seguridad.	*No se cumple*	*Se cumple*	*Se cumple en parte*	
6.2.	Se cuenta con una estrategia para fortalecer, aprender y desarrollar capacidades, con un plan claro de puesta en práctica, y su finalidad es mejorar la capacidad a largo plazo de las copartes.				
6.3.	La organización comparte con regularidad recursos y respalda el acceso a oportunidades adecuadas y específicas del contexto para fortalecer, aprender y desarrollar capacidades en la gestión de los riesgos de seguridad con las organizaciones copartes.				

Parte 7. Monitoreo de incidentes

N.º de ref.	Pregunta	Respuesta		
7.1.	¿Cómo deberían compartir las copartes información sobre incidentes entre ellas?	ONGN/L		
		ONGI		
7.2.	¿Cómo pueden respaldarse mutuamente las copartes en la gestión de información sobre incidentes de seguridad? Por ejemplo, con procedimientos para reportar incidentes, sistemas de registro de incidentes y herramientas para analizar los datos sobre incidentes y utilizarlos para fundamentar las decisiones sobre seguridad, programas, operaciones, incidencia, finanzas, etc.	ONGN/L		
		ONGI		
7.3.	¿A qué datos sobre incidentes de seguridad en la ubicación pertinente tiene acceso cada organización, ya sea por sus propias operaciones o a través de sus redes, que pueda compartir con su coparte de manera periódica?	ONGN/L		
		ONGI		

continuación

Parte 7. Monitoreo de incidentes *continuación*

N.º de ref.	Indicador que evaluar	Partenariado	ONGN/L	ONGI	Notas y evidencias
7.1.	Se dispone de un proceso para gestionar y compartir información relativa a seguridad para el contexto operativo, incluso datos sobre incidentes, entre las copartes y ambas lo respetan.	*No se cumple*	*Se cumple*	*Se cumple en parte*	
7.2.	Existe un acuerdo sobre cómo se utilizan los datos sobre incidentes para fundamentar la toma de decisiones, donde se incluye una política clara sobre si han de adoptarse medidas disciplinarias a raíz de que se informe o se deje de informar de incidentes.				
7.3	La organización revisa de manera periódica los incidentes que afectan a su personal para identificar las tendencias y las preocupaciones respecto a incidentes de seguridad, y lo comparte con las organizaciones copartes.				

Parte 8. Gestión de crisis

N.º de ref.	Pregunta	Respuesta			Notas
8.1.	¿Cómo colaborarán/se coordinarán las copartes si se produce una crisis o un incidente crítico que afecte a alguna de las organizaciones en la ubicación pertinente?	ONGN/L			
		ONGI			
8.2.	Si se produce una crisis o un incidente crítico y afecta a ambas copartes, ¿quién debería encabezar la respuesta de gestión de crisis? ¿Cuáles son las responsabilidades y quién tiene autoridad para tomar decisiones?	ONGN/L			
		ONGI			
8.3.	¿Qué apoyo puede proporcionar cada coparte a la otra si alguna de las organizaciones experimenta un incidente crítico en la ubicación del partenariado?	ONGN/L			
		ONGI			

N.º de ref.	Indicador que evaluar	Partenariado	ONGN/L	ONGI	Notas y evidencias
8.1.	Se han acordado las responsabilidades y la autoridad para tomar decisiones en caso de crisis o de incidente crítico que afecte a ambas copartes. Lo idóneo sería que eso constase por escrito o estuviera plasmado de una forma visual (p. ej., en un diagrama de flujo).	*No se cumple*	*Se cumple*	*Se cumple en parte*	
8.2.	Las copartes disponen de una estructura y de un plan para gestión de crisis.				
8.3.	Las copartes tienen acceso a servicios de apoyo de emergencia (tanto médicos como no médicos) dentro de la cobertura del seguro de cada una de las organizaciones.				

Parte 9. Colaboraciones y redes en materia de seguridad

N.º de ref.	Pregunta	Respuesta		Notas	Notas
9.1.	¿Existen plataformas que traten temas de seguridad en el contexto pertinente? Si la respuesta es afirmativa, ¿tienen acceso ambas copartes y una voz igual en esas redes y plataformas de coordinación en sus áreas operativas, incluso en las plataformas para compartir información sobre seguridad?	ONGN/L			
		ONGI			
9.2.	¿Cuáles son los obstáculos y los desafíos que impiden la participación activa de ambas copartes en los foros, las reuniones y las conversaciones interinstitucionales sobre seguridad en los ámbitos local, nacional, regional e internacional?	ONGN/L			
		ONGI			
9.3.	¿Qué acciones puede emprender cada una de las organizaciones que faciliten la inclusión de su coparte en esas conversaciones?	ONGN/L			
		ONGI			

N.º de ref.	Indicador que evaluar	Partenariado	ONGN/L	ONGI	Notas y evidencias
9.1.	Ambas copartes participan activamente en foros, plataformas, reuniones y consorcios sobre gestión de riesgos de seguridad, y comparten información sobre seguridad con otras en los ámbitos local, nacional, regional o internacional.	*No se cumple*	*Se cumple*	*Se cumple en parte*	
9.2.	Ambas organizaciones promueven y facilitan que participen sus copartes, cuando sea posible, en foros, plataformas, reuniones y conversaciones interinstitucionales para fortalecer que se comparta información y la colaboración en materia de seguridad. Eso incluye compartir con las copartes los datos de contacto de partes pertinentes que puedan proporcionar apoyo en la gestión de riesgos de seguridad.				

Parte 10. Monitoreo de cumplimiento y eficacia

N.º de ref.	Pregunta	Respuesta			Notas
10.1.	¿Cómo deberían revisar ambas copartes con regularidad la gestión de riesgos de seguridad dentro del partenariado?	ONGN/L			
		ONGI			
10.2.	¿Qué grado de supervisión del cumplimiento y de la eficacia en lo respectivo a la gestión de riesgos de seguridad dentro de cada organización o en el partenariado es aceptable para ambas copartes?	ONGN/L			
		ONGI			
10.3.	¿Cuánta información quieren las copartes compartir entre sí respecto a lecciones aprendidas, revisiones, auditorías de seguridad y análisis tras el incidente que haga referencia al contexto, el partenariado o un proyecto concreto?	ONGN/L			
		ONGI			

N.º de ref.	Indicador que evaluar	Partenariado	ONGN/L	ONGI	Notas y evidencias
10.1.	Ambas copartes comparten y hablan de las conclusiones de las lecciones aprendidas, las revisiones, los análisis tras incidentes y las auditorías de seguridad relativas al contexto, al partenariado o al proyecto/programa.	*No se cumple*	*Se cumple*	*Se cumple en parte*	
10.2.	Las personas responsables de supervisar la puesta en práctica del sistema de seguridad y su cumplimiento (tanto dentro de cada organización como dentro del partenariado) tienen la formación adecuada, participaron en la revisión conjunta de la GRS, y dichas responsabilidades constaban de manera expresa en la descripción de su puesto.				
10.3.	Los sistemas de gestión de desempeño del personal hacen mención explícita de las responsabilidades de seguridad y del cumplimiento de las políticas de la organización.				

Parte 11. Recursos de apoyo					
N.º de ref.	**Pregunta**	**Respuesta**			**Notas**
11.1.	¿Los recursos de apoyo sobre gestión de riesgos de seguridad están disponibles y son accesibles para todo el personal? Y, si no es así, ¿qué acciones se pueden emprender para mejorar la accesibilidad?	ONGN/L			
		ONGI			
11.2	¿Las copartes han compartido entre ellas sus recursos respectivos sobre gestión de riesgos de seguridad?	ONGN/L			
		ONGI			
11.3.	¿Qué otros recursos podrían aprovechar las copartes que les sirvan para gestionar riesgos de seguridad?	ONGN/L			
		ONGI			
N.º de ref.	**Indicador que evaluar**	**Partenariado**	**ONGN/L**	**ONGI**	**Notas y evidencias**
11.1.	Se comparten periódicamente recursos sobre gestión de riesgos de seguridad que satisfacen las necesidades de todo el personal pertinente de las copartes y en un formato que es accesible para él.	*No se cumple*	*Se cumple*	*Se cumple en parte*	
11.2.	Las copartes ponen a disposición una serie de orientaciones, herramientas y plantillas como parte de una biblioteca de seguridad que les sirva mutuamente para gestionar los riesgos de seguridad.				

Herramienta 4
Plantilla de plan de acción para la revisión conjunta de la GRS

Esta plantilla de plan de acción sirve para ayudar a las copartes a convenir en qué acciones son necesarias para abordar las lagunas que se han identificado durante la evaluación de los indicadores de la gestión de riesgos de seguridad. No hace falta incluir en el plan de acción los indicadores que se consideraron presentes en el ejercicio de evaluación

El plan de acción para la revisión conjunta de la GRS es una herramienta para ayudar a las copartes a llevar a cabo el proceso de revisión conjunta de la GRS que se presenta en esta guía y, por lo tanto, es una herramienta de gestión del partenariado. NO es una herramienta para gestionar riesgos de seguridad efectivos.

Parte 1. Deber de cuidado		
N.º de referencia		*Introducir el número de referencia del indicador*
Indicadores		*Introducir indicador*
Evaluación	**Partenariado**	*Presente*
	ONGN/L	*Presente en parte*
	ONGI	*No presente*
Prioridad		*Urgente/ Intermedia/ No urgente*
Acciones necesarias		*Detallar las acciones necesarias para abordar la carencia.* *Tener en cuenta si existe financiación suficiente para llevar a cabo las acciones pertinentes.*
Responsable		*Identificar una persona o un departamento de la organización coparte pertinente que sea responsable de esta acción.*
Calendario		*Establecer un calendario realista.*
Fecha de la revisión		*Acordar una fecha en la que ambas copartes revisarán el progreso.*

Parte 2. Gobernanza y rendición de cuentas		
N.º de referencia		*Por ejemplo: 2.2.*
Indicadores		*Por ejemplo: Existe un proceso de informar y rendir cuentas (con contenido y frecuencia definidos) para comunicar a cada coparte cuestiones de seguridad.*
Evaluación	**Partenariado**	*Por ejemplo: Presente*
	ONGN/L	*Por ejemplo: No presente*
	ONGI	*Por ejemplo: No corresponde*
Prioridad		*Por ejemplo: Urgente*
Acciones necesarias		*Por ejemplo: Acordar y elaborar un proceso como parte del grupo de trabajo sobre seguridad del partenariado. No precisa de financiación adicional ni de otros recursos. Tener en cuenta si existe financiación suficiente para llevar a cabo las acciones pertinentes.*
Responsable		*Por ejemplo: Grupo de trabajo sobre seguridad del partenariado (introducir los nombres).*
Calendario		*Por ejemplo: Para el 15 de febrero de 2022*
Fecha de la revisión		*Por ejemplo: Marzo de 2022 reunión mensual*
Parte 3. Política y principios		
Parte 4. Operaciones y programas		
Parte 5. Gestión de viajes y apoyo		
Parte 6. Sensibilización y fortalecimiento de capacidades		
Parte 7. Monitoreo de incidentes		
Parte 8. Gestión de crisis		
Parte 9. Colaboración y redes en materia de seguridad		
Parte 10: Monitoreo de cumplimiento y eficacia		
Parte 11. Recursos de apoyo		

Herramienta 5
Plantilla de plan de diagnóstico conjunto de riesgos de seguridad y su gestión

La presente plantilla de plan de diagnóstico conjunto de riesgos de seguridad y su gestión permite a las copartes determinar de manera conjunta los riesgos a los que están expuestas, cómo puede verse afectada cada una de las organizaciones por el partenariado, y diagnosticar las maneras en las que se pueden mitigar las amenazas identificadas para cada una de las copartes. La herramienta debería utilizarse para establecer un diálogo continuado entre las copartes y se debería revisar de manera habitual

Cabe percatarse de que se trata de una plantilla de ejemplo y de que cada partenariado puede diagnosticar sus riesgos de seguridad de una manera distinta. Esta herramienta es diferente de la "revisión conjunta de la GRS" que se describe en esta guía. La plantilla de diagnóstico conjunto de riesgos de seguridad y su gestión trata de identificar y gestionar riesgos de seguridad efectivos y es, por lo tanto, una "herramienta de gestión de riesgos de seguridad", mientras que la "revisión conjunta de la GRS" y las herramientas relacionadas tratan de explorar la GRS de una manera más amplia dentro de los acuerdos de partenariado y es, por lo tanto, una "herramienta de gestión del partenariado".

Paso I: Diagnosticar los riesgos

1.1. Identificar las amenazas.

1.2. Contemplar amenazas externas a las organizaciones (p. ej., secuestro, robo), amenazas internas de cada organización y amenazas internas del partenariado (p. ej., acoso, fraude).

1.3. Dialogar sobre cómo afecta la amenaza a cada una de las copartes. ¿Cuáles son las similitudes y las diferencias?

1.4. Hablar de cómo las vulnerabilidades a las amenazas pueden ser distintas para cada una de las copartes y si se ven afectadas por la relación entre las copartes (p. ej., cuando el personal internacional de un grupo étnico concreto es trasladado a la organización local).

1.5. Abordar cómo los impactos de las amenazas son distintos para cada coparte y si les afecta el partenariado; por ejemplo, cambios en la percepción de la comunidad local a causa del partenariado (p. ej., afiliación política, riqueza).

1.6. Mediante una matriz de riesgos acordada, calificar la probabilidad y el impacto, e identificar si el grado de riesgo es aceptable para una o ambas partes.

Aviso: La herramienta descargable es una hoja de cálculo Excel. Aquí se ha segmentado para que se entienda con más facilidad.

N.º de ref.	Amenaza Descripción del tipo de amenaza dentro del contexto, incluido cómo el partenariado puede cambiar la amenaza	Parte ONGN/L, ONGI o el partenariado en su conjunto	Vulnerabilidad ¿El partenariado cambia la vulnerabilidad/exposición a la amenaza? Exposición de la ONGN/L Exposición de la ONGI	Impacto de la amenaza sobre las copartes ¿Cómo repercute la amenaza en el partenariado? ¿Cómo repercute la amenaza en la ONGN/L? ¿Cómo repercute la amenaza en la ONGI?	Riesgo inherente			¿Riesgo aceptable? Sí/No
					Probabilidad (1-5)	Impacto (1-5)	Calificación del riesgo (P x I)	
Por ejemplo: 1a	*Por ejemplo: Accidente de tráfico rodado en la ubicación del programa.*	***Partenariado***	*El partenariado aumenta la exposición a la amenaza porque aumenta la necesidad de que el personal que implementa viaje a la ubicación del nuevo programa.*	*Un accidente de tráfico afectaría a la seguridad y al bienestar del personal por las lesiones. Puede afectar al partenariado al retrasar o impedir la realización efectiva de los programas. Un accidente de tráfico también puede afectar a la reputación del partenariado y de las copartes.*	*De probabilidad moderada: 3*	*Bajo: 1*	***3***	*Sí*
1b		***ONGN/L***	*La exposición del personal de la ONGN/L es alta ya que lleva a cabo el programa y tiene más probabilidad de viajar con conductores sin formación o en transporte público.*	*Las repercusiones para la ONGN/L serían mayores, ya que un accidente de tráfico afectaría al personal que implementa, a los vehículos de la ONGN/L, así como que tendría un vínculo más estrecho con la ONGN/L en lo que respecta a cuestiones legales y reputacionales.*	*De probabilidad moderada: 3*	*Moderado: 3*	***9***	*Sí*
1c		***ONGI***	*La exposición del personal de la ONGI es baja ya que no viaja a la ubicación del programa salvo que sea en una visita planificada.*	*El accidente puede tener un impacto indirecto en la ONGI si afecta a la realización del programa, a la reputación del partenariado o de las copartes, y si tiene consecuencias presupuestarias de las que se encargue la ONGI.*	*Muy improbable: 1*	*Moderado: 3*	***3***	*Sí*

Parte 5: Herramientas

Paso 2: Identificar medidas de mitigación

2.1. Identificar los riesgos que causan especial preocupación al partenariado o a alguna de las copartes.

2.2. Identificar medidas de mitigación para cada riesgo, incluida la función de cada coparte en la mitigación de ese riesgo.

2.3. Identificar recursos adicionales o contribuciones que puedan ser necesarios para la mitigación sostenible y a largo plazo (p. ej., equipos de comunicación, formación).

2.4. Calcular el riesgo residual.

N.º de ref.	¿Riesgo aceptable? Sí/No	Medidas de mitigación Contemplar las funciones de cada parte en la mitigación de riesgos (ONGN/L, ONGI o en colectivo a través del partenariado).	Recursos necesarios Introducir todos los recursos necesarios (por ejemplo, personal, equipo, formación).	Riesgo residual			¿Riesgo aceptable? Sí/No	Plan continuo de gestión de riesgos de seguridad • Resumir los pasos que han de darse para aplicar las medidas de mitigación y crear un plan de gestión de riesgos de seguridad. • Identificar puntos de monitoreo habituales. • Identificar los indicadores clave de cambio para las amenazas.
				Probabilidad (1-5)	Impacto (1-5)	Calificación del riesgo (P x I)		
1b	*No*	*ONGN/L: Limitar los viajes en transporte público dentro de lo posible. Formar a conductores que transportan al personal.* *ONGI: Compartir recursos sobre conducción segura con la ONGN/L.*	*Personal* *Formación*	*Muy improbable: 1*	*Moderado: 2*	**2**	*Sí*	*Cartografiar el uso de transporte público.* *Comunicarse con el personal sobre las restricciones de los viajes.* *Identificar a formadores de conducción segura.* *Efectuar la formación.*
1c	*No*	*ONGI: Tener normas formales para el personal de la ONGI que restrinjan los viajes en transporte público. Formar a conductores que transportan al personal.* *ONGN/L: Compartir información sobre carreteras de riesgo elevado con la ONGI.*	*Personal* *Formación*	*Muy improbable: 1*	*Moderado: 2*	**2**	*Sí*	

Parte 5: Herramientas

Paso 3: Plan de gestión de riesgos de seguridad

3.1. Resumir los pasos que han de darse para aplicar las medidas de mitigación y crear un plan de gestión de riesgos de seguridad.

3.2. Identificar puntos de monitoreo habituales.

3.3. Identificar los indicadores clave de cambio para las amenazas.

N.º de ref.	Plan continuo de gestión de riesgos de seguridad	Indicadores de cambio	Monitoreo
1b	*Cartografiar el uso de transporte público.* *Comunicarse con el personal sobre las restricciones de los viajes.* *Identificar a formadores de conducción segura.* *Efectuar la formación.*	*Aumento de los accidentes de tráfico rodado* *Muestras de incumplimiento (p. ej., uso del transporte público).*	*Quién:* *Cuándo:* *Cómo:*

Herramienta 6
Plantilla de presupuesto de gestión de riesgos de seguridad en partenariados

Esta es una plantilla de una cartera de gastos de gestión conjunta de riesgos de seguridad. La plantilla incluye ejemplos de costes de la gestión de riesgos de seguridad que cada coparte debe considerar en el presupuesto de un partenariado. Cuando sea preciso, las dos últimas columnas permiten calcular a las copartes cuánta financiación se dedica concretamente a la gestión de riesgos de seguridad donde se pueden compartir los costes con otros departamentos (p. ej., salarios de cargos que tengan responsabilidades en materia de seguridad).

La presente herramienta ha sido adaptada de la herramienta de cartera de gastos de gestión de riesgos (RMEP, por sus siglas en inglés) que aparece en el documento de investigación del EISF "The Cost of Security Risk Management for NGOs". Consulte dicha herramienta de para ver otros ejemplos de gastos relativos a la gestión de riesgos de seguridad.

N.º de ref.	Categoría	Coparte	Descripción del gasto	Unidades	Coste unitario	Total	% de la partida presupuestaria destinada a la gestión de riesgos de seguridad	Total de la gestión de riesgos de seguridad
	Salarios	ONGI	*Por ejemplo, referente de seguridad del partenariado.*			*= unidades x coste unitario*		*= % total de la partida presupuestaria destinada a la gestión de riesgos de seguridad*
		ONGN/L	*Por ejemplo, referentes de seguridad en sede y en terreno, cargos con responsabilidades en materia de gestión de riesgos de seguridad.*					
	Admin. y logística	ONGI	*Gastos relativos a apoyar la gestión de riesgos de seguridad dentro de un partenariado; p. ej., viajes a los lugares de trabajo en terreno de la coparte.*					
		ONGN/L	*Por ejemplo, viajes y alojamiento para referentes de seguridad.*					

continuación

Parte 5: Herramientas

Plantilla de presupuesto de gestión de riesgos de seguridad en partenariados *continuación*

N.º de ref.	Categoría	Coparte	Descripción del gasto	Unidades	Coste unitario	Total	% de la partida presupuestaria destinada a la gestión de riesgos de seguridad	Total de la gestión de riesgos de seguridad
	Formación, aprendizaje y desarrollo	ONGI	*Por ejemplo, respaldo a las iniciativas para fortalecer las capacidades del partenariado; p. ej., traducción.*			*= unidades x coste unitario*		*= % total de la partida presupuestaria destinada a la gestión de riesgos de seguridad*
		ONGN/L	*Por ejemplo, jornadas de formación al personal sobre seguridad (incluidas HEAT, formación en conducción, formación en primeros auxilios) y los viajes y el alojamiento consiguientes.*					
	Información y gestión del conocimiento	ONGI	*Por ejemplo, costes relacionados con realizar la evaluación conjunta de la gestión de riesgos de seguridad.*					
		ONGN/L	*Por ejemplo, gastos relativos a llevar a cabo los diagnósticos de seguridad, elaborar los planes y los procedimientos de seguridad, y supervisar que el personal los cumple.*					
	Acceso	ONGI	*Por ejemplo, incidencia con partes interesadas clave para mejorar la seguridad de las copartes.*					
		ONGN/L	*Por ejemplo, actividades de participación comunitaria.*					
	Gestión de instalaciones	ONGI	*Normalmente, no se aplica a las ONGI cuando la ONGN/L es la coparte que implementa.*					
		ONGN/L	*Por ejemplo, arrendamiento del edificio, sistema de alarma, construcción de una sala de seguridad y mantenimiento.*					
	Activos comunicativos	ONGI	*Por ejemplo, servicios de traducción para mejorar la accesibilidad a la comunicación relativa a seguridad.*					
		ONGN/L	*Por ejemplo, equipo de comunicación, internet.*					
	Activos médicos	ONGI	*Normalmente, no se aplica a las ONGI cuando la ONGN/L es la coparte que implementa.*					
		ONGN/L	*Por ejemplo, botiquines de primeros auxilios.*					
	Activos de transporte	ONGI	*Normalmente, no se aplica a las ONGI cuando la ONGN/L es la coparte que implementa.*					
		ONGN/L	*Por ejemplo, vehículos que cumplen las medidas adecuadas de seguridad, conductores.*					

continuación

Parte 5: Herramientas

Plantilla de presupuesto de gestión de riesgos de seguridad en partenariados *continuación*

N.º de ref.	Categoría	Coparte	Descripción del gasto	Unidades	Coste unitario	Total	% de la partida presupuestaria destinada a la gestión de riesgos de seguridad	Total de la gestión de riesgos de seguridad
	Activos de gestión de crisis	ONGI	*Por ejemplo, el coste de gestionar una crisis, como los viajes del personal internacional, si las copartes convienen en que la ONGI participará en la gestión de crisis.*			*= unidades x coste unitario*		*= % total de la partida presupuestaria destinada a la gestión de riesgos de seguridad*
		ONGN/L	*Por ejemplo, suministros de hibernación y reubicación.*					
	Seguros	ONGI	*Por ejemplo, cobertura de seguro para el personal que participe en el partenariado.*					
		ONGN/L	*Por ejemplo, traslados médicos, seguro personal de accidentes.*					
	Contingencias generales	ONGI	*Normalmente, no se aplica a las ONGI cuando la ONGN/L es la coparte que implementa.*					
		ONGN/L	*Fondos de libre disponibilidad a los que puede acceder de inmediato en caso de una crisis o un incidente imprevistos.*					

Parte 5: Herramientas

Glosario

Aceptación del riesgo: proceso que conlleva una decisión consciente que la organización entiende y acepta sobre la cantidad de riesgo residual que desea asumir.

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

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

Árbol de seguridad: proceso para comunicar noticias con rapidez a toda una organización sin sobrecargar a ninguna persona en concreto. El proceso del árbol de seguridad implica asignar a cada integrante del personal un grupo pequeño de otras personas a las que tiene la responsabilidad de llamar si se produce una emergencia.

Compartir riesgos: las organizaciones comparten la responsabilidad por los riesgos de seguridad que les afectan.

Coparte: integrante de un partenariado formalizado (contractual) entre organizaciones de ayuda; normalmente, partenariados entre entidades internacionales-locales/nacionales.

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

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

Diagnóstico (conjunto) de riesgos de seguridad: proceso a través del cual las organizaciones identifican las distintas amenazas de seguridad que podrían afectar a su personal, sus activos y programas, y analizan su probabilidad e impacto a fin de determinar el grado de riesgo que implican. Un diagnóstico conjunto de riesgos de seguridad lo realizan las copartes juntas y también analiza las amenazas que puedan surgir a causa del propio partenariado.

Gestión de riesgos de seguridad: intentar reducir la exposición a los riegos más graves (incluidos los coyunturales, programáticos e institucionales) al identificar, supervisar y lidiar con los factores clave de riesgos. También implica sopesar riesgos y oportunidades, o un conjunto de riesgos frente a otro. La gestión de riesgos debería verse como un proceso propiciatorio, no como uno de mera precaución.

Habituación al riesgo: proceso normalmente inconsciente de acostumbrarse a la presencia de riesgos a consecuencia de una exposición constante al peligro, lo que disminuye la respuesta consciente a ellos. La habituación al riesgo es un reto al que puede enfrentarse el personal tanto de ONGI como de ONGN/L tras periodos prolongados de tiempo en una ubicación.

Localización: "el proceso de reconocer, respetar y fortalecer la independencia en el liderazgo y la toma de decisiones de las partes nacionales (y locales) de la acción humanitaria para así abordar mejor las necesidades de las poblaciones afectadas".[1]

Marco de gestión de riesgos de seguridad: conjunto de políticas, protocolos, planes, mecanismos y responsabilidades que faciliten reducir los riesgos de seguridad para el personal.

Organización no gubernamental internacional (ONGI): ONG cuyas operaciones tienen alcance más allá de un país o de una subregión.

Organización no gubernamental local (ONG): ONG que sobre todo opera en una zona geográfica determinada de un país. Su personal proviene principalmente de las comunidades a las que sirve la ONG. Las ONG locales suelen ser más grandes que las organizaciones comunitarias o las organizaciones de la sociedad civil, y disponen de una estructura más formal y desarrollada.

Organización no gubernamental nacional/local (ONGN/L): ONG local o nacional cuyas operaciones tienen lugar en su país de origen.

Organización no gubernamental nacional (ONGN): ONG que opera en varias partes de un país. Su personal puede ser trasladado para trabajar en otras zonas que no son su lugar de origen.

Partenariado: relación formalizada (contractual) entre organizaciones de ayuda, que suelen ser internacionales-locales/nacionales. Los partenariados en el sector de la ayuda pueden tener diversa forma, duración, ámbito y grado de colaboración.

1 Definición de la FICR, recuperada de https://media.ifrc.org/ifrc/document/ifrc-policy-brief-localization/

Plan de acción para la revisión conjunta de la gestión de riesgos de seguridad (el "plan de acción para la revisión conjunta de la GSR"): una lista minuciosa de tareas para que las copartes aborden conjuntamente las lagunas en los indicadores identificados mediante el proceso de revisión conjunta de la GRS.

Plan de gestión (conjunta) de riesgos de seguridad: a veces citado como "plan de seguridad". Se trata de un documento clave –normalmente en el ámbito de país– donde se describen las medidas y los procedimientos de seguridad de los que se dispone, y las funciones y las responsabilidades que tiene todo el personal en la gestión de los riesgos identificados. Un plan de gestión conjunta de riesgos de seguridad es un plan de seguridad elaborado y puesto en práctica por las organizaciones copartes juntas.

Propiedad del riesgo: cuando una persona o entidad tiene la responsabilidad y la autoridad para gestionar un riesgo.

Revisión conjunta de la gestión de riesgos de seguridad (la "revisión conjunta de la GRS"): enfoque o proceso mediante el cual las copartes exploran conjuntamente los conceptos de seguridad y sus planteamientos de seguridad, e identifican lo que tienen que hacer ambas (y con lo que deben contar) para fortalecer la gestión de riesgos de seguridad en el partenariado. Se realiza al rellenar un cuestionario, acordar los indicadores clave y evaluar si están presentes o no.

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

Riesgos de seguridad: riesgos físicos o psicológicos que surjan de actos bélicos, violencia, delitos y otros peligros.

Riesgo residual: riesgo que permanece tras aplicar las medidas de mitigación.

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

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

Sesgo: inclinación injusta o prejuicio hacia (o contra) un grupo determinado por motivos de raza, grupo étnico y otros aspectos identitarios, incluida la nacionalidad. Los sesgos tienen cuatro dimensiones principales:

1. **estructural:** políticas y prácticas sesgadas que mantienen múltiples instituciones, lo que se manifiesta en desigualdades en términos de poder, oportunidades, acceso, trato, y repercusiones y resultados de las políticas, ya sea de forma deliberada o no.
2. **institucional:** políticas y prácticas que refuerzan los prejuicios a consecuencia de la distribución desigual sistemática de recursos, poder y oportunidades en una organización.
3. **interpersonal:** actos y microagresiones que se basan en prejuicios entre personas.
4. **internalizada:** mensajes sutiles y manifiestos de personas que refuerzan creencias y estereotipos negativos y de odio.

Transferencia de riesgos: formación o transformación de riesgos (que aumentan o disminuyen) para una parte causada por la presencia o acción de otra parte, ya sea de forma intencionada o no.

Umbral de riesgo: se alcanza el umbral de riesgo aceptable cuando, tras poner en práctica las medidas de mitigación, el grado de riesgo residual/actual no lo soporta la actitud hacia el riesgo que ha declarado una organización.

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

Referencias

Stop Impunity: Call for Action for Safeguarding of Humanitarian Space and Ending Impunity for Attacks against Humanitarians (s.f.). Recuperado de: https://www.stopimpunity.net/

Aid Reimagined (s.f.): https://medium.com/aidreimagined

Alliance for Empowering Partnership (A4EP). (s.f.). 'Resource Centre'. Disponible en: https://a4ep.net/?cat=17

Behn, O. y Kingston, M. (2010). *Risk Thresholds in Humanitarian Assistance*. European Interagency Security Forum (EISF). Recuperado de: https://gisf.ngo/resource/risk-thresholds-in-humanitarianassistance/

Bickley, S. (2017). *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*. European Interagency Security Forum (EISF). Retrieved from: https://gisf.ngo/wp-content/uploads/2019/05/Gestio%CC%81n-de-riesgos-de-seguridad-Spanish.pdf

Buth, P. (2010). *Crisis Management of Critical Incidents*. European Interagency Security Forum (EISF). Recuperado de: https://gisf.ngo/resource/crisis-management-of-critical-incidents/

Charter4Change (s. f.). "Resources". Disponible en: https://charter4change.org/resources/

cinfo (s.f.). "Duty of Care Maturity Model Tool", cinfo. Recuperado de: http://dutyofcare.cinfo.ch/

Davis, J. et al. (2020). *Seguridad en práctica: herramientas de gestión de riesgos para organizaciones de ayuda humanitaria, 2º edición*. Global Interagency Security Forum (GISF). Recuperado de: https://gisf.ngo/resource/security-to-go/

DisasterReady (s.f.): https://get.disasterready.org/?gclid=Cj0KCQiAgomBBhDXARIsAFNyUqPRVm_69sS6omcjFq5CmIpTLNLdpl8ppnlibqLHMfMxaAYe994pikMaAkKaEALw_wcB

EISF (2019). *Gestión de la violencia sexual contra el personal humanitario prevención, preparación, respuesta y atención posterior*. European Interagency Security Forum (EISF). Recuperado de: https://gisf.ngo/resource/managing-sexual-violence-against-aid-workers/

EISF y cinfo (2018). *Duty of Care Maturity Model*. EISF y cinfo. Recuperado de: https://www.cinfo.ch/sites/default/files/matrix_web_pdf.pdf

EISF (2017). *Abduction and Kidnap Risk Management*. European Interagency Security Forum (EISF).

EISF (2018). *Gestión de la Seguridad del Personal Humanitario con Perfiles Diversos*. European Interagency Security Forum (EISF). Recuperado de: https://gisf.ngo/resource/gestion-de-la-seguridad-del-personal-humanitario-con-perfiles-diversos/

EISF (2019). "An open letter to non-governmental and donor organisations from the European Interagency Security Forum", *European Interagency Security Forum (EISF)*. Recuperado de: https://gisf.ngo/an-open-letter-to-non-governmental-and-donor-organisations-from-the-european-interagency-security-forum/

Fairbanks, A. (2018). *Duty of Care under Swiss law: How to improve your safety and security risk management processes*. EISF y cinfo. Recuperado de: https://www.cinfo.ch/sites/default/files/duty_of_care_eisf.pdf

Fast, L. y Bennett, C. (2020). *From the ground up: it's about time for local humanitarian action*. Humanitarian Practice Group (HPG). Recuperado de: https://www.odi.org/publications/16991-ground-it-s-about-time-local-humanitarian-action

Featherstone, A. (2019). *Localisation Performance Measurement Framework*. Network for Empowered Aid Response (NEAR). Recuperado de: https://ngocoordination.org/system/files/documents/resources/near-localisation-performance-measurement-framework.pdf

Finucane, C. (2013). *Auditorías de seguridad*. European Interagency Security Forum (EISF). Recuperado de: https://gisf.ngo/resource/security-audits/

Finucane, C. (2013). *The Cost of Security Risk Management for NGOs*. European Interagency Security Forum (EISF). Recuperado de: https://gisf.ngo/resource/the-cost-of-srm-for-ngos/

GISF (2020). *Partnerships and Security Risk Management: from the local partner's perspective*. Global Interagency Security Forum (GISF). Recuperado de: https://gisf.ngo/resource/partnerships-and-security-risk-management-from-the-local-partners-perspective/

Global Mentoring Initiative (2019). *Partnerships: Pre-conditions, Principles and Practices*. Global Mentoring Initiative. Recuperado de: https://static1.squarespace.com/static/58256bc615d5db852592fe40/t/5d93782768d49710fa7a8349/1569945640280/Partnership+conditions+principles+practices.pdf

Global Mentoring Initiative (s.f.). Resources. Disponible en: https://www.gmentor.org/competencies-development-centre

Humanitarian Leadership Academic (s.f.). Kaya Connect. Disponible en: https://kayaconnect.org/

Humanitarian Outcomes (s.f.). Aid Worker Security Database. Disponible en: https://aidworkersecurity.org/

IFRC (s.f.). Learning Platform. Disponible en: https://www.ifrc.org/en/get-involved/learning-education-training/learning-platform1/

IFRC (2018). *IFRC Policy Brief: Localization – what it means and how to achieve it*. IFRC. Recuperado de: https://media.ifrc.org/ifrc/document/ifrc-policy-brief-localization/

INSSA (s.f.): https://inssa.org/

Insecurity Insight (s.f.): "Aid in Danger". Disponible en: http://www.insecurityinsight.org/aidindanger/

International NGO Safety Organisation (INSO) (s.f.). 'INSO Key Data Dashboard'. Disponible en: https://ngosafety.org/keydata-dashboard/

Kemp, E. y Merkelbach, M. (2016). *Duty of Care: a review of the Dennis v. Norwegian Refugee Council ruling and its implications*. European Interagency Security Forum (EISF). Recuperado de: https://gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/

McManus, S. y Tennyson, R. (2008). *Talking the Walk: A Communication Manual for Partnership Practitioners*. International Business Leaders Forum on behalf of The Partnering Initiative. Recuperado de: https://thepartneringinitiative.org/wp-content/uploads/2014/08/TalkingTheWalk.pdf

Moutard, L. (2021). "How to effectively advocate for aid workers' protection?", Global Interagency Security Forum (GISF). Recuperado de: https://gisf.ngo/blogs/how-to-effectively-advocate-for-aid-workers-protection/

NEAR (s.f.): https://www.near.ngo/

Newton, M. (2020). "Developing a 'COVID-19 Secure' HEAT course", Global Interagency Security Forum (GISF). Recuperado de: https://gisf.ngo/blogs/developing-a-covid-19-secure-heat-course/

Persaud, C. (2012). *Género y seguridad: directrices para transversalización del género en la gestión de riesgos de seguridad*. European Interagency Security Forum (EISF). Recuperado de: https://gisf.ngo/resource/genero-y-seguridad/

Plataforma Humanitaria Mundial (2007). *Principios de asociación*. Recuperado de: https://iecah.org/plataforma-humanitaria-mundial-ghp/

Race Forward (2015). *Race Reporting Guide*. Race Forward. Retrieved from: https://www.raceforward.org/sites/default/files/Race%20Reporting%20Guide%20by%20Race%20Forward_V1.1.pdf

RedR UK, Insecurity Insight y EISF (2017). *Manual de gestión de la información sobre incidentes de seguridad*. Recuperado de: https://www.eisf.eu/library/security-incident-information-management-handbook/

Safeguarding Health in Conflict Coalition (s.f.): https://www.safeguardinghealth.org/

Singh, I. (2012). *Security Management and Capacity Development: International agencies working with local partners*. European Interagency Security Forum (EISF). Recuperado de: https://gisf.ngo/resource/international-agencies-working-withlocal-partners/

Stoddard, A., Czwarno, M. y Hamsik, L. (2019). *NGOs and Risk: Managing Uncertainty in Local-International Partnerships. Global Report*. Humanitarian Outcomes/Interaction. Recuperado de: https://www.humanitarianoutcomes.org/publications/ngos-risk2-partnerships

Sweeney, A. (2019). "Reflections on GISF's 'At What Cost?' Campaign", *European Interagency Security Forum (EISF)*. Recuperado de: https://gisf.ngo/blogs/reflections-on-eisfs-at-what-cost-campaign/

Syrian Network for Human Rights (s.f.): https://sn4hr.org/

The Partnering Initiative (s.f.). "The Partnering Cycle and Partnering Principles", The Partnering Initiative. Recuperado de: https://thepartneringinitiative.org/the-partnering-cycle-and-partnering-principles/

UNDSS (s.f.). Training. Disponible en: https://training.dss.un.org/

van Brabant, K. (2010). *Informe de buenas prácticas 8 - Gestión de la seguridad de las operaciones en entornos violentos*. Overseas Development Institute (ODI). Recuperado de: https://odihpn.org/wp-content/uploads/2011/04/GPR8_revised_edition_Spanish.pdf

Whiting, C. (2016). *Manual de Incidencia de Foros de ONG: realizando incidencia conjunta*. ICVA. Recuperado de: https://www.icvanetwork.org/system/files/versions/NGO_Incidencia_Foro.pdf

Working Group on Protection of Humanitarian Action. (2018). *Toolkit: Responding to Violence against Humanitarian Action on the Policy Level*. Recuperado de: https://reliefweb.int/report/world/toolkit-responding-violence-against-humanitarian-action-policy-level

Otras publicaciones del GISF

Disponible en **www.gisf.ngo**

Si le interesa contribuir en próximos proyectos de investigación o quiere proponer temas para investigar en un futuro, póngase en contacto con **gisf-research@gisf.ngo**.

In 2020, EISF (European Interagency Security Forum) became GISF (Global Interagency Security Forum), reflecting the extension of its network.

You can access all the resources mentioned in this guide on GISF's new website: **www.gisf.ngo**

Documentos informativos e informes

Partenariados y gestión de riesgos de seguridad: desde la perspectiva de la coparte local
Octubre de 2020
Moutard, L. – GISF

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

Gestión de la seguridad del personal humanitario con perfiles diversos
Septiembre de 2018
Jones, E. et al. – EISF

Communications Technology and Humanitarian Delivery: Challenges and Opportunities for Security Risk Management – 2º edición
Diciembre de 2016
Vazquez Llorente, R. y Wall, I. (eds.)

Security Risk Management and Religion: Faith and Secularism in Humanitarian Assistance
Agosto de 2014
Hodgson, L. et al. Edición de Vazquez, R.

The Future of Humanitarian Security in Fragile Contexts
Marzo de 2014
Armstrong, J. Con el apoyo del Secretariado del EISF

The Cost of Security Risk Management for NGOs
Febrero de 2013
Finucane, C. Edición de Zumkehr, H. J. – Secretariado del EISF

Security Management and Capacity Development: International Agencies Working with Local Partners
Diciembre de 2012
Singh, I. y el Secretariado del EISF

Género y seguridad: Directrices para la transversalización del género en la gestión de riesgos de seguridad
Septiembre de 2012 – Disponible en español, francés e inglés
Persaud, C. Edición de Zumkehr, H. J. – Secretariado del EISF

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
Diciembre de 2011 – Disponible en francés
Glaser, M. Con el apoyo del Secretariado del EISF (edición)

Risk Thresholds in Humanitarian Assistance
Octubre de 2010
Kingston, M. y Behn O.

Abduction Management
Mayo de 2010
Buth, P. Con el apoyo del Secretariado del EISF (edición)

Crisis Management of Critical Incidents
Abril de 2010
Buth, P. Con el apoyo del Secretariado del EISF (edición)

The Information Management Challenge
Marzo de 2010
Ayre, R. Con el apoyo del Secretariado del EISF (edición)

Joint NGO Safety and Security Training
Enero de 2010
Kingston, M. Con el apoyo del Grupo de Trabajo de Formación del EISF

Humanitarian Risk Initiatives: 2009 Index Report
Diciembre de 2009
Finucane, C. Edición de Kingston, M.

Artículos

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

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

Demystifying Security Risk Management
Febrero de 2017, (en PEAR Insights Magazine)
Fairbanks, A.

Duty of Care: A Review of the Dennis v Norwegian Refugee Council Ruling and its Implications
Septiembre de 2016
Kemp, E. y Merkelbach, M. Edición de Fairbanks, A.

Organisational Risk Management in High-risk Programmes: The Non-medical Response to the Ebola Outbreak
Julio 2015, (en Humanitarian Exchange, nº 64)
Reilly, L. y Vazquez Llorente, R.

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

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

Otras publicaciones del GISF

Whose Risk Is it Anyway? Linking Operational Risk Thresholds and Organisational Risk Management
Junio de 2010, (en *Humanitarian Exchange*, nº. 47)
Behn, O. y Kingston, M.

Risk Transfer through Hardening Mentalities?
Noviembre de 2009
Behn, O. y Kingston, M.

Guías

Seguridad en práctica: herramientas de gestión de riesgos para organizaciones de ayuda humanitaria – 4º edición
Octubre de 2020 – Disponible en español, inglés y francés
Davis, J. et al.

Gestión de la violencia sexual contra el personal humanitario: prevención, preparación, respuesta y atención posterio
Marzo de 2019
EISF

Abduction and Kidnap Risk Management
Noviembre de 2017
EISF

Manual de Gestión de la Información sobre Incidentes de Seguridad
Septiembre de 2017
Insecurity Insight, Redr UK, EISF

Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas
Junio de 2017
Bickley, S.

Office Opening
Marzo de 2015 – Disponible en francés
Source8

Auditorías de seguridad
Septiembre de 2013 – Disponible en español, francés e inglés
Finucane C. Edición de French, E. y Vazquez Llorente, R. (ES y FR) – Secretariado del EISF

Managing the Message: Communication and Media Management in a Crisis
Septiembre de 2013 – Disponible en francés
Davidson, S. Edición de French, E. – Secretariado del EISF

Family First: Liaison and Support During a Crisis
Febrero de 2013 – Disponible en francés
Davidson, S. Edición de French, E. – Secretariado del EISF

Office Closure
Febrero de 2013
Safer Edge. Edición de French, E. y Reilly, L. – Secretariado del EISF