

Gestión de riesgos de seguridad humanitaria

Informe de buenas
prácticas 8
Tercera edición



Humanitarian Practice Network (HPN)

ODI Global
4 Millbank
Londres, SW1P 3LL
Reino Unido

Correo electrónico: hpn@odi.org.uk

Sitio web: www.odihpn.org

Impreso y encuadernado en el Reino Unido por Formara Print
and Marketing

Maquetación y producción: Jessica Rennoldson

Esta edición fue traducida con el apoyo de CLEAR Global
(clearglobal.org/).

Traductoras: María Eugenia Bergamin, Silvina Alejandra
Villosio, Ana Lilia Moreno Trejo, Ana Patricia Castañeda
Revisoras: Ivana Benzaquen, Mariana Duque-Díez, Adelicia
Fairbanks

© ODI Global, Londres, 2025

ISBN: 978-1-0682923-2-3

Se invita a los lectores a reproducir el material para sus
propias publicaciones, siempre que no se destine a la venta
comercial. ODI Global exige el debido reconocimiento y una
copia de la publicación.

Las solicitudes para la reproducción comercial del material de
HPN deben dirigirse a ODI Global como titular de los derechos
de autor. El coordinador de la red de HPN agradecerá que se
le comuniquen los detalles sobre el uso de cualquiera de estos
materiales en actividades de formación, investigación o de
diseño, aplicación o evaluación de programas.

Las opiniones presentadas en este documento pertenecen a
sus autores y no representan necesariamente las opiniones de
ODI Global o de nuestros socios.

Esta obra se ha publicado bajo la licencia CC BY-NC-ND 4.0.

Informe de buenas prácticas

Gestión de riesgos de seguridad humanitaria

Junio de 2025

Tercera edición

Índice

Autoría y reconocimientos	7
Descargo de responsabilidad	11
Glosario de términos de seguridad	12
Prólogo	19
Introducción	21

Primera parte Fundamentos de la gestión de riesgos de seguridad humanitaria 27

- 1.1 Conceptos y principios clave
- 1.2 Enfoque de seguridad centrado en la persona

Segunda parte Los ecosistemas de la gestión de riesgos de seguridad 61

- 2.1 Redes y colaboración de seguridad
- 2.2 Incidencia y seguridad

Tercera parte Elementos organizativos: estructuras e instrumentos para políticas 85

- 3.1 El sistema de gestión de riesgos de seguridad humanitaria
- 3.2 Acceso y seguridad
- 3.3 Financiación de la gestión de riesgos de seguridad
- 3.4 Monitoreo del cumplimiento, la eficacia y el impacto
- 3.5 Gestión de riesgos de seguridad en las alianzas

Cuarta parte Elementos operativos: procesos y herramientas 147

- 4.1 Elementos analíticos
- 4.2 Elaborar una estrategia de seguridad
- 4.3 Planes y disposiciones de seguridad
- 4.4 Respuesta a incidentes y gestión de crisis

Quinta parte Las personas en la gestión de riesgos de seguridad **249**

- 5.1 Recursos humanos
- 5.2 Capacitación en seguridad
- 5.3 Comunicación sobre seguridad en la organización
- 5.4 Cuidado del personal
- 5.5 Consideraciones médicas y de salud

Sexta parte Tecnología y seguridad **331**

- 6.1 Gestión de la seguridad de la información y las comunicaciones
- 6.2 La seguridad en un mundo digital

Séptima parte Gestión de amenazas y situaciones de riesgo específicas **383**

- 7.1 Seguridad en los viajes
- 7.2 Seguridad del sitio
- 7.3 Seguridad del dinero en efectivo
- 7.4 Criminalidad
- 7.5 Vigilancia hostil
- 7.6 Disturbios civiles
- 7.7 Violencia sexual
- 7.8 Detención y arresto
- 7.9 Rapto, secuestro y situaciones de rehenes
- 7.10 Amenazas relacionadas con el combate y los restos de material de guerra

Epílogo **526**

Autoría y reconocimientos

Esta versión revisada del *Informe de buenas prácticas* está dedicada a los numerosos especialistas en seguridad humanitaria que trabajan incansablemente para apoyar a sus colegas y organizaciones. Está dedicada a quienes ya no están entre nosotros, cuyas contribuciones y dedicación a este campo serán siempre recordadas.

Esta tercera edición fue coeditada por Adelia Fairbanks y Abby Stoddard de Humanitarian Outcomes, quienes contaron con el apoyo de Mónica Czwarno y Meriah-Jo Breckenridge, también de Humanitarian Outcomes. Samiha Ahmed coordinó el proceso de producción para HPN, y Matthew Foley, editor en ODI Global, editó el manuscrito. Este informe se basa en el trabajo de ediciones anteriores, dirigidas por Koenraad Van Brabant, Adele Harmer, Abby Stoddard y Katherine Haver.

Los colaboradores del presente documento dedicaron generosamente su tiempo para revisar contenidos, facilitar recursos, compartir conocimientos y consejos, y contribuir a la redacción. Este informe es realmente un esfuerzo colectivo, que cuenta con las contribuciones de:

Banu Altunbas

Tara Arthur, Collective Security Group

Javeria Ayaz Malik, ActionAid e International NGO Safety and Security Association

Petro Babyak, Mercy Corps Ucrania

Shaun Bickley, Tricky Locations

Awil Bihi, CARE

Tamsin Blake, Medair

Donald S. Bosch, Ph.D., Psya.D., Humanitarian Psychological Services

Phil Candy, Medair

Araba Cole

Amaury T. Cooper

Gonzalo de Palacios, Oxfam

Steve Dennis, Consultoría en Recuperación, Proper Support

Catherine Deseure-Plumridge, UNDSS

Gurpreet Dhoot, Fauna & Flora

Neil Elliot, MSyl, Oxfam Internacional

Daniel Elliott, Catholic Agency for Overseas Development

Shannon Fariel-Mureithi, ChildFund International

Anthony Val Flynn, Dirección General de Asociaciones Internacionales de la Comisión Europea

Alexandra Godoi, Oxfam Reino Unido y Oxfam Internacional
Paul Herridge, Itad
Henrieke Hommes, ZOA
Heather Hughes, Global Interagency Security Forum
Stephen Ingram, Mines Advisory Group
Rafael K. Khusnutdinov, RTI International
Jean-Philippe Kiehl, Comité Internacional de la Cruz Roja
Sarah Kilani, Centre on Armed Groups
Jenna Kuokkanen, World Vision International
Elodie Leroy-Le Moigne, Plan International
Armstrong Maina, Proyecto HOPE
Steven A. Mercer, Samaritan's Purse International Relief
Alan Mordaunt, Trócaire
Robert Muggah, Instituto Igarapé
Noemi Muñoz Zamora, International Rescue Committee
Michael O'Neill, International NGO Safety and Security Association
Kevin Pedone, Clements Worldwide
Carina Peña, Programa Mundial de Alimentos
Christine Persaud, Universidad de Quebec, Montreal
William Plowright, Universidad de Durham
Adrian Powell, Proelium Law LLP
Pegah Rajabi, International NGO Safety Organisation
Jeremy Reeves
Lisa Reilly
Jochen Riegg, Norwegian Refugee Council
Scott Ruddick, Cowater International
Rod Slip, Oxfam
Craig Spencer, Doctor en Medicina, Magíster en Salud Pública, Escuela de Salud Pública de la Universidad Brown
Barry Steyn, International Rescue Committee
Matt Stockton, Global Interagency Security Forum
Sandrine Tiller, Médicos sin Fronteras
Marieke van Weerden
Julian Visser, ZOA

Ron Waldman, Doctor en Medicina, Magíster en Salud Pública, Escuela de Salud Pública del Instituto Milken, Universidad George Washington

Benjamin Whelan, Access Now

Christina Wille, Insecurity Insight

Chris Williams, CARE

Christine Williamson, Duty of Care International

Ian Woodmansey, Crucial Safety

Tara Yip-Bannicq Ward, Plan International

Hannah Zitner, International Rescue Committee

Descargo de responsabilidad de este Informe de buenas prácticas

ODI Global, en toda la extensión permitida por la ley;

1. No realizará ni implicará ninguna representación, promesa o garantía en cuanto a las orientaciones o el asesoramiento proporcionados en este *Informe de buenas prácticas* (GPR, por sus siglas en inglés).
2. No realizará, implicará ni garantizará la calidad, la vida o el uso de este GPR publicado en 2025, ni que sea adecuado para algún propósito en particular o para su uso en condiciones específicas.
3. No asumirá responsabilidad alguna por pérdidas, daños o inconvenientes derivados del uso, o de la imposibilidad de uso, o de la interpretación de la información contenida en este GPR.
4. No asumirá ningún deber de cuidado ni responsabilidad y no será responsable ante usted, o ante cualquier otra persona, por ningún daño incurrido por cualquier decisión tomada o acción emprendida a la luz de la información proporcionada en este GPR.

Toda la información contenida en este GPR es presentada por ODI Global o sus colaboradores externos que contribuyeron a este GPR según su entendimiento en el momento de la publicación de la guía de gestión de riesgos de seguridad para fines generales. El presente GPR no debe considerarse una declaración adecuada o válida sobre ningún procedimiento operativo estándar, patrones de amenaza en un país concreto o la gestión de riesgos de seguridad de uno o más organismos.

Pese a que ODI Global se ha esforzado por asegurar la exactitud y la calidad de la información presentada aquí, no puede garantizar la exactitud o la calidad de la información presentada en este GPR. Usted debe evaluar por su cuenta el riesgo y el comportamiento que debe adoptar en entornos de alto riesgo, violentos o potencialmente de alto riesgo o violentos, incluso en las condiciones descritas en este GPR. Ese documento no puede, bajo ninguna circunstancia, reemplazar sus obligaciones de realizar su propia diligencia debida o evaluación antes de operar en cualquier entorno violento, de alto riesgo o potencialmente violento o de alto riesgo. Este GPR se hace público con carácter no vinculante.

El presente GPR puede incluir opiniones o recomendaciones de terceros y no refleja necesariamente las opiniones de ODI Global ni indica un compromiso con un curso de acción en particular.

Glosario de términos de seguridad

El siguiente glosario contiene términos y conceptos clave pertinentes para este *Informe de buenas prácticas*.¹

Acceso humanitario Capacidad de los agentes humanitarios para llegar a las poblaciones afectadas, y capacidad de las personas afectadas para acceder a la asistencia y a los servicios.

Acoso Conducta abusiva o no deseada, continuada y dirigida a una persona, que le causa angustia o malestar.

Alianza Cualquier relación de trabajo formalizada entre dos o más organizaciones para alcanzar objetivos acordados, como en la ejecución de un programa de ayuda.

Amenaza Cualquier acontecimiento, acción o entidad con el potencial de causar daño al personal, a los programas o a los activos, o de obstaculizar la consecución de los objetivos de la ayuda.

Antivigilancia Práctica consistente en detectar actividades de vigilancia para, por ejemplo, determinar si se están estudiando los movimientos del personal o las instalaciones con fines maliciosos.

Análisis de aceptación Proceso de evaluación de los niveles de aceptación que tiene la organización entre las distintas partes interesadas del entorno.

Análisis del contexto Proceso de comprensión del entorno en el que opera una organización como primer paso para identificar posibles amenazas y vulnerabilidades de seguridad.

Análisis o mapeo de actores Ejercicio dirigido a identificar y analizar a los actores o las partes interesadas en un entorno determinado que son clave para comprender el contexto y que pueden afectar la seguridad de una organización.

Apetito de riesgo Comprensión compartida del nivel y del tipo de riesgo que una organización está dispuesta a aceptar para alcanzar sus objetivos.

Apoyo psicosocial Enfoque que integra los aspectos psicológicos y sociales del bienestar y aborda el impacto de las relaciones, el entorno y la comunidad en la salud mental.

1 Este glosario adapta y se ajusta al glosario del Global Interagency Security Forum (GISF): <https://gisf.ngo/glossary-spanish/>.

Arresto Captura y detención de una persona por una autoridad oficial (policial o militar) en relación con un crimen, un delito o una infracción.

Auditoría de seguridad Examen interno o externo basado en pruebas que evalúa la eficacia de la gestión de riesgos de seguridad de la organización y su cumplimiento del deber de cuidado del personal.

Cadena de comunicación Sistema jerárquico utilizado para difundir rápidamente información a un grupo numeroso de personas por teléfono, mensajes de texto, correo electrónico u otros medios.

Colaboración de seguridad Organizaciones que actúan conjuntamente para abordar preocupaciones comunes en materia de seguridad y acceso, intercambiar información sobre incidentes y riesgos y reforzar sus capacidades colectivas de gestión de riesgos.

Compartir riesgos Compartir equitativamente la responsabilidad entre los socios de la organización por los riesgos que afectan a ambas.

Convoy Grupo de vehículos (o embarcaciones) que viajan juntos de forma organizada, para apoyarse y protegerse mutuamente.

Coordinación civil-militar Interacción entre las fuerzas militares y las organizaciones humanitarias o los actores civiles necesaria para promover los principios humanitarios, asegurar el acceso y proteger a los trabajadores humanitarios y a otros civiles.

Crisis Acontecimiento o serie de acontecimientos que perturban de forma significativa el funcionamiento normal de una organización y que tienen consecuencias graves para el personal o la organización, por lo que exigen medidas extraordinarias y la actuación inmediata del equipo directivo.

Criticidad del programa Medida del grado en que la vida o la liberación del sufrimiento extremo de las personas dependen de la continuidad de la actividad de ayuda.

Cultura de seguridad Suposiciones, creencias y valores compartidos que conforman el comportamiento en torno a la seguridad en las organizaciones. Puede ser positiva o negativa.

Deber de cuidado Obligación (moral y legal) de una organización de velar por la seguridad y el bienestar de las personas que realizan su trabajo.

Detención Retención de una persona contra su voluntad por una persona o un grupo, pero sin cargos formales ni una fecha o condiciones claras para su liberación.

Discurso de odio Contenido escrito u oral que se dirige contra un grupo o una persona por motivos relacionados con sus características inherentes, como su grupo étnico, religión o género.

Empresas o servicios de seguridad privada Entidad privada que presta servicios de seguridad remunerados a personas u organizaciones.

Enfoque centrado en el superviviente Enfoque que prioriza las necesidades, los derechos y la seguridad de las personas afectadas por sucesos traumáticos. Hace hincapié en el respeto, la confidencialidad y la autonomía, permite que los supervivientes tomen decisiones informadas y reconoce su posible necesidad de apoyo durante el proceso de recuperación.

Enfoque de aceptación Enfoque de la gestión de riesgos de seguridad que intenta reducir o eliminar las amenazas mediante el establecimiento de relaciones con las comunidades locales y las partes interesadas relevantes en la zona de operaciones y la obtención de su aceptación y/o consentimiento respecto a la presencia y el trabajo de la organización.

Enfoque de disuasión Enfoque de seguridad que consiste en reducir o eliminar las amenazas por medio de una contraamenaza que disuada o influya en los posibles agresores.

Enfoque de protección Enfoque de seguridad cuyo objetivo es reducir la exposición del personal a determinadas amenazas mediante mecanismos y procedimientos de protección.

Enfoque de seguridad centrado en la persona Enfoque de gestión de riesgos de seguridad que sitúa a las personas en el centro de las actividades de gestión de riesgos de seguridad y tiene en cuenta sus perfiles de riesgo personales. Reconoce los riesgos específicos del perfil a los que se enfrentan las personas debido a su identidad interseccional, su comportamiento, su función y organización, y el contexto en el que trabajan.

Estrategia de seguridad Enfoque de una organización sobre la gestión de la seguridad que depende del entorno operacional y de los riesgos existentes en ese lugar y en el que inciden los principios y los valores de la organización.

Estrés Reacción emocional, cognitiva, física o conductual ante presiones y situaciones difíciles.

Evacuación Proceso de retirar al personal por razones de seguridad y trasladarlo a un lugar seguro al otro lado de las fronteras internacionales de un país.

Evaluación de amenazas Proceso de identificación y análisis de fuentes potenciales de daño en un entorno operacional.

Evaluación de vulnerabilidad Proceso de análisis del grado en que el personal, las propiedades y los activos de una organización están expuestos a amenazas.

Evaluación y análisis del riesgo Proceso analítico de varias etapas mediante el cual las organizaciones identifican los riesgos para el personal, los activos, los programas y la reputación y los evalúan según su probabilidad e impacto a fin de determinar su gravedad.

Desconflicción (“deconfliction”, en inglés) Intercambio de información entre los agentes humanitarios y las fuerzas militares para prevenir ataques contra instalaciones, personal y operaciones de ayuda, notificando a las partes en conflicto la ubicación y los movimientos del personal y las actividades humanitarias.

Extorsión Uso de coacción, amenazas o intimidación para obtener dinero, bienes o acciones del objetivo.

Formación sobre sensibilización para entornos hostiles (HEAT, por sus siglas en inglés) Capacitación en seguridad personal concebida para quienes trabajan en entornos de alto riesgo, que suele incluir actividades basadas en escenarios.

Gestión de información sobre incidentes de seguridad Proceso de recopilación y utilización de la información relativa a los incidentes de seguridad para controlar las tendencias e informar la toma de decisiones.

Gestión de los riesgos institucionales Proceso organizativo de identificación y gestión de todos los riesgos, incluidos, entre otros, los riesgos de seguridad, que podrían afectar a sus objetivos, las operaciones y las partes interesadas.

Gestión de riesgos de seguridad Sistema organizativo para evaluar y mitigar los riesgos y responder a los incidentes.

Hibernación Cese temporal de las actividades habituales de un proyecto mientras el personal permanece en la oficina, en casa o en otro lugar seguro, para evitar una amenaza emergente o hasta que las condiciones mejoren.

Identidad interseccional La interconexión de los múltiples factores de la identidad de las personas que conforman sus perfiles de riesgo personales.

Incidente crítico Suceso o serie de sucesos que amenazan gravemente el bienestar del personal y que pueden provocar la muerte, lesiones o enfermedades potencialmente mortales. Un incidente crítico puede ser demasiado grave para tratarse a través de las estructuras de gestión estándar y requiere apoyo y capacidades adicionales.

Incidente Evento de seguridad adverso que provoca o puede provocar daños al personal, interrupciones en los programas y en las actividades o pérdidas o daños a los activos o a la reputación de la organización.

Información errónea, desinformación e información manipulada La información errónea es información inexacta o falsa que se transmite sin la intención de engañar. La desinformación es información deliberadamente falsa o engañosa. La información manipulada es información verdadera que se extrae de su contexto original o se manipula para inducir a error o causar daño.

Marco de gestión de riesgos de seguridad Conjunto de políticas, protocolos, planes, mecanismos y responsabilidades que apoyan la reducción de los riesgos de seguridad para el personal.

MEDEVAC Evacuación médica. Traslado de un paciente por carretera, mar o aire mediante transporte sanitario especializado y con asistencia durante el viaje, con el fin de obtener tratamiento médico en otro lugar.

Mitigación de riesgos Acciones que, para reducir los riesgos, disminuyen la probabilidad y el impacto potencial del daño.

Niveles de seguridad Sistema utilizado para clasificar y comunicar el nivel de riesgo para el personal en un contexto o lugar específico y para orientar las decisiones, las acciones y las medidas de gestión de riesgos de seguridad en respuesta al aumento de la inseguridad (también denominado *fases de seguridad*).

Niveles o clasificación de los riesgos Riesgos evaluados y clasificados en función de su gravedad en términos de probabilidad e impacto.

Perfil de riesgo personal Conjunto único de riesgos a los que se enfrenta una persona en función de su identidad interseccional, que está conformado en parte por la forma en que sus atributos personales son percibidos por los demás.

Personal o referente de seguridad Miembro del personal cuya función incluye las responsabilidades relacionadas con la seguridad.

Plan de contingencia Conjunto de procedimientos y medidas preestablecidos y adaptados al contexto local que guían al personal en la coordinación de una respuesta rápida y eficaz a perturbaciones o incidentes de seguridad específicos.

Plan de seguridad Documento o conjunto de documentos sobre un lugar específico en los que se describen las medidas y los procedimientos establecidos para gestionar la seguridad, así como las responsabilidades y los recursos necesarios para aplicarlos.

Política de seguridad Documento de gobernanza que establece el enfoque de la organización sobre la seguridad y los riesgos de seguridad, los principios clave que sustentan este enfoque y las funciones y responsabilidades que tienen todos los miembros del personal en la gestión de riesgos.

Primeros auxilios Prestación de asistencia inmediata a una persona enferma, herida o emocionalmente angustiada (primeros auxilios psicológicos) hasta que obtenga ayuda profesional.

Procedimientos operativos estándar (POE) Conjunto de instrucciones paso a paso para ayudar al personal a llevar a cabo operaciones rutinarias o responder a situaciones específicas de forma que se maximice la seguridad.

QBRN Amenazas o armas químicas, biológicas, radiológicas y nucleares.

Rapto Cualquier captura ilegal y forzada de una persona o un grupo.

Requisitos mínimos de seguridad Protocolos que la organización espera que todo el personal aplique para garantizar la seguridad de los activos, el personal y la información.

Rescate Dinero, bienes o servicios exigidos o pagados a cambio de la liberación segura de personas raptadas.

Reubicación Retirar al personal y los bienes de lugares inseguros y trasladarlos a zonas más seguras dentro del país hasta que la situación se estabilice.

Riesgo La probabilidad de que ocurra algo perjudicial, y la magnitud del daño en caso de que ocurra.

Riesgo residual Nivel de riesgo restante después de haber tomado todas las medidas de mitigación de riesgos adecuadas.

Riesgos basados en la identidad Los riesgos que corre el personal como consecuencia de sus atributos personales y de cómo estos son percibidos.

Salvar Vidas Juntos (SLT, por sus siglas en inglés) Marco para la colaboración de seguridad entre el Sistema de Gestión de la Seguridad de las Naciones Unidas, las organizaciones no gubernamentales internacionales y otras organizaciones internacionales a escala mundial y en contextos de respuestas humanitarias compartidas.

Secuestro Captura por la fuerza de una persona o de un grupo de personas que se retienen contra su voluntad en un lugar desconocido hasta que se satisfacen las demandas de pago de un rescate u otras concesiones.

Seguridad (ante hechos accidentales) (“safety”, en inglés) Ausencia de riesgos o daños derivados de actos no intencionados (accidentes, fenómenos naturales o enfermedades). También llamado salvaguarda.

Seguridad (ante hechos intencionales) (“security”, en inglés) Ausencia de riesgos o daños derivados de la violencia u otros actos intencionados. También llamado salvaguarda.

Seguridad de la información Práctica consistente en proteger la información contra el acceso no autorizado, el hurto, la divulgación, la alteración, la modificación o la destrucción.

Seguridad digital Medidas, estrategias y procesos destinados a mitigar los riesgos relacionados con el uso de las tecnologías digitales, y con la presencia y los comportamientos digitales de una persona o de una organización.

Situación de rehén Retención de una persona o de un grupo por la fuerza en un lugar conocido, como en una situación de asedio, hasta que se satisfacen las demandas específicas.

Transferencia de riesgos Creación, transformación o traslado intencional o no intencional de riesgos de un agente a otro.

Trauma Experiencia angustiante o perturbadora que sobrepasa la capacidad de una persona para afrontarla y que tiene efectos adversos duraderos en su funcionamiento y bienestar.

Umbral de riesgo Límite de riesgo aceptable que la organización o una persona no está dispuesta a traspasar.

Vigilancia hostil Observación rigurosa de personas, bienes o propiedades con intenciones maliciosas, como la planificación de un ataque.

Violencia sexual Cualquier acto sexual que ocurra por la fuerza, coacción o sin consentimiento.

Prólogo

La primera edición de este *Informe de buenas prácticas* representaba el conocimiento colectivo de los trabajadores humanitarios y de organizaciones no gubernamentales (ONG) que se habían reunido en 1998 —primero en Estados Unidos y más tarde ese mismo año en el Reino Unido— para participar en una capacitación en seguridad durante una semana. Esto reflejaba el creciente reconocimiento de que, como comunidad, necesitábamos colaborar si queríamos mejorar nuestro enfoque sobre la gestión de la seguridad institucional. La preparación y elaboración del informe fue un esfuerzo totalmente colectivo en el que participaron trabajadores humanitarios y de desarrollo, consolidadores de la paz, ingenieros, formadores, desminadores, teóricos y un puñado de profesionales de gestión de la seguridad de las ONG empeñados en abordar los retos actuales de la gestión de la seguridad. Dicho informe se convirtió en el libro de texto fundamental con plantillas y orientaciones para una generación de gerentes y referentes de seguridad humanitaria y de las ONG.

En la edición revisada del 2010 se reconoció la valiosa aportación de un gran número de profesionales de la gestión de la seguridad humanitaria y de las ONG, cuyos puestos no existían en muchos casos cuando se publicó la primera edición en el 2000. Sus experiencias en la aplicación de los principios y las orientaciones presentados en el texto original reforzaron las buenas prácticas y permitieron mejorar los enfoques y perfeccionar las herramientas. Entre los temas destacados figuraban la mejora de los diagnósticos de riesgos, la aplicación de un enfoque de aceptación activa, el estudio de las dimensiones de seguridad de la programación de gestión remota, el fomento de la coordinación interinstitucional de seguridad y la gestión de incidentes críticos.

Sobre la base de las ediciones anteriores, este tercer informe se nutre de los conocimientos y la experiencia de los últimos quince años e incorpora los resultados de investigaciones recientes sobre los enfoques existentes y emergentes de la gestión de los riesgos de seguridad. También refleja los numerosos y significativos cambios que se han producido en el panorama humanitario en general durante este periodo. Uno de los más importantes es el reconocimiento, merecido desde hace tiempo, del importante papel que desempeñan los actores nacionales en los ecosistemas de respuesta humanitaria y de gestión de riesgos de seguridad humanitaria, así como de los retos específicos a los que se enfrentan.

En esta versión se destaca claramente que una buena gestión de riesgos de seguridad es necesaria en todos los contextos de respuesta humanitaria, no solo en los entornos más violentos, y se anima a los lectores a reflexionar críticamente sobre dónde y cómo surgen las amenazas y los riesgos, y a quién se considera amenazador y por qué. Para ello es fundamental reconocer que los límites entre los lugares de programación y

otros espacios supuestamente seguros, como el hogar, la oficina central, la suboficina y las instalaciones, son porosos. Una novedad importante de esta edición reside en el concepto y aplicación de un enfoque centrado en la persona para la gestión de riesgos de seguridad. Este enfoque anima a los profesionales de la gestión de riesgos de seguridad a centrarse tanto en “quién está seguro” como en “dónde es seguro”, lo que permite comprender mejor la importancia de los riesgos basados en la identidad.

En esta nueva edición también se abordan estos temas: la gestión de riesgos de seguridad en el marco de las alianzas en la ejecución y de las operaciones gestionadas a distancia; la importancia de las nuevas tecnologías para la gestión de riesgos de seguridad; las necesidades, los tipos y las fuentes de formación, y la manera en que la incidencia externa puede contribuir a la gestión de riesgos de seguridad y afectarla.

Esperamos que este informe actualizado y ampliado ayude a los responsables de la respuesta humanitaria a identificar y gestionar los riesgos de seguridad con mayor eficacia. La naturaleza dinámica del entorno operacional, agravada por fenómenos globales que probablemente desplazarán a millones de personas en los próximos años, exige que reflexionemos constantemente y evaluemos de nuevo los principios básicos de una gestión de riesgos de seguridad eficaz y los medios para ponerlos en práctica.

Wendy Fenton

Excoordinadora de HPN

Michael O'Neill

International NGO Safety and Security Association

Introducción

El *Informe de buenas prácticas en la gestión de la seguridad de las operaciones en entornos violentos* (GPR8, por sus siglas en inglés), publicado en el 2000, se convirtió rápidamente en un elemento básico en el naciente campo de la gestión de riesgos de seguridad de las operaciones humanitarias. En aquel momento, muy pocas organizaciones contaban con personal especializado o habían desarrollado mecanismos para la seguridad, de manera que el informe sirvió como una alerta respecto a la necesidad de gestionar mejor los riesgos y también como un modelo para los primeros esfuerzos de muchas organizaciones.

En una edición revisada en el 2010 se incluyeron ejemplos actualizados que reflejaban los cambios en el sector humanitario y en las amenazas a las que se enfrentaban los trabajadores humanitarios en el contexto de crisis y conflictos posterior al 11 de septiembre.

Aunque los conceptos y los principios introducidos en estas dos primeras ediciones siguen siendo válidos, ha transcurrido una década y media, las capacidades humanitarias y los entornos de seguridad continúan evolucionando, y las nuevas ideas en materia de gestión de riesgos de seguridad merecen otra revisión. Pese a que ya no es un recurso indispensable único como lo fue en el momento de su primera publicación, este documento puede servir como texto fundamental y compendio útil de principios y prácticas tanto para los expertos en gestión de riesgos de seguridad humanitaria como para quienes recién se inician en este campo.

Antecedentes de la nueva edición

Al igual que las dos ediciones anteriores, esta publicación es el resultado del esfuerzo conjunto de un gran número de profesionales expertos. El proyecto de actualización del documento comenzó en el 2022 como una colaboración entre Humanitarian Outcomes, el Global Interagency Security Forum (GISF) y la Humanitarian Practice Network (HPN), con financiación de la Oficina de Ayuda Humanitaria de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID/BHA).

Como primer paso, el equipo editorial realizó una encuesta mundial entre los profesionales de la gestión de riesgos de seguridad humanitaria, con el fin de evaluar el uso y la pertinencia actuales del GPR8. La encuesta reveló que la mayoría del personal de seguridad estaba familiarizado con la publicación y que más de una cuarta parte seguía incluyéndola en materiales informativos para el personal. También se expresó apoyo para una tercera edición. Sin embargo, la encuesta confirmó que, con la proliferación de orientaciones técnicas y de manuales de procedimientos sobre la gestión de riesgos de

seguridad, el GPR8 se valora ahora más como una referencia acreditada para el personal de seguridad y un manual básico sobre conceptos y principios clave para quienes se inician en el tema, que como un manual práctico.

Teniendo esto en cuenta, el equipo inició un estudio en profundidad de las prácticas actuales y de las nuevas ideas en materia de gestión de riesgos de seguridad en contextos humanitarios. La investigación abarcó estudios de casos concretos en cinco entornos humanitarios (República Centroafricana, Colombia, Etiopía, Irak y Ucrania) y consultas con más de 250 profesionales humanitarios de todo el mundo. Las conclusiones, publicadas por el GISF y Humanitarian Outcomes en un informe en el 2024, han servido de base para gran parte del contenido nuevo de este documento, junto con las contribuciones y las revisiones críticas independientes aportadas por los expertos participantes.¹ Desde el principio, el proyecto ha contado con la orientación de un grupo consultivo formado por las principales partes interesadas y referentes en gestión de riesgos de seguridad. Cada capítulo fue revisado y corregido por los editores y, a continuación, fue compartido con un grupo de expertos en la materia para recibir sus valiosas aportaciones. Además, algunos capítulos nuevos fueron redactados por expertos y sometidos al mismo proceso de revisión entre pares. Tras incorporar los comentarios, se revisaron los borradores para verificar el contenido general, la estructura, la precisión técnica y la adecuación del lenguaje y del tono.

Novedades

Además de un título abreviado que abarca aspectos no operacionales de la gestión de riesgos de seguridad y que refleja la realidad de que los riesgos de seguridad pueden surgir en todo tipo de entornos, esta edición actualiza el contenido de versiones anteriores e introduce temas nuevos, informados por las últimas investigaciones y reflexiones en el sector. En particular, introduce y aplica el concepto de *enfoque centrado en la persona* a la gestión de riesgos de seguridad, que ubica a las personas en el centro de la gestión de riesgos de seguridad. La nueva edición también hace hincapié en la labor crítica y en la desproporcionada carga de riesgo de los agentes humanitarios nacionales y locales, y analiza cómo funciona la gestión de riesgos de seguridad en las alianzas nacionales-internacionales.

Los temas nuevos incluyen las dimensiones de seguridad de las tareas relacionadas con el acceso y la desconflicción, así como la nueva variedad de riesgos digitales a los que se enfrentan las organizaciones humanitarias en la forma de desinformación, información errónea, robo de datos, vigilancia y delitos cibernéticos. También hay contenidos nuevos relacionados con la criminalidad en general y contenidos complementarios sobre formación, financiación, cumplimiento y deber de cuidado. La estructura revisada del documento reconoce que la gestión de riesgos de seguridad tiene lugar en diferentes

1 Global Interagency Security Forum y Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

ecosistemas —la organización, el sistema humanitario y el espacio más amplio de la ayuda y el ámbito político—, cada uno con sus propias consideraciones y dificultades.

Esta edición del GPR8 hace más hincapié en las buenas prácticas y en los principios rectores que en brindar instrucciones paso a paso sobre los procedimientos técnicos. La abundancia de recursos nuevos en el espacio humanitario, en su mayoría en línea, que ofrecen directrices detalladas, satisfacen ampliamente esta necesidad, y tratar de reproducirlos haría que este documento resultara superfluo y quedara rápidamente obsoleto. En su lugar, se centra en introducir ideas y conceptos para fomentar la reflexión e informar el debate político de alto nivel, y en compartir buenas prácticas de expertos, al tiempo que remite al lector a recursos pertinentes para obtener ejemplos concretos, plantillas y orientaciones prácticas.

Por último, los editores y los colaboradores de esta revisión han intentado desplazar del centro en la medida de lo posible a las organizaciones internacionales occidentales como la principal perspectiva y audiencia de este material, en un esfuerzo por garantizar que el lenguaje y el enfoque del contenido sean pertinentes e incluyan a todos los proveedores de ayuda humanitaria.

Audiencia destinataria

El GPR8 original se dirigía principalmente al equipo directivo de las operaciones de las organizaciones humanitarias que supervisa las actividades en los entornos hostiles. Esta edición se dirige a un público un poco más amplio. En primer lugar, procura incluir a todas las organizaciones humanitarias locales, nacionales e internacionales, desde las más pequeñas hasta las más grandes. Sin embargo, dado que las organizaciones de distintos tamaños y presupuestos tienen necesidades y capacidades diferentes, algunas de las buenas prácticas descritas para las organizaciones grandes con múltiples departamentos y oficinas pueden ser menos pertinentes o factibles de aplicar para las organizaciones más pequeñas. En la medida de lo posible, esto se señala en el texto con un recordatorio de los principios básicos que sustentan estas prácticas, que son de aplicación universal.

Además del personal humanitario con responsabilidades en materia de seguridad (denominado *personal de seguridad* en todo el documento), este informe puede ser de interés para los equipos directivos y los consejos de administración de las organizaciones humanitarias, así como para estudiantes, periodistas, investigadores y cualquier persona interesada en aprender más sobre la gestión de riesgos de seguridad en las operaciones humanitarias. Otras organizaciones que operan en condiciones de riesgo también pueden encontrarlo útil.

Las buenas prácticas que aquí se describen se refieren a la gestión de riesgos de seguridad a nivel organizativo y están destinadas al personal responsable de mejorar la seguridad de todos los miembros del personal. Este documento no está escrito para los miembros del personal considerados de manera individual con el fin de tratar su seguridad personal o las medidas que deben tomar durante un incidente. Esto no resta importancia a las intervenciones individuales en materia de seguridad, sino que simplemente refleja el alcance de las orientaciones.

El término *personal* hace referencia a cualquier persona que trabaje en nombre de la organización, incluidos los voluntarios. El término *organizaciones* engloba a todo tipo de organizaciones humanitarias, desde los organismos de las Naciones Unidas (ONU) y el Movimiento Internacional de la Cruz Roja y de la Media Luna Roja hasta las ONG y las organizaciones comunitarias. La diversidad de los agentes humanitarios hace que, en ocasiones, algunos de los contenidos puedan ser más o menos pertinentes para un determinado tipo de organización. Una vez más, al hacer hincapié en los principios fundamentales y en la reflexión, esperamos que esta guía sea útil para todos.

A tener en cuenta

El tema central de este documento es la seguridad frente a los actos dirigidos a causar daño deliberadamente (como la violencia y la criminalidad), que se diferencia de la seguridad ante accidentes u otras circunstancias que provocan daños de manera involuntaria (como los incendios y los peligros medioambientales). Aunque en la práctica ambas situaciones suelen superponerse, no se profundiza aquí en los aspectos de la acción humanitaria relacionados con la seguridad ante hechos accidentales.

En este documento se utiliza deliberadamente un lenguaje no prescriptivo y se ofrecen buenas prácticas para que el personal responsable de la seguridad las tenga en cuenta, en lugar de establecer normas o requisitos. Todas las prácticas descritas deben adaptarse a las necesidades específicas y al contexto operacional de cada organización.

En las crisis humanitarias, la población en general suele estar expuesta a un riesgo de violencia igual o mayor que los trabajadores humanitarios y necesita una mayor asistencia y protección. Sin embargo, las estrategias utilizadas para proteger a las personas afectadas suelen ser bastante diferentes de las empleadas para proteger a los trabajadores humanitarios y, además, en la mayoría de las organizaciones, atañen a departamentos distintos de los de gestión de riesgos de seguridad.

Por último, es importante reconocer y reforzar la idea de que lograr una gestión de riesgos de seguridad eficaz no es un fin en sí mismo. Se trata más bien de un medio para alcanzar el objetivo más amplio de atender las necesidades humanitarias de las personas en situaciones de crisis.

Estructura de este informe

Comenzamos con los principios generales y fundamentales de la gestión de riesgos de seguridad humanitaria, para luego profundizar en ámbitos más específicos de la práctica. Las personas que recién se inician en la gestión de riesgos de seguridad pueden seguir el orden de los capítulos para obtener una introducción completa al tema, pero cada sección es autónoma y puede leerse de forma independiente.

En la **primera parte** se explican conceptos clave como amenaza, riesgo, deber de cuidado y criticidad del programa, y se introducen las últimas ideas sobre el enfoque de seguridad centrado en la persona. En la **segunda parte** se describen los ecosistemas en los que tiene lugar la gestión de riesgos de seguridad: el contexto operacional, la comunidad interinstitucional y los mecanismos conjuntos, el círculo más amplio de actores, como Gobiernos y ejércitos, y la interacción con otros objetivos organizativos, como la incidencia. En la **tercera y cuarta parte** se analizan los principales elementos estratégicos, de políticas y operativos del desarrollo y de la aplicación de un sistema de gestión de riesgos de seguridad de la organización. En la **quinta parte** se abordan cuestiones relacionadas con los recursos humanos, las buenas prácticas en materia de comunicación, la formación y el bienestar del personal. En la **sexta parte** se trata la gestión de riesgos de seguridad en el ámbito de las tecnologías de la información y la comunicación, incluida la información perjudicial. Por último, en la **séptima parte** se ofrecen ejemplos de mitigación de riesgos para situaciones y tipos de amenaza específicos. Estos se han revisado y actualizado para reflejar las tendencias recientes en materia de inseguridad y los contextos operacionales actuales.

1 Fundamentos de la gestión de riesgos de seguridad humanitaria

1.1 Conceptos y principios clave

En este capítulo se presentan las ideas fundamentales relacionadas con la gestión de riesgos de seguridad para la acción humanitaria. Entre ellas figuran los conceptos básicos de amenaza y riesgo, deber de cuidado y umbrales de riesgo, así como su correspondencia con la criticidad de los programas. También se describen los principios fundamentales de la acción humanitaria y su relación con la seguridad, así como las buenas prácticas para crear una cultura de seguridad en la organización.

1.1.1 ¿Qué son los riesgos de seguridad y qué significa gestionarlos?

La acción humanitaria, que a menudo tiene lugar en condiciones de inestabilidad, conflicto y crisis, conlleva inevitablemente ciertos riesgos de seguridad. Aunque los riesgos nunca pueden eliminarse por completo, su gestión eficaz puede marcar la diferencia entre que las personas reciban o no ayuda vital.

La inseguridad es solo un tipo de riesgo al que pueden enfrentarse las personas y las organizaciones. Hay muchos otros tipos, como los riesgos financiero, operativo, fiduciario y reputacional, y todos ellos pueden relacionarse entre sí y con los riesgos de seguridad. La definición más amplia de riesgo, según la *norma ISO 31000*, es “el efecto de la incertidumbre sobre los objetivos”.² Esta definición supone dos distinciones importantes: un riesgo no es lo mismo que una amenaza y, aunque la gestión del riesgo está vinculada a los objetivos, no es sinónimo de ellos. En el contexto humanitario, por tanto, la gestión de riesgos de seguridad está, en última instancia, al servicio de los objetivos humanitarios: evitar daños y pérdidas es un medio, no el fin en sí mismo. Esto es importante porque, cuando mantener a salvo a las personas se convierte en el objetivo primordial, la aversión al riesgo es el resultado inevitable.

Los conceptos clave que hay que entender son los siguientes:

- Amenaza
- Vulnerabilidad
- Riesgo
- Mitigación/reducción de riesgos

En un entorno operacional, una amenaza es cualquier cosa que pueda causar daños o pérdidas, mientras que la vulnerabilidad se refiere a la probabilidad de verse frente a una amenaza y al impacto que tendría como consecuencia. La combinación de una amenaza a la seguridad y la vulnerabilidad de una persona ante esa amenaza constituye el riesgo de seguridad. En otras palabras, los riesgos de seguridad tienen que ver con la

2 Organización Internacional de Normalización (2018), *ISO 31000:2018, Risk management – Guidelines* (www.iso.org/standard/65694.html).

posibilidad de daño: la probabilidad de que ocurra algo perjudicial y el alcance de ese daño en caso de que ocurra.

Una organización puede optar por evitar por completo determinados riesgos (por ejemplo, puede decidir no trabajar en un zona determinada) y puede transferir el riesgo a alguien más, como un contratista o un socio en la ejecución (más adelante se ofrece más información al respecto). Sin embargo, al realizar una programación directa e intentar reducir y mitigar los riesgos para el personal, hay tres tipos principales de medidas que una organización puede adoptar, ninguna de las cuales es mutuamente excluyente:

- Neutralizar la amenaza, que supone disminuir la amenaza en sí (mediante, por ejemplo, la negociación de acuerdos de acceso seguro con un grupo armado para reducir la hostilidad).
- Reducir la probabilidad, que implica reducir la exposición a la amenaza.
- Reducir el impacto mediante la adopción de medidas para garantizar que, ante la amenaza, el impacto sea limitado.

A partir del 2000, el sector humanitario ha desarrollado y puesto en marcha un conjunto de conocimientos, políticas y prácticas conocido como *gestión de riesgos de seguridad*, que es el tema de este informe. La gestión de riesgos de seguridad es un sistema organizativo que permite identificar, evaluar y prepararse ante los riesgos, con el fin de evitar que se produzcan incidentes de seguridad y minimizar su impacto si se producen, respondiendo a ellos con eficacia. Al tomar medidas activas para reducir los riesgos de seguridad, una organización humanitaria maximiza su capacidad para cumplir sus objetivos programáticos, al tiempo que cumple con su deber de cuidado hacia las personas que prestan la ayuda.

En esencia, la gestión de riesgos de seguridad en el ámbito humanitario es un factor que facilita el acceso seguro. No puede haber acceso sin cierto grado de protección de los miembros del personal, que les permita trabajar dentro de un umbral de riesgo razonable y convenido. Cuando la gestión de riesgos de seguridad es eficaz, garantiza que el personal ayude a las personas necesitadas y que se sienta seguro y confiado al realizar su trabajo. Esto, a su vez, puede ayudar a cumplir las responsabilidades de la organización hacia el personal, reforzar la reputación de la organización como un socio legítimo ante los donantes, así como limitar las pérdidas y ampliar el alcance y la ventaja competitiva de una organización. En pocas palabras, la gestión de riesgos de seguridad se convierte en un elemento potente y esencial para alcanzar los objetivos estratégicos y programáticos generales de la organización.

1.1.2 Deber de cuidado

El deber de cuidado se refiere a la obligación de una organización de velar por la seguridad y el bienestar de las personas que realizan su trabajo. El concepto tiene importantes implicaciones jurídicas y morales para las organizaciones humanitarias. En sentido estrictamente jurídico, el deber de cuidado es el requisito que exige que las organizaciones adopten todas las medidas razonables y adecuadas para mejorar la seguridad del personal. Muchos países han incorporado el deber de cuidado a la legislación laboral y de otro tipo. No informar plenamente al personal sobre los riesgos y no tomar medidas de mitigación de riesgos razonables puede exponer a una organización a demandas por negligencia y responsabilidad legal. Más importante aún, el incumplimiento de este deber puede tener consecuencias devastadoras o fatales para las personas.

Aunque no existe un conjunto único y estándar de acciones que definan una política de deber de cuidado, sí hay elementos comunes de buenas prácticas:

- Evaluar los riesgos para el personal que suponen las nuevas condiciones, lugares o actividades en las que vayan a trabajar.
- Informar al personal de los riesgos a los que puede enfrentarse, de lo que la organización ha puesto en marcha para hacer frente a esos riesgos y de las medidas que se espera que tomen las propias personas (incluidas las expectativas de comportamiento).
- Trabajar para evitar que se produzcan incidentes, por ejemplo, estableciendo medidas de mitigación de riesgos basadas en los riesgos evaluados.
- Monitorear la aplicación y la pertinencia de las medidas de gestión de riesgos de seguridad.
- Intervenir en caso de que se produzca un incidente a fin de reducir las consecuencias negativas, por ejemplo, creando equipos de gestión de crisis y prestando atención posterior al incidente al personal afectado.

Como se detallará en capítulos posteriores, lo anterior está estrechamente relacionado con las actividades esenciales de una buena gestión de riesgos de seguridad. Es importante señalar que el deber de cuidado también puede extenderse más allá de la relación establecida formalmente entre empleador y empleado. Las organizaciones contratan a consultores, voluntarios y una variedad de proveedores de servicios con los que tal vez no tengan automáticamente un deber de cuidado, pero ante los que pueden seguir teniendo cierta responsabilidad. La responsabilidad legal de una organización puede entenderse, según la jurisdicción, como relativa al grado de control que tiene sobre una persona en un entorno determinado, como su alojamiento, ubicación y elección de transporte.³

3 Kemp, E. y Merkelbach, M. (2011) *Can you get sued? Legal liability of international humanitarian aid agencies toward their staff*, Security Management Initiative (www.gisf.ngo/resource/can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/).

Cada vez con más frecuencia, las organizaciones elaboran políticas y marcos de deber de cuidado para orientar estratégicamente estos diferentes aspectos del cuidado del personal y para comunicar al personal el compromiso de la organización con su bienestar general. Esto incluye adaptar las políticas de deber de cuidado para atender a una fuerza laboral diversa, teniendo en cuenta sus diferentes procedencias personales y culturales, que pueden afectar el riesgo de seguridad. Estas políticas pueden revisarse periódicamente para reflejar los nuevos retos y circunstancias.

Ejemplo de marco del deber de cuidado

Existe una serie de procesos que respaldan el deber de cuidado, y un marco puede ayudar a comunicar visualmente cuáles son. Una organización ha estructurado su marco del deber de cuidado con la “cultura” (valores compartidos y objetivos relativos al bienestar) en el centro y la seguridad operacional como uno de los muchos elementos de apoyo, entre los que se incluyen la gobernanza, la formación, las comunicaciones y la gestión de crisis. La figura 1 representa un ejemplo de marco del deber de cuidado diseñado para ayudar a delinear y transmitir la intención del deber de cuidado, con la seguridad como un elemento distintivo en él.

Figura 1 Visualización del marco del deber de cuidado



Cultura: valores, formas de trabajar, compromiso e inclusión, bienestar.

Gobernanza, liderazgo y rendición de cuentas: fijar políticas, dar claridad respecto al apetito y el umbral de riesgo y establecer estructuras de supervisión, rendición de cuentas, transparencia y aprendizaje.

Seguridad operacional: diagnósticos de riesgos y planes de seguridad específicos para cada lugar y actividad, gestión de riesgos de viaje, incluidos los riesgos de identidad personal y los compromisos de fuentes, socios e interlocutores.

Gestión de crisis: personas, planes, seguros y consultores, formación, comunicación, apoyo antes y después del incidente y revisiones posteriores a la acción.

Recursos: financiación, dotación de personal y apoyo de consultoría.

Comunicación: métodos, protocolos, seguridad de la información, dispositivos, licencias, formación y simulacros.

Formación: incorporación, seguridad personal y del equipo, y gestión de riesgos de seguridad.

La buena comunicación e informar al personal sobre los riesgos son elementos centrales del deber de cuidado. Las organizaciones tienen la responsabilidad de informar al personal y al personal potencial (incluidos voluntarios y consultores) sobre los riesgos de seguridad a los que pueden enfrentarse y las medidas de mitigación que se utilizarán. Un compromiso pleno respecto a estas cuestiones permite a las personas tomar una decisión explícita, deliberada e informada sobre aceptar o no los riesgos identificados.

Garantizar la comunicación y el compromiso del personal puede implicar lo siguiente:

- **Divulgación exhaustiva de la información.** Incluye detalles sobre la naturaleza específica de los riesgos, las medidas de protección establecidas, las funciones y las responsabilidades individuales y cualquier posible repercusión sobre la salud y la seguridad. También podría ser útil indicar en qué áreas la información es deficiente o inexistente.

- **Debate explícito y aceptación del riesgo.** La decisión libre y plenamente informada del personal de aceptar los riesgos relacionados con el trabajo se deriva de una comprensión clara de los riesgos y de las medidas de mitigación, sin presiones ni temor a sufrir consecuencias negativas por rechazar el trabajo. Hacer explícita esta decisión ayuda a garantizar que tanto la organización como el personal se involucren y sean conscientes de la gravedad de la situación.
- **Documentación.** Puede ser aconsejable que los miembros del personal manifiesten la comprensión y aceptación del riesgo explícitamente y que esto quede documentado, sobre todo cuando las situaciones de seguridad cambian o cuando el personal empieza a trabajar en lugares nuevos. Es importante comprender que este proceso tiene por objeto garantizar que el debate se produzca y que el personal esté plenamente informado e involucrado. No se trata de una protección contra una posible responsabilidad legal. Aunque algunas organizaciones piden al personal que firme documentos de consentimiento informado u otras exenciones de responsabilidad, estos documentos no gozan del mismo reconocimiento en las distintas jurisdicciones jurídicas y no impiden necesariamente que las personas que los han firmado presenten demandas por negligencia.
- **Comunicación continua.** Las organizaciones deben procurar proporcionar actualizaciones sobre cualquier cambio en el diagnóstico de riesgos e informar al personal de los nuevos riesgos a medida que surjan.
- **Derecho a retirarse.** Se debe recordar periódicamente al personal que tiene el derecho a cambiar de opinión e interrumpir su participación en cualquier momento si se siente inseguro o si las condiciones cambian significativamente.

La gestión de riesgos de seguridad es a menudo un ejercicio de equilibrio entre los objetivos humanitarios de la organización y su deber de cuidado. Al mismo tiempo, una buena gestión de riesgos de seguridad es vital para cumplir con el deber de cuidado, y un buen deber de cuidado puede igualmente reforzar la gestión de riesgos de seguridad creando unas condiciones en las que el personal está bien informado de los riesgos y se siente valorado y apoyado. Para ello, la organización debe considerar y transmitir su deber de cuidado como un valor fundamental, no como un medio para evitar demandas y daños a la reputación. Sin embargo, las demandas son una realidad. El caso emblemático de Dennis contra el Consejo Noruego para los Refugiados (NRC, por sus siglas en inglés) confirmó la responsabilidad legal que tienen las organizaciones humanitarias hacia su personal en materia de seguridad (véase el ejemplo a continuación).

Ejemplo: Deber de cuidado legal. Lecciones del fallo en el caso de Dennis contra el NRC

En 2012 varios trabajadores humanitarios fueron atacados durante una visita a un campamento de refugiados en Dadaab (Kenia), mientras trabajaban para el NRC. Un miembro del personal falleció y otros cuatro fueron secuestrados. Cuatro días después fueron rescatados. En 2015 Steve Dennis, una de las personas secuestradas y heridas durante el ataque, presentó una demanda de indemnización contra el NRC. El Tribunal de Distrito de Oslo dictaminó que el NRC había actuado con negligencia grave y concedió una indemnización por daños y perjuicios a Dennis.

Este caso se ha descrito como un fallo histórico y muchos lo han considerado un momento decisivo, que ha llevado a muchas organizaciones humanitarias a reforzar sus sistemas de gestión de riesgos de seguridad. Aunque la obligación legal de cuidado puede variar de una jurisdicción a otra, las enseñanzas de este caso pueden servir de guía a las organizaciones que buscan mejorar sus procesos de gestión de riesgos de seguridad y de deber de cuidado.

A continuación se mencionan algunas de las lecciones clave del fallo del Tribunal de Oslo.

- **Alcance del deber de cuidado:** El deber de cuidado es tanto una obligación legal para las organizaciones humanitarias como para cualquier otro empleador, y exige que las medidas de mitigación sean proporcionales al riesgo.
- **Previsibilidad del riesgo y medidas de mitigación razonables:** El NRC no evaluó adecuadamente los riesgos previsible de secuestro, no mitigó los riesgos identificados, no siguió las directrices de seguridad (internas y externas) ni consultó a especialistas en seguridad para tomar decisiones clave.
- **Consentimiento informado:** No se informó al personal de los riesgos, no se pidió su consentimiento ni se le permitió retirarse del lugar cuando cambiaron los planes de seguridad.
- **Práctica comunitaria:** Dada la ausencia de normas de seguridad concretas y de aplicación universal en el sector humanitario, el tribunal analizó las prácticas de la comunidad humanitaria en Dadaab para comprender si las decisiones y prácticas del NRC diferían de las de sus pares, y de qué manera. Si bien desviarse de las prácticas comúnmente aceptadas no es inherentemente un error, cualquier desviación de este tipo debe responder a una decisión cuidadosamente justificada, basada en un razonamiento sólido y en información fáctica.

En resumen, el fallo del Tribunal de Distrito de Oslo destaca la necesidad de que las organizaciones humanitarias realicen diagnósticos de riesgos sólidos y adopten medidas de protección razonables según corresponda como parte de su deber legal de cuidado.

Fuentes: Hoppe, K. y Williamson, C. (2016) *Dennis vs Norwegian Refugee Council: implications for duty of care*, Humanitarian Practice Network (<https://odihpn.org/publication/dennis-vs-norwegian-refugee-council-implications-for-duty-of-care/>) y Merkelbach, M. y Kemp, E. (2016) *Duty of care: a review of the Dennis v Norwegian Refugee Council ruling and its implications*, Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

El firme cumplimiento del deber de cuidado está vinculado al éxito general de la organización. En términos más amplios, el deber de cuidado puede contribuir a la satisfacción y retención del personal y a la reputación de la organización, lo que a su vez puede apoyar los objetivos globales de la organización. Es importante subrayar que la mayoría de los incidentes graves en el sector humanitario no dan lugar a procesos judiciales; el caso Dennis contra el NRC es muy conocido porque es excepcional. Existen pruebas de que un factor importante que impulsó la búsqueda de una reparación jurídica fue la deficiente atención proporcionada al personal tras el incidente, incluidas la falta de información y transparencia sobre lo ocurrido y de medidas de seguimiento. Aunque no es posible eliminar todos los riesgos, las organizaciones sí tienen control sobre cómo se apoya al personal tras un incidente, y este apoyo es un aspecto importante del deber de cuidado.

► *Para obtener más información sobre la atención posterior a un incidente, véase el capítulo 5.4, “Cuidado del personal”.*

En los últimos años, el término *deber de cuidado* se ha aplicado a las obligaciones éticas que las organizaciones internacionales tienen para con sus socios y beneficiarios locales. Aunque una organización no puede ser considerada legalmente responsable de las personas empleadas por otras entidades, es evidente que estas alianzas implican a menudo una transferencia significativa del riesgo, por lo que les corresponde a las organizaciones prestar todo el apoyo posible y adecuado a sus socios para el cuidado del personal.

► *Para obtener más información sobre la transferencia de riesgos y las alianzas, véase el capítulo 3.5.*

1.1.3 Riesgo residual, umbrales de riesgo y criticidad del programa

Participar en los esfuerzos de respuesta humanitaria exige estar dispuesto a asumir algunos riesgos. El apetito de riesgo de una organización se determinará por sus objetivos estratégicos, su misión y su cultura, y equivale a un entendimiento compartido del nivel de riesgo que es adecuado para alcanzar los objetivos de la organización. El umbral de riesgo es un entendimiento compartido del límite que la organización no está dispuesta sobrepasar. A la hora de determinar este umbral, es necesario comprender el riesgo residual. Este es el nivel de riesgo que queda después de tomar todas las medidas de mitigación adecuadas; es un concepto que implica reconocer que siempre quedará algún riesgo. Fijar el umbral de riesgo aceptable como una decisión explícita y transparente puede ayudar a regir todas las demás decisiones de gestión sobre qué hacer al enfrentarse al riesgo. Hay tres momentos importantes en los que debe discutirse el umbral de riesgo aceptable:

- Cuando se decide entrar o expandirse en un entorno de riesgo.
- Cuando se determinan los umbrales de riesgo aceptable individuales.
- Cuando se trazan las líneas rojas (límites o umbrales claros) para los casos en que una situación se deteriora.

En el primer caso, decidir qué constituye un riesgo aceptable para una organización requiere criterios y condiciones explícitos que garanticen un proceso de toma de decisiones disciplinado y transparente.

En el segundo caso, cuando se determinan los umbrales de riesgo individuales, es importante no asumir que todo el personal actual y potencial tiene el mismo umbral respecto a lo que considera un riesgo aceptable. Un clima de confianza dentro de la organización puede ayudar a que las personas se sientan capaces de expresar su ansiedad si una situación supera su tolerancia al riesgo, y las personas que entren en un entorno de mayor riesgo deben hacerlo informadas de los riesgos que allí existen. También es importante ser consciente de los incentivos económicos o la presión del grupo que pueden llevar a las personas a asumir riesgos más allá de su nivel de comodidad. Los umbrales de riesgo aceptable individuales también dependerán inevitablemente de los perfiles de riesgo personales.

► *Los perfiles de riesgo personales se tratan con más detalle en el capítulo 1.2, “Enfoque de seguridad centrado en la persona”.*

El objetivo de las líneas rojas es evitar el síndrome de la rana hervida. Cuando el riesgo aumenta gradualmente, no es poco común que los trabajadores humanitarios se habitúen a los entornos peligrosos. Aunque haya conciencia de que la situación se está deteriorando, es posible que el personal no se retire ni refuerce sus medidas de

protección hasta después de que se haya producido un incidente. Tener claro cuáles son los factores desencadenantes o las “líneas rojas” puede ayudar a determinar cuándo se ha deteriorado significativamente la seguridad y si las actividades del programa justifican claramente el mayor riesgo. Esto introduce otro concepto clave en la gestión de riesgos de seguridad: la *críticidad del programa*. La criticidad del programa es una medida del grado en que la vida de las personas o el alivio del sufrimiento extremo dependen de la continuidad de la actividad de ayuda. Cuanto más crítico o vital sea el programa, más riesgos estará dispuesta a aceptar una organización a fin de mantener dicho programa.

1.1.4 Principios fundamentales de la acción humanitaria

A estas alturas debería estar claro que la gestión de riesgos de seguridad no es una formulación o un conjunto de reglas invariables que seguir, sino más bien un proceso elástico en el que las decisiones implicarán equilibrar un conjunto de preocupaciones frente a otro a medida que cambie su peso relativo. Hay otros aspectos importantes que diferencian la gestión de riesgos de seguridad de las operaciones humanitarias de la de otros sectores, que se relacionan con los principios humanitarios esenciales y la condición de los trabajadores humanitarios conforme al derecho internacional humanitario. En los conflictos armados, por ejemplo, en virtud de los Convenios de Ginebra y los Protocolos Adicionales, las organizaciones humanitarias tienen derecho a prestar ayuda, y las partes beligerantes están obligadas a facilitar sus operaciones, proteger a su personal y permitir su libre circulación.⁴ El corolario es que las organizaciones humanitarias actúan como entidades neutrales y prestan ayuda de forma imparcial, independientemente de cualquier agenda política o de otro tipo, y únicamente en función de las necesidades.

Los principios humanitarios de neutralidad, imparcialidad e independencia están directamente relacionados con la seguridad, ya que afectan la forma en que las comunidades locales y las partes beligerantes perciben a las organizaciones humanitarias y a su personal. Estas percepciones pueden ser decisivas para la aceptación de una organización (una medida por la cual la organización es una entidad conocida en una zona determinada, y su trabajo apreciado o al menos tolerado). Esto, a su vez, puede repercutir en su nivel de acceso a los lugares donde se necesita. Es principalmente a través de la aceptación que una organización humanitaria puede obtener y mantener un acceso seguro para trabajar en zonas de alto riesgo.

El principio de “no hacer daño”⁵ destaca que las organizaciones humanitarias deben evitar exacerbar los conflictos existentes o crear nuevas formas de daño. Esto significa operar de manera que se reduzcan las consecuencias negativas involuntarias en las comunidades a las que se presta asistencia, y garantizar que la programación y, por

4 Para obtener más información, véase www.icrc.org/en/document/geneva-conventions-1949-additional-protocols.

5 Anderson, M.B. (1999) *Do no harm: How aid can support peace – or war*, Lynne Rienner Publishers.

extensión, las medidas de protección empleadas, no contribuyan a la tensión, la violencia o la desigualdad.

Los conceptos y principios rectores mencionados arriba son específicos de la gestión de riesgos de seguridad humanitaria y, por lo general, no se observan entre los actores de los sectores privado, militar y diplomático que pueden compartir los mismos espacios. Estos principios fundamentales a menudo deben explicarse y reiterarse tanto al personal como a los interlocutores externos.

► *Para obtener más información sobre el enfoque de aceptación, véase el capítulo 4.2.*

1.1.5 Crear una cultura de seguridad positiva

En esencia, la gestión de riesgos de seguridad consiste en que el personal tome decisiones informadas que salvaguarden su bienestar y el de los demás. Esto puede respaldarse con sistemas y herramientas adecuados, pero se basa fundamentalmente en valores, creencias y comportamientos compartidos respecto a la seguridad. Puede decirse que una organización cuyo personal es muy consciente de los riesgos de seguridad y cree activamente que la seguridad es esencial para lograr sus objetivos de ayuda, posee una cultura de seguridad fuerte o positiva. Aunque la cultura no se puede diseñar ni imponer, sí se puede alimentar y moldear de forma significativa mediante el liderazgo y el ejemplo. Una organización puede establecer todo tipo de políticas y procedimientos, pero la mayor parte de la gestión de riesgos de seguridad consiste en conseguir que el personal los entienda y los acepte.

Fomentar una cultura positiva de seguridad empieza por garantizar que todo el personal conozca la organización y su misión. Lo ideal sería que cualquier persona que trabaje para la organización pueda responder a preguntas sobre su propósito y actividades, cómo se financia y su independencia de cualquier interés político.

Las organizaciones deben tratar la seguridad como una prioridad para todo el personal, no como una cuestión delicada de gestión que solo unos pocos miembros del personal pueden discutir a puerta cerrada. El personal directivo debe transmitir la importancia que concede a la gestión de riesgos de seguridad si quiere que los demás sigan su ejemplo. En concreto, las organizaciones pueden:

- Insistir en la información y la comunicación, haciendo de la seguridad un punto permanente del orden del día de todas las reuniones de dirección y de personal, y garantizar que la seguridad sea una consideración clave en toda la planificación de programas.

- Destacar la importancia de reportar y monitorear todos los incidentes, ya que son vitales para la concienciación, no como medio para culpar o adoptar medidas disciplinarias.
 - Asegurarse de que todo el personal tenga claras sus responsabilidades individuales con respecto a la gestión de riesgos de seguridad y de que se incluyan en las descripciones de los puestos de trabajo y en las evaluaciones del desempeño.
 - Reconocer y reforzar las buenas prácticas, destacando los casos de conocimientos y comportamientos adecuados en materia de seguridad y aquellos en que las estrategias eficaces de gestión de riesgos de seguridad hayan contribuido al éxito de los resultados operacionales.
- En el capítulo 5.1 se ofrecen orientaciones más detalladas sobre las habilidades de comunicación para mejorar la colaboración interdepartamental.
- Véase el capítulo 5.3, “Comunicación sobre la seguridad dentro de la organización”.

Promover una cultura de seguridad positiva, tanto a nivel de cada miembro del personal como de la organización, supone tener en cuenta las implicaciones de la seguridad en todo lo que la organización hace (o decide no hacer), desde los debates sobre el diseño de los programas y los mensajes públicos hasta las decisiones de financiación y la contratación de proveedores de servicios externos. Tener una cultura de seguridad positiva significa que las personas consideran los riesgos y las implicaciones de seguridad en todos los aspectos del trabajo porque comprenden su importancia, y se las respeta por hacerlo.

Más información

General

Anderson, M.B. (1999). *Do no harm: How aid can support peace – or war*. Lynne Rienner Publishers.

Bickley, S. (2017). *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*. Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Comité Internacional de la Cruz Roja. (s.f.). *Los Convenios de Ginebra de 1949 y sus Protocolos adicionales* (www.icrc.org/en/document/geneva-conventions-1949-additional-protocols).

Organización Internacional de Normalización. (2018). *ISO 31000:2018: Risk management – Guidelines* (www.iso.org/standard/65694.html).

Deber de cuidado

CHS Alliance. (2019). *Introduction to duty of care* (www.chsalliance.org/get-support/article/introduction-duty-care/).

Duty of Care International. (s.f.). *Why duty of care?* (<https://dutyofcareinternational.co.uk/why-duty-of-care/>).

Global Interagency Security Forum. (s.f.). *What is security risk management?* (www.gisf.ngo/about/what-is-humanitarian-security-risk-management/).

Hoppe, K. y Williamson, C. (2016). *Dennis vs Norwegian Refugee Council: implications for duty of care*. Humanitarian Practice Network (<https://odihp.org/publication/dennis-vs-norwegian-refugee-council-implications-for-duty-of-care/>).

Kemp, E. y Merkelbach, M. (2011). *Can you get sued? Legal liability of international humanitarian aid agencies toward their staff*. Security Management Initiative (www.gisf.ngo/resource/can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/).

Merkelbach, M. y Kemp, E. (2016). *Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

The Swiss Centre of Competence for International Cooperation. (s.f.). *Duty of care under Swiss law*. cinfo (www.cinfo.ch/en/publications/duty-of-care-under-swiss-law).

1.2 Enfoque de seguridad centrado en la persona

Un enfoque de seguridad centrado en la persona reconoce que es crucial tener en cuenta las características de identidad interseccionales para gestionar eficazmente los riesgos de seguridad. En lugar de tratar a los trabajadores humanitarios como un grupo homogéneo, igualmente vulnerable a las mismas amenazas, este enfoque fomenta la inclusión, la reflexión y la consideración de cómo los retos y necesidades de seguridad de las personas se ven afectados por sus perfiles personales. En este capítulo se abordan los riesgos basados en la identidad y la justificación para adoptar un enfoque centrado en la persona. A lo largo de este documento hay recordatorios y ejemplos de cómo adoptar un enfoque de seguridad centrado en la persona y este capítulo debe considerarse una introducción al concepto.

1.2.1 Riesgos basados en la identidad

Las organizaciones humanitarias se benefician significativamente de la diversidad de su personal, que mejora su capacidad para comprender y relacionarse eficazmente con las diversas comunidades destinatarias, lo que garantiza a su vez que las intervenciones tengan en cuenta las diferencias culturales y sean bien recibidas. Al aportar perspectivas, experiencias y competencias variadas, los equipos diversos también pueden contribuir a un análisis más exhaustivo y a la resolución innovadora de problemas, por lo que las organizaciones estarán mejor preparadas para gestionar las crisis y adaptarse al cambio. Las organizaciones que dan prioridad a la diversidad también pueden registrar mayores niveles de compromiso y retención del personal. Por tanto, es imprescindible que las organizaciones cuenten con una diversidad e inclusión adecuadas, y un componente de ello es garantizar que esta fuerza laboral diversa se mantenga a salvo. Para ello es fundamental comprender cómo la identidad puede afectar al riesgo.

Es importante señalar que cada persona tiene vulnerabilidades y fortalezas. Un enfoque inclusivo de la gestión de riesgos de seguridad implica cuestionar los estereotipos que sugieren que determinados perfiles son inherentemente más vulnerables. Estas suposiciones no siempre son exactas y pueden pasar por alto las valiosas contribuciones que un conjunto más diverso de perfiles y antecedentes del personal puede aportar a la gestión de riesgos de seguridad y a la labor humanitaria en su conjunto. Al centrarse tanto en las vulnerabilidades como en las fortalezas, las organizaciones pueden crear un enfoque más equilibrado y eficaz.

Riesgos basados en la identidad

Los riesgos de seguridad a los que se enfrenta el personal se ven afectados por su identidad, que nunca es una sola cosa, y, lo que es más importante, por cómo su combinación de atributos personales —su identidad interseccional— es percibida por los demás.

La interseccionalidad describe cómo diversos factores sociales (género, grupo étnico, orientación sexual, nivel socioeconómico, discapacidad) interactúan y se solapan para crear experiencias únicas de discriminación y privilegio. Aquí nos referimos a la *identidad interseccional*, que reconoce que las personas tienen múltiples identidades interconectadas que no pueden entenderse de forma aislada. Los aspectos interrelacionados de la identidad de una persona crean un perfil de riesgo único que requiere un enfoque de seguridad matizado y exhaustivo.

Aunque no es posible abarcar todos los perfiles personales de riesgo, los siguientes ejemplos ilustran algunas consideraciones basadas en la identidad.

- **Raza, grupo étnico y nacionalidad.**⁶ Las percepciones de la raza, el grupo étnico y la nacionalidad pueden influir en el trato que recibe el personal dentro y fuera de una organización. Las percepciones y los sesgos pueden aumentar el riesgo de violencia selectiva, discriminación, exclusión, caracterizaciones discriminatorias y otras expresiones de racismo y xenofobia, según el contexto y su dinámica social.⁷
- **Discapacidad y accesibilidad.** El personal con discapacidad puede enfrentarse a retos adicionales, como movilidad reducida o acceso limitado a suministros y servicios médicos, sobre todo en situaciones de emergencia. También pueden experimentar una mayor vulnerabilidad a la violencia y la explotación, así como aislamiento social.
- **Factores culturales y religiosos.** La lengua, la cultura y la religión pueden repercutir en la comunicación, la integración y la seguridad. El personal puede enfrentarse a riesgos específicos basados en sus creencias religiosas o en sus diferencias culturales en regiones donde las tensiones religiosas o de otro tipo son elevadas.
- **Género, sexualidad e identidad.** Los riesgos relacionados con el género y la sexualidad afectan a todas las personas, pero pueden ser más pronunciados para el personal cuya orientación sexual, identidad y expresión de género estén estigmatizadas, restringidas, marginadas, infrarrepresentadas o penalizadas en el lugar en cuestión. El género puede determinar la naturaleza y la gravedad de las amenazas a las que se enfrenta el personal, incluso en las relaciones interpersonales, más allá de los riesgos simplemente diferentes que corren hombres y mujeres.
- **Otras consideraciones.** El nivel socioeconómico, las funciones de trabajo, la edad y la experiencia laboral previa pueden afectar la forma en que se percibe y trata al personal y, en consecuencia, los riesgos a los que puede enfrentarse. La percepción de la jerarquía también puede influir (tanto en la sociedad como dentro

6 Reconocemos que los factores identitarios como el género, la nacionalidad, el grupo étnico y la raza son conceptos contruidos socialmente. Aunque reconocemos su carácter artificial, se incluyen aquí para destacar que la percepción de estos factores puede acarrear consecuencias de seguridad reales y a veces graves para las personas.

7 Para obtener un análisis más detallado, véase Arthur, T. y Moutard, L. (2022) *Toward inclusive security: The impact of 'race', ethnicity, and nationality on aid workers' security*, Global Interagency Security Forum (www.gisf.ngo/resource/toward-inclusive-security-the-impact-of-race-ethnicity-and-nationality-on-aid-workers-security/).

de una organización); el personal con peor remuneración o el que ocupa puestos más vulnerables (como conductores, limpiadores o becarios) está potencialmente más expuesto al peligro, pero a menudo tiene acceso a menos recursos y menos protección. Debido a percepciones y sesgos, es posible que las personas pertenecientes a grupos infrarrepresentados y marginados no reciban la atención adecuada dentro de sus organizaciones, lo que puede traducirse en un apoyo insuficiente a la seguridad de estos miembros del personal.

Ejemplo: Deficiencias al abordar los riesgos basados en la identidad

En un contexto con una población predominantemente blanca, una funcionaria internacional de tez más oscura sufrió acoso callejero en mayor medida que otras compañeras de la organización. Esto no solo afectó su capacidad para moverse libremente entre su casa y la oficina, sino que también repercutió en su salud mental y en su vida social fuera del trabajo.

Cuando expresó sus preocupaciones, la oficina las minimizó y sugirió que tal acoso era de esperarse. Esta respuesta le planteó dificultades para denunciar el acoso continuado y en aumento al que se enfrentaba, y el engorroso proceso para solicitar un vehículo para desplazarse con seguridad la disuadió aún más de buscar ayuda. Al final, la persona optó por marcharse. Una estrategia de mitigación de bajo costo, como mejorar los procesos administrativos para solicitar un viaje seguro y fomentar una mayor sensibilidad hacia las experiencias individuales, podría haber mejorado su situación y posiblemente se hubiera quedado en la organización.

Es crucial subrayar que la forma en que se percibe a una persona es a menudo una consideración de seguridad más importante que la forma en que esa persona se autoidentifica. Estas percepciones suelen estar arraigadas en sesgos que el cambio de comportamiento no necesariamente puede abordar. Es importante considerar cómo los rasgos de la identidad interseccional del personal pueden contribuir, exacerbar o influir en la respuesta y el comportamiento de los diferentes actores, tanto internos como externos a la organización, hacia esa persona.

Consideraciones adicionales

- **Visibilidad.** No todas las características identitarias son visibles o inmediatamente aparentes (por ejemplo, la orientación sexual y algunas discapacidades). Esto demuestra la necesidad de adoptar un enfoque inclusivo de la gestión de riesgos de seguridad que asuma por defecto que el personal tiene necesidades de seguridad diversas y que tenga en cuenta esta diversidad en la mayor medida posible mediante procesos de orientación y consulta. También supone crear un entorno organizativo que permita al personal expresar sus preocupaciones y buscar orientación sobre los riesgos relacionados con sus perfiles de identidad.
- **Ubicación.** Muchos enfoques de gestión de riesgos de seguridad se centran en los riesgos basados en la ubicación y tienen en cuenta las amenazas generales de la zona. Aunque son innegablemente importantes, no son la única consideración, ni necesariamente la principal en todos los casos. Con algunas excepciones generales (como las zonas de combate activo u otros contextos en los que la violencia es indiscriminada), que un lugar sea “seguro” para un miembro del personal a menudo puede tener más que ver con quién es la persona y cómo es percibida que con el lugar en el que se encuentra.⁸ Incluso en el caso de las excepciones mencionadas, determinados perfiles, como los trabajadores humanitarios nacionales, tienen más probabilidades de estar en estos lugares y, por tanto, corren un mayor riesgo debido a su mayor exposición. El aumento de las amenazas digitales y el resurgimiento de conflictos graves en Europa en los últimos años son una prueba más de la necesidad de cambiar las conversaciones sobre la seguridad y no hablar ya de “dónde es seguro” sino de “quién está seguro”.

► Véase el capítulo 6.2 para conocer más detalles sobre cómo los aspectos de la identidad afectan la seguridad digital.

- **Amenazas internas frente a amenazas externas.** Muchos sistemas de gestión de riesgos de seguridad se centran en las amenazas externas. Sin embargo, cada vez hay más pruebas de que las amenazas a la seguridad del personal provienen de los propios colegas. Los trabajadores humanitarios que se identifican como lesbianas, gays, bisexuales, trans, queer e intersexuales (LGBTQI+) o como personas con discapacidad han declarado que les preocupan más las amenazas internas que las externas.⁹ Las amenazas internas pueden incluir abusos verbales y físicos, chantaje, acoso, discriminación y violencia. Los comportamientos y los entornos contribuyen a crear culturas laborales hostiles y los casos menores de hostilidad pueden convertirse en formas más graves de agresión. Esta escalada se describe a menudo como un “continuo” o una “pirámide” de violencia en la que incidentes aparentemente triviales de acoso, incivilidad y exclusión no solo se normalizan,

8 Para obtener una ilustración detallada de este punto, véase Hoppe, K. (19 de diciembre de 2017) *Where is safe?*, TEDxBristol (www.youtube.com/watch?v=Q9RxE9p9T3w).

9 Foro Europeo Interinstitucional para la Seguridad (2018) *Gestión de la seguridad del personal humanitario con perfiles diversos* (www.gisf.ngo/resource/managing-the-security-of-aid-workers-with-diverse-profiles/).

sino que sientan las bases para abusos más graves.¹⁰ Una cultura que tolera estas agresiones menores aumenta el riesgo de que estos incidentes se intensifiquen.

- **Clasificación del personal.** Históricamente, en los planes de seguridad se ha hecho mucho hincapié en cómo se clasifica al personal dentro de una organización (por ejemplo, nacional, internacional, residente o móvil). Esto puede resultar problemático, ya que la categorización puede ser compleja y no tener en cuenta factores de identidad importantes, como la doble nacionalidad o si el personal nacional proviene de una localidad en particular o no. Esto también puede llevar a suposiciones incorrectas sobre la vulnerabilidad de los miembros del personal a las amenazas y sobre su conocimiento de los contextos de seguridad. A menudo es más eficaz considerar la situación específica de cada persona, así como las necesidades y las circunstancias contextuales, que basarse en clasificaciones generales. Los esfuerzos por localizar los puestos en organizaciones internacionales también deben sopesarse cuidadosamente en relación con los perfiles de riesgo personales y las fortalezas y vulnerabilidades individuales.

► Para obtener más información sobre la dotación de personal, véase el capítulo 5.1 sobre recursos humanos.

1.2.2 Un enfoque centrado en la persona

Históricamente, cuando los sistemas de gestión de riesgos de seguridad han tenido en cuenta la identidad, se han centrado sobre todo en cuestiones relacionadas con el género, el grupo étnico y la nacionalidad, y a menudo de forma *ad hoc*. Con los años, este enfoque se ha ampliado para incluir una variedad más amplia de rasgos de identidad.¹¹ Este cambio, impulsado por la necesidad de una cultura de seguridad más inclusiva en el sector, llevó a la introducción de un enfoque de gestión de riesgos de seguridad centrado en la persona. Este enfoque incorpora consideraciones basadas en la identidad y sitúa a las personas en el centro de las actividades de gestión de riesgos de seguridad. En la práctica, implica reconocer los riesgos específicos de cada perfil debido a la intersección de las características individuales (identidad interseccional) y el comportamiento, los factores organizativos y el contexto en el que trabaja el personal, tanto en la esfera física como en la digital, (véase la figura 2).

10 Para saber más sobre la pirámide de violencia, véase EISF (2019) *Gestión de la violencia sexual contra el personal humanitario: prevención, preparación, respuesta y atención posterior* (<https://gisfprod.wpengine.com/resource/managing-sexual-violence-against-aid-workers/>).

11 Global Interagency Security Forum y Humanitarian Outcomes. (2024) *State of practice: the evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Figura 2 Un enfoque de riesgos de seguridad centrado en la persona



Adaptado de Arthur, T. y Moutard, L. (2022) *Toward inclusive security risk management: the impact of 'race', ethnicity and nationality on aid workers' security*, Global Interagency Security Forum (www.gisf.ngo/resource/toward-inclusive-security-the-impact-of-race-ethnicity-and-nationality-on-aid-workers-security/).

Un enfoque de la gestión de riesgos de seguridad centrado en la persona implica adaptar las medidas de protección a las necesidades y vulnerabilidades específicas de cada trabajador humanitario, en lugar de aplicar un modelo único para todos. Promueve la mitigación equitativa del riesgo, ya que tiene en cuenta las identidades interseccionales únicas de los trabajadores humanitarios.

Esfuerzos de seguridad y descolonización

Además de mejorar la gestión de riesgos de seguridad, un enfoque de la seguridad centrado en la persona puede apoyar los esfuerzos de “descolonización” que están realizando cada vez más organizaciones internacionales. El personal de seguridad puede promover ambos objetivos mediante las siguientes acciones prácticas.

- **Reflexión crítica.** Plantear una reflexión crítica sobre los factores históricos y estructurales que influyen en los riesgos de seguridad. Las desigualdades históricas, contextuales y estructurales pueden exponer a determinadas personas a mayores riesgos que a otras, a menudo sin las medidas de protección correspondientes para protegerlas, sin el poder para garantizar que sus necesidades de seguridad sean escuchadas y satisfechas o sin la capacidad para dar realmente su consentimiento a los riesgos a los que están expuestas.
- **Diálogo inclusivo.** Fomentar el diálogo inclusivo para comprender las diversas perspectivas y experiencias. Esto puede ayudar a identificar y abordar los sesgos y las desigualdades en las prácticas de seguridad y garantizar que las medidas de gestión de riesgos de seguridad sean inclusivas. Incluye la adopción de una actitud receptiva hacia los conocimientos y las buenas prácticas de personas con perspectivas diversas.
- **Apoyo equitativo.** Garantizar que los recursos se asignen equitativamente para apoyar la seguridad de todo el personal, independientemente de su identidad. Esto puede significar la adopción de un enfoque de seguridad centrado en la persona y puede implicar la redistribución de los recursos para abordar las disparidades y garantizar un apoyo equitativo a la seguridad de los grupos marginados o infrarrepresentados. La cuestión del apoyo equitativo también es pertinente cuando se trabaja con socios (*véase el capítulo 3.5 para obtener un análisis más detallado*).
- **Empoderamiento y representación.** Promover la representación del personal marginado e infrarrepresentado en los procesos de toma de decisiones, incluidos los diagnósticos de riesgos y la planificación de seguridad. El personal de seguridad puede desempeñar un papel importante facilitando los debates y aportando conocimientos y experiencia que pueden traducirse en marcos organizativos más inclusivos. Esto también puede incluir la búsqueda de una mayor diversidad de profesionales de la seguridad en todos los niveles de una organización. Los equipos directivos también pueden hacer oír su voz sobre cómo la diversidad de las identidades y las experiencias es una ventaja en las operaciones humanitarias y en la labor de gestión de riesgos de seguridad.

1.2.3 Consideraciones sobre buenas prácticas

Cultura organizativa

Las normas y los tabúes culturales locales pueden hacer especialmente difíciles las conversaciones sobre las características de identidad específicas, como el grupo étnico y la orientación sexual. Esta resistencia cultural puede obstaculizar la aplicación de iniciativas inclusivas de gestión de riesgos de seguridad, que pueden requerir debates abiertos y delicados sobre estos temas. A algunos directivos de organizaciones también puede preocuparles que investigar las experiencias del personal con perfiles minoritarios pueda llamar la atención sobre posibles deficiencias de la organización, con el riesgo de dañar su reputación.

La creación y la aplicación de políticas que apoyen sistemáticamente un enfoque centrado en la persona exige compromiso y apoyo institucional. Esto puede incluir la elaboración de directrices exhaustivas, la asignación de recursos para formación y la integración de estas políticas en la cultura organizativa general. Muchas organizaciones siguen teniendo dificultades para incorporar sistemáticamente consideraciones y lenguaje inclusivos en sus políticas, formación y comunicaciones diarias.

Los equipos directivos pueden centrarse en empoderar a los referentes de seguridad para que adopten una perspectiva centrada en la persona en todos los aspectos de su trabajo, incluido el desarrollo colaborativo de un marco de gestión de riesgos de seguridad inclusivo. El personal de seguridad puede desempeñar un papel importante en la promoción de una cultura de confidencialidad, colaboración, inclusión y confianza y debe esforzarse para que lo consideren accesible y fiable dentro de la organización. Algunas organizaciones cuentan con referentes de seguridad en cada oficina, que son mujeres y/o habitantes de la zona, para mejorar la notificación de cuestiones delicadas.

Un reto clave es determinar el equilibrio entre la responsabilidad individual y el deber de cuidado de la organización. Es aconsejable que los equipos directivos investiguen a fondo y comprendan sus responsabilidades en el cumplimiento de este deber, sobre todo teniendo en cuenta los perfiles diversos del personal. Si no se abordan adecuadamente los riesgos basados en la identidad, se podría incumplir este deber de cuidado, sobre todo cuando la inmensa mayoría de la fuerza laboral humanitaria se compone de personas de diversas procedencias. Un sistema de gestión de riesgos de seguridad que tenga en cuenta las diversas necesidades de seguridad del personal no solo ayuda a mitigar estos riesgos, sino que también puede mejorar el bienestar y la retención del personal, así como los resultados de los programas. Las organizaciones deben ser claras sobre el nivel de apoyo que ofrecen para gestionar los riesgos basados en la identidad y al mismo tiempo animar a las personas a buscar orientación y apoyo para necesidades específicas.

Abordar la discriminación

Las preocupaciones sobre la discriminación constituyen un obstáculo importante para las organizaciones a la hora de ocuparse de los riesgos basados en la identidad. Las organizaciones no quieren que se considere que invaden la intimidad del personal o que toman decisiones de empleo basadas en los atributos personales, y pueden preocuparse, con razón, por las implicaciones jurídicas de hacerlo. Esto ha provocado que algunas organizaciones adopten un enfoque de “no preguntes, no digas”, en el que las decisiones de seguridad basadas en aspectos identitarios no se comunican de forma transparente ni se discuten abiertamente. Sin embargo, tratar a todos los miembros del personal como si compartieran un único perfil de riesgo puede derivar en una protección inadecuada, en un aumento de las vulnerabilidades e incluso en mayores riesgos organizativos. Según estudios recientes, a los trabajadores humanitarios les gustaría que las medidas de protección abordaran de forma más transparente y abierta los riesgos basados en la identidad.¹²

En algunas circunstancias y contextos, las personas con determinados perfiles pueden tener que seguir medidas de protección distintas o necesitar un apoyo de seguridad adicional. Si las medidas y los recursos impuestos están justificados dependerá de si estas acciones son legítimas y proporcionales al riesgo o de si existen alternativas menos drásticas. Debe procurarse que todas las decisiones se basen en pruebas documentadas y no en suposiciones o percepciones individuales.¹³ En efecto, lo que convertiría estas medidas en injustificables es que fueran arbitrarias y que las diferencias dieran lugar a un trato injusto o desigual.

Para entenderlo mejor, conviene hacer una distinción entre trato equitativo e igualdad de trato. La igualdad de trato implica proporcionar los mismos recursos y medidas a todas las personas, independientemente de sus circunstancias. Sin embargo, este enfoque puede pasar por alto vulnerabilidades específicas y no proporcionar una protección adecuada. El trato equitativo implica proporcionar recursos y medidas específicas para garantizar que todas las personas tengan el mismo nivel de seguridad y apoyo, teniendo en cuenta sus necesidades y riesgos específicos. El objetivo es garantizar que el nivel de riesgo resultante sea aceptable para todos. Este enfoque no es discriminatorio, sino que implica más bien un ajuste necesario para afrontar eficazmente amenazas reales y variadas.

Las siguientes acciones permiten garantizar que las medidas no sean discriminatorias y que sean más fácilmente aceptadas por el personal:

- **Desarrollo colaborativo de políticas y prácticas.** Al involucrar a miembros diversos del personal en el desarrollo y en la revisión de las políticas y las prácticas

¹² Foro Europeo Interinstitucional para la Seguridad (2018).

¹³ Para obtener un análisis más detallado de las consideraciones jurídicas contra la discriminación, véase Foro Europeo Interinstitucional para la Seguridad (2018), capítulo 2, “Legal duty of care and anti-discrimination”.

de seguridad, se garantiza que el enfoque de la organización refleje una amplia variedad de perspectivas y aborde las preocupaciones y los riesgos específicos a los que se enfrentan los distintos grupos de identidad. Las organizaciones pueden establecer espacios consultivos, comités asesores o grupos de trabajo que incluyan a representantes de diversos grupos de identidad para contribuir al desarrollo o la revisión de las medidas de protección.

- **Comunicación explícita y oportuna.** Informar al personal de los riesgos y comunicar claramente las razones que justifican medidas de protección particulares en el momento oportuno (por ejemplo, antes de un viaje o durante la selección de personal) ayuda a garantizar que todos comprenden la necesidad y legitimidad de estas medidas.
- **Mecanismos de retroalimentación.** Establecer canales para que el personal pueda dar su opinión sobre las medidas de protección, solicitarla periódicamente y actuar en consecuencia ayudan a identificar cualquier problema de discriminación percibida y permite adaptar y mejorar continuamente las prácticas de seguridad a medida que cambian los entornos y los riesgos.

Sistemas, políticas y prácticas de seguridad inclusivas

Introducir una nueva forma de trabajar puede ser abrumador. El personal de seguridad suele trabajar con plazos exigentes y una gran carga de trabajo, lo que dificulta la asignación de tiempo para considerar un enfoque nuevo y adoptar formas de trabajo centradas en la persona. El personal de seguridad también puede sentirse incapaz de participar en conversaciones sobre riesgos basados en la identidad debido a la falta de experiencia. A pesar de estos retos, algunas organizaciones han hecho grandes progresos en la adopción de un enfoque de seguridad centrado en la persona, a menudo impulsado desde el nivel directivo, que ha tomado las medidas iniciales, entre ellas, motivar y empoderar al personal para que adopte este enfoque. Para algunas organizaciones, esto ha conllevado la realización de consultas con el personal para comprender los riesgos basados en la identidad a los que se enfrentan; para otras, ha supuesto la contratación de equipos de seguridad más diversos, y para una organización internacional ha implicado la evaluación de todos los aspectos de sus sistemas de seguridad para identificar formas en las que podrían ser más inclusivos (véase el ejemplo en el recuadro más adelante).

Muchos esfuerzos han empezado a pequeña escala, con cambios específicos en ámbitos concretos, que luego se multiplicaron. Para comenzar a aplicar un enfoque centrado en la persona no es indispensable una inversión significativa de dinero o de tiempo, sino que es posible empezar con un cambio de perspectiva, por ejemplo, por el simple hecho de que el personal de seguridad pregunte cómo puede repercutir una situación o un programa en la seguridad de compañeros con diferentes perfiles y necesidades.

Ejemplo: Aplicación de un enfoque sistemático de seguridad centrado en la persona

El equipo de seguridad global de una organización internacional puso en marcha un proyecto para establecer un marco orientativo para un enfoque de gestión de riesgos de seguridad centrado en la persona. El objetivo principal del proyecto era identificar las deficiencias en materia de diversidad e inclusión en la gestión de riesgos de seguridad (mediante investigación y consultas al personal) y, a continuación, ofrecer recomendaciones prácticas.

La mayoría del personal consultado para el proyecto consideraba que los perfiles personales eran un factor importante a la hora de determinar el nivel y el tipo de riesgos de seguridad a los que se enfrentaban, pero que la organización y, en particular, los gerentes, debían hacer más por abordar los riesgos específicos de cada perfil.

Según la investigación, los principales problemas de seguridad relacionados con el perfil son la falta de acceso a información pertinente, la discriminación interna o el trato desigual y los prejuicios o la hostilidad externos en el entorno local. Entre los factores que hacen que el personal se sienta más seguro figuran la comunicación abierta sobre cuestiones relacionadas con la seguridad por parte del equipo directivo, la existencia por escrito de políticas y procedimientos de seguridad claros y la disponibilidad de mecanismos para reportar incidentes o cualquier información pertinente, para comprender mejor el entorno de trabajo en general, así como para atender las quejas.

La investigación señaló la necesidad de adoptar un enfoque más sistemático e inclusivo sobre la gestión de riesgos de seguridad, así como una cultura de gestión más proactiva e inclusiva. Después del proyecto, la organización adoptó medidas para aplicar las recomendaciones identificadas, lo que requirió la participación de varios equipos de trabajo internos y de los responsables de la toma de decisiones. Puesto que era necesario hacer cambios en toda la organización, era importante garantizar que la aplicación fuera una responsabilidad compartida por varias partes interesadas, como Seguridad, Recursos Humanos y otros departamentos implicados en la formación, la elaboración de políticas y la recopilación de datos.

Las consideraciones relativas a la diversidad pueden incluirse en todo el marco de gestión de riesgos de seguridad.

- **Diagnósticos de riesgos inclusivos.** Un proceso exhaustivo de diagnóstico de riesgos que integra factores de riesgo individuales (identidad y comportamientos interseccionales), organizativos y externos, y que considera las amenazas internas y externas y sus interrelaciones. Otro factor a tener en cuenta puede ser el tiempo (ya que ciertos periodos, como, por ejemplo, los electorales, pueden ser más inseguros que otros). Las organizaciones más pequeñas, o aquellas con menos movimiento de personal, pueden estar en mejores condiciones para realizar diagnósticos de riesgos individualizados para cada miembro del personal cuando se incorporan a la organización, comienzan un proyecto nuevo o viajan (este es un enfoque adoptado por algunas organizaciones de derechos humanos, por ejemplo). A las organizaciones más grandes, que podrías tener dificultades con esto, puede resultarles útil asegurarse de que los diagnósticos de riesgos involucren la mayor diversidad posible de personal, para garantizar la incorporación de una variedad de perspectivas y para proporcionar al personal las herramientas y la formación necesarias para llevar a cabo sus propios diagnósticos de riesgos individuales y buscar orientación cuando sea necesario.
- **Planes de seguridad y medidas de respuesta.** Garantizar que las medidas de mitigación de riesgos, los planes de seguridad y los mecanismos de respuesta tienen en cuenta las diversas necesidades del personal. Esto puede significar, por ejemplo, garantizar que se tenga debidamente en consideración al personal con discapacidades en los planes de seguridad y evacuación del sitio, o que se tengan en cuenta las nacionalidades del personal en los planes de contingencia (por ejemplo, la evacuación de personas de algunas nacionalidades a un país concreto puede suponer un mayor riesgo para ellas). Para el personal residente, tanto nacionales como extranjeros, puede ser aconsejable incorporar consideraciones familiares a los planes de contingencia. Esto puede lograrse mediante los enfoques de colaboración que se describen en varias partes de este capítulo.¹⁴
- **Herramientas de seguridad.** Incorporar a las herramientas de seguridad existentes preguntas e información sobre los riesgos basados en la identidad. Esto puede incluir opciones para seleccionar elementos calificadoros basados en la identidad en los formularios de los informes de incidentes, a fin de permitir un mejor análisis de estos y así ayudar a determinar si los incidentes son el resultado de discriminación, homofobia, ataques por motivos étnicos u otros factores.
- **Orientación.** Proporcionar orientación para que el personal que no desee revelar preocupaciones relativas a su identidad personal tenga acceso a información que le permita tomar decisiones de seguridad informadas. La clave aquí es que la información sobre los riesgos específicos de cada perfil se comunique sistemáticamente a todo el personal, independientemente de sus perfiles personales. Para ello, se puede incorporar información sobre riesgos basados en la identidad en los documentos de seguridad compartidos con el personal y poner a su disposición referentes con los que puedan hablar de forma confidencial y personalizada. Las organizaciones pueden colaborar con grupos e iniciativas especializadas para incorporar sus conocimientos y recursos a la orientación interna. Esto podría incluir trabajar con organizaciones que abordan la violencia de género o apoyan a las personas LGBTQI+.

¹⁴ Para consultar ejemplos detallados sobre medidas de mitigación de riesgos inclusivas, véase EISF (2018).

El personal puede contar con sus propios recursos y orientaciones, pero la forma en que una organización pone a disposición la información y el tipo de circuito de retroalimentación que ofrece pueden marcar una gran diferencia en la forma en que el personal interactúa con las orientaciones que recibe. Esto también puede mejorar el contenido de las orientaciones que la organización elaborada y mantiene.

- **Cultura de seguridad.** Construir una cultura de seguridad positiva e inclusiva en la organización comunicando al personal los riesgos basados en la identidad, desestigmatizando las discusiones y abordando los “mitos” sobre la vulnerabilidad personal en entornos grupales, como reuniones informativas y formaciones. Este tipo de comunicación puede empoderar al personal para expresar sus preocupaciones y tomar decisiones de seguridad más informadas para sí mismos y para los demás.
- **Composición del personal de seguridad.** Selección de personal de seguridad diverso. Cada vez son más las organizaciones que aspiran a una mayor diversidad de su personal en general, pero también en los puestos de seguridad. La identidad de los referentes de seguridad puede influir significativamente en la percepción que tiene el personal de las medidas de protección y en su participación en ellas.¹⁵ En la práctica, esto puede significar tener en cuenta los requisitos del puesto. Por ejemplo, en los países en los que las mujeres tienen prohibido desempeñar funciones policiales o militares, hacer que esta experiencia sea un requisito para los puestos de seguridad excluirá a las candidatas nacionales.

Funciones y perfiles de riesgo personales

En algunos contextos, determinados visitantes pueden tener perfiles de riesgo elevado debido a su visibilidad o función (por ejemplo, los visitantes VIP). Entre estas personas pueden encontrarse directivos de organizaciones, expertos, donantes, funcionarios públicos y auditores, cuya presencia puede atraer una atención o agresión no deseadas (dentro y fuera de una organización). Los ataques dirigidos hacia estas personas pueden tener graves repercusiones tanto en su seguridad personal como en la de toda la organización. También pueden aumentar los riesgos de seguridad del personal, lo que plantea importantes cuestiones sobre la criticidad de estas visitas. Si la visita justifica el riesgo que conlleva para el visitante y el resto del personal, las organizaciones pueden aplicar medidas de protección adecuadas, que pueden incluir escoltas de seguridad discretas, alojamiento seguro, protocolos de viaje especiales, medidas de seguridad de la información (como no revelar públicamente información sobre la ubicación) y planes de contingencia para emergencias. Para las organizaciones en las que las visitas de personas VIP son habituales, es conveniente impartir formaciones periódicas a estas personas y a quienes interactúan con ellas sobre concienciación en materia de seguridad personal y comportamiento en entornos de alto riesgo.

¹⁵ Para obtener más información, véase Global Interagency Security Forum y Humanitarian Outcomes (2024).

Orientación sobre riesgos basados en la identidad

Los miembros del personal tienen derecho a la privacidad, lo que significa que las organizaciones no pueden obligarlos a revelar información sobre sus perfiles personales si no se sienten cómodos con ello. Al proporcionar orientación general sobre los riesgos basados en la identidad, las organizaciones evitan presionar al personal para que revele información sensible o señalar directamente al personal en función de suposiciones sobre su identidad. Esto también contribuye a crear una cultura de seguridad que permita a cada persona plantear preguntas y reflexionar sobre sus propias necesidades de seguridad.

Los siguientes ejemplos de preguntas pueden ayudar a las organizaciones a decidir qué orientación proporcionar:

- ¿Cuál es la composición del personal? Contar con información agregada y anonimizada de recursos humanos puede ser útil. Utilizando estos datos junto con factores contextuales, ¿qué perfiles de personal pueden requerir más orientación?
- ¿Comprende el personal el deber de cuidado de la organización hacia ellos? ¿Hay algún ámbito específico en el que necesiten más información, y podría abordarse esto mediante orientaciones adicionales?
- ¿A qué recursos relacionados con los riesgos basados en la identidad (externos e internos) tiene acceso el personal? ¿Cómo puede la organización facilitar el acceso a esta información?
- ¿Puede el personal acceder de forma cómoda y confidencial a los recursos relacionados con los riesgos basados en la identidad?
- ¿Existe un referente al que el personal pueda dirigirse confidencialmente para hablar de sus preocupaciones?

Una organización se ha asegurado de que, como parte de sus procedimientos de viaje, se proporcionen enlaces a recursos externos e internos para riesgos y orientación pertinentes para el personal LGBTQI+. El sitio de intranet de la organización también cuenta con una página específica de orientación.

Hacer inclusivas las prácticas organizativas más amplias

Puede ser útil aplicar una perspectiva centrada en la persona a las prácticas organizativas generales que puedan afectar la seguridad del personal.

- **Revisiones del sistema.** Llevar a cabo revisiones de la organización que evalúen si todo el personal tiene un acceso adecuado a apoyo y recursos (incluidos los de seguridad), independientemente de su perfil personal, y abordar cualquier barrera o desigualdad estructural detectada. En cualquier organización, sobre todo en las internacionales, conviene adaptar la comunicación y las interacciones al público destinatario. Un ejemplo sencillo es garantizar que el personal acceda a las comunicaciones pertinentes en su lengua materna. En muchas organizaciones internacionales, el personal internacional y nacional puede tener acceso a distintos niveles de apoyo, incluida la cobertura de seguros. En algunas circunstancias, estos servicios de apoyo adicionales están justificados y son necesarios, pero esto también puede indicar problemas de equidad entre todo el personal. También es importante señalar que estas distinciones pueden no deberse a sesgos o descuidos, sino a factores que escapan al control de la organización, como las barreras legales a la evacuación del personal nacional y las limitaciones de las pólizas de seguros.
- **Selección de personal general y despliegue.** Integrar las consideraciones de seguridad basadas en la identidad en los procedimientos de selección y, si procede, en las conversaciones con el personal antes de las nuevas asignaciones.¹⁶ En la práctica, esto puede significar estar abierto a diferentes experiencias y garantizar que los requisitos del puesto no excluyan indebidamente a determinados perfiles (véase el recuadro más adelante).

¹⁶ Para consultar un análisis más profundo sobre la consideración de los riesgos basados en la identidad en la selección de personal, véase Foro Europeo Interinstitucional para la Seguridad (2018).

Cuestiones de identidad en la selección y en el despliegue de personal

La selección o el despliegue de personal en el sector humanitario es más complejo que en muchos otros ámbitos de trabajo. Algunas personas pueden correr un mayor riesgo en lugares o funciones nuevos debido a sus perfiles de riesgo personales. Es aconsejable fomentar el debate siempre que sea posible, en lugar de prohibir de forma absoluta determinados perfiles. Dicho esto, en algunos casos puede ser aconsejable indicar en la descripción del puesto que determinados cargos no están abiertos a perfiles de identidad específicos debido a la situación de seguridad. La legalidad de este tipo de discriminación indirecta depende del país; las medidas deben ser siempre justificables, proporcionales y legítimas. Un ejemplo sería no contratar a hombres para trabajar en un refugio o albergue de mujeres.

Involucrar a los referentes de seguridad en la selección y en el despliegue de personal, y ser claros en las descripciones de los puestos y durante las entrevistas sobre los elevados riesgos a los que se enfrentan determinados perfiles, garantiza que estas preocupaciones se debatan y decidan abiertamente junto con el personal afectado.

Formación

Abordar los riesgos basados en la identidad durante las capacitaciones en seguridad puede mejorar los resultados para todo el personal, desde cómo los miembros del equipo pueden apoyar a compañeros con discapacidad en caso de emergencia hasta cómo mantener la confidencialidad de la orientación sexual de un compañero tras un incidente de seguridad, especialmente si la divulgación de esta información puede suponer un riesgo de seguridad para el miembro del personal o la organización.

A pesar de que los formadores han notado cierta resistencia a tratar estos temas, abordar la diversidad en estos cursos puede ser una oportunidad para el diálogo y para compartir las experiencias vividas por perfiles infrarrepresentados entre los miembros del equipo que, de otro modo, nunca habrían sido escuchadas o comprendidas por los compañeros. Aunque no se puede esperar que los formadores tengan todas las respuestas a todas las preguntas relativas a los riesgos basados en la identidad, sí pueden crear un espacio para que los participantes examinen las preguntas por sí mismos para sus perfiles individuales, al tiempo que se benefician de conocer las experiencias comunes de los demás.

La identidad del formador también puede influir en el nivel de comodidad de los participantes en la formación a la hora de reaccionar a preguntas sobre sus perfiles individuales. Si bien es fundamental aumentar el número de formadores procedentes de grupos infrarrepresentados, también lo es la capacidad de todos los formadores, sea cual sea su perfil, para fomentar un entorno en el que las preocupaciones puedan acogerse y considerarse con seguridad.

- *Para conocer más detalles sobre la formación y las consideraciones relativas a la inclusión, véase el capítulo 5.2.*

Consideraciones sobre la formación específica

Además de procurar que la capacitación en seguridad tenga más en cuenta perfiles de riesgo diversos, las organizaciones también pueden ofrecer al personal, incluido el de seguridad, formación sobre sesgos inconscientes, poder, privilegios, interseccionalidad y cómo ser testigos empoderados, por citar algunos ejemplos. Algunas organizaciones han integrado estos aspectos en su capacitación en seguridad existente. Estas áreas de aprendizaje pueden ayudar a crear conciencia sobre los riesgos a los que se enfrentan los distintos grupos de identidad y promover una cultura de inclusión y respeto. Cuando el personal comprende la justificación de las medidas de protección particulares, es más probable que las considere justas y necesarias, lo que reduce la resistencia y la percepción de discriminación. Para el personal de seguridad, la formación en estas áreas puede deconstruir las suposiciones en torno a los perfiles de riesgo personales, ayudar a generar empatía y promover habilidades prácticas para gestionar los riesgos basados en la identidad.

Es aconsejable formar al personal de seguridad y a otros colegas pertinentes (como los de Recursos Humanos) sobre cómo adoptar un enfoque centrado en la persona: por ejemplo, cómo realizar una evaluación de los riesgos para la seguridad inclusiva. Esto garantiza que el personal responsable sea capaz de abordar los riesgos basados en la identidad y se sienta cómodo hablando de estos temas con el personal.

Ejemplo: Salvaguardia operacional de la ONU

El Departamento de Seguridad de las Naciones Unidas (UNDSS) ha desarrollado el concepto de *salvaguardia operacional*, que se aplica a políticas, procedimientos, medidas y formación aplicados en la ONU para proteger a su personal, bienes y operaciones de daños interpersonales. Se centra tanto en las amenazas internas como externas contra el personal y reconoce que los esfuerzos para hacer frente a las amenazas internas contra el personal de la ONU van de la mano con los esfuerzos para hacer frente a la explotación y abuso sexuales por parte del personal de la ONU.

La salvaguardia operacional promueve un enfoque de seguridad centrado en la persona mediante la aplicación de herramientas de seguridad inclusivas y centrándose en los agresores (conocidos y desconocidos), sus aliados, el entorno operativo y las vulnerabilidades personales y situacionales de los objetivos potenciales.

Entre los elementos clave de este enfoque se incluyen los siguientes:

- Reconocer que los comportamientos y los entornos pueden conducir al abuso de poder y que los casos menores de hostilidad pueden escalar a formas de daño más graves (*pirámide de la violencia*). Tolerar el acoso, la incivildad y la exclusión aumenta la probabilidad de que se produzcan incidentes más graves, incluidas las agresiones sexuales.
- Reconocer que todas las formas de agresión interpersonal tienen relevancia para el personal de seguridad, ya que constituyen un problema transversal grave que requiere la colaboración de todos los departamentos que tratan con el personal.
- Asegurarse de que todos los miembros del personal estén informados de todas las posibles amenazas, no solo de las que parezcan relevantes para cada individuo. Al dotar a todo el personal de los conocimientos y las herramientas necesarios para mitigar los riesgos de forma universal, la ONU pretende mejorar la seguridad para todos. Esencialmente, la seguridad colectiva solo se consigue cuando cada miembro está seguro: nadie está realmente seguro hasta que todos lo están.
- Promover un enfoque defensor de las Naciones Unidas, motivando al personal capacitado a convertirse en testigos empoderados en caso de incidentes y a promover la salvaguardia operacional en el curso de su trabajo.

La ONU ha puesto en marcha una formación mixta sobre salvaguardia operacional. La formación interactiva pretende crear conciencia entre el personal sobre cómo aplicar este enfoque y mejorar sus habilidades como “defensores de la ONU”. Además de sensibilizar y empoderar al personal, el propósito de la formación es constituir un importante elemento disuasorio para los posibles agresores.

Más información

Investigación y análisis

Arthur, T. y Moutard, L. (2022). *Toward inclusive security: The impact of ‘race’, ethnicity, and nationality on aid workers’ security*. Global Interagency Security Forum (www.gisf.ngo/resource/toward-inclusive-security-the-impact-of-race-ethnicity-and-nationality-on-aid-workers-security/).

Foro Europeo Interinstitucional para la Seguridad. (2018). *Gestión de la seguridad del personal humanitario con perfiles diversos* (www.gisf.ngo/resource/managing-the-security-of-aid-workers-with-diverse-profiles/).

Global Interagency Security Forum y Humanitarian Outcomes. (2024). *State of practice: The evolution of security risk management in the humanitarian space* (www.humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Hoppe, K. (2017). *Where is safe?* TEDxBristol (www.youtube.com/watch?v=Q9RxE9p9T3w).

Orientación y herramientas

Bond. (2022). *Becoming locally led as an anti-racist practice: a guide to support INGOs* (www.bond.org.uk/resources/becoming-locally-led-as-an-anti-racist-practice-a-guide/).

Comité Internacional de la Cruz Roja. (2021). 3.3. Is everyone equally at risk?. En *SAFE: Security and safety manual for humanitarian personnel* (www.icrc.org/en/publication/4425-safe-manuel-de-securite-pour-les-humanitaires).

Foro Europeo Interinstitucional para la Seguridad. (2019a). *Gestión de la violencia sexual contra el personal humanitario: prevención, preparación, respuesta y atención posterior* (<https://gisfprod.wpengine.com/resource/managing-sexual-violence-against-aid-workers/>).

Foro Europeo Interinstitucional para la Seguridad. (16 de diciembre de 2019b). *Beyond the tick box: Developing a person-centred and inclusive approach to security risk management* (www.gisf.ngo/blogs/beyond-the-tick-box-developing-a-person-centred-and-inclusive-approach-to-security-risk-management/).

Global Interagency Security Forum. (2021). *HNPW / A person-centred approach to security risk management / Resources* (<https://gisf.ngo/resource/hnpw-a-person-centred-approach-to-security-risk-management-resources/>).

Global Interagency Security Forum. (s.f.). 2. *Inclusive security*. NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/inclusive-security/>).

Naciones Unidas. (s.f.). *Gender & security* (www.un.org/en/safety-and-security/gender-and-security/).

Persaud, C. (2012). *Género y seguridad. Directrices para la transversalización del género en la gestión de riesgos de seguridad*. Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/gender-and-security/>).

RedR UK y Foro Europeo Interinstitucional para la Seguridad. (2016). *Workshop report: Inclusion and security of LGBTI aid workers* (<https://gisf.ngo/resource/report-inclusion-and-security-of-lgbti-aid-workers-workshop-22012016/>).

2 Los ecosistemas de la gestión de riesgos de seguridad

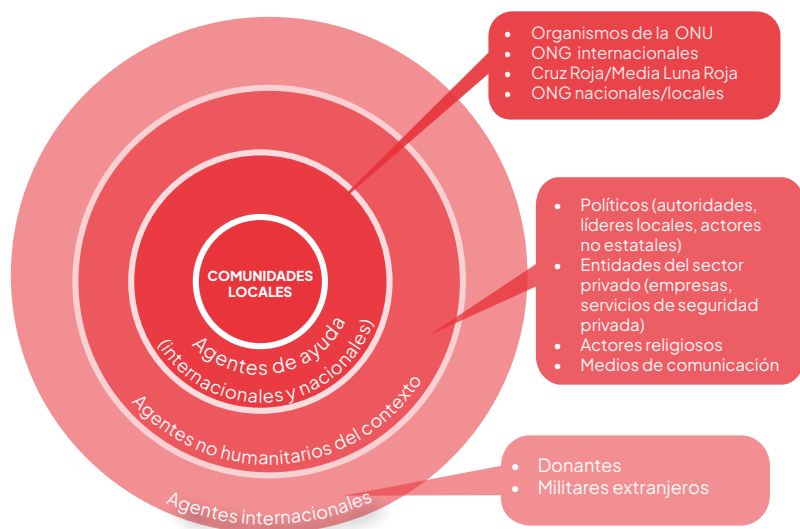
2.1 Redes y colaboración de seguridad

Las organizaciones humanitarias no actúan en el vacío. A diario interactúan con agentes amistosos, hostiles y neutrales en distintos niveles. El número de interlocutores no ha hecho más que crecer en los últimos años a medida que más agentes humanitarios, entidades del sector privado y grupos armados no estatales operan en los mismos espacios. En este capítulo se describen los principales actores y relaciones que influyen en la gestión de riesgos de seguridad humanitaria y se explora cómo el personal de seguridad puede profundizar su comprensión y mejorar la coordinación y la colaboración para mejorar la seguridad y, al mismo tiempo, avanzar hacia los objetivos humanitarios.

2.1.1 Comprender el ecosistema externo

Cuando se produce una crisis humanitaria, diversos agentes locales, nacionales y, a menudo, internacionales responden con intervenciones dirigidas a atender las necesidades de las personas y de las comunidades afectadas. Estos agentes humanitarios, tanto formales como informales, son diversos; cada uno tiene su propio estatuto jurídico, objetivos y políticas. En este espacio humanitario complejo, y a menudo abarrotado, la coordinación es imprescindible para alcanzar objetivos humanitarios comunes. Fuera del ámbito humanitario, las organizaciones navegan por un ecosistema aún más amplio de organizaciones públicas y privadas, entidades políticas, grupos militares e instituciones financieras (figura 3).

Figura 3 El ecosistema exterior



Cada uno de estos actores puede presentar posibles amenazas u oportunidades para la gestión de riesgos de seguridad.

2.1.2 Coordinación y colaboración de seguridad

Colaboración de seguridad interinstitucional

A medida que la gestión de riesgos de seguridad se ha ido desarrollando en las organizaciones humanitarias, también lo han hecho las estructuras, los medios y las prácticas para que las organizaciones en el mismo entorno operativo cooperen entre sí en materia de seguridad. La colaboración eficaz entre organizaciones permite a cada participante mejorar significativamente la eficacia de sus propios sistemas de gestión de riesgos de seguridad del modo que se expone a continuación.

- **Un mejor sistema de alerta.** Al compartir información entre sí, las organizaciones obtienen una visión más completa de las amenazas o las alertas de seguridad reales o potenciales en su entorno, lo que mejora la planificación de la respuesta y aumenta las posibilidades de evitar un incidente.

- **Mejor diagnóstico de riesgos.** Una compilación centralizada de todos los incidentes y cuasiaccidentes de seguridad en los que se hayan visto implicados trabajadores humanitarios en un entorno operacional determinado constituye una mejor base para evaluar los riesgos para la seguridad que el registro parcial de una sola organización.
- **Capacidad adicional rentable.** En lugar de que cada organización asuma individualmente los costos de los insumos adicionales, estos pueden conseguirse en un régimen de costos compartidos. Por ejemplo, los costos de consultas especializadas o de una capacitación en seguridad pueden compartirse entre varias organizaciones.
- **Incidencia y negociación colectivas con las autoridades.** En lugar de intervenir de manera individual en cuestiones relacionadas con la seguridad, las organizaciones pueden presentar argumentos más sólidos a los Gobiernos y a otras partes interesadas si actúan como grupo.
- **Incidencia para obtener financiación de los donantes.** Si la situación de seguridad se deteriora y varias organizaciones llegan a la conclusión de que necesitan recursos financieros adicionales para adoptar medidas de mitigación suplementarias, quizá puedan argumentar su posición de manera más eficaz a los donantes de forma colectiva.
- **Asistencia directa y resolución de carencias.** Si una organización tiene la capacidad de acoger personal adicional durante un confinamiento o dispone de transporte para reubicar o evacuar al personal cuando otras no lo tienen, la coordinación y la planificación previas pueden garantizar el uso eficaz de estos recursos.
- **Prestación de servicios comunes.** Los mecanismos de coordinación establecidos pueden aprovechar las economías de escala para proporcionar servicios como información y análisis de seguridad centralizados y capacitación.
- **Difusión de las buenas prácticas.** Las organizaciones pueden aprender unas de otras cuando colaboran e intercambian información, consejos y buenas prácticas sobre cómo gestionar los riesgos en un área específica de operación.
- **Gestión de riesgos interdependientes.** Las medidas de protección (o la falta de ellas) de una organización pueden repercutir en las demás. Por ejemplo, si una organización utiliza escoltas de seguridad armadas o paga “tasas de facilitación” en los puestos de control, esto puede crear problemas para las que no lo hacen. Mediante la cooperación se pueden detectar y abordar estas incoherencias.

Mecanismos interinstitucionales de coordinación de seguridad

Existen mecanismos interinstitucionales de coordinación de seguridad a nivel mundial, regional, nacional y local. Pueden ser formales e informales.¹⁷

¹⁷ Para obtener información más detallada sobre la colaboración de seguridad, véase Global Interagency Security Forum (2022) *NGO Security Collaboration Guide* (<https://gisf.ngo/long-read/ngo-security-collaboration-guide/>).

Los mecanismos formales para las ONG —como la International NGO Safety Organisation (INSO), la Partner Liaison Security Operation (PLSO) de USAID y las ramas de seguridad de los organismos de coordinación de las ONG— pueden brindar productos analíticos, como informes periódicos y análisis de tendencias de seguridad. Estos mecanismos también ofrecen un espacio para el debate y pueden organizar foros y oportunidades de capacitación en seguridad.

Los órganos de seguridad de las ONG suelen interactuar con los organismos de la ONU en cuestiones de seguridad a través del equipo humanitario de la ONU en el país y el UNDSS. La coordinación y la colaboración entre las ONG y los organismos de la ONU pueden ayudar a realizar evaluaciones conjuntas del acceso, diseñar estrategias de acceso seguro, coordinar los planes de contingencia para emergencias y gestionar la labor de incidencia y la coordinación con las autoridades gubernamentales, los organismos de la ONU, las fuerzas militares y los agentes de seguridad privados.

Cuando no existe un organismo formal de coordinación, los referentes de seguridad de las diferentes organizaciones suelen establecer una red informal para compartir información, alertas y asesoramiento, a menudo utilizando plataformas en línea o basadas en SMS. La participación en estos grupos suele ser voluntaria y *ad hoc*, basada en la representación de individuos y no de organizaciones.¹⁸ En el momento de redactar este documento, existen redes informales para el personal de seguridad regional en África Occidental y América Latina y el Caribe.

Históricamente, los mecanismos de coordinación de seguridad en contextos humanitarios han sido creados por organizaciones internacionales y se han centrado además en ellas, lo que supone una menor representación de las organizaciones locales y nacionales. Esto se está abordando poco a poco, ya que cada vez se entiende mejor que el valor de la coordinación aumenta con el número de actores que participan, especialmente los que aportan conocimientos contextuales profundos y diversas fuentes de información.

A nivel mundial, la coordinación entre las ONG, y entre la ONU y las ONG, también ha avanzado en los últimos años. El GISF es una plataforma interinstitucional a través de la que se comparten información y buenas prácticas relacionadas con la gestión de riesgos de seguridad humanitaria. Funciona como un centro de conocimientos especializados, puesto que elabora orientaciones y realiza investigaciones originales. La INSO también desempeña un papel a nivel mundial y proporciona análisis, productos de formación y datos sobre seguridad. La International NGO Safety & Security Association (INSSA) es una organización de miembros que ofrece una certificación profesional para gestores de riesgos de seguridad a nivel nacional y regional, específica para el sector humanitario. Los grupos de trabajo globales se centran en temas concretos relacionados con la gestión de riesgos de seguridad, como la salvaguardia y el acceso humanitario.

¹⁸ Para consultar un análisis más a fondo, véase Global Interagency Security Forum y Humanitarian Outcomes (2024) *State of practice: The evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Varios países cuentan con redes de coordinación de seguridad para las organizaciones con sede en su territorio, por ejemplo, la red danesa Danish Interagency Security Network y el grupo británico UK NGO Security Focal Point Group. La coordinación en materia de seguridad también puede ser un componente de un mecanismo de coordinación más amplio, como InterAction en los Estados Unidos y La Coordinadora en España. A medida que se ha ido desarrollando el ámbito de la seguridad humanitaria, también ha aumentado el número de puestos especializados en seguridad y de plataformas de coordinación específicas para estos profesionales.

Salvar Vidas Juntos

Desde el 2001, la colaboración y coordinación de seguridad entre la ONU y las ONG internacionales se ha estructurado mediante un marco escrito conocido hoy como Salvar Vidas Juntos (SLT, por sus siglas en inglés).¹⁹ Este marco ha pasado por varias iteraciones a lo largo de los años, pero desde el principio ha pretendido facilitar una comprensión común de las oportunidades que tienen las ONG, los organismos de la ONU y el Movimiento Internacional de la Cruz Roja y de la Media Luna Roja para trabajar conjuntamente ante los retos comunes en materia de seguridad. Su propósito es mejorar la capacidad de los socios para tomar decisiones informadas y gestionar los riesgos mediante información y recursos compartidos.

Los participantes en el SLT se comprometen a cumplir seis objetivos o requisitos principales:

- establecer acuerdos y foros de coordinación en materia de seguridad;
- compartir información relevante en materia de seguridad;
- cooperar en la capacitación en seguridad;
- cooperar en los acuerdos operacionales y logísticos, cuando sea factible;
- identificar los requisitos relativos a los recursos para mejorar la coordinación de seguridad entre la ONU, las ONG internacionales y las organizaciones internacionales, y abogar por financiación, y
- consultar sobre las normas básicas comunes en materia de acción humanitaria.

El Comité de Supervisión del SLT, copresidido por el UNDSS y representantes de ONG internacionales, garantiza una aplicación y coordinación eficaces. Pueden participar todas las ONG internacionales que operen en un país, sin tasas, aunque algunos servicios pueden conllevar la recuperación de costos. Pese a que las organizaciones locales no pueden alcanzar el estatus de alianza en el SLT, pueden beneficiarse a través de las redes de seguridad de ONG existentes.²⁰

19 La primera encarnación del SLT fue un memorando de entendimiento denominado Menú de Opciones, establecido por el Comité Permanente entre Organismos (IASC) con el coordinador de seguridad de la ONU (UNSECOORD, precursor del UNDSS).

20 Para saber más sobre el SLT, véase <https://gisf.ngo/themes/coordination-for-hsrm/saving-lives-together/>.

Aunque el marco SLT se ha revisado y relanzado, su puesta en práctica a nivel de país ha sido difícil, limitada y lenta. El conocimiento de la existencia y de la finalidad del marco sigue siendo limitado tanto entre las ONG como entre el personal de la ONU, y en algunas zonas la falta de confianza entre las comunidades de la ONU y de las ONG dificulta aún más los avances.²¹ Aun así, el SLT ha tenido éxito en contextos en los que existe un liderazgo fuerte y eficaz en el UNDSS y en los equipos humanitarios en el país, así como una extensión coordinada y proactiva por parte de las ONG.

Servicios de seguridad privada

La seguridad comercial privada ha crecido considerablemente en las dos últimas décadas. El término *servicios de seguridad privada* puede referirse tanto a empresas registradas oficialmente como a grupos no registrados, como milicias contratadas, que prestan servicios similares. El uso más común de estos servicios por parte de las organizaciones humanitarias es la contratación de empresas privadas de vigilancia para asegurar los edificios y las instalaciones de los programas.

Los servicios de seguridad privada ofrecen una amplia variedad de servicios, como protección estática (seguridad de oficinas y residencias), protección móvil (escortas), protección cercana (guardaespaldas), evaluación de amenazas, análisis de riesgos, auditorías de seguridad, formación, consultoría, gestión de incidentes críticos, apoyo en situaciones de crisis, logística (como seguridad en el transporte de fondos) y suministro de equipos.

Aunque es poco frecuente que los servicios de seguridad privada recurran a la protección armada, las organizaciones humanitarias los han contratado en ocasiones para la vigilancia desarmada y otros servicios de apoyo, incluido el trabajo analítico. La decisión de contratar estos servicios suele basarse en suposiciones sobre su experiencia especializada, eficiencia y rentabilidad, pero estas suposiciones deben examinarse cuidadosamente. Aunque la externalización de la seguridad pueda parecer inicialmente más barata, los costos ocultos podrían incluir la incapacidad de desarrollar las capacidades internas, posibles daños a la reputación, responsabilidades legales y el riesgo de depender de un enfoque de seguridad basado en la disuasión, que podría resultar más caro con el tiempo.

A la hora de emplear servicios de seguridad privada, las organizaciones deben considerar cuidadosamente a quién contratan y de qué manera. Los guardias en las oficinas, alojamientos y depósitos suelen ser la cara pública de la organización, lo que los hace esenciales para la seguridad general más allá de sus tareas básicas de vigilancia. También es crucial evaluar los posibles vínculos entre los servicios de seguridad privada y los actores militares o políticos, ya que pueden estar relacionados con las fuerzas de seguridad del Estado, la policía o individuos con un historial de comportamientos ilegales o abusivos, incluidas las violaciones de los derechos humanos. Puede resultar complicado evaluar las prácticas más generales de los servicios de seguridad privada debido a la confidencialidad y a las complejas estructuras de propiedad de algunas empresas.

21 Para obtener más información sobre estas dificultades, véase Global Interagency Security Forum y Humanitarian Outcomes (2024).

Un recurso útil es la Asociación Internacional del Código de Conducta (ICoCA), que se creó a partir del Documento de Montreux sobre las obligaciones jurídicas y las buenas prácticas de las empresas militares y de seguridad privadas, y que proporciona normas de buenas prácticas entre los servicios de seguridad privada. La ICoCA actúa como el órgano de gobernanza y supervisión del Código Internacional de Conducta para los servicios de seguridad privada, cuyo objetivo es garantizar el respeto de los derechos humanos, el cumplimiento del derecho internacional y la rendición de cuentas por conductas indebidas. Determinar si un servicio de seguridad privada está registrado en la ICoCA puede constituir una parte valiosa del proceso de diligencia debida, ya que la asociación promueve la buena gobernanza, los derechos humanos, el derecho internacional humanitario y altos estándares profesionales en el sector de la seguridad privada.

A la hora de considerar el uso de estos servicios, puede ser necesario tener en cuenta varios factores estratégicos, operativos y legales. También puede ser útil la experiencia externa, como la orientación de organismos como la ICoCA, especialmente si la capacidad interna es limitada. Las organizaciones podrían evaluar si la contratación de un servicio de seguridad privada se ajusta a su mandato y a su estrategia de seguridad, si reduce los riesgos a largo plazo y cómo podría afectar su reputación, tanto a nivel local como internacional, así como su capacidad para gestionar a dichos proveedores. También es importante determinar si el uso de estos servicios podría sentar un precedente o contribuir a la inflación del mercado, y posiblemente afectar a las comunidades locales y a otros agentes humanitarios. El modo en que los servicios de seguridad privada pueden mejorar la seguridad pública y garantizar el cumplimiento de la normativa gubernamental pertinente son también consideraciones importantes.

Durante la verificación de antecedentes y el proceso de contratación, puede ser útil aplicar procedimientos sólidos de diligencia debida, mantener modelos de contratos claros y conservar registros de desempeño detallados. Verificar si un servicio de seguridad privada opera con un código de conducta claro, cuenta con personal bien formado con reglas de actuación definidas y se adhiere a las normas legales puede garantizar su fiabilidad. También es importante tener en cuenta los compromisos éticos, los programas de formación y las medidas anticorrupción del proveedor. Los contratos podrían especificar el monitoreo del desempeño y los requisitos de cumplimiento. Se recomienda encarecidamente asegurarse de que los servicios de seguridad privada dispongan de mecanismos internos para abordar las conductas indebidas y los abusos.

La supervisión y el monitoreo continuos de los servicios de seguridad privada pueden ayudar a las organizaciones a garantizar que los proveedores mantengan altos niveles de calidad y protejan tanto sus intereses como los del público. También puede ayudar a mitigar riesgos ocultos, como la dependencia excesiva de proveedores externos, que podría afectar a la capacidad de una organización para adquirir experiencia interna en la gestión de riesgos de seguridad.²²

22 Para obtener más recomendaciones de buenas prácticas, véase Davis, J. et al. (2020) "Module 14, Contracting private security providers" en *Security to go: a risk management toolkit for humanitarian aid agencies*, 4.ª edición, Global Interagency Security Forum (<https://gisf.ngo/resource/contracting-private-security-providers/>).

- Para obtener más información sobre el uso de escoltas armadas, véase el capítulo 4.2.

2.1.3 Interactuar con las autoridades

El Gobierno de un país afectado por una crisis tiene ciertas responsabilidades respecto a la seguridad y a la protección de las organizaciones humanitarias, que se reflejan en la legislación nacional, el derecho internacional humanitario y los acuerdos de las Naciones Unidas con el país anfitrión. En principio, se trata de las siguientes responsabilidades.

- **Garantizar la seguridad.** Como principales “titulares de obligaciones”, los Gobiernos son responsables de mantener la ley y el orden, garantizar un entorno seguro y proteger a todas las personas y las entidades de la violencia y la criminalidad.
- **Facilitar un acceso seguro.** Los Gobiernos son responsables de ayudar a facilitar el acceso humanitario a las zonas donde se necesita ayuda, garantizando que los trabajadores humanitarios puedan operar sin restricciones, interferencias o amenazas indebidas. Esto incluye la concesión de visados, permisos y licencias.
- **Proporcionar un marco jurídico y normativo.** Establecer y hacer cumplir leyes que protejan a las organizaciones humanitarias del acoso, los ataques u otras amenazas al personal, las operaciones y los bienes.
- **Coordinación y comunicación.** Se espera que los Gobiernos se coordinen con las organizaciones humanitarias, intercambien información sobre amenazas, riesgos o incidentes de seguridad y que colaboren en las medidas de seguridad.
- **Investigar y procesar a los agresores de los ataques.** En caso de ataques o incidentes en los que estén implicadas organizaciones humanitarias, el Gobierno es responsable de investigar, detener y procesar a los agresores para garantizar la rendición de cuentas.
- **Respetar los principios humanitarios.** Se deben respetar la neutralidad, la independencia y la imparcialidad de las operaciones humanitarias, por lo que es necesario evitar acciones que puedan comprometer los principios o dañar la percepción de las organizaciones humanitarias en entornos conflictivos.

En realidad, el gobierno puede ser más o menos capaz de proporcionar un entorno seguro y puede ser parte en el conflicto que generó la crisis humanitaria. En casos excepcionales, como las entregas transfronterizas de ayuda humanitaria a Siria durante la guerra civil siria, sancionadas por el Consejo de Seguridad de la ONU, y las operaciones encubiertas de ayuda a Myanmar a través de la frontera tailandesa, las organizaciones pueden operar sin el acuerdo o la participación del gobierno. También variará la medida en que los gobiernos lideren, apoyen o participen en la coordinación de la respuesta humanitaria. En ocasiones, pueden politizar, impedir, atacar o interferir en la prestación de la ayuda. También puede ser el caso de Gobiernos extranjeros con intereses militares o de otro tipo en el país en cuestión.

Por su parte, las organizaciones humanitarias están obligadas a consultar y buscar la aprobación y el apoyo gubernamentales para su presencia y a explicar la finalidad y los objetivos de sus actividades, incluso cuando el gobierno es parte en el conflicto o impide activamente la labor humanitaria. Suele ser de vital importancia mantener un intercambio continuo con las contrapartes gubernamentales pertinentes, incluidas, en ocasiones, las autoridades extranjeras, para garantizar la acción humanitaria; las organizaciones pueden cultivar una relación y un entendimiento continuos con las contrapartes gubernamentales a través del contacto periódico, reuniones y visitas de cortesía.

Al mismo tiempo, es aconsejable que el personal de seguridad actúe con cautela a la hora de relacionarse con sus homólogos gubernamentales, sobre todo en contextos en los que las autoridades pueden mostrarse hostiles a los esfuerzos de ayuda. A veces, incluso el uso de un término como *seguridad* puede levantar sospechas o invitar al escrutinio, lo que puede dar lugar a restricciones en las operaciones o a una mayor vigilancia de la organización. Resulta útil abordar estas interacciones con delicadeza, definir claramente los objetivos para evitar malentendidos y permanecer alerta a cualquier intento del gobierno de aprovecharse de la interacción para recabar información o socavar las actividades de la organización. Trabajar en coordinación con otros agentes humanitarios a través de las redes de colaboración establecidas puede facilitar estas interacciones.

Cuando operan en entornos de crisis, las organizaciones humanitarias también pueden tener que colaborar con actores subestatales, como las autoridades regionales o locales. Estos actores, aunque no tienen la misma autoridad que los gobiernos nacionales, a menudo ejercen una influencia considerable en zonas específicas. Puede ser crucial establecer una relación con las autoridades subestatales para asegurar el acceso humanitario, sobre todo en regiones en las que el alcance del gobierno central es limitado o en las que es necesario cooperar con varias autoridades *de facto* diferentes. Una comunicación clara acerca del mandato humanitario de la organización, que haga hincapié en la neutralidad y en la imparcialidad, puede ayudar a mitigar las tensiones y fomentar la confianza. Los actores subestatales pueden tener sus propios intereses, lo que podría repercutir en la seguridad y en la percepción de la labor humanitaria. Puede resultar beneficioso mantener un diálogo constante y trabajar en coordinación con otros agentes humanitarios, así como con líderes comunitarios de confianza.

Actores armados no estatales

En zonas de conflicto donde grupos armados no estatales controlan el territorio, las organizaciones humanitarias quizás deban entablar un diálogo para negociar el acceso y garantizar la seguridad de su personal. Los agentes no estatales pueden diferir significativamente en su enfoque de la ayuda humanitaria: algunos reconocen y facilitan el acceso, mientras que otros pueden ser más hostiles.

La interacción con estos agentes exige una preparación cuidadosa, que supone entender sus motivaciones, afiliaciones políticas y relaciones con las otras partes en conflicto, así como con las comunidades locales. Incluso las interacciones cotidianas pueden ser difíciles y, además de los riesgos de seguridad, pueden crear dilemas en relación con los principios humanitarios y las propias líneas rojas de la organización. El Centro de Competencia en Negociación Humanitaria fue creado por el Comité Internacional de la Cruz Roja (CICR) y otras organizaciones para prestar apoyo, coordinación y desarrollo de capacidades en las negociaciones humanitarias, y puede ser un recurso importante.ⁱ

Antes de entablar cualquier tipo de diálogo con agentes armados no estatales, es recomendable que las organizaciones hagan lo siguiente:

- Definan el alcance y los objetivos de la interacción.
- Analicen el contexto específico en el que se va a desarrollar el diálogo.
- Tracen un mapa de los diferentes actores y comprendan los motivos y los intereses (declarados y ocultos) de cada uno de ellos.
- Comprendan las circunscripciones que representan esos actores (si las hay).
- Diseñen y acuerden una estrategia de compromiso de acceso específica para el contexto.
- Acuerden lo que es negociable y lo que no lo es en términos de políticas, principios, mandatos y recursos.
- Colaboren y se coordinen con otras organizaciones que trabajan en el mismo espacio para comprender su punto de vista sobre el acceso y compartir enseñanzas.
- Comprendan la condición jurídica (local e internacional) de estos actores.

ⁱ Véase <https://frontline-negotiations.org/home/discover/about-us/>.

- *Para obtener más información sobre la interacción con agentes armados, véase el capítulo 4.2, “Diseñar una estrategia de seguridad”.*

2.1.4 Interacción con las fuerzas militares

Coordinación civil-militar

Los militares suelen ser actores principales en contextos de crisis, ya sea porque participan en conflictos armados o porque los Gobiernos afectados por crisis a veces utilizan fuerzas militares nacionales e internacionales y sus activos para prestar socorro en emergencias complejas. En cualquiera de estos escenarios, la coordinación entre los militares y los agentes humanitarios suele ser vital para facilitar una acción humanitaria segura.

Las principales entidades de coordinación entre las organizaciones humanitarias y las fuerzas militares son las siguientes.

- **Coordinación humanitaria civil-militar de la ONU (ONU-CMCoord)** bajo los auspicios de la Oficina de Coordinación de Asuntos Humanitarios de la ONU (OCHA). La ONU-CMCoord mantiene el diálogo con las fuerzas militares y otros agentes armados, incluidos los grupos armados no estatales, para promover la interacción y la cooperación entre todos los actores, de conformidad con la Resolución 46/182 de la Asamblea General de las Naciones Unidas y las directrices existentes de coordinación civil-militar.
 - **Centros de operaciones civiles y militares.** Los centros de operaciones civiles y militares son centros físicos de coordinación establecidos en zonas de conflicto o afectadas por desastres, donde las organizaciones militares, gubernamentales y humanitarias pueden intercambiar información y coordinar actividades. A menudo funcionan como un centro de comunicación y planificación.
 - **Grupos de trabajo sobre acceso humanitario.** Por iniciativa de la OCHA, las organizaciones humanitarias han colaborado en entornos inseguros y de difícil acceso a través de grupos de trabajo sobre acceso humanitario. Estos grupos pueden servir como un punto de entrada para el diálogo con agentes militares, permitiendo a las organizaciones humanitarias comunicar sus prioridades, negociar el paso seguro y abogar por la adhesión a los principios humanitarios.
- *Para obtener más información acerca de los grupos de trabajo sobre acceso y negociaciones, véase el capítulo 3.2, “Acceso y seguridad”.*

Es importante señalar que los mecanismos específicos de coordinación utilizados pueden variar en función del contexto y la naturaleza de la crisis. El marco de ONU-CMCoord ofrece flexibilidad para adaptar las estrategias de coordinación, que van desde la cooperación hasta la coexistencia, en función de la situación específica. Los acuerdos de colaboración y la capacitación común desempeñan un papel crucial a la

hora de facilitar una coordinación eficaz entre los agentes humanitarios y militares. En el *Manual de campo de ONU-CMCoord* se describen diversos elementos y tareas de coordinación, como el establecimiento del diálogo, el intercambio de información y el monitoreo de las actividades militares para garantizar que no repercutan negativamente en la acción humanitaria.²³

Las actividades de coordinación civil-militar pueden ser especialmente tensas en situaciones de conflicto, en las que la interacción con agentes militares puede parecer que compromete la neutralidad, la imparcialidad y la independencia de las operaciones de los agentes humanitarios. En tales situaciones, las organizaciones humanitarias a menudo intentarán mantener una distancia operativa y evitar depender excesivamente de los medios y servicios militares para la protección y el apoyo logístico.

Sistema de notificación humanitaria

El mecanismo del Sistema de Notificación Humanitaria para la Desconflicción (HNS4D, por sus siglas en inglés) tiene por objeto mejorar la seguridad de las operaciones humanitarias notificando a los agentes militares la ubicación de las instalaciones, los movimientos y las actividades humanitarias en las zonas de conflicto. Su objetivo es minimizar el riesgo de ataques accidentales contra el personal y las infraestructuras humanitarias, garantizando que las fuerzas militares conozcan estos lugares protegidos.

El HNS4D exige a las organizaciones que presenten información detallada sobre sus instalaciones, personal y desplazamientos previstos a un intermediario, generalmente la OCHA. Esta información suele incluir las coordenadas del Sistema de Posicionamiento Global (GPS), descripciones de las instalaciones y la naturaleza de las actividades. A continuación, la OCHA consolida esta información y la comparte con los agentes militares pertinentes para asegurarse de que disponen de datos actualizados y precisos sobre las operaciones humanitarias en la zona. El objetivo del proceso es ofrecer una capa de protección, con actualizaciones periódicas para mantener la exactitud de la información a medida que las operaciones evolucionan.

Ha habido casos en los que las organizaciones humanitarias han perdido la confianza en el HNS4D debido a los reiterados fallos y a la falta de garantías por parte de los homólogos militares. En Siria, Afganistán y Gaza, fuerzas militares internacionales bombardearon instalaciones gestionadas por ONG, incluso cuando las organizaciones humanitarias habían proporcionado repetidamente información y las coordenadas de estos lugares. Una comprensión realista de las capacidades y de las limitaciones del HNS4D debe guiar las decisiones de las organizaciones sobre su participación.²⁴

23 Coordinación humanitaria civil-militar de las Naciones Unidas. (2018). *UN-CMCoord field handbook*, Versión 2.0, Oficina de Coordinación de Asuntos Humanitarios (<https://gisf.ngo/wp-content/uploads/2021/11/E-Version-UNCMCoord-Field-Handbook-2.0-2018.pdf>).

24 Para obtener más información, véase Global Interagency Security Forum y Humanitarian Outcomes (2024).

2.1.5 Otros agentes no humanitarios

También puede haber otra serie de actores diversos, como empresas, instituciones financieras locales y grupos comunitarios, que pueden proporcionar apoyo logístico y operativo. Los agentes de desarrollo, las organizaciones locales de la sociedad civil y los grupos de derechos humanos suelen tener compromisos a largo plazo en muchos ámbitos y pueden aportar ideas y apoyo valiosos. Al colaborar con estas entidades, el personal humanitario también puede garantizar que sus intervenciones sean complementarias a los esfuerzos existentes, evitando la interrupción de la labor en curso de estos grupos y fomentando una respuesta más sostenible y local.

Más información

Investigación y análisis

Bebbington, C. et al. (2022). *Reviewing guidance and perspectives on humanitarian notification systems for deconfliction*. Center for Human Rights and Humanitarian Studies, Watson Institute for International and Public Affairs, Universidad Brown y Humanitarian Response Program, College of Maritime Operational Warfare, US Naval War College (<https://watson.brown.edu/chrhs/files/chrhs/imce/research/2022%20HNS4D%20Research%20Paper%20-%20CHRHS%20%26%20HRP.pdf>).

Global Interagency Security Forum y Humanitarian Outcomes. (2024). *State of practice: The evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Global Interagency Security Forum. (2023). Humanitarian notification systems: Unpacking the complexities and possibilities (n.º 3) [Podcast]. En *Evolving NGO security risk management* (<https://gisf.ngo/resource/evolving-ngo-security-risk-management-ep3-humanitarian-notification-systems-unpacking-the-complexities-and-possibilities-gisf-podcast/>).

Oficina de Coordinación de Asuntos Humanitarios de las Naciones Unidas. (2021). *Concept note on humanitarian notification in support of access and protection in Syria* (<https://reliefweb.int/report/syrian-arab-republic/concept-note-humanitarian-notification-support-access-and-protection>).

Orientación y recursos

Alto Comisionado de las Naciones Unidas para los Refugiados. (2020). *Manual para situaciones de emergencia: Coordinación civil-militar* (<https://emergency.unhcr.org/coordination-and-communication/working-others/civil-military-coordination>).

Asociación Internacional del Código de Conducta. (2021). El código internacional de conducta para los proveedores de servicios de seguridad privada (<https://icoca.ch/the-code/>).

Coordinación humanitaria civil-militar de las Naciones Unidas. (2018). UN-CMCoord field handbook, Versión 2.0 (<https://gisf.ngo/wp-content/uploads/2021/11/E-Version-UNCMCoord-Field-Handbook-2.0-2018.pdf>).

Davis et al. (2020). Module 14, Contracting private security providers. En *Security to go: a risk management toolkit for humanitarian aid agencies*. 4.^a edición. Global Interagency Security Forum (<https://gisf.ngo/resource/contracting-private-security-providers/>).

Global Interagency Security Forum. (2022). *NGO security collaboration guide* (<https://gisf.ngo/long-read/ngo-security-collaboration-guide/>).

Global Interagency Security Forum. (s.f.a). 1. *NGO security collaboration*. NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/1-ngo-security-collaboration/>).

Global Interagency Security Forum. (s.f.b). Salvar vidas enre todos (<https://gisf.ngo/themes/coordination-for-hsrm/saving-lives-together/>).

Inter-Agency Standing Committee. (2013). *IASC non-binding guidelines on the use of armed escorts for humanitarian convoys* (<https://reliefweb.int/report/world/iasc-non-binding-guidelines-use-armed-escorts-humanitarian-convoys>).

Oficina de Coordinación de Asuntos Humanitarios. (s.f.). Civil-military coordination” (www.unocha.org/es/node/62).

2.2 Incidencia y seguridad

La relación entre incidencia (*advocacy*) y seguridad en el sector humanitario puede ser compleja, ya que la incidencia plantea tanto riesgos como oportunidades para la seguridad de los trabajadores humanitarios. El personal de seguridad puede desempeñar un papel crucial a la hora de garantizar que los esfuerzos de incidencia no comprometan la gestión de riesgos de seguridad, sino que, por el contrario, refuercen las medidas de protección.

2.2.1 La incidencia en el sector humanitario

La incidencia humanitaria pretende influir en las políticas y en el comportamiento de los actores poderosos en beneficio de las personas afectadas por las crisis. Esto implica generar conciencia sobre las necesidades humanitarias, pedir la protección de los civiles en conflicto y presionar para que las actividades humanitarias tengan un acceso seguro y sin obstáculos. La labor de incidencia suele coincidir con los esfuerzos por conseguir acceso y está igualmente respaldada por el derecho internacional humanitario y de los derechos humanos. Las organizaciones humanitarias también pueden abogar por promover cambios sociales, económicos o políticos específicos destinados a mejorar la vida de las personas marginadas o desfavorecidas.

Las organizaciones pueden llevar a cabo actividades de incidencia a través de diversos medios, tanto en público como entre bastidores.

- **Campañas públicas:** implican hablar abiertamente de los problemas, a menudo a través de campañas en los medios de comunicación y declaraciones públicas. Su objetivo es sensibilizar, movilizar apoyos y presionar a los responsables políticos llamando la atención sobre las injusticias o las necesidades humanitarias.
- **Campañas privadas:** pueden implicar negociaciones entre bastidores, apelaciones directas y conversaciones confidenciales con funcionarios gubernamentales, grupos armados y otras personas con poder o influencia. El objetivo puede ser garantizar el acceso seguro de los trabajadores humanitarios, influir discretamente en las políticas o resolver problemas concretos sin atraer la atención pública.

Suele ser necesario que las organizaciones equilibren estos enfoques, eligiendo el método más apropiado en función del contexto, los posibles riesgos y los resultados deseados. Sin embargo, independientemente de la estructura y del enfoque de la organización, la eficacia de la incidencia puede depender de su adecuación a los objetivos estratégicos generales y de la manera en que se apoya en medidas de gestión de riesgos de seguridad para mitigar las posibles repercusiones negativas.²⁵

²⁵ Humanitarian Outcomes (2024) *Aid Worker Security Report 2024: Balancing advocacy and security in humanitarian action* (www.humanitarianoutcomes.org/AWSR_2024).

En algunas organizaciones con mandatos múltiples existe cierta tensión entre las actividades humanitarias tradicionales y la labor de incidencia. Mientras que el trabajo humanitario es susceptible de sufrir amenazas como la criminalidad, el trabajo de incidencia política presenta distintos tipos de riesgos, como el acoso por parte de las autoridades, el encarcelamiento, la expulsión del país, el cierre de las actividades o la incautación de documentos y ordenadores.

En muchos contextos, los Gobiernos están adoptando posturas más extremas, convirtiendo a las ONG con programas políticos en objetivos prioritarios e incluso apuntando a organizaciones cuyo mandato se centra más en la prestación de servicios que en la labor de incidencia. En estos casos puede resultar complicado aplicar medidas de mitigación eficaces, ya que las organizaciones humanitarias se enfrentan contra todo el peso del aparato gubernamental. Establecer contactos dentro del Gobierno y contratar a expertos jurídicos especializados puede ayudar a reducir estos riesgos. Si bien esto afecta a los actores humanitarios tanto nacionales como internacionales, es probable que el personal de las organizaciones nacionales sea más vulnerable.

2.2.2 Incidencia y seguridad

La incidencia política puede tener repercusiones tanto positivas como negativas en la seguridad de los trabajadores humanitarios y en el entorno general de seguridad en el que operan.

Posibles interacciones negativas

- **Aumento de los riesgos.** La incidencia política, especialmente cuando implica desafiar a actores poderosos o políticas gubernamentales, puede provocar reacciones adversas, como acoso, detenciones, expulsiones e incluso ataques violentos contra los trabajadores humanitarios. En países con un espacio cívico cada vez más reducido, como Nicaragua y Myanmar, los esfuerzos de incidencia política han dado lugar a medidas enérgicas por parte del Gobierno, como la expulsión de organizaciones y la persecución de su personal.
- **Acceso comprometido.** Las campañas públicas de incidencia pueden dar lugar a restricciones de acceso a las poblaciones afectadas cuando los Gobiernos o los agentes no estatales las perciben como hostiles o como un menoscabo de su autoridad.
- **Posibilidad de ataques.** Hablar de temas delicados, como las violaciones de los derechos humanos, puede convertir a las organizaciones humanitarias y a su personal en el blanco de acciones violentas; en estos casos, la labor de incidencia conduce a ataques directos contra los trabajadores humanitarios.

Ejemplo: Restricción del espacio cívico

En el 2022, el Gobierno nicaragüense promulgó leyes y resoluciones que han dado lugar a la cancelación de los registros legales de más de 770 ONG y fundaciones, lo que las obligó a cerrar. Estas acciones han repercutido en un amplio abanico de organizaciones, entre ellas las dedicadas a los servicios médicos, la protección de la infancia, los derechos de la mujer y el cambio climático. Desde el 2018, el Gobierno ha revocado los registros de más de 950 organizaciones, por tanto, se ha restringido gravemente el espacio cívico y se ha obstaculizado la capacidad de las ONG para operar y defender a los grupos marginados.

Posibles interacciones positivas

- **La incidencia como herramienta de protección.** Cuando se corresponde con los esfuerzos de gestión de riesgos de seguridad, la incidencia puede ayudar a mejorar la protección de los trabajadores humanitarios fomentando el respeto del derecho internacional humanitario y generando conciencia sobre la necesidad de proteger las operaciones humanitarias. Campañas como #NoSonUnObjetivo han tratado de sensibilizar a la opinión pública para ayudar a reducir la violencia contra los trabajadores humanitarios.
- **Aprovechar la incidencia para la seguridad.** El personal de seguridad puede utilizar las herramientas de incidencia para conseguir la aceptación de las comunidades locales y su apoyo a las operaciones de ayuda, reduciendo así la probabilidad de los ataques.
- **Incidencia en favor de la justicia.** La incidencia para obtener justicia para los trabajadores humanitarios puede incluir esfuerzos para responsabilizar a los autores de ataques, acoso y violaciones contra el personal humanitario. Las organizaciones se benefician del establecimiento de protocolos claros sobre cuándo y cómo llevar a cabo actividades de incidencia relacionadas con la justicia, lo que garantiza que cualquiera de estas actividades se base en un sólido proceso de diagnóstico de riesgos.
- **Incidencia colaborativa.** Formar alianzas con otras organizaciones, expertos jurídicos y organismos internacionales puede amplificar el mensaje al tiempo que se comparten los riesgos conexos.

La incidencia tiene limitaciones importantes. Aunque ha tenido cierto éxito a la hora de lograr cambios políticos, como las Resoluciones del Consejo de Seguridad sobre la protección de los trabajadores humanitarios,²⁶ en la práctica ha sido en gran medida

26 Por ejemplo, la Resolución 2730 (2024) del Consejo de Seguridad de las Naciones Unidas sobre la protección del personal humanitario y del personal de las Naciones Unidas y el personal asociado en los conflictos armados [[https://docs.un.org/es/S/RES/2730\(2024\)](https://docs.un.org/es/S/RES/2730(2024))].

ineficaz cuando se trata de influir en los actores estatales implicados en conflictos armados: véanse, por ejemplo, los conflictos en Gaza y Sudán, donde los actores estatales han seguido obstruyendo y poniendo en peligro las operaciones humanitarias a pesar de los amplios esfuerzos de incidencia.²⁷

2.2.3 Involucrar al personal de seguridad en la incidencia

El personal de seguridad puede desempeñar un papel importante en garantizar que las iniciativas de incidencia mejoren los resultados en materia de seguridad y no comprometan la seguridad de los trabajadores humanitarios.

Apoyo a la incidencia para mejorar la seguridad

- **Uso de los datos de seguridad para la labor de incidencia.** El personal de seguridad puede proporcionar datos valiosos sobre incidentes, amenazas y el contexto local para apoyar las actividades de incidencia. Por ejemplo, los datos sobre incidentes pueden poner de relieve las zonas en las que los trabajadores humanitarios corren más peligro, lo que puede servir para abogar por mejores medidas de protección de los Gobiernos y los grupos armados.
- **Apoyo a las campañas públicas de incidencia.** Los equipos de seguridad pueden ayudar a dar forma a las campañas públicas de incidencia proporcionando información sobre las implicaciones para la seguridad de los distintos mensajes y estrategias. Así se garantiza que las campañas no solo sean eficaces para crear conciencia, sino también para mantener la seguridad del personal.

Garantizar que los esfuerzos de incidencia no socavan la seguridad

- **Directrices internas.** Es conveniente adoptar un enfoque estructurado con directrices claras que integren las consideraciones de seguridad en los esfuerzos de incidencia. Esto podría incluir protocolos para expresarse, determinar cuándo y cómo interactuar con los medios de comunicación y garantizar que se examine cuidadosamente cualquier declaración pública para evitar poner en peligro al personal. Una buena política organizativa podría consistir en evaluar, en primer lugar, el impacto probable sobre el personal y las operaciones, y solicitar la opinión del personal de seguridad y de los miembros del personal más susceptibles de verse afectados, antes de hacer cualquier declaración pública sobre una situación concreta.
- **Enfoque equilibrado.** Mantener un equilibrio entre la incidencia pública y la privada puede ayudar a garantizar que los esfuerzos no expongan inadvertidamente al personal a mayor riesgo ni obstaculicen las actividades humanitarias en curso.
- **Diagnóstico y coordinación de riesgos.** Antes de poner en marcha cualquier iniciativa de incidencia, puede ser beneficioso realizar un diagnóstico de riesgos para evaluar los posibles riesgos para el personal y para las operaciones de este tipo de actividades. Para ello puede ser necesario analizar el entorno político, comprender las posibles reacciones adversas y evaluar la forma en que los mensajes de incidencia

27 Humanitarian Outcomes (2024) *Aid worker security report 2024: balancing advocacy and security in humanitarian action* (www.humanitarianoutcomes.org/AWSR_2024).

pueden ser percibidos por los diferentes actores. Lo ideal es que en el diagnóstico de riesgos se consideren las repercusiones a corto y largo plazo sobre los trabajadores humanitarios nacionales y las organizaciones socias, cuando corresponda.

- **Medidas de mitigación.** El personal de seguridad puede ayudar a diseñar y aplicar medidas de mitigación para proteger al personal durante las campañas de incidencia.
- **Análisis de riesgos-beneficios.** A menudo, las organizaciones se esfuerzan por equilibrar los riesgos inmediatos de la incidencia con los posibles beneficios a largo plazo, debido a la falta de pruebas mensurables y de marcos para evaluar los riesgos. Para abordar esta cuestión, las organizaciones podrían aplicar un marco de análisis de riesgos-beneficios que compare los posibles resultados negativos con los efectos positivos previstos de las actividades de incidencia. Este marco podría consistir en identificar y clasificar los riesgos potenciales, evaluar los beneficios previstos de las actividades y utilizar un sistema de puntuación para sopesarlos entre sí. La planificación de escenarios puede ayudar a explorar los posibles resultados, y pueden elaborarse medidas de mitigación para abordar los riesgos detectados. El monitoreo y la reevaluación continuos permitirían realizar ajustes en función de los cambios en las circunstancias, y la documentación de los resultados puede ayudar a crear un conjunto de pruebas que sirva de base para esfuerzos de incidencia futuros.

Lista de verificación de buenas prácticas

- **Aprovechar las herramientas existentes.** Utilizar y difundir herramientas establecidas de diagnóstico de riesgos de la incidencia política, como la Herramienta de Seguimiento Espacio para la Sociedad Civil de Oxfam.
- **Fomentar la incidencia colectiva.** Animar a los diferentes actores (foros de ONG, OCHA, Gobiernos donantes) a abogar colectivamente, valiéndose de actores no operativos, por un diálogo más enérgico con las autoridades.
- **Integrar la seguridad en la planificación de la incidencia.** Incorporar la gestión de riesgos de seguridad a los esfuerzos de incidencia, garantizando que todas las actividades se basen en diagnósticos de riesgos exhaustivos y se lleven a cabo con medidas de mitigación de riesgos establecidas.
- **Primero las campañas privadas.** Comunicar los mensajes de incidencia de manera privada a los actores objetivo antes de hacerlos públicos.
- **Involucrar al equipo directivo y a los mensajeros externos.** Recurrir al equipo directivo, al personal de fuera del país o a terceras organizaciones para transmitir mensajes delicados de incidencia (la información sobre abusos podría transmitirse discretamente a organizaciones de derechos humanos, por ejemplo).

- **Determinar las vías de escalada.** Establecer vías claras para escalar los mensajes de incidencia, manteniendo informadas a otras organizaciones y a las partes interesadas pertinentes.
- **Plan de contingencia en caso de retroceso.** Prepararse para posibles reacciones, incluido el acoso o la violencia, teniendo a mano contactos y apoyo jurídico ya determinados.
- **Monitoreo del impacto de la incidencia.** Poner en marcha mecanismos para controlar los efectos positivos y negativos de los esfuerzos de incidencia, incluidas las repercusiones sobre la seguridad de los trabajadores humanitarios.
- **Monitoreo y uso de los datos sobre incidentes.** Hacer un monitoreo de los incidentes de violencia o acoso y utilizar estos datos para abogar por la protección de los trabajadores humanitarios.
- **Evaluar las estrategias de incidencia para la protección de los trabajadores humanitarios.** Diseñar herramientas para evaluar sistemáticamente los pros y los contras de los distintos enfoques de incidencia política a la hora de abordar la violencia contra los trabajadores humanitarios.

Fuente: Humanitarian Outcomes (2024) *Aid Worker Security Report 2024: balancing advocacy and security in humanitarian action* (www.humanitarianoutcomes.org/AWSR_2024).

2.2.4 Consecuencias en la seguridad de las relaciones con los medios de comunicación

Relación con los medios de comunicación

Las organizaciones humanitarias se dirigen a los medios de comunicación por diversas razones, entre ellas, la incidencia, que puede tener implicaciones para la seguridad. Una declaración mal redactada, inexacta o provocativa puede poner al personal en peligro directo e incluso provocar su expulsión de un país. A veces, un departamento de medios de comunicación en la oficina central y el personal ubicado en los lugares donde se ejecutan los proyectos pueden tener objetivos contrapuestos. Lo que eleva el perfil de una organización a nivel internacional puede no ayudar a generar confianza con las comunidades y las autoridades locales. Se puede establecer un sistema claro para evitar incidentes negativos.

- **Contacto con los medios de comunicación.** Definir claramente quién es la persona responsable de contactar con los medios de comunicación, redactar comunicados de prensa y hacer declaraciones públicas (también en las redes sociales).
- **Aprobación de las declaraciones públicas.** Por razones de seguridad, es aconsejable que el jefe de la organización en el país tenga la autoridad final sobre los mensajes a los medios de comunicación, y que se implique al personal de seguridad, regional y de la oficina central, según proceda.
- **Portavoces autorizados.** Determinar y capacitar a personal autorizado para realizar entrevistas y cerciorarse de que esté bien preparado. Puede limitarse al equipo directivo en el país o a personas con cualificaciones similares.
- **Planificación estratégica de medios de comunicación en caso de crisis.** Puede diseñarse y acordarse un enfoque antes de que se produzcan las crisis, con declaraciones preparadas para diversos escenarios. La interacción debe ser oportuna y pertinente, centrándose en los acontecimientos actuales para maximizar el impacto y evitar retrasos.

► *Para obtener más información sobre las comunicaciones durante crisis o incidentes críticos, véase el capítulo 6.1.*

Definir objetivos y dar forma al mensaje

Cualquiera que sea el objetivo del trabajo con los medios de comunicación —por ejemplo, impulsar los objetivos de incidencia o la visibilidad pública para la recaudación de fondos—, las organizaciones querrán sopesarlo cuidadosamente respecto a las cuestiones de seguridad. Por ejemplo, un comunicado de prensa en el que se culpe a un determinado grupo armado de la violencia contra la población civil podría enfurecer a ese grupo y poner en peligro al personal. Puede ser útil preparar una lista de posibles preguntas y respuestas antes de una entrevista, con vistas a mantener los mensajes focalizados, teniendo en cuenta cómo podrían recibirse las respuestas a la luz del contexto y el entorno de seguridad.

Establecer normas básicas

Las entrevistas con los medios de comunicación exigen práctica y experiencia. Es fácil dejarse llevar por una pregunta provocadora y decir algo imprevisto.

- **Hay que tener cuidado al atribuir la culpa de una crisis.** En muchas emergencias políticas complejas, puede que no sea posible decir inequívocamente quién es el responsable. Es importante acordar de antemano una respuesta institucional para los medios de comunicación. El personal debe tener cuidado al transmitir información y asegurarse de que ha sido verificada por una fuente fiable; en caso contrario, debe decirlo claramente. Difundir rumores inexactos podría exacerbar las tensiones.

- **Hay que asegurarse de que existe un entendimiento mutuo sobre los comentarios extraoficiales.** El personal debe ser claro con los periodistas cuando haga comentarios extraoficiales y comprobar cómo se atribuirán las fuentes a los distintos elementos de su entrevista. Algunas formas habituales de ocultar ligeramente las fuentes en los informes de los medios de comunicación, como, por ejemplo, con las frases “una fuente de alto nivel de la ONU” u “organismos humanitarios que operan en la zona de conflicto”, pueden no ser muy eficaces. Es posible que solo haya unas pocas organizaciones humanitarias y que resulte obvio quién es la fuente.

Por último, como ya se ha mencionado, no todas las cuestiones requieren la atención mediática, y puede ser conveniente debatir previamente las posibles preocupaciones con los actores destinatarios para ver si los problemas pueden resolverse por otros medios.

Más información

Investigación y análisis

Humanitarian Outcomes. (2024). *Aid worker security report 2024: balancing advocacy and security in humanitarian action* (www.humanitarianoutcomes.org/AWSR_2024).

Legal Action Worldwide. (2024). *Justice and accountability for attacks on aid workers: What are the barriers and how to overcome them?* (<https://legalactionworldwide.org/accountability-rule-of-law/report-justice-and-accountability-for-attacks-on-aid-workers-what-are-the-barriers-and-how-to-overcome-them/>).

Magone, C., Neuman, M. y Weissman, F. (2012). *Humanitarian negotiations revealed: the MSF experience*. Centre de Réflexion sur l'Action et les Savoirs Humanitaires (<https://msf-crash.org/en/war-and-humanitarianism/humanitarian-negotiations-revealed-msf-experience>).

Rubenstein, L. y Fairbanks, A. (2018). Evidence based advocacy: how incident information can help. Global Interagency Security Forum (www.gisf.ngo/evidence-based-advocacy-how-incident-information-can-help/).

Slim, H. (2022). *Humanitarian resistance: its ethical and operational importance*, Network Paper 87, Humanitarian Practice Network (<https://odihpn.org/publication/humanitarian-resistance-its-ethical-and-operational-importance/>).

Orientación

CARE International. (2014). *The CARE International advocacy handbook* (www.care-international.org/resources/care-international-global-advocacy-handbook).

Consejo Internacional de Organizaciones Voluntarias. (2017). *Manual de Incidencia de Foros de ONG: Realizando Incidencia Conjunta* (www.icvanetwork.org/resource/ngo-fora-advocay-guide-delivering-joint-advocay/).

Davidson, S. (2013). *Managing the message: communication and media management in a security crisis*. Foro Europeo Interinstitucional para la Seguridad (<https://gisfprod.wpengine.com/resource/managing-the-message/>).

Global Interagency Security Forum. (2021). *Partenariados y gestión de riesgos de seguridad: Guía de acción conjunta para organizaciones de ayuda locales e internacionales* (<https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/>).

Tactical Tech. (s.f.). *Holistic security manual* (<https://holistic-security.tacticaltech.org/>).

Herramientas

Grupo de Trabajo sobre Protección de la Acción Humanitaria. (2018). *Toolkit: responding to violence against humanitarian action on the policy level* (<https://alnap.org/help-library/resources/toolkit-responding-to-violence-against-humanitarian-action-on-the-policy-level/>).

Oxfam. (2019). *Herramienta de Seguimiento Espacio para la Sociedad Civil* (<https://policy-practice.oxfam.org/resources/civic-space-monitoring-tool-understanding-what-is-happening-in-civic-space-at-a-620874/>).

3 Elementos organizativos: estructuras e instrumentos para políticas

3.1 El sistema de gestión de riesgos de seguridad humanitaria

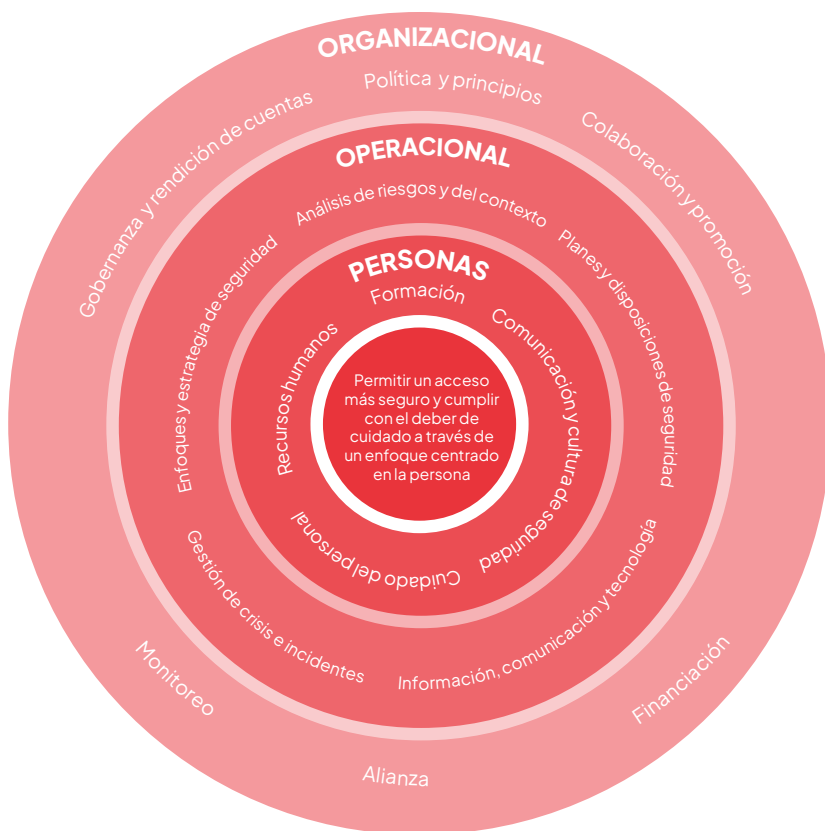
En este capítulo se describen algunos de los elementos clave del sistema de gestión de riesgos de seguridad de una organización: los instrumentos políticos, las estructuras y las funciones y responsabilidades organizativos implicados en la reducción de los riesgos para el personal y en el cumplimiento del deber de cuidado.

3.1.1 Marco de gestión de riesgos de seguridad

La gestión de riesgos de seguridad implica muchos procesos y se solapa con distintas áreas de trabajo y funciones. Para ayudar a orientar la planificación y la aplicación de la gestión de riesgos de seguridad, puede resultar útil visualizar un marco que refleje la arquitectura, las estructuras, los procesos y las disposiciones de la gestión de riesgos de seguridad de toda una organización, todo ello construido a partir del objetivo fundamental de lograr un acceso más seguro y cumplir con el deber de cuidado mediante un enfoque centrado en la persona (véase la figura 4).

Los distintos elementos de este marco se analizan más a fondo en varios capítulos de este documento.

Figura 4 Ejemplo de un marco de gestión de riesgos de seguridad



3.1.2 Política de seguridad

Descripción general

Una política de seguridad es un documento de gobernanza esencial que suele ser aprobado por la junta directiva de la organización o por un órgano de autoridad similar. La política refleja la cultura y los valores de la organización y describe la forma en que se mantendrá el deber de cuidado mientras se trabaja para alcanzar los objetivos estratégicos. Una política de seguridad bien definida no solo aborda los riesgos operacionales, sino que también fomenta una cultura de vigilancia y

responsabilidad. Esta política debe elaborarse en consonancia con los objetivos y las modalidades operativas de la organización. En el contexto del marco de gobernanza de una organización, la política de seguridad sirve como documento fundacional que respalda su dirección estratégica general y su integridad operacional. Lo ideal es que esta política no se elabore de forma aislada, sino que se conecte con otros documentos de gobernanza para garantizar un enfoque cohesivo en toda la organización.²⁸

Elementos de una política de seguridad

Los documentos de la política de seguridad pueden abarcar los elementos que se mencionan a continuación.

- **Declaración del enfoque.** En ella se describe el enfoque general de la organización en materia de seguridad, incluida su estructura de gobernanza. También se puede indicar si la organización aplica un enfoque centrado en la persona (*véase el capítulo 1.2*). Asimismo, se puede especificar el alcance de la política y a quién se aplica, incluido el personal, los voluntarios, los consultores, los trabajadores eventuales y los socios de la organización. Esto ayuda a todos los miembros de la organización a comprender su papel y las expectativas de seguridad que se depositan en ellos.
- **Funciones y responsabilidades.** Las funciones y las responsabilidades específicas relacionadas con la gestión de riesgos de seguridad en la organización. Definen la jerarquía y los mecanismos de rendición de cuentas, lo que garantiza que todos, desde el equipo directivo hasta el personal operativo, comprendan su función en el mantenimiento de la seguridad.
- **Requisitos mínimos de seguridad.** Los requisitos mínimos de seguridad que la organización espera que el personal mantenga en cada lugar donde se ejecutan operaciones. Pueden ser útiles para estandarizar las prácticas de seguridad y garantizar un enfoque coherente en toda la organización. (Para obtener más información, véase más abajo).
- **Integración con otras políticas.** La política de seguridad debe estar vinculada a otros documentos de política organizacional pertinentes, como los relativos a la coordinación civil-militar, la explotación, el abuso y el acoso sexuales y el deber de cuidado. Esta integración ayuda a garantizar la cohesión y puede reforzar el compromiso de la organización con la gestión integral de riesgos y la conducta ética. Al armonizar estas políticas, la organización garantiza que las consideraciones de seguridad se integren en todas las áreas de funcionamiento y gobernanza.
- **Principios y cultura.** La política debe indicar el umbral de riesgo de la organización, la cultura de seguridad y otros principios rectores que conforman su enfoque de la gestión de riesgos de seguridad. También puede poner de relieve el compromiso de

28 Mientras que una política de seguridad proporciona directrices prácticas para aplicar medidas de protección, una estrategia de gestión de riesgos de seguridad esboza los objetivos a largo plazo de la organización y el enfoque para gestionar los riesgos de seguridad. Para obtener más información sobre cómo diseñar y aplicar una estrategia de gestión de riesgos de seguridad, véase GISF (2024) *Estrategia de gestión de riesgos de seguridad (GRS) y desarrollo de políticas: Una guía interfuncional* (<https://gisf.ngo/resource/srm-strategy-and-policy-guide/>).

la organización de mantener un enfoque de seguridad que se ajuste a los principios, los valores y las normas éticas pertinentes (véanse ejemplos en la tabla 1). Especificar claramente el umbral de riesgo de la organización le permite al personal tomar decisiones acordes con la actitud ante el riesgo de la organización.²⁹

Tabla 1 Principios, valores y normas éticas en materia de seguridad

Término	Definición
Principios humanitarios	Observancia de los principios humanitarios básicos de humanidad, neutralidad, imparcialidad e independencia, que guían la acción humanitaria haciendo hincapié en la necesidad de abordar el sufrimiento humano, permanecer neutral en los conflictos, proporcionar ayuda basada únicamente en las necesidades sin discriminación y mantener la autonomía respecto a objetivos políticos u otros objetivos no humanitarios.
No hacer daño	Las organizaciones deben evitar exacerbar los conflictos existentes o crear nuevas formas de daño con su presencia y su trabajo.
Responsabilidad compartida en materia de seguridad	La seguridad es una responsabilidad compartida entre la organización y su personal en todos los niveles.
Primacía de la vida	El principio de darle la máxima prioridad e importancia a la vida y al bienestar humanos. Esto está estrechamente relacionado con el concepto de criticidad del programa.
Criticidad del programa (o riesgo proporcional)	Las actividades del programa justifican el nivel de riesgo que se pide que el personal asuma. Cuanto más crítico o vital sea el programa, más riesgos estará dispuesta a aceptar una organización a fin de mantener dicho programa.
Deber de informar	Las medidas de protección reducen, pero no eliminan, todos los riesgos. Se debe informar al personal del nivel de riesgo que subsiste tras la aplicación de las medidas de mitigación y se le debe dar la oportunidad de analizar este riesgo residual y tomar una decisión informada en función de sus umbrales de riesgo personales.
Derecho a retirarse	El personal tiene derecho a retirarse de un lugar o actividad por motivos de seguridad.
Ningún derecho a permanecer	El personal no tiene derecho a permanecer en un lugar si la dirección de la organización ha decidido suspender las actividades debido a la inseguridad.

29 Véase en GISF (2024) un ejemplo de declaración de apetito de riesgo.

Uso de armas/ activos armados	Una organización debe tener un principio organizativo claro sobre cuándo y cómo el personal puede utilizar armas y otros recursos armados (como escoltas) como parte de su trabajo.
Seguridad equitativa	Las medidas de protección se aplican equitativamente a todo el personal en función de sus necesidades individuales. Equitativo no siempre significa igual, sino que se tienen en cuenta las circunstancias individuales para ajustar las medidas de protección de acuerdo con las necesidades. Se trata de una piedra angular del enfoque de la seguridad centrado en la persona.
Enfoque centrado en la persona	Un enfoque que sitúa a las personas en el centro de las actividades de gestión de riesgos de seguridad. Esto implica, en particular, reconocer los riesgos específicos del perfil a los que se enfrentan las personas debido a su identidad interseccional, su función y organización, y el contexto en el que trabajan.
Alianzas equitativas	Un enfoque cuyo propósito es establecer vías de colaboración para abordar conjuntamente los problemas de seguridad a los que se enfrentan todas las organizaciones socias, y compartir así el riesgo entre los socios.

Adaptado de Bickley, S. (2017) *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*, EISF (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Es necesario evaluar periódicamente el marco de gobernanza de la organización para mantener su eficacia. Una mejora continua, por ejemplo, a través de la retroalimentación, el monitoreo, las revisiones posteriores a la acción y las lecciones aprendidas, puede ayudar a perfeccionar las políticas de seguridad a lo largo del tiempo.

Requisitos de seguridad

Los requisitos mínimos de seguridad son protocolos que la organización espera que todo el personal aplique para garantizar la seguridad de los activos, el personal y la información. Estos requisitos pueden constituir la base de un sistema de seguridad sólido, adaptado para hacer frente a las amenazas y vulnerabilidades específicas inherentes a cada localidad, miembro del personal (teniendo en cuenta los perfiles de riesgo personales) y flujo de trabajo. Un ejemplo de un requisito mínimo de seguridad podría ser un plan de seguridad para cada oficina o lugar de implementación del programa.

A veces, los requisitos de seguridad se estructuran en niveles, en función de los niveles de seguridad o las clasificaciones de riesgo asignadas a las distintas localidades (por ejemplo, alto, medio y bajo). Las medidas de protección pueden adaptarse según los factores de riesgo y la vulnerabilidad específicos de cada lugar, lo que garantiza una

asignación adecuada de los recursos y la atención necesaria para la gestión de riesgos de seguridad.

Lo que constituye un riesgo alto, medio y bajo variará según la organización e idealmente debería determinarse mediante una evaluación exhaustiva, en la que se considere la composición del personal y las vulnerabilidades individuales y organizativas frente a amenazas específicas.

- **Lugares de alto riesgo.** Estas zonas suelen requerir las medidas de protección más estrictas, que pueden incluir sistemas avanzados de vigilancia, mecanismos de control del acceso exhaustivos y protección armada.
- **Lugares de riesgo medio.** Estos lugares suelen requerir medidas rigurosas pero menos intensivas, como barreras físicas reforzadas, auditorías de seguridad periódicas y planes detallados de respuesta a incidentes.
- **Lugares de riesgo bajo.** Estos lugares suelen requerir protocolos de seguridad básicos, centrados en la sensibilización general y en las medidas preventivas.

Para muchas organizaciones internacionales es habitual que el personal que viaja a un lugar de alto riesgo reciba algún tipo de formación sobre sensibilización para entornos hostiles (HEAT, por sus siglas en inglés).

► Para obtener más información sobre los cursos de HEAT, véase el capítulo 5.2.

Los requisitos básicos específicos también pueden aplicarse a otros factores, incluso a puestos de personal y a proyectos concretos. Los perfiles de riesgo personales también influyen a la hora de determinar si un lugar es o no de alto riesgo, y es aconsejable que las organizaciones lo tengan en cuenta al momento de decidir los requisitos de seguridad.

Monitoreo del cumplimiento y la eficacia

Los requisitos de seguridad pueden desempeñar un papel importante en el monitoreo del cumplimiento y la eficacia mediante las siguientes acciones:

- Establecer una base de referencia para las prácticas de seguridad en todas las localidades, que garantice la coherencia y la comparabilidad.
- Proporcionar criterios claros para las auditorías de seguridad internas y externas, y ayudar a identificar deficiencias y áreas de mejora.
- Facilitar la revisión y la actualización periódicas de las medidas de protección en función de los resultados de las auditorías y la evolución de las amenazas.
- Garantizar el cumplimiento de la legislación, la normativa y las buenas prácticas del sector.
- Asignar las responsabilidades relativas a las medidas de protección, y fomentar una cultura de rendición de cuentas y vigilancia.

- *Para obtener más información sobre el monitoreo del cumplimiento y las auditorías de seguridad, véase el capítulo 3.4.*

Buenas prácticas de aplicación

La aplicación de los componentes prácticos de una política de seguridad puede suponer todo un reto. Uno de los principales problemas es la asignación de recursos, que implica garantizar financiación y personal suficientes para lograr una aplicación eficaz. Otro reto es la adaptabilidad; las medidas de protección deben modificarse continuamente para hacer frente a los riesgos y las necesidades operacionales de los distintos lugares y del personal. El cumplimiento y la aplicación también plantean un reto. Mantenerse informado acerca de la evolución de las tecnologías de seguridad e integrarlas en los sistemas existentes exige un esfuerzo y una inversión continuos. Las diferencias culturales y regionales también deben tratarse con cuidado. Es esencial respetar las leyes, las costumbres y las prácticas empresariales locales, manteniendo al mismo tiempo unas expectativas de seguridad coherentes en las distintas localidades.

Teniendo en cuenta estos retos, a continuación se mencionan medidas que pueden respaldar la aplicación.

- **Liderazgo y rendición de cuentas.** Garantizar el compromiso del equipo directivo, integrando la seguridad en la estructura general de gobernanza de la organización.
- **Asignación de recursos.** Garantizar los recursos económicos y humanos adecuados para aplicar la política de seguridad.
- **Integración interfuncional.** El objetivo es integrar la seguridad en todas las funciones, como recursos humanos, finanzas, tecnologías de la información y programas.
- **Adaptación contextual.** Garantizar que la política tenga suficiente flexibilidad en su aplicación para permitir la adaptación a contextos locales u otras circunstancias, teniendo en cuenta, por ejemplo, factores identitarios, culturales, lingüísticos, tecnológicos y medioambientales.
- **Monitoreo continuo.** Controlar, revisar y adaptar periódicamente el enfoque de la organización a través de la retroalimentación y la denuncia de incidentes.
- **Difusión.** Garantizar que la política se comparta con todo el personal mediante un formato accesible y pertinente.

3.1.3 Gobernanza y rendición de cuentas

Como empleadores y entidades jurídicas, las organizaciones tienen una responsabilidad formal hacia todo su personal, en consonancia con su deber de cuidado. El deber de cuidado de una organización hacia su personal debería definirse idealmente en su política de seguridad, así como en documentos como los contratos de trabajo. Aunque la seguridad es una responsabilidad compartida entre la organización y su personal, las organizaciones son responsables de establecer estructuras de gobernanza eficaces y

de garantizar que el personal conozca y comprenda sus funciones y responsabilidades dentro de esta estructura.

► Véase el capítulo 1.1 para consultar un análisis más detallado del deber de cuidado.

Funciones y responsabilidades

Situar adecuadamente la gestión de riesgos de seguridad en la estructura de gobernanza de la organización significa tener claro quién es responsable de qué. Puede ser beneficioso adoptar una matriz RACI de asignación de responsabilidades.³⁰

► Para obtener más información sobre la matriz RACI, véase el capítulo 5.1.

Dirección ejecutiva

La responsabilidad última de la seguridad suele recaer en el director ejecutivo de la organización (o equivalente) o, en algunos casos, en la junta directiva. En la mayoría de las organizaciones, los directores ejecutivos determinan el nivel de tolerancia al riesgo, se aseguran del cumplimiento de las obligaciones legales (como el deber de cuidado) y asignan recursos para aplicar las medidas de protección. Esta responsabilidad abarca a menudo la supervisión de las políticas, la gestión de crisis y la integración de la seguridad en la planificación de la continuidad de las operaciones. La junta directiva también puede desempeñar un papel clave en la supervisión estratégica y en la gobernanza de riesgos. Esto garantiza que la seguridad no sea solo una preocupación técnica u operacional, sino un aspecto fundamental de la gobernanza y la resiliencia de la organización.

La gestión operacional de la seguridad está vinculada a las prácticas de gestión y de toma de decisiones de toda la organización, y la mayoría de las organizaciones descentralizan las decisiones de seguridad al nivel de autoridad pertinente más cercano. Las decisiones sobre la conveniencia de iniciar operaciones en una nueva localidad y sobre el tipo de programa que emprender, suelen ser responsabilidad del equipo directivo. La organización también puede exigir que el personal directivo contribuya o brinde asesoramiento a la hora de tomar decisiones importantes en materia de seguridad (por ejemplo, si se debe trasladar o evacuar al personal). Los asuntos relativos a los medios de comunicación, la comunicación y la recaudación de fondos, así como las cuestiones relativas a los recursos humanos, como el establecimiento de pólizas de seguros, suelen decidirse y gestionarse en la oficina central. Algunas decisiones específicas también pueden requerir la aprobación formal del equipo directivo, entre ellas, las siguientes:

- subir o bajar la clasificación del riesgo de un lugar;
- volver a entrar en una zona de la que el personal ha sido reubicado o evacuado debido a riesgos de seguridad;

30 Para consultar un ejemplo detallado de una matriz RACI en relación con las responsabilidades de seguridad, véase GISF (2024).

- adoptar un enfoque de “baja visibilidad” y retirar logotipos y banderas de las oficinas y los vehículos;³¹
- utilizar protección armada; y
- recurrir a servicios de seguridad privada.

Personal de seguridad

Muchas organizaciones contratan a personal de seguridad para que aporte sus conocimientos especializados y asesore a los directivos (que suelen ser los responsables finales de las decisiones sobre seguridad). Estos referentes de seguridad suelen encargarse de emprender acciones relativas a la seguridad, como elaborar planes de seguridad y compartir conocimientos y experiencia con colegas ajenos al ámbito de la seguridad. La mayoría de las organizaciones disponen de referentes de seguridad con dedicación exclusiva o con múltiples funciones en distintos niveles, desde funcionarios de la sede hasta de proyectos locales, siendo los lugares de mayor riesgo los que suelen recibir la mayor inversión en personal. En algunas organizaciones, la seguridad se gestiona a través de equipos, comités o grupos de trabajo, en los que las tareas y las decisiones de gestión de riesgos de seguridad se comparten entre una serie de miembros clave del personal. En otras organizaciones, la gestión de riesgos de seguridad está integrada en la línea jerárquica, y no existe una función de seguridad separada (véase más abajo un análisis más detallado de estos tipos de estructuras de gobernanza).

► Consulte el capítulo 5.1 para obtener más información sobre los puestos de seguridad.

Liderazgo a nivel de país (para organizaciones internacionales)

En el país generalmente es responsabilidad del representante superior (es decir, el director en el país o el jefe de misión) garantizar la aplicación y el cumplimiento de las políticas y los procedimientos de la organización, y la mayoría de las tareas relativas a la gestión de riesgos de seguridad suelen delegarse a un referente de seguridad.

Gerentes

Los gerentes de todos los niveles de una organización tienen una responsabilidad respecto al personal, que incluye garantizar su seguridad. Lo que esto significa en la práctica variará de una organización a otra, pero puede incluir garantizar que el personal asista a sesiones informativas y de formación sobre seguridad, prestar apoyo a los referentes de seguridad y contribuir a los diagnósticos de riesgos y la planificación de la seguridad.

31 Los donantes gubernamentales pueden imponer obligaciones contractuales relativas a la visibilidad (“marca”) de la ayuda que financian, en tal caso es posible que la organización deba solicitar su aprobación formal para renunciar a este requisito.

Personal

Todo el personal, desde los directores de programa hasta los becarios, es responsable de su propia seguridad y de la seguridad del equipo en su conjunto, así como de la organización. Lo ideal sería que todo el personal participe en debates y actividades periódicas relacionadas con la seguridad, incluida la formación.

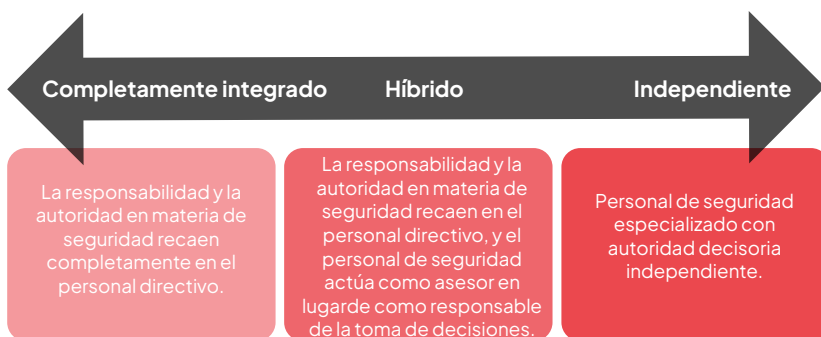
Tipos de estructuras de gobernanza de la seguridad

Las estructuras de gobernanza de la seguridad pueden variar en función del enfoque general de la organización. Esto puede concebirse como un continuo con una gestión de riesgos de seguridad totalmente integrada por un lado y una estructura de seguridad independiente y con abundantes recursos por el otro (véase la figura 5).

- **Totalmente integrada.** La responsabilidad y la autoridad en materia de seguridad recaen plenamente en el personal directivo. No suele haber personal de seguridad designado específicamente.
- **Híbrida.** La responsabilidad y la autoridad en materia de seguridad recaen en el personal directivo, pero las tareas de seguridad, como la realización de diagnósticos de riesgos y la creación de planes, recaen en el personal de seguridad designado. El personal de seguridad de estas organizaciones suele actuar como asesor, pero no toma decisiones.
- **Independiente.** Las organizaciones que adoptan esta estructura cuentan con personal de seguridad designado específicamente en múltiples niveles y disponen de autoridad para tomar decisiones de gestión de riesgos de seguridad independientemente de otras funciones directivas. Esta estructura es más común en entornos corporativos y a veces se describe como un modelo de “seguridad corporativa”.

La mayoría de las organizaciones suelen situarse en algún punto de este continuo en función de su enfoque de gestión de riesgos de seguridad, sus recursos y sus preferencias. Por ejemplo, una organización puede emplear a un gran número de profesionales de seguridad, pero mantener toda la autoridad decisoria relativa a la seguridad en la dirección. Algunas organizaciones también pueden utilizar estructuras diferentes en distintos lugares, como puestos de asesoramiento de seguridad más específicos en contextos de riesgo alto y un enfoque más integrado en entornos de riesgo bajo. Lo importante es la coherencia y una comunicación clara sobre quién tiene la responsabilidad final de las decisiones de seguridad en los distintos niveles de la organización.

Figura 5 Tipos de estructuras de gobernanza de la seguridad



Todas estas estructuras tienen sus puntos fuertes y débiles.

En el enfoque integrado, los directivos son totalmente responsables de la seguridad del personal, lo que puede contribuir a que la seguridad se considere parte del proceso de toma de decisiones operacionales, y, por tanto, es más probable que la seguridad se ajuste a los objetivos del programa. Sin embargo, los directivos a los que se encomiendan responsabilidades de seguridad pueden carecer de experiencia en este ámbito, así como del tiempo necesario para llevar a cabo adecuadamente las tareas de seguridad además de sus otras responsabilidades. La dependencia de servicios de seguridad contratados externamente puede ser mayor en estas circunstancias (aunque no necesariamente).

Esta estructura híbrida permite a las organizaciones beneficiarse de conocimientos especializados en materia de seguridad y mantener al mismo tiempo la toma de decisiones en la dirección. Esto ofrece un enfoque equilibrado, con asesoramiento sobre seguridad integrado en el proceso de planificación, sin socavar los objetivos del programa. La flexibilidad de esta estructura la hace adaptable a diferentes necesidades organizativas. Sin embargo, la función de asesoramiento del personal de seguridad puede limitar su capacidad para hacer cumplir las medidas de protección. Esta dependencia del personal directivo para la toma de decisiones finales puede dar lugar a retrasos en las acciones o a una aplicación incoherente de las medidas de protección, especialmente si los gerentes de programa no dan prioridad a los problemas de seguridad.

La estructura independiente de las funciones de seguridad es la que mayor cantidad de recursos y autoridad otorga al personal de seguridad. El personal de seguridad puede adoptar medidas directas, lo que puede mejorar la mitigación de riesgos, la formación del personal y el cumplimiento. Sin embargo, esta estructura puede provocar el

aislamiento de la seguridad de otras funciones. La seguridad puede percibirse como un obstáculo para las actividades del programa, especialmente si las decisiones tomadas por el personal de seguridad entran en conflicto con los objetivos del programa. Esto puede obstaculizar la flexibilidad y la capacidad de respuesta necesarias en determinados contextos operacionales y socavar la aceptación de las medidas de protección por parte del personal.

En resumen, las estructuras totalmente integradas pueden ofrecer una mejor armonización con los programas, pero pueden carecer de conocimientos especializados; los enfoques híbridos pueden ofrecer un equilibrio, pero pueden tener problemas de coherencia y aplicación; y las estructuras independientes pueden ofrecer una seguridad sólida, pero pueden considerarse restrictivas. Mucho puede depender de cómo se relacione el personal de seguridad con sus colegas. Por ejemplo, en una estructura independiente, aunque el personal de seguridad tenga autoridad para hacer cumplir medidas estrictas, puede optar por reservarla para casos extremos y preferir la colaboración con otros equipos para llegar a decisiones equilibradas. En última instancia, aunque los modelos de gobernanza pueden dar forma al enfoque general de la organización en materia de seguridad, las actitudes y los enfoques de las personas también pueden desempeñar un papel importante en la manera en que se gestiona y percibe la seguridad.

- *Este tema se trata con más detalle en la quinta parte, “Las personas en la gestión de riesgos de seguridad”.*

Proveedores de servicios externos

Algunas organizaciones contratan a asesores de seguridad externos, ya sea como proveedores exclusivos de conocimientos especializados y recursos de seguridad o para apoyar funciones internas que carecen de la capacidad, las competencias o el tiempo necesarios. Aunque los proveedores externos ofrecen una amplia experiencia, perspectivas imparciales y conocimientos sobre buenas prácticas, pueden carecer de un compromiso o de un entendimiento profundo de la cultura y las relaciones internas de la organización. Depender excesivamente de ellos puede debilitar la capacidad interna y los conocimientos institucionales.

- *Para obtener más información sobre los servicios de seguridad privada, véase el capítulo 2.1.*

Integrar la seguridad con otras funciones organizativas

En una organización, la gestión de riesgos de seguridad se interrelaciona con muchas áreas de trabajo. La función de gestión de riesgos de seguridad en una organización puede estar situada bajo un paraguas general de “gestión de riesgos”, en operaciones o en otra área funcional, según la estructura de la organización. Independientemente del lugar que ocupe la seguridad, la colaboración en toda la organización y otras medidas pertinentes de gestión de riesgos es clave y a menudo, el mayor reto.

El personal de seguridad puede mejorar la colaboración si comprende el ecosistema interno de la organización y el papel de la función de seguridad en él. Esto implica comprender la dinámica organizativa interna y los entornos externos, y anticiparse y responder a las tendencias de riesgos, aprovechar las oportunidades para desarrollar y mejorar las formas de trabajar y fomentar relaciones que beneficien a la organización en su conjunto. Este enfoque holístico fomenta la resiliencia y la adaptabilidad organizativa.

El personal de gestión de riesgos de seguridad puede beneficiarse de lo siguiente:

- **Promoción de una visión integral de la dinámica interna de la organización, las influencias externas y las interacciones interfuncionales.** Este enfoque ayuda a los profesionales y a los líderes de seguridad a detectar los riesgos de seguridad en todos los departamentos, procesos y sistemas, en lugar de tratarlos de forma aislada. Además, esto se corresponde con los principios de gestión de los riesgos institucionales (véase más abajo).
- **Colaboración interdisciplinaria activa.** La complejidad de una organización requiere a menudo la colaboración con otros departamentos y ámbitos de especialización. La integración de la gestión de riesgos de seguridad en las áreas de trabajo existentes supone reunir diversas perspectivas, experiencias y conocimientos para abordar la naturaleza polifacética de los riesgos.
- **Incorporación del pensamiento sistémico.** Esto permite a las organizaciones identificar, comprender y mitigar mejor los riesgos mediante el análisis de las interacciones dinámicas y los circuitos de retroalimentación en toda la organización. El pensamiento sistémico para una gestión de riesgos de seguridad eficaz implica comprender las interdependencias entre las diversas funciones organizativas y los factores externos, fomentar la colaboración interfuncional para realizar diagnósticos de riesgos exhaustivos y diseñar estrategias de gestión adaptables y dinámicas.

Comprender la interrelación de la seguridad con otras funciones organizativas

Preguntas para el personal de seguridad:

- ¿Cómo se integra la gestión de riesgos de seguridad en otras funciones de la organización, que a su vez incide en su resiliencia y adaptabilidad generales?
- ¿Permite la estrategia de gestión de riesgos de seguridad de su organización que todos alcancen sus objetivos y metas con eficacia, fomentando una cultura de éxito y colaboración?
- ¿La visión y el propósito del equipo de seguridad son adecuados para reforzar la resiliencia?
- Para apoyar una mayor colaboración, ¿hay personas o equipos clave en otras funciones organizativas a los que se deba dar prioridad en las tareas de comunicación?

Algunas organizaciones internacionales de mayor tamaño han adoptado un enfoque de gestión de los riesgos institucionales, que implica identificar, evaluar y gestionar todos los riesgos de una organización. La seguridad es un tipo de riesgo que las organizaciones gestionan a diario. Otros riesgos son los estratégicos, fiduciarios y financieros, cibernéticos, de seguridad, jurídicos, de información, de reputación y operacionales. Estos tipos de riesgos suelen solaparse y pueden afectar a la seguridad y verse afectados por ella. Las organizaciones que adoptan un enfoque de gestión de los riesgos institucionales pretenden integrar las prácticas de gestión de riesgos en la estrategia general y en los procesos de toma de decisiones para garantizar un enfoque coordinado y sistemático. Al situar los riesgos de seguridad en el marco general de gestión de riesgos de una organización, los responsables de la toma de decisiones pueden equilibrar las consideraciones de seguridad con otros riesgos, como los financieros o reputacionales, lo que garantiza que las medidas de protección no obstaculicen inadvertidamente las operaciones o los objetivos estratégicos de la organización.

Una buena práctica de gestión de los riesgos institucionales es la definición clara de las actitudes y la tolerancia ante el riesgo, así como de los umbrales de riesgo, que ayuda a orientar la toma de decisiones en todos los departamentos. También es aconsejable vincular los esfuerzos de gestión de los riesgos institucionales con la continuidad de las operaciones y la gestión de crisis, garantizando que la gestión de riesgos de seguridad refuerce la resiliencia organizativa en general. La aplicación de un enfoque de este tipo implica la participación del equipo directivo, la colaboración interfuncional

y el monitoreo y la evaluación periódicos para adaptar la estrategia a los riesgos emergentes. La integración interfuncional es sumamente importante. La gestión de riesgos de seguridad no debe aislarse ni considerarse un flujo de trabajo separado, sino que debe conectarse con otros departamentos. Los equipos interfuncionales pueden trabajar en colaboración para gestionar los riesgos y garantizar un flujo de información fluido. La comunicación periódica, los objetivos compartidos y la responsabilidad colectiva de todas las funciones impulsan mejores prácticas de gestión de riesgos. Esta integración permite afrontar diversos riesgos, ya sean riesgos relacionados con el acceso a las comunidades, la protección de datos o la continuidad de las operaciones, y fomentar una cultura de seguridad positiva en toda la organización.³²

Más información

Orientación

Bickley, S. (2017). *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*. Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Global Interagency Security Forum. (2024). *Estrategias de gestión de riesgos de seguridad (GRS) y desarrollo de políticas: Una guía interfuncional* (<https://gisf.ngo/resource/srm-strategy-and-policy-guide/>).

32 Para obtener más recomendaciones prácticas sobre la integración interfuncional, véase GISF (2024).

3.2 Acceso y seguridad

El acceso humanitario, aunque no es un fin en sí mismo, es un requisito previo para la acción humanitaria. La inseguridad suele ser un obstáculo para el acceso humanitario y, del mismo modo, los esfuerzos para mejorar y ampliar el acceso tienen importantes implicaciones para la seguridad.

En esta sección se definen el concepto y los múltiples retos del acceso humanitario respecto a la gestión de los riesgos de seguridad, tanto en los esfuerzos externos de las organizaciones para conseguir, mantener y ampliar el acceso, como en las funciones internas del personal. Un acceso bien establecido y negociado es esencial para mantener la seguridad en entornos altamente disputados, tanto para el personal de las organizaciones humanitarias como para las personas a las que asisten.

3.2.1 Conceptos clave

El acceso humanitario se define como “el acceso de los agentes humanitarios a las personas que necesitan asistencia y protección, así como el acceso de estas personas a los bienes y servicios esenciales para su supervivencia y salud, en conformidad con los principios humanitarios básicos”.³³

El acceso se basa en dos pilares fundamentales: los principios humanitarios y el derecho internacional humanitario, consagrados en los Convenios de Ginebra y sus Protocolos Adicionales.³⁴ El principio de humanidad obliga a los agentes humanitarios a esforzarse por ayudar a todas las personas en crisis, dando prioridad a los más necesitados, mientras que el derecho internacional humanitario estipula que los agentes y las operaciones humanitarias imparciales deben estar protegidos, y que las partes en conflicto deben permitirles un acceso libre de obstáculos.³⁵ Las organizaciones disponen de diversas herramientas para lograr un acceso humanitario basado en estos principios, como la diplomacia de alto nivel, la coordinación civil-militar y las negociaciones de acceso.

Tanto la gestión de riesgos de seguridad como la maximización del acceso son esenciales para la acción humanitaria, pero a menudo se tratan como dos objetivos distintos y mutuamente excluyentes. Muchos profesionales sienten la necesidad de encontrar un “equilibrio” entre la seguridad y el acceso en contextos dinámicos de alto riesgo, en los que una gestión del riesgo excesivamente conservadora puede

33 Oficina de Coordinación de Asuntos Humanitarios de las Naciones Unidas (2012) *OCHA on message: humanitarian principles* (<https://reliefweb.int/report/world/ocha-message-humanitarian-principles-enar>).

34 Comité Internacional de la Cruz Roja (2014) *Los Convenios de Ginebra de 1949 y sus Protocolos adicionales* (www.icrc.org/en/document/geneva-conventions-1949-additional-protocols).

35 Comité Internacional de la Cruz Roja (2015) “Preguntas y respuestas y léxico del CICR sobre acceso humanitario”, *Revista Internacional de la Cruz Roja* 96(893) (<https://international-review.icrc.org/es/articulos/preguntas-y-respuestas-y-lexico-del-cicr-sobre-acceso-humanitario>).

obstaculizar la búsqueda activa del acceso a las personas necesitadas. Sin embargo, en lugar de plantearlo como una disyuntiva, un enfoque más productivo utiliza la criticidad del programa para orientar los objetivos de acceso y emplea la gestión de riesgos de seguridad para limitar el peligro en la consecución de dichos objetivos. Como primer paso, es útil que el personal de seguridad comprenda los obstáculos al acceso, así como la forma en que se llevan a cabo los esfuerzos relativos al acceso en la práctica y cómo la seguridad puede contribuir a estos esfuerzos.

3.2.2 Retos de acceso externo

Los obstáculos al acceso humanitario se presentan de muchas formas, intencionadas y no intencionadas. Las organizaciones humanitarias suelen clasificarlos en tres grandes grupos:

- conflicto e inseguridad;
- impedimentos burocráticos y administrativos, y
- limitaciones medioambientales y logísticas.

Aunque la gestión de riesgos de seguridad se ocupa más directamente de la primera categoría, las tres tienen dimensiones de riesgo, y los esfuerzos para superarlas y ampliar el acceso podrían involucrar provechosamente al personal de gestión de riesgos de seguridad.

Conflicto activo e inseguridad

En los conflictos armados, los obstáculos al acceso relacionados con la inseguridad comprenden los siguientes:

- amenazas y actos de violencia dirigidos contra el personal y los activos humanitarios por las partes en conflicto;
- ataques indirectos (violencia colateral) que afectan al personal y a los activos, y
- daños colaterales al entorno de las operaciones, incluida la infraestructura civil.

En contextos de conflicto activo, la inseguridad para los agentes humanitarios también puede aumentar a causa de la ruptura del orden social, el aumento de la criminalidad y de la actividad económica ilícita y los actos de desesperación de la población.

Los conflictos armados pueden servir de excusa para la injerencia política con el fin de restringir el acceso. En particular, si el Gobierno es parte en el conflicto, puede utilizar las condiciones de violencia e inseguridad como motivo para denegar o restringir el acceso de los grupos de ayuda a determinadas zonas. Se sabe que los Gobiernos y los ejércitos deniegan permisos de viaje a las organizaciones humanitarias, a menos que

viajen con escolta militar (que a menudo deben pagar); estos acuerdos pueden afectar negativamente la percepción pública y, por tanto, crear más riesgos que los que mitigan.

Las partes en conflicto pueden imponer bloqueos en zonas específicas e impedir que las organizaciones humanitarias presten ayuda y entreguen suministros esenciales a los civiles atrapados. Los bloqueos pueden ser una táctica de castigo colectivo o de presión sobre los grupos de la oposición, puesto que provocan escasez de alimentos, medicamentos y otros productos de primera necesidad.

Impedimentos burocráticos y administrativos

Los procesos burocráticos engorrosos, largos y poco claros, como la obtención de permisos para viajes y proyectos, visados o despachos de aduanas, a menudo retrasan la ayuda humanitaria y aumentan los costos operativos. Por ejemplo, en Sudán, tanto el Gobierno como las fuerzas de la oposición han retrasado la respuesta humanitaria al exigir múltiples permisos para los desplazamientos y han impedido la importación de equipos médicos y humanitarios esenciales.

Los Gobiernos también pueden utilizar el acoso legal y la interferencia contra las organizaciones humanitarias, como, entre otros, la vigilancia, las redadas, las detenciones, los arrestos y los recursos legales que implican largos procesos judiciales. En el peor de los casos, se puede denegar el registro a las organizaciones y expulsarlas del país. Las leyes de antiterrorismo pueden restringir la interacción con determinados grupos e imponer sanciones severas; la investigación excesiva por parte de los donantes y las prácticas de reducción del riesgo por parte de los bancos agravan estos desafíos. En Rusia se impide a las ONG reportar públicamente sobre acciones gubernamentales o militares. Deliberadamente o no, las barreras financieras, como los embargos comerciales, la congelación de activos y las tasas burocráticas también pueden obstruir las operaciones humanitarias.

Limitaciones medioambientales y logísticas

Entre los obstáculos logísticos y medioambientales figuran la falta de infraestructura de transporte o las interrupciones y los daños causados por fenómenos relacionados con el clima.

Este tipo de obstáculo al acceso no siempre es totalmente fortuito o involuntario. La falta de prioridad por parte del Gobierno respecto a estas áreas y cuestiones puede ser una forma indirecta de denegación de acceso. El cierre selectivo de carreteras, los toques de queda y la interrupción de servicios (por ejemplo, Internet y telecomunicaciones) pueden limitar la capacidad de la población para acceder a la información y a los servicios y dificultar el alcance de las organizaciones humanitarias en zonas donde se necesita asistencia. Las soluciones alternativas pueden ser costosas (por ejemplo, utilizar medios aéreos cuando las carreteras son intransitables) y potencialmente peligrosas (utilizar vehículos alternativos y rutas peligrosas).

3.2.3 Impedimentos internos al acceso humanitario

No todas las restricciones de acceso son externas. Entre los factores internos figuran los siguientes:

- **Cultura organizativa y apetito de riesgo.** Aunque a nivel de programación existan el deseo y los incentivos para maximizar el acceso, si el apetito de riesgo y la cultura de gestión de riesgos de seguridad no están claras y no se comunican en todos los niveles, las vacilaciones, la inercia y las prioridades contrapuestas pueden limitar la acción. Por esta razón, entre otras, es importante que las organizaciones integren sus estrategias dirigidas a mejorar el acceso en su sistema de gestión de riesgos de seguridad y viceversa.
- **Sistemas y políticas.** Los mandatos y las aspiraciones de la organización no siempre coinciden con los procedimientos y los procesos organizativos internos. Los debates en torno al acceso humanitario suelen limitarse a los equipos de programas y políticas. Sin embargo, las funciones de apoyo, como recursos humanos, finanzas, logística, seguridad y comunicación, desempeñan un papel igualmente importante en el desarrollo de las estrategias de acceso y programáticas. Las organizaciones que han ejecutado programas de forma sostenible han utilizado eficazmente todos los aspectos de su capacidad organizativa.
- **Capacidad organizativa y de personal.** Dado los problemas de recursos humanos que afectan a todo el sector, puede resultar difícil contratar a personas cualificadas en materia de acceso y negociaciones humanitarias. Cada vez son más las organizaciones que recurren a la formación en el puesto de trabajo para subsanar las carencias de competencias.

3.2.4 Consideraciones prácticas y enfoques para el acceso

Las organizaciones pueden gestionar las limitaciones referidas al acceso con adaptaciones programáticas, incidencia e interacción, y coordinación. Las estrategias de acceso suelen incluir una combinación de estas medidas y enfoques diversos para abordar los entornos más difíciles. Por ejemplo, en Irak, durante la respuesta a la crisis de desplazamiento de 2016, las organizaciones emplearon una estrategia de acceso polifacética, que incluyó el aumento de la capacidad de acceso especializada e independiente, la negociación directa con los grupos armados, la adopción de programas de gestión remota y la participación en grupos de trabajo operativos y de coordinación civil-militar.

Los elementos de una estrategia de acceso diversificada pueden ser los siguientes:

- **Incidencia y diplomacia de alto nivel.** Implicar a los Gobiernos donantes, las autoridades nacionales, las organizaciones internacionales y regionales y otros actores influyentes en la protección de los trabajadores humanitarios y en la responsabilidad de garantizar una ayuda humanitaria sin obstáculos. Esto puede

ocurrir a través del coordinador de asuntos humanitarios de la ONU o de consorcios de ONG centrados en la incidencia política, en representación de los organismos de la ONU y/o de organizaciones humanitarias.

- **Grupos de trabajo interinstitucionales sobre acceso.** Colaborar con otras organizaciones humanitarias a través de mecanismos generales para intercambiar información y diseñar estrategias comunes para mejorar el acceso. Esto puede ayudar a evitar la duplicación de esfuerzos al tiempo que diluye los riesgos para cualquier organización individual. Tradicionalmente, los grupos de trabajo sobre acceso suelen estar presididos por la OCHA y copresididos por una ONG. Sus funciones varían según el contexto, pero en principio sus objetivos principales son intercambiar información, ofrecer un espacio de debate seguro, supervisar el acceso y reforzar las capacidades.
- **Acuerdos a distancia o trabajo a través de socios.** Se puede facilitar el acceso mediante la formación de alianzas con organizaciones locales y grupos comunitarios que hayan establecido redes y gocen de la confianza de las comunidades afectadas.
- **Negociaciones humanitarias.** Entablar conversaciones con actores diversos, incluidas las partes en conflicto, para obtener un acceso seguro a las poblaciones afectadas. Esto puede abarcar desde conversaciones informales con los guardias de los puestos de control hasta esfuerzos formales interinstitucionales o diplomáticos, e implica formar al personal en negociación, distensión y mediación de conflictos. Los marcos para las negociaciones humanitarias, como el diseñado por el Centro de Competencia en Negociación Humanitaria,³⁶ pueden proporcionar herramientas y métodos útiles para analizar los entornos de negociación, evaluar las posiciones e intereses de las partes, crear redes, definir objetivos y líneas rojas, y aplicar los acuerdos. El personal de seguridad, presente en gran parte de este análisis, puede estar bien posicionado para dirigir estas negociaciones o proporcionar información y apoyo. Estas negociaciones pueden llevarse a cabo por organizaciones individuales o mediante esfuerzos colectivos (a nivel local, nacional o internacional).
- **Aceptación, participación comunitaria y sensibilización.** Colaborar con las comunidades locales y el sector privado en los procesos de planificación y toma de decisiones para determinar mejor las necesidades locales y los obstáculos al acceso, así como las posibles soluciones. Adoptar enfoques comunitarios de acceso y seguridad que impliquen una interacción periódica e intencionada con una serie de guardianes, incluidos los líderes locales, las personas mayores y las organizaciones comunitarias, puede ayudar a mitigar los riesgos de seguridad y a promover la aceptación de la ayuda humanitaria. Esto puede reforzar y ampliar la red de una organización y funcionar como un sistema de alerta temprana que prevenga a las organizaciones de cambios en el contexto.

36 Centro de Competencia de Negociación Humanitaria (2019) *Manual del CCHN sobre negociación humanitaria*, Frontline Negotiations (<https://frontline-negotiations.org/es/home/resources/field-manual/>).

- **Gestión de la información.** Recopilación y análisis de datos sobre las limitaciones de acceso y los riesgos de seguridad para adaptar las estrategias y tomar decisiones informadas. Para trazar un panorama completo del entorno de acceso y elaborar estrategias adecuadas, las organizaciones pueden incorporar la información de seguridad a un análisis más amplio (como el análisis de la economía política y los conflictos) para comprender las causas profundas de los problemas de acceso.
 - **Facilitar el acceso seguro a todas las funciones de la organización.**
 - Administración. Garantizar el cumplimiento de los marcos jurídicos y normativos para evitar o reducir las cuestiones legales o burocráticas que puedan obstaculizar el acceso.
 - Logística. Elaborar y aplicar planes de contingencia para la prestación de ayuda, incluidos rutas y métodos de transporte alternativos.
 - Gestión de riesgos de seguridad. Comprender el contexto local y las posibles limitaciones de acceso. Formar al personal para que tome decisiones de seguridad informadas y disponer de planes de contingencia para afrontar cambios en las condiciones.
 - **Tecnología.** Utilizar la tecnología para mejorar el acceso, como las imágenes por satélite para analizar el contexto, las aplicaciones móviles para reportar en tiempo real y las plataformas digitales para el monitoreo y la coordinación a distancia.
 - **Participación civil-militar.** La coordinación civil-militar para el acceso humanitario se basa en el derecho internacional humanitario y en las directrices elaboradas por el Comité Permanente entre Organismos (IASC) y el Servicio de Coordinación Civil-Militar de la OCHA.
- *Para obtener más información, véase el capítulo 2.1 sobre redes y colaboración de seguridad.*

3.2.5 Integrar la seguridad con el acceso para alcanzar los objetivos de programación

Las funciones de acceso pueden abarcar múltiples puestos estándar, incluidos los equipos de logística, incidencia, programas y seguridad. Para abordar este reto multidisciplinario, las organizaciones han empleado tres modelos diferentes.

- **Capacidades de acceso independientes.** Pocas organizaciones han invertido en la contratación de personal dedicado exclusivamente a conseguir y mejorar el acceso. Aunque tener un puesto independiente dedicado al acceso puede señalar la importancia del acceso como un aspecto facilitador de los programas, este modelo puede resultar caro, difícil de reproducir y redundante si el equipo directivo no tiene experiencia en aprovechar los puntos fuertes de las funciones de seguridad y acceso. En este modelo es importante que el personal de seguridad y acceso colabore tanto como sea posible; por ejemplo, incluir consideraciones sobre el acceso en la fase de diseño y de iniciación permite detectar riesgos y aplicar adaptaciones programáticas y operacionales, incluida la gestión de riesgos de seguridad.

- **Integrar las funciones de acceso en diversos puestos, incluidos los equipos de seguridad.** Algunas organizaciones han adoptado un enfoque integrado de seguridad y gestión de acceso, combinando ambos puestos. Aunque este modelo requiere menos recursos y podría evitar la confusión entre funciones y responsabilidades, su éxito dependerá probablemente de la capacidad de la organización para elaborar una descripción del puesto que incluya adecuadamente ambas funciones y, posteriormente, para contratar a la persona con el perfil adecuado. Esto puede resultar especialmente difícil si los especialistas en seguridad que se contratan proceden de la policía o las fuerzas armadas.

Ejemplo: Marco para un Acceso más Seguro —un modelo integrado—

El Marco para un Acceso más Seguro, elaborado por el CICR para ayudar a las sociedades nacionales de la Cruz Roja y de la Media Luna Roja a conseguir un acceso seguro a las poblaciones afectadas, tiene ocho categorías de medidas para mejorar la aceptación, la seguridad y el acceso. Entre ellas figuran comprender el contexto y los riesgos locales, situar a la organización dentro de los marcos jurídico y político, conseguir y mantener la aceptación entre las partes interesadas locales, garantizar la visibilidad de la organización, asegurar una comunicación interna y externa eficaz y aplicar un sistema sólido de gestión de riesgos de seguridad operacional.

Este enfoque reconoce los vínculos entre aceptación, seguridad y acceso, y ofrece medidas clave para mejorar los tres aspectos. En la práctica, esto ha supuesto, por ejemplo, garantizar que las tareas relacionadas con la seguridad y la aceptación se incorporen a la formación de los voluntarios, reforzar los equipos de comunicación para monitorear las percepciones públicas y salvaguardar la reputación de la organización en línea, y establecer equipos de coordinación en las oficinas locales que trabajen en los distintos departamentos y programas para aplicar los principios y las prioridades de dicho marco.

Para obtener más información, véase <https://saferaccess.icrc.org>.

- **Modelo híbrido.** Algunas organizaciones han separado la responsabilidad del apoyo técnico al acceso operacional. En la oficina central, los expertos técnicos en acceso trabajan separadamente de los equipos de seguridad y proporcionan orientación y asesoramiento a los equipos de país, lo que incluye formación y la elaboración de estrategias. A nivel regional y nacional, los equipos de seguridad gestionan el acceso operacional cotidiano. Este modelo proporciona capacidad de acceso técnica dentro de la organización, al tiempo que reconoce la dificultad de contratar personal adicional especializado a nivel nacional. Sin embargo, no aborda la cuestión de que los equipos técnicos no tienen una línea técnica con el personal de seguridad a nivel regional o nacional, lo que significa que el control de calidad depende de si se han contratado los perfiles adecuados en todas las funciones de seguridad y de la solidez de la relación entre el equipo de acceso y los directores de cada país.

Más información

Investigación y análisis

ACAPS. (Julio de 2025). Humanitarian Access Overview (www.acaps.org/en/thematics/all-topics/humanitarian-access).

Global Interagency Security Forum y Humanitarian Outcomes. (2024). *State of practice: the evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Magone, C., Neuman, M. y Weissman, F. (2012). *Humanitarian negotiations revealed: the MSF experience*. Centre de Réflexion sur l'Action et les Savoirs Humanitaires (<https://msf-crash.org/en/war-and-humanitarianism/humanitarian-negotiations-revealed-msf-experience>).

Oficina de Coordinación de Asuntos Humanitarios de las Naciones Unidas. (2012). OCHA on message: humanitarian principles (<https://reliefweb.int/report/world/ocha-message-humanitarian-principles-enar>).

Orientación y recursos

Centro de Competencia de Negociación Humanitaria. (2019). *Manual del CCHN sobre negociación humanitaria*. Frontline Negotiations (<https://frontline-negotiations.org/home/resources/field-manual/>).

Comité Internacional de la Cruz Roja. (s.f.). *Los Convenios de Ginebra de 1949 y sus Protocolos adicionales* (www.icrc.org/en/document/geneva-conventions-1949-additional-protocols).

Comité Internacional de la Cruz Roja. (2015). Preguntas y respuestas y léxico del CICR sobre acceso humanitario. *Revista Internacional de la Cruz Roja* 96(893) (<https://international-review.icrc.org/es/articulos/preguntas-y-respuestas-y-lexico-del-cicr-sobre-acceso-humanitario>).

Comité Internacional de la Cruz Roja. (s.f.). Safer access for all national societies. Overview (<https://saferaccess.icrc.org/overview/>).

3.3 Financiación de la gestión de riesgos de seguridad

Independientemente de la combinación de medidas de gestión de riesgos de seguridad que empleen las organizaciones humanitarias, inevitablemente conllevarán costos. Estos costos, al igual que las propias medidas, deben tenerse en cuenta desde las primeras fases del diseño del programa e incluirse en los presupuestos de las propuestas. Es de vital importancia cerciorarse de que se dispone de la financiación adecuada para que las organizaciones puedan operar con seguridad. Asimismo, es un tema sobre el que las organizaciones y sus donantes deben estar dispuestos a mantener conversaciones francas. En este capítulo se exponen buenas prácticas relativas a la presupuestación de los gastos relacionados con la seguridad y destaca algunas de las cuestiones y de los desarrollos clave en las iniciativas de financiación y coordinación de los donantes.

3.3.1 Costos y presupuesto

No existen fórmulas presupuestarias uniformes ni definiciones comunes de gastos para los insumos y las actividades destinados a mejorar la seguridad de las operaciones. La forma en que se presupuestan los costos relacionados con la seguridad varía entre organizaciones y donantes. Algunos incluyen la financiación de la seguridad en los gastos generales o en los servicios de apoyo, otros la incluyen como una partida separada o como un porcentaje fijo de los costos del programa, o integran totalmente los costos de seguridad en los costos de los programas. Por ejemplo, los vehículos necesarios para que el personal viaje en convoyes irían en la partida de “vehículos/transporte”, la instalación de medidas de protección física como verjas o alarmas entraría en “reparaciones/mantenimiento de instalaciones” y los profesionales de la gestión de riesgos de seguridad podrían entrar en “personal de apoyo”. Del mismo modo, los miembros del personal con capacidades de negociación o de enlace con la comunidad suelen ser imprescindibles para aplicar medidas de aceptación para la gestión de riesgos de seguridad, pero es posible que no se etiqueten como costos relacionados con la seguridad.

En la actualidad, por lo general se reconoce que una gestión de riesgos de seguridad eficaz es esencial para la ejecución sostenible de los programas, por lo que idealmente no debería considerarse un gasto general. En cambio, cuando los donantes exigen estimaciones de los costos de seguridad en las propuestas (como lo hacen algunos de los principales Gobiernos donantes), esto no solo les permite a las organizaciones incluir los insumos necesarios, sino que también las incentiva a pensar activamente en las necesidades de seguridad como parte del proceso de presupuestación y diseño de programas. Al igual que muchos otros aspectos de la gestión de riesgos de seguridad, el cálculo y la presupuesto de los costos de seguridad se derivan principalmente del

diagnóstico de riesgos, que puede orientar la asignación de atención y recursos. El diagnóstico de riesgos también puede incluir la consideración de los riesgos a los que se enfrentan las organizaciones socias que trabajan en el programa, y estos costos se incorporan en cualquier propuesta. En resumen, los costos de gestión de riesgos de seguridad pueden referirse a cualquier gasto relacionado con la reducción de los posibles daños o pérdidas para la organización, el personal y los socios o con la respuesta y la compensación por daños o pérdidas reales, mientras que al tiempo se maximiza el potencial de éxito de las operaciones.

Para cumplir con su deber de cuidado, las medidas de gestión de riesgos de seguridad de una organización deben ser proporcionales al nivel de riesgo al que se enfrenta el personal en el desempeño de su trabajo. No presupuestar adecuadamente los riesgos previsibles sería negligente. Esto exige una comunicación abierta y directa con los donantes y los equipos organizativos pertinentes, no solo en la fase de elaboración de la propuesta, sino a lo largo de todo el ciclo del programa, ya que las condiciones de seguridad pueden evolucionar. También exige que las organizaciones comprendan y documenten los costos incurridos en la gestión de riesgos de seguridad, lo que puede demostrar a los donantes el uso óptimo de los recursos al permitir la continuidad de los programas de ayuda.

La presupuesto de la seguridad a nivel de proyecto o programa normalmente debe ajustarse a los requisitos de los donantes, pero a menudo las organizaciones también necesitarán una política general de presupuestación de la seguridad que abarque toda la organización y no dependa de presupuestos de proyectos individuales con fechas de finalización. El uso de financiación básica, ya sea obtenida a través de gastos generales acumulativos, financiación no restringida o subvenciones específicas, puede permitir funciones, estructuras y puestos de personal de gestión de riesgos de seguridad sostenibles, que trasciendan proyectos y años. Esto puede ser difícil de conseguir para las organizaciones locales, que tienen un acceso mucho más limitado a la financiación básica que las organizaciones internacionales, por lo que se encuentran en una posición de desventaja estructural a la hora de reforzar sus capacidades organizativas.

Presupuesto para seguridad

La cartera de gastos de gestión de riesgos del GISF es una herramienta de presupuestación en hojas de cálculo que ofrece orientación sobre el alcance completo de los costos de seguridad tangibles e intangibles en áreas como activos y equipos, salarios y formación. La herramienta presenta las siguientes categorías presupuestarias, en las que pueden incluirse los gastos de seguridad como costos directos:¹

- salarios,
- administración y logística,
- formación, aprendizaje y desarrollo,

- gestión de la información y el conocimiento,
- acceso,
- gestión de instalaciones,
- activos de comunicaciones,
- activos médicos,
- activos de transporte,
- activos de gestión de crisis,
- seguros, y
- fondos generales de contingencia (por ejemplo, para respuestas a incidentes críticos o evacuaciones).

Nota: Una herramienta poderosa para justificar los costos puede ser la inclusión de notas explicativas en el presupuesto para cada partida, con referencias cruzadas con el texto de la descripción de la propuesta.

ⁱ Para obtener más información, consulte www.gisf.ngo/resource/the-cost-of-srm-for-ngos/.

3.3.2 Procesos internos

Cuando el personal encargado de elaborar las propuestas y los presupuestos no supervisa las necesidades de gestión de riesgos de seguridad o no involucra adecuadamente a quienes sí lo hacen, surge un problema. En estos casos, se corre el riesgo de que los costos relacionados con la seguridad no se presupuesten adecuadamente o de que, si se producen recortes presupuestarios, estos costos sean los primeros en eliminarse.

Es un error elaborar un programa de ayuda y determinar cómo “hacerlo seguro” posteriormente. Para facilitar realmente la acción humanitaria, la gestión de riesgos de seguridad debe integrarse en la programación en todas las etapas. Para ello se requiere una colaboración estrecha entre el personal de programación, finanzas y gestión de subvenciones, gestión de riesgos de seguridad, logística y demás personal pertinente desde las fases iniciales de diseño y elaboración de propuestas, así como en cualquier momento de cambio, como modificaciones presupuestarias o extensiones sin costo. Es aconsejable que las organizaciones que cuentan con asesores o gestores dedicados a la gestión de riesgos de seguridad se cercioren de que estos miembros del personal participen desde el principio, trabajando en colaboración y no de forma aislada. Además,

pueden desarrollar habilidades en los procesos de presupuestación para colaborar eficazmente con sus colegas de finanzas y gestión de subvenciones.

Lo ideal sería que el personal de las organizaciones socias en un programa o proyecto también participe en las principales reuniones de planificación y presupuestación, para garantizar que las necesidades de gestión de riesgos de seguridad de todos los socios se tengan en cuenta en el proceso de presupuestación desde las primeras fases.

► *Para más información sobre la financiación de la seguridad entre socios, véase el capítulo 3.5, “Gestión de riesgos de seguridad en las alianzas”.*

Ejemplo: presupuesto para seguridad

El personal de seguridad de una organización internacional comienza a planificar los costos de gestión de riesgos de seguridad de los programas durante la fase de elaboración del presupuesto operacional para el siguiente año fiscal. De este modo se garantiza que los costos de seguridad generales y no específicos de los proyectos se contabilicen en los costos compartidos del programa para el año fiscal y se reduce el tiempo que lleva esbozar e incluir estos costos en cualquier propuesta de proyecto específica. Estos costos pueden incluir aprendizaje y desarrollo, suministros y equipamiento, y administración y logística. El objetivo de las propuestas de costos relacionados con los proyectos es reflejar con exactitud los costos añadidos de mantener la política y las normas de seguridad de la organización.

La organización también se asegura de que su fase de desarrollo presupuestario implique la coordinación con los colegas pertinentes de recursos humanos, administración, finanzas, cadena de suministro, alianzas y otros, para garantizar que no haya duplicación o eliminación de costos por conceptos que pueden estar relacionados con la seguridad, pero que se gestionan por esos departamentos.

3.3.3 Participación de los donantes

En general, los principales donantes humanitarios gubernamentales están dispuestos a financiar gastos adecuados y justificados relativos a la seguridad. Las directrices para la presentación de propuestas de unos pocos organismos donantes oficiales contienen referencias explícitas a la gestión de riesgos de seguridad y los gastos relacionados, y un pequeño número de donantes cuenta con unidades o referentes específicos de gestión y coordinación de riesgos de seguridad, que pueden brindar orientaciones útiles, especialmente durante la planificación de los programas y las fases iniciales de presupuestación. Algunos organismos donantes también han organizado reuniones y talleres para asesorar a las organizaciones humanitarias sobre cómo incluir los costos de seguridad en las propuestas. Aunque algunos donantes no piden activamente que se incluyan los costos de gestión de riesgos de seguridad en una propuesta, pueden financiarlos si se presentan y justifican.

Sin embargo, cuando las organizaciones internacionales subvencionan o subcontratan a organizaciones locales, es posible que no ofrezcan o no permitan incluir en el presupuesto los costos de gestión de riesgos de seguridad. Esto puede crear un peligro moral, ya que la organización local se ve incentivada a asumir riesgos y a no incluir insumos destinados a la seguridad en su presupuesto para ser más competitiva en la búsqueda de contratos internacionales. A fin de no crear más burocracia innecesaria, las organizaciones internacionales pueden tratar de garantizar el mismo nivel de debate abierto, comunicación clara de las necesidades y planificación por escrito respecto a la gestión de riesgos de seguridad con sus socios en la ejecución que con sus donantes. Lo ideal es que las alianzas incluyan un componente de costos básicos que permita a la organización local desarrollar capacidades sostenibles de gestión de riesgos de seguridad.

Si bien los donantes varían en cuanto a lo que financian, las áreas comunes de gasto incluyen equipos de comunicaciones, artículos y renovaciones de seguridad física, capacitación en seguridad, equipamientos de protección, botiquines de primeros auxilios o emergencias y personal de seguridad (parcial o totalmente, según el nivel de riesgo del contexto y del donante). El apoyo de seguridad adicional a las operaciones, como el que ofrecen los servicios de seguridad privada, se considera normalmente caso por caso.

Algunas agencias de Gobiernos donantes fomentan activamente una mayor concienciación y competencias en materia de seguridad en las organizaciones humanitarias que financian y esperan ver gastos relacionados con la seguridad en los presupuestos. Es posible que las propuestas deban ir acompañadas de un plan de seguridad detallado que incluya un análisis del contexto y un diagnóstico de riesgos. A fin de evitar revisiones sustanciales de los presupuestos de los proyectos una vez firmados los contratos, los diagnósticos de riesgos pueden describir posibles escenarios —y necesidades— futuros en caso de que la seguridad se deteriore. Fuera de esto, sin

embargo, los donantes suelen no dictar políticas o prácticas de seguridad concretas, sino que prefieren dejar que las organizaciones determinen su propia postura en materia de seguridad y ejerzan su propio control de calidad en este ámbito. En parte, esto se debe a que los donantes carecen de personal con el tiempo, las competencias y la presencia operativa necesarios para ejercer una influencia más directa. Los donantes también se cuidan de ser considerados como quienes imponen un modelo de seguridad concreto a las organizaciones. Implicarse formalmente en el aseguramiento de la calidad posiblemente también expondría a los donantes a reclamaciones de responsabilidad. Muchos donantes no piden explícitamente presupuestos para seguridad, y los profesionales de la seguridad se han encontrado con algunos que afirman que no financiarán la seguridad. En los casos en que no exista una partida presupuestaria explícita de seguridad, los costos relacionados con la seguridad pueden cubrirse a través de otras partidas presupuestarias.

Participación de los donantes más allá de la financiación de las necesidades operacionales de seguridad

Aunque los donantes nunca asumirán la responsabilidad de la gestión de riesgos de seguridad de una organización, muchos de ellos han proporcionado recursos adicionales para reforzar los esfuerzos de las organizaciones humanitarias en este ámbito. Por ejemplo, los donantes gubernamentales apoyaron las capacidades y las competencias interinstitucionales mediante financiación al GISF y a la INSO. También han financiado investigaciones para examinar la evolución de los retos en la gestión de riesgos de seguridad y evaluar las prácticas de seguridad actuales entre las organizaciones humanitarias.

Los donantes también aportan fondos al UNDSS para personal y actividades adicionales, con especial atención a las responsabilidades de enlace con las ONG a través de la iniciativa Salvar Vidas Juntos y a la complementación de la seguridad en todo el sector, por ejemplo, para capacitación complementaria sobre seguridad personal y primeros auxilios.

Dado que las organizaciones suelen financiar programas con contribuciones de múltiples donantes, la coordinación entre ellos es importante (aunque actualmente limitada) para garantizar la coherencia de los requisitos y de las directrices de presupuestación en materia de seguridad.

Algunos donantes exigen visibilidad por su financiación y mantienen políticas de marca que requieren que sus logotipos aparezcan en los activos que pagan, incluidas las oficinas, los vehículos y los artículos de socorro. En algunos casos, esta asociación puede considerarse una amenaza para la seguridad, sobre todo si el donante en cuestión es impopular en el contexto en particular o si la organización está intentando adoptar un enfoque de baja visibilidad. En tales casos, la organización puede solicitar formalmente una exención del requisito de visibilidad. Los donantes pueden ser flexibles en cuanto a estos requisitos cuando las cuestiones de seguridad exigen cautela.

Más información

Investigación y orientación

Foro Europeo Interinstitucional para la Seguridad. (2013). *The Cost of Security Risk Management for NGOs* (www.gisf.ngo/resource/the-cost-of-srm-for-ngos/).

Global Interagency Security Forum y Humanitarian Outcomes. (2024). *State of practice: the evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Stoddard, A. y Harmer, A. (2010). *Supporting security for humanitarian action: a review of critical issues for the humanitarian community*. Humanitarian Outcomes (www.humanitarianoutcomes.org/publications/supporting-security-humanitarian-action).

Políticas y ejemplos de financiación de donantes gubernamentales

Ministerio de Relaciones Exteriores, del Commonwealth y de Desarrollo. (s.f.). *FCDO Humanitarian funding guidelines for NGOs applying for CHASE humanitarian response funding*, Annex B: Budget template (www.gov.uk/guidance/humanitarian-response-funding).

Protección Civil y Operaciones de Ayuda Humanitaria. (2023). *Humanitarian implementation plans (HIPs). Thematic policy annex 2024. General considerations: safe and secure provision of aid* (https://ec.europa.eu/echo/files/funding/hip2024/thematic_policies_annex_2024.pdf).

3.4 Monitoreo del cumplimiento, la eficacia y el impacto

Un componente fundamental de la gestión de riesgos de seguridad es garantizar que las políticas, los planes y los procedimientos se revisen y evalúen periódicamente para medir su cumplimiento, eficacia e impacto en toda la organización y en cada localidad.

3.4.1 Mecanismos de monitoreo

El monitoreo del cumplimiento, la eficacia y el impacto de la gestión de riesgos de seguridad puede garantizar que la seguridad permita a la organización alcanzar sus objetivos y apoye sus programas de manera eficaz. Asimismo, es un elemento importante en el cumplimiento del deber de cuidado y puede aportar información esencial para detectar los puntos fuertes y débiles, lo que permite a las organizaciones concentrar los recursos donde más se necesitan.

Sin embargo, uno de los principales problemas de los mecanismos de monitoreo es cuando son percibidos como impedimentos para la ejecución de los programas, que crean cargas adicionales y más capas de burocracia. Otro motivo de preocupación es cuando el enfoque está orientado al cumplimiento, es decir, cuando se centra principalmente en asegurarse de que se cumplan los requisitos mínimos, en lugar de examinar la eficacia de las medidas aplicadas. Para abordar estas cuestiones, los mecanismos de monitoreo deben ser adaptables y expansibles. No deben abrumar a los gestores ni utilizarse para crear un arreglo de seguridad innecesario (aunque sea con buena intención) que pueda convertirse en un impedimento para una programación fluida. Es aconsejable disponer de medidas de monitoreo diferentes para entornos de bajo y alto riesgo, que sean proporcionales a las necesidades y la capacidad y que se adapten a estas. Los mecanismos de monitoreo también pueden ofrecer a los equipos de seguridad la oportunidad de dar un paso atrás y preguntarse por qué una organización utiliza ciertas herramientas y procesos y si las cosas podrían simplificarse, y de asegurarse de que la seguridad apoya a todo el personal en el cumplimiento de los objetivos organizativos y programáticos.

Un monitoreo eficaz favorece el aprendizaje organizativo. Esto puede ser particularmente difícil cuando hay mucha información que absorber, y es especialmente importante que el conocimiento y el aprendizaje no se limiten solo a los equipos de seguridad. En el nivel más básico, las conclusiones y las recomendaciones de las auditorías de seguridad y de otros mecanismos de monitoreo pertinentes deben comunicarse a quienes participaron y, en la medida de lo posible, deben estar disponibles para el personal en general. Dar a conocer los resultados de estos procesos puede favorecer la transparencia y crear conciencia sobre cómo el personal de

seguridad emplea la información recopilada para crear un entorno de trabajo más seguro y propicio.

La labor de monitoreo puede agruparse en tres áreas interrelacionadas (y a veces solapadas).

- **Cumplimiento.** Revisión periódica de la aplicación de las prácticas de gestión de riesgos de seguridad, incluidos informes periódicos y el monitoreo de los indicadores clave para garantizar que las cosas funcionan y comprobar si es necesario introducir cambios. Los tableros de información desempeñan un papel muy útil en este sentido.
- **Eficacia.** Profundización periódica en los procesos para medir la eficacia de las prácticas y de los sistemas de seguridad, incluidas las auditorías de seguridad formales.
- **Impacto.** Análisis en profundidad a partir de la información procedente de las labores de monitoreo y otras fuentes, para comprender si el sistema de gestión de riesgos de seguridad de la organización está influyendo en el cambio o contribuyendo a él.

A continuación se analizan con más detalle.

3.4.2 Monitoreo del cumplimiento

Para monitorear el cumplimiento, las organizaciones pueden utilizar una combinación de métodos, como listas de verificación e indicadores clave de rendimiento. El objetivo principal es comprender las razones del incumplimiento, no sancionar al personal. Es posible que los procesos no se estén siguiendo porque son poco realistas o inadecuados para el contexto. El incumplimiento también puede revelar problemas, como recursos insuficientes, percepciones negativas de las prácticas de seguridad entre el personal y falta de conocimientos. Un monitoreo de esta naturaleza puede ayudar a detectar las deficiencias y los retos que deben abordarse, como capacitación, orientación, apoyo u otras actividades positivas de fomento de la cultura de seguridad. En la tabla 2 figuran algunos ejemplos de medidas de monitoreo del cumplimiento.

Tabla 2 Ejemplos de medidas de monitoreo del cumplimiento

Medida	Información
Listas de verificación	Una lista de verificación ayuda a evaluar el cumplimiento de las políticas de seguridad y los requisitos mínimos, sobre todo a nivel de oficina o de proyecto. También puede ayudar a los directivos a verificar rápidamente que la información que reciben del personal es correcta.
Indicadores clave de rendimiento	Los indicadores clave de rendimiento miden y registran el desempeño con respecto a los objetivos estratégicos y operacionales. Se utilizan para tomar decisiones y mejorar el rendimiento. Estos indicadores pueden servir para múltiples funciones en el monitoreo del cumplimiento. Pueden vincularse a las funciones y responsabilidades individuales, en particular a las de los directivos y del personal responsables del cumplimiento en materia de seguridad. Los programas y las oficinas también pueden tener indicadores clave de rendimiento relacionados con la seguridad, como porcentajes y cifras, por ejemplo, relativos a planes de seguridad actualizados, sesiones informativas sobre seguridad para el personal itinerante, cantidad de miembros del personal capacitados, porcentaje de financiación de la seguridad en el presupuesto general, presupuesto previsto frente al presupuesto real concedido y consumo de financiación de la seguridad y cobertura de las necesidades. Algunos de los indicadores clave de rendimiento de seguridad también pueden ser globales. Los tableros de información pueden ser especialmente útiles para supervisar estos indicadores, sobre todo para monitorear los indicadores en las distintas oficinas, países y regiones (para obtener más información, consulte la siguiente sección).
Evaluación del personal	Es posible evaluar al personal directivo y a otros miembros del personal responsables de la gestión de riesgos de seguridad para valorar su desempeño en las áreas de trabajo relacionadas con la seguridad. En la mayoría de los casos, se espera que todo el personal, independientemente de su cargo, cumpla con las normas de seguridad y comunique la información relevante al personal de seguridad. También se puede evaluar a los jefes de equipo en relación con la forma en que ellos y sus equipos han cumplido con el sistema de gestión de riesgos de seguridad. Para este fin, habrá que incluir elementos de seguridad en los procesos de selección, como las descripciones de puestos y las preguntas en las entrevistas.

Medida	Información
Informes periódicos de seguridad	Los informes y análisis periódicos de seguridad, tanto cuantitativos como cualitativos, pueden brindar una descripción general de las prácticas de gestión de riesgos de seguridad y de su aplicación. Estos informes pueden ayudar al personal responsable a entender si se están cumpliendo los requisitos mínimos, detectar problemas y deficiencias e impulsar medidas correctivas. Los informes y el monitoreo periódicos pueden reducir la probabilidad de que se produzcan resultados y conclusiones inesperados en las auditorías más formales. Los indicadores para la elaboración de informes periódicos podrían incluir: • Validez/vencimiento de los planes de seguridad. • Cambios en los niveles de seguridad. • Número y gravedad de los incidentes y de las personas afectadas. • Presupuesto disponible para seguridad e importe gastado. • Número de empleados capacitados en seguridad contra los objetivos organizacionales. Las herramientas en línea pueden facilitar el monitoreo de algunos indicadores clave. Por ejemplo, las organizaciones que disponen de recursos de capacitación en línea pueden proporcionar rápidamente información sobre el cumplimiento, cuando sea necesario, en relación con la participación en la capacitación.
Informes y análisis de incidentes	El monitoreo del número de incidentes que afectan a un lugar concreto puede proporcionar una visión general de las tendencias y señalar cuándo puede ser necesario dedicar más atención a los procesos de gestión de riesgos de seguridad. Sin embargo, esto puede inducir a error si no se dispone de un valor o punto de referencia, ya que los aumentos podrían indicar una mejora en los informes en lugar de una mayor inseguridad. Además de la cantidad de incidentes, el monitoreo de cómo se gestionan los informes —por ejemplo, los retrasos en su presentación, la exhaustividad de las plantillas de informes y los niveles de subregistro de información— puede ayudar a evaluar el cumplimiento de las prácticas de seguridad. El análisis de incidentes también sirve de apoyo a las personas afectadas y de alerta para evaluar la eficacia de los diagnósticos de riesgos, las medidas de mitigación y el sistema general de gestión de riesgos de seguridad. También ayuda a detectar problemas de cumplimiento o deficiencias en los procedimientos, el apoyo y la capacitación, analizando el tipo, la frecuencia y las causas de los incidentes que afectan al personal. <i>(Para obtener más información sobre los informes de incidentes, véase el capítulo 4.4).</i>
Revisiones posteriores a incidentes o crisis	De forma similar al análisis de incidentes, una evaluación en profundidad tras un incidente crítico o una crisis puede ofrecer una visión general del cumplimiento de las medidas de protección, así como de su pertinencia y eficacia.

El equipo directivo debe dar retroalimentación para fomentar la presentación de informes y la aplicación de otros mecanismos de cumplimiento. Los resultados de este monitoreo, incluidos los informes, pueden ponerse a disposición de los directivos y demás personal pertinente y transmitirse por correo electrónico, en reuniones o a través de un tablero de información (véase más abajo).

Mejorar la gestión de riesgos de seguridad mediante el monitoreo puede significar a veces responsabilizar al personal del incumplimiento de la política y los procedimientos. En caso de que haya pruebas de incumplimiento que merezcan una sanción, es importante que la política de la organización correspondiente se respete con transparencia. La política de la organización a este respecto debe comunicarse claramente al personal con antelación. El objetivo debe ser apoyar una cultura de seguridad positiva, en lugar de crear rechazo o animosidad hacia los procesos de seguridad.

Ejemplo: Forjar relaciones para mejorar el cumplimiento

Una ONG internacional descubrió que el cumplimiento y la cultura de seguridad general mejoraron tras una revisión de la forma en que el equipo de seguridad se relacionaba con el resto del personal. Esto implicó la eliminación de la jerga de seguridad de las comunicaciones y la adopción de otras medidas para generar confianza y hacer que el equipo de seguridad pareciera más accesible. Se hicieron esfuerzos para contratar personal de seguridad de diversas procedencias y para animar al personal a ver al equipo de seguridad como un recurso esencial y útil. También se realizaron actividades de divulgación, como sesiones mensuales sobre seguridad y reuniones con distintos equipos de la organización. Además, para lograr este cambio fue fundamental la modificación del tono de la dirección de la organización sobre el papel de la seguridad como un elemento facilitador del trabajo del personal.

El personal de seguridad también se beneficia de ser creativo a la hora de promover el cumplimiento de las normas, por ejemplo, buscando diferentes tipos de incentivos. En algunos casos, las recompensas, así como las medidas de denuncia y descrédito, han resultado eficaces. Por ejemplo, algunas organizaciones internacionales utilizan foros organizativos para enumerar las oficinas de país que no cumplen o no alcanzan los principales indicadores clave de rendimiento. Los tableros de información pueden ser una herramienta eficaz para este fin, como se ilustra en la sección siguiente.

3.4.3 Monitoreo de la eficacia

Para controlar la eficacia, cada vez más organizaciones realizan auditorías, revisiones y consultas de seguridad. Estas van más allá del monitoreo del cumplimiento de las normas y examinan más a fondo la aplicación y la eficacia de los sistemas y las medidas de protección.

Auditorías de seguridad

El objetivo principal de una auditoría de seguridad es examinar si las medidas de gestión de riesgos de seguridad de una organización le permiten cumplir los objetivos del programa sin exponer a la organización y a su personal a riesgos evitables. Lo ideal es que el resultado de la auditoría sea un plan de acción que ayude al personal a realizar su trabajo de forma segura (figura 6).

El aspecto de una auditoría de seguridad, su periodicidad, quién la realiza y su profundidad variarán de una organización a otra. Sin embargo, estas auditorías pueden dividirse en dos grandes categorías: a nivel de toda la organización y específicas de un lugar.

Las auditorías de seguridad, sobre todo las específicas de un lugar, pueden utilizarse para verificar que se hayan aplicado las medidas de mitigación determinadas en el diagnóstico de riesgos y el plan de seguridad y para evaluar en qué medida se han seguido las políticas y los procedimientos. Asimismo, pueden ayudar a determinar si las evaluaciones y los planes iniciales siguen siendo pertinentes y pueden utilizarse para verificar la exactitud de la información periódica de seguridad (por ejemplo, mediante informes de seguridad) de un lugar de trabajo concreto.

Las auditorías pueden ser *ad hoc* o periódicas. Las auditorías específicas de un lugar se llevan a cabo de acuerdo con las políticas de la organización. Además, suelen anunciarse con antelación, aunque no siempre es así.

Aunque las distintas organizaciones desarrollarán sus propios procesos y herramientas de auditoría, con sus indicadores clave, la guía *Auditorías de seguridad* del GISF (antes EISF)³⁷ y el modelo de madurez del deber de cuidado del Swiss Centre of Competence for International Cooperation (CINFO)³⁸ ofrecen ejemplos de indicadores que pueden servir como plantillas para evaluar el rendimiento de una organización en el ámbito de la seguridad.³⁹ Las organizaciones se benefician de hacer un mapeo de los indicadores

37 Finucane, C. (2013) *Auditorías de seguridad*, Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/security-audits/>).

38 Véase <https://dutyofcare.cinfo.ch/> (disponible en inglés).

39 Foro Europeo Interinstitucional para la Seguridad (ahora Global Interagency Security Forum) *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas* ofrece una guía de referencia rápida sobre una serie de elementos relacionados con la seguridad que pueden ser útiles para planificar una auditoría o una revisión (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

y de los resultados confrontándolos con los sistemas, los marcos o los requisitos de seguridad.

Auditorías frente a revisiones

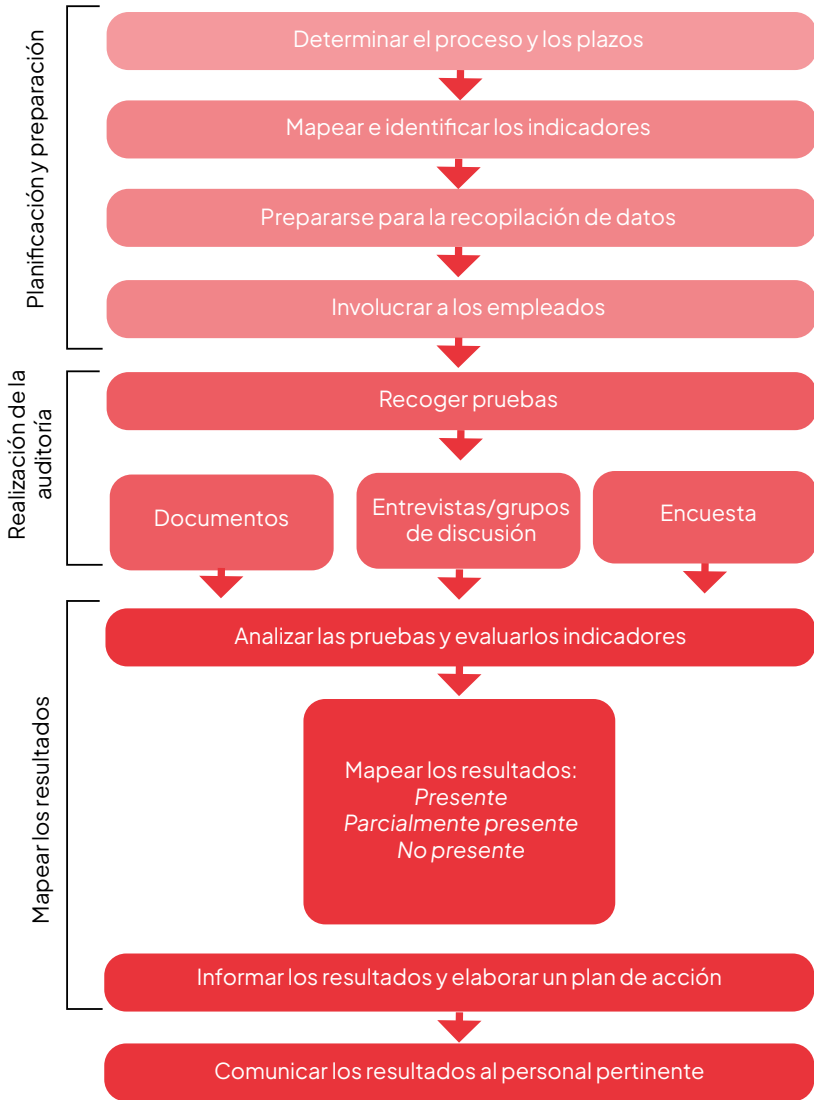
Una auditoría de seguridad es una evaluación formal, centrada en el cumplimiento de las políticas, los procedimientos y las prácticas de seguridad de una organización con respecto a los requisitos e indicadores organizativos establecidos. Por el contrario, una revisión de seguridad suele ser un proceso más flexible e informal que evalúa la eficacia de las medidas de protección, detecta los puntos débiles y ofrece recomendaciones de mejora, centrándose en la optimización de la seguridad general y no solo en el cumplimiento de las normas. Las auditorías de seguridad se planifican, mientras que es más probable que las revisiones se lleven a cabo después de un incidente crítico o tras un cambio repentino del contexto.

Algunas organizaciones también realizan revisiones globales u organizativas de los sistemas y los enfoques de seguridad, que son evaluaciones formales basadas en términos de referencia específicos. Estas suelen ir más allá de una evaluación de las normas o de los requisitos internos; aunque pueden establecer comparaciones con enfoques comunes y buenas prácticas en el sector, no existen normas externas específicas que sirvan de referencia para la auditoría, por lo que a menudo se habla de revisión y no de auditoría.

Algunas organizaciones han optado por no utilizar el término *auditoría* debido a las connotaciones negativas que conlleva y prefieren términos como *revisiones* o *comprobaciones*, para alejarse de la percepción de que los revisores están evaluando el desempeño individual o buscando deficiencias en el trabajo del personal. Por lo tanto, la distinción entre lo que se considera una auditoría y una revisión variará según la organización.

Tanto las auditorías de seguridad como las revisiones evalúan la “salud” de los sistemas de seguridad y el conocimiento y la comprensión por parte del personal de los recursos y las medidas de protección. Estas evaluaciones ofrecen al personal la oportunidad de poner de relieve los riesgos de seguridad o los retos a los que se enfrentan en su vida y en su trabajo, que podrían no haberse considerado adecuadamente en las medidas de protección existentes.

Figura 6 Proceso de auditoría de seguridad



Adaptado de Finucane, C. (2013) *Auditorías de seguridad*, EISF (www.gisf.ngo/resource/security-audits/).

Las auditorías pueden incluir un examen de la documentación pertinente, datos sobre incidentes, entrevistas, debates en grupo con personal clave y encuestas. Pueden llevar mucho tiempo.

Lo ideal sería que las auditorías de seguridad incluyeran consultas a un amplio grupo de personal, no solo a aquellos con responsabilidades en la gestión de riesgos de seguridad. Tras la recopilación de los datos pertinentes y la evaluación de los indicadores clave, se analizan las conclusiones, se presentan los resultados y se elabora un plan de acción. En este plan se enumeran las actividades específicas que deben llevarse a cabo, se señala a los responsables, se establecen prioridades, se fija un calendario y se cuantifica el presupuesto necesario para su ejecución.

En algunos casos, puede ser aconsejable que las auditorías de seguridad se lleven a cabo por revisores o consultores externos. Esto puede dar lugar a resultados más objetivos y también puede servir para comparar una organización con sus homólogas aprovechando los conocimientos del revisor externo. En algunos casos, un revisor externo también puede obtener respuestas más francas de los miembros del personal sobre la eficacia y las debilidades del sistema de gestión de riesgos de seguridad. Cuando el costo de un revisor externo puede representar un obstáculo, a veces las organizaciones trabajan conjuntamente en la realización de revisiones entre pares.

Ejemplo: Proceso de auditoría

Una ONG internacional ha desarrollado un amplio proceso de auditoría de seguridad, que lleva varios años en marcha. Cada año se auditan varios países. Se recurre a auditores externos para realizar una combinación de consultas presenciales y a distancia. La auditoría se realiza analizando más de 100 indicadores clave de rendimiento. Los auditores elaboran un informe sobre los indicadores clave de rendimiento (centrado en el cumplimiento) y un informe narrativo que analiza la eficacia del sistema general de seguridad: qué funciona bien, cuáles son las carencias y sus recomendaciones.

Medir la aceptación

Una debilidad inherente a las auditorías de seguridad, y a todos los mecanismos de monitoreo, es la tendencia a centrarse en datos fáciles de recopilar y analizar, con un sesgo particular hacia los datos cuantitativos (como el porcentaje de personal capacitado y el número de incidentes de seguridad). Esto puede llevar a centrarse en las actividades de protección, que son más tangibles y más fáciles de registrar que las medidas de aceptación.

Los mecanismos de monitoreo de la seguridad pueden medir la aceptación y las percepciones extrayendo datos de las actividades de monitoreo programáticas y de las encuestas de percepción, desarrollando y aplicando herramientas adicionales (como los análisis de aceptación) o incorporando métricas de aceptación a las herramientas existentes, como el mapeo de los actores. Las evaluaciones de los programas pueden servir para supervisar las percepciones y la aceptación, pero rara vez se tienen en cuenta en los esfuerzos de monitoreo de la gestión de riesgos de seguridad.

El proyecto Acceptance Research y la herramienta Acceptance Toolkit ofrecen algunos consejos útiles sobre cómo evaluar la aceptación: <https://acceptanceresearch.wordpress.com>. Véase también el capítulo 4.2, “Diseñar una estrategia de seguridad”.

Para consultar herramientas y orientaciones sobre cómo controlar la aceptación con más frecuencia, véase, por ejemplo, la plantilla de análisis de la aceptación del GISF (<https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/>) y el capítulo 4 de *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Consultas

Las consultas *ad hoc* al personal sobre los retos y las debilidades son cada vez más habituales en el sector humanitario. A menudo se realizan tras la presentación de una queja o denuncia por mala conducta o negligencia, y pueden referirse a cuestiones como racismo, explotación y abuso sexuales, acoso e intimidación. Los equipos de seguridad pueden utilizar lo aprendido a partir de estas consultas para mejorar su trabajo y también pueden beneficiarse de llevar a cabo sus propias consultas sobre temas concretos relacionados con la seguridad. Los mecanismos confidenciales de

reporte y denuncia de irregularidades pueden ayudar a las organizaciones a descubrir prácticas de seguridad deficientes.

Ejemplo: Consultas

Una ONG internacional consultó a más de 2000 empleados en varios países para conocer sus preocupaciones relativas a la seguridad. Los resultados dieron lugar a un informe y a un plan de acción globales, y a un cambio para abordar institucionalmente los riesgos basados en la identidad. Se han programado consultas futuras sobre otros riesgos e inquietudes relacionados con la identidad.

3.4.4 Evaluación del impacto

El impacto se refiere a los cambios, tanto intencionados como no intencionados, que se producen como consecuencia de las actividades de una organización. La medición del impacto es el proceso de evaluación de estos cambios, tanto cualitativa como cuantitativamente. Se evalúa qué parte del cambio observado puede atribuirse a medidas concretas adoptadas por una organización.

Para medir el impacto, las organizaciones pueden aplicar un enfoque basado en la teoría del cambio, que implica la creación de una hoja de ruta detallada que describa los resultados deseados a largo plazo, como la creación de un entorno de trabajo más seguro, y los pasos necesarios para lograrlos. El proceso suele conllevar la fragmentación del objetivo a largo plazo en resultados intermedios, como la mejora de la gestión de crisis y la reducción de los índices de incidentes, que pueden supervisarse a lo largo del tiempo y apoyarse mediante actividades específicas, como la capacitación en seguridad y la planificación de la gestión de crisis. Es aconsejable identificar indicadores adecuados de cambios positivos y negativos, centrándose en determinar la causalidad (es decir, qué parte del cambio se debió a la influencia o contribución de las prácticas y sistemas de gestión de riesgos de seguridad). Los mecanismos de monitoreo descritos en este capítulo pueden ayudar a evaluar el impacto.

Los ejercicios de evaluación del impacto no tienen por qué centrarse en hallar pruebas concluyentes de que una intervención ha contribuido a un cambio o conjunto de cambios. En lugar de ello, el proceso puede centrarse en producir una narrativa creíble y basada en pruebas que indique el impacto. Las preguntas de aprendizaje basado en pruebas pueden ser útiles en este ejercicio (véanse ejemplos en el recuadro más adelante).

Ejemplos de preguntas de aprendizaje basado en pruebas

- ¿En qué medida los programas de capacitación en seguridad de la organización mejoran el conocimiento y el comportamiento del personal con respecto a los riesgos de seguridad?
 - Registros de asistencia a la capacitación, evaluaciones previas y posteriores a la capacitación, encuestas de retroalimentación del personal y cambios observados en el comportamiento o en la toma de decisiones.
- ¿Qué impacto han tenido los incidentes de seguridad en la capacidad de la organización para prestar ayuda humanitaria?
 - Registros de interrupciones operacionales, retrasos o cambios en la ejecución de programas debido a incidentes de seguridad. Entrevistas con el personal sobre cómo los incidentes de seguridad han afectado las operaciones.
- ¿Existen mejoras observables en los resultados de la gestión de riesgos de seguridad en comparación con periodos anteriores y otras organizaciones homólogas que operan en las mismas zonas?
 - Datos históricos sobre incidentes de seguridad, análisis de tendencias (en comparación con otras organizaciones) y comparaciones de la eficacia de la gestión de riesgos a lo largo del tiempo.
- ¿Qué lecciones se han aprendido de los últimos incidentes de seguridad y cómo se han aplicado para mejorar la práctica?
 - Revisiones posteriores a los incidentes, planes de acción, lecciones aprendidas documentadas, cambios introducidos en las políticas o en los procedimientos en función de estas lecciones y supervisión de la eficacia de estos cambios.
- ¿Cómo han influido las medidas de protección en la retención y en la selección de l personal? (Un entorno de trabajo seguro puede ser un factor clave para atraer y retener al personal).
 - Índices de rotación de personal por localidad frente a indicadores de seguridad, retroalimentación de las entrevistas de salida (motivos de salida), número de solicitantes de empleo y su opinión sobre la reputación de seguridad de la organización.

3.4.5 Visualización de datos y tableros de información

Las organizaciones utilizan cada vez más los tableros de información digitales en la gestión de riesgos de seguridad. Un tablero de información consiste en un conjunto de métricas y datos clave que se muestran en una única plataforma en tiempo real. Estos tableros facilitan la visualización de datos en varios formatos, como mapas, indicadores clave de rendimiento, tablas y gráficos. Se puede acceder a estas herramientas de forma pública o privada, y la compatibilidad con dispositivos móviles es cada vez más habitual.⁴⁰

Los tableros de información admiten numerosas aplicaciones relativas a la gestión de riesgos de seguridad, como la visualización de los niveles de seguridad y las restricciones de viaje por ubicación; el almacenamiento y acceso a diagnósticos de riesgos y planes de seguridad; el monitoreo del cumplimiento; la visualización de cifras de incidentes; y la ayuda en la detección de carencias para priorizar la financiación y otros apoyos. También ayudan a informar al personal contratado recientemente, a preparar informes y a hacer un seguimiento de las asignaciones presupuestarias. Estos datos en tiempo real permiten a las organizaciones tomar medidas correctivas rápidamente, sin necesidad de esperar informes o actualizaciones periódicas.

A la hora de diseñar un tablero de información, es fundamental definir su finalidad, la información necesaria para sustentarlo, los métodos de recopilación de datos, las funciones y las responsabilidades, y los permisos de acceso. Hay varias plataformas de visualización de datos disponibles para comprar; algunas de ellas gratuitas hasta cierto nivel de uso. Es esencial tener en consideración su compatibilidad con los sistemas existentes.

Ejemplo: Tableros de información, cumplimiento e impacto

Una importante ONG internacional invirtió en la mejora de la tasa de planes de seguridad válidos, simplificando el formato y haciendo un seguimiento más cercano, y para ello resultó esencial disponer de un tablero de información. El tablero creó inadvertidamente una “competencia sana” entre los equipos de país para demostrar quién cumplía mejor los requisitos de seguridad. Antes de la introducción del tablero, la organización luchaba por mejorar el cumplimiento. Los planes no se actualizaban antes de la fecha de vencimiento, y había poca visibilidad desde y entre las oficinas de país, regionales y mundiales.

40 Para ver un ejemplo de un tablero de información de acceso público, consulte INSO: <https://ngosafety.org/conflict-data-dashboard/#dashboard>.

Gracias al tablero, los directivos pudieron ver cómo estaban actuando los países y las regiones en términos de cumplimiento, utilizando un sencillo sistema de colores de semáforo para clasificar los datos. Posteriormente, el tablero se publicó en la intranet del equipo de seguridad y se compartió con los responsables de la toma de decisiones.

Se creó un indicador clave de rendimiento de seguridad basado en el número de planes de seguridad actualizados y visible para el personal de las oficinas de país, regionales y mundiales. Un año después de la introducción del tablero, el indicador aumentó a un 70 % simplemente por hacer que los datos fueran visibles para el personal. En el segundo año, había aumentado a un 79 %.

Los tableros de información fiables requieren datos pertinentes, fiables y accesibles, tanto internos como externos. Deben establecerse procesos de recopilación y gestión de datos, que garanticen la confidencialidad. Los tableros de información deben procurar equilibrar la necesidad de comunicar información con los requisitos de confidencialidad y las normas de protección de datos, garantizando que la información sensible se maneje adecuadamente.

Las herramientas de visualización de datos están diseñadas para mostrarse y compartirse, y para ayudar a los directivos a tomar decisiones. Cualquier conflicto entre confidencialidad e intercambio de información debería abordarse idealmente durante la fase de diseño y planificación.

Más información

Orientación e investigación

Bickley, S. (2017). *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*. Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Billaudel, R. (2021). Measuring and improving acceptance: ACF's experience and perspectives. En Global Interagency Security Forum (Ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Finucane, C. (2013). *Auditorías de seguridad*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/security-audits/).

Global Interagency Security Forum. (2024). *Estrategia de gestión de riesgos de seguridad (GRS) y desarrollo de políticas: Una guía interfuncional* (<https://gisf.ngo/resource/srm-strategy-and-policy-guide/>).

Global Interagency Security Forum y Humanitarian Outcomes. (2024). *State of practice: the evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Herramientas

CINFO (s.f.) *Duty of care maturity model* (<https://dutyofcare.cinfo.ch/model.html>).

Collaborative Learning Approach to NGO Security Management. (2011). *Acceptance Toolkit* (<https://acceptanceresearch.wordpress.com/acceptance-toolkit/>).

Global Interagency Security Forum. (s.f.). Acceptance analysis template - xlsx. 2. *Acceptance analysis*. NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/>).

International NGO Safety Organisation. (s.f.). *Conflict data dashboard* (<https://ngosafety.org/conflict-data-dashboard/#dashboard>).

3.5 Gestión de riesgos de seguridad en las alianzas

En el ámbito de la ayuda humanitaria, es habitual que una parte o la totalidad de un programa sea diseñado y “pertenezca” a una organización, pero que sea ejecutado en parte o en su totalidad por otra. Trabajar con y a través de otras organizaciones o alianzas puede ser más rentable, más acertado en términos programáticos o formar parte de una estrategia deliberada, como el fortalecimiento de las capacidades locales o la reducción del riesgo. El número de alianzas en el sector humanitario ha aumentado en los últimos años debido, en parte, a los esfuerzos de localización y descolonización. En este capítulo se examinan las alianzas equitativas desde el punto de vista de la seguridad. Aunque se reconoce la diversidad de las alianzas en el sector humanitario y se pretende ser ampliamente aplicable, se centra en las alianzas entre organizaciones internacionales y actores nacionales y locales.⁴¹

3.5.1 Principios y consideraciones estratégicas

Una alianza es cualquier relación de trabajo formalizada entre dos o más organizaciones para alcanzar objetivos acordados. Las alianzas en el sector humanitario pueden variar en forma, duración, alcance y grado de colaboración, pueden ser estratégicas y a largo plazo o pueden basarse en proyectos concretos a corto plazo. Suelen ser bilaterales entre organizaciones internacionales y agentes nacionales (por ejemplo, ONG locales y grupos comunitarios), pero también pueden concertarse entre varias organizaciones (por ejemplo, a través de consorcios y subvenciones generales), y entre organizaciones y empresas privadas, así como entre ONG nacionales. Para algunas organizaciones internacionales, la implementación a través de socios locales puede ser su principal forma de trabajo, mientras que para otras puede ser solo una alternativa ocasional a la implementación directa por parte de su propio personal.

Los acuerdos o contratos de alianzas suelen dictar el alcance de este tipo de acuerdos, con responsabilidades de seguridad a veces marcadas en los acuerdos como pertenecientes a cada entidad jurídica individual. En algunas circunstancias, los acuerdos pueden establecer un cruce de apoyos, por ejemplo, ante un incidente crítico. En muchos casos, sin embargo, las responsabilidades no están claras y la cooperación en la gestión de riesgos de seguridad no está explicitada, lo que da lugar a grandes diferencias en la forma de tratar estas cuestiones.

Lamentablemente, la creciente demanda de “localización” en el sector humanitario no se ha traducido en un debate proporcional acerca de la gestión de riesgos de seguridad y el deber de cuidado en los acuerdos de alianzas entre agentes internacionales y locales. Esto suele ir en detrimento de los actores locales, que a menudo se enfrentan a un mayor riesgo de sufrir un incidente de seguridad grave, pero reciben un apoyo

41 En algunas publicaciones se distingue entre organizaciones y actores nacionales y locales. En este documento se utilizan ambos términos indistintamente para hacer referencia a todo tipo de organizaciones que operan únicamente en un país, ya sea en varias localidades o en una sola, incluidos los grupos comunitarios.

mínimo en materia de seguridad (tanto dentro de sus organizaciones como por parte de sus socios internacionales).⁴² La investigación también ha demostrado que, en las alianzas internacionales-locales, los riesgos más discutidos y mitigados son los fiduciarios, mientras que los riesgos de seguridad suelen tratarse someramente. Aunque esto parece estar cambiando, sigue habiendo retos.⁴³

La consideración o no de la gestión de riesgos de seguridad en los acuerdos de alianzas, y la forma en que se aborda, suele ser un reflejo de estos aspectos:

- en qué medida cada organización socia considera y aborda internamente los riesgos de seguridad, y
- las circunstancias y los objetivos de la alianza.

Las organizaciones que carecen de conocimientos o capacidad, o en las que no existen sistemas internos sólidos de gestión de riesgos de seguridad, pueden sentirse incapaces de mantener conversaciones sobre seguridad o de brindar apoyo más allá de su propia organización y personal o pueden no tener la cultura de seguridad organizativa necesaria para siquiera plantearse hacerlo. La interacción también puede variar dentro de la misma organización debido a las distintas capacidades de gestión de riesgos de seguridad en las diferentes oficinas y localidades.

La intencionalidad o finalidad de una alianza también afecta la forma en que se considera y gestiona la alianza, con consecuencias sobre la forma en que los socios debaten los riesgos a los que se enfrentan en el desempeño de su trabajo. Por ejemplo, la investigación sobre las alianzas locales-internacionales ha demostrado que los modelos de alianzas a corto plazo y basados en proyectos no favorecen los debates ni el apoyo a la gestión de riesgos de seguridad.⁴⁴

42 Global Interagency Security Forum (2020) *Partenariado y gestión de riesgos de seguridad: desde la perspectiva de la coparte local* (<https://gisf.ngo/resource/partnerships-and-security-risk-management-from-the-local-partners-perspective/>) y Global Interagency Security Forum y Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

43 Humanitarian Outcomes (2019) *NGOs & risk: managing uncertainty in local-international partnerships (global report)* (<https://humanitarianoutcomes.org/publications/ngos-risk2-partnerships>) y GISF y Humanitarian Outcomes (2024).

44 Global Interagency Security Forum (2020).

3.5.2 Retos

Los socios se enfrentan a una serie de retos y obstáculos cuando intentan participar en una gestión de riesgos de seguridad mutuamente beneficioso.

Deber de cuidado: consideraciones jurídicas y éticas

Como se ha expuesto en el capítulo 1.1, “Conceptos y principios clave”, por lo general se entiende que el deber legal de cuidado se aplica únicamente a los empleados propios de una organización y no a los de las organizaciones socias. No obstante, existe un deber ético de apoyar a los socios en la gestión de riesgos de seguridad y de compartir la información, los conocimientos y las buenas prácticas pertinentes. A algunas organizaciones internacionales les preocupa que, al ofrecer este tipo de apoyo, puedan asumir inadvertidamente la responsabilidad legal del personal de sus socios. Algunos miembros del personal de seguridad han recibido el consejo de asesores jurídicos de abstenerse de tratar asuntos de seguridad con sus socios por este motivo.⁴⁵

Aunque el alcance y la naturaleza de la responsabilidad legal pueden variar significativamente en función de la jurisdicción y las circunstancias específicas, estas preocupaciones pueden ser exageradas. Al igual que en el caso de los particulares,⁴⁶ la responsabilidad legal de una organización hacia un socio puede depender del “grado de control” que ejerza sobre los procesos de toma de decisiones del socio.

Si bien es una buena práctica tener en cuenta los instrumentos jurídicos pertinentes y sus implicaciones en la gestión de riesgos de seguridad en las alianzas, ignorar por completo la cuestión es un fallo ético que, potencialmente, podría acarrear consecuencias jurídicas. En general, es conveniente para toda organización que establece alianzas con regularidad definir una política sobre el tipo de apoyo que prestará o esperará de sus socios. Además de dejar claro dónde recae la responsabilidad, el apoyo prestado a los socios en materia de seguridad debe tener como objetivo mantener la colaboración, sin imponer un enfoque concreto sobre otro, y mantener la toma de decisiones claramente dentro de cada organización. En este sentido, también es importante ser consciente de cómo los desequilibrios de poder y los incentivos económicos pueden hacer que el apoyo y el asesoramiento parezcan un mandato. En algunas jurisdicciones, una entidad jurídica puede ser considerada responsable si se demuestra que un acuerdo es perjudicial para una de las partes, aunque ambas lo hayan aceptado. Esto es especialmente preocupante, ya que los socios en la ejecución

45 Global Interagency Security Forum y Humanitarian Outcomes (2024).

46 La responsabilidad jurídica de una organización hacia una persona puede estar relacionada con el grado de control que la organización tenga sobre las circunstancias de esa persona. Por ejemplo, una organización que recibe la visita de una persona que no pertenece a su plantilla en un país determinado y que tiene pleno control sobre el lugar donde el visitante se aloja, sus condiciones de viaje y su itinerario general probablemente tendrá una obligación legal *de facto* de deber de cuidado hacia esa persona, exista o no un acuerdo contractual. Véase Kemp, E. y Merkelbach, M. (2016) *Duty of care: a review of the Dennis v Norwegian Refugee Council ruling and its implications*, Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

pueden sentirse presionados a asumir más riesgos de seguridad de los que aceptarían normalmente con el fin de conseguir contratos. Para solucionarlo, los socios pueden dar prioridad al fomento de la confianza mutua y al desarrollo de una comunicación sólida en torno a estas cuestiones.

Transferencia de riesgos

A veces, las ONG internacionales se asocian con actores locales para reducir los riesgos a los que se enfrenta su propio personal. La transferencia de riesgos en estas circunstancias se convierte en un componente de una estrategia de gestión de riesgos operacionales, en la que una organización busca a otra persona para llevar a cabo determinadas actividades en un contexto altamente inseguro con el fin de reducir los riesgos para su propio personal. Esta definición clásica de *transferencia de riesgos* ha sido objeto de mucho debate en los últimos años y se están realizando esfuerzos para abordar los fallos del deber de cuidado ético que puede plantear, especialmente cuando no existe una evaluación clara que indique que el personal de una organización local corre menos riesgos que el de una organización internacional.

Aunque a veces es más fácil para los actores locales mantener el acceso en entornos volátiles que para las organizaciones internacionales, esto debe evaluarse y acordarse adecuadamente por ambos socios. Los actores internacionales y locales pueden enfrentarse a riesgos y retos diferentes en contextos diferentes, incluidos los riesgos que pueden transferirse o crearse mutuamente a través de la alianza. De hecho, al establecer una alianza, las organizaciones transfieren automáticamente el riesgo, tanto de forma intencionada como no intencionada. Por ejemplo, al asociarse con una organización internacional para ejecutar un programa de alto perfil, un grupo comunitario puede correr mayores riesgos debido a la atención adicional que puede recibir, incluso por parte de las autoridades y las comunidades locales.

Así planteada, la transferencia de riesgos se entiende mejor como “la formación o transformación de riesgos (que aumentan o disminuyen) para un actor, causada por la presencia o las acciones de otro”.⁴⁷ Esto puede extenderse más allá de las alianzas internacionales-locales e incluye las relaciones con los donantes y otros actores, como las organizaciones comunitarias.

Las buenas prácticas animan a los socios a reflexionar sobre el impacto que una alianza puede tener en su exposición a amenazas concretas y la capacidad de cada organización para hacer frente a los riesgos antes de concertar una alianza.

Déficits de financiación

Las organizaciones nacionales reciben sistemáticamente una financiación insuficiente, esporádica y basada en proyectos, lo que les dificulta desarrollar sistemas internos

47 Global Interagency Security Forum (2021) *Partenariados y gestión de riesgos de seguridad: Guía de acción conjunta para organizaciones de ayuda locales e internacionales* (<https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/>).

e insumos necesarios para gestionar eficazmente los riesgos de seguridad.⁴⁸ Ante la escasez general de fondos y un entorno de financiación extremadamente competitivo, los presupuestos de las alianzas pueden no incluir partidas presupuestarias específicas para la seguridad o costos básicos adecuados, mientras que los actores locales pueden verse incentivados a dar prioridad a los costos de los programas frente a los gastos relacionados con la seguridad a la hora de suscribir acuerdos de alianzas. Los socios locales también pueden sentirse obligados a aceptar mayores niveles de riesgo para asegurar la financiación. Conscientes de ello, una buena práctica es que las organizaciones internacionales se aseguren sistemáticamente de que existe financiación para la seguridad en los presupuestos de los socios, ya sea para los costos de seguridad evaluados o como un porcentaje estándar de la financiación general proporcionada.

Retos de comunicación y confianza

Hay muchos obstáculos a la comunicación sobre la seguridad en las alianzas, pero el principal es, en primera instancia, la falta de debate sobre este tema. Con demasiada frecuencia, la comunicación sobre las cuestiones de seguridad se limita a las comprobaciones de diligencia debida de los socios en la ejecución o a ser considerada un elemento de un paquete más amplio de “fortalecimiento de capacidades” impulsado por un socio internacional. Es posible que no se involucre adecuadamente a los referentes de seguridad de ambas organizaciones en estas conversaciones iniciales.

La seguridad puede ser un tema delicado y los actores responsables de la ejecución pueden verse disuadidos de hablar con franqueza sobre sus dificultades de seguridad y el apoyo que necesitan por miedo a las repercusiones financieras y de reputación. Los socios que aportan la financiación pueden temer incurrir en responsabilidades jurídicas si abordan el tema, como ya se ha comentado. Los debates sobre seguridad suelen plantear problemas debido a la falta de un vocabulario común, a las diferencias en la forma de entender la seguridad, el riesgo y el apetito de riesgo, y a los desequilibrios de poder. Se necesita tiempo para construir y mantener relaciones de confianza, que la financiación a corto plazo y basada en proyectos puede socavar aún más.

3.5.3 Consideraciones prácticas

Un enfoque estratégico y político sobre las alianzas facilita que las organizaciones adopten un enfoque equitativo de la gestión de riesgos de seguridad. El objetivo es que las conversaciones sobre seguridad en las alianzas no se limiten a comprobaciones unilaterales de diligencia debida y transferencia de riesgos, sino que se conviertan en debates colaborativos sobre cómo “compartir riesgos”, en los que participen directamente los referentes de seguridad y el personal pertinente de los programas de todos los socios.

48 Global Interagency Security Forum (2020) y Global Interagency Security Forum y Humanitarian Outcomes (2024).

La guía del GISF *Partenariados y gestión de riesgos de seguridad* ofrece una hoja de ruta para aplicar este enfoque, que se resume en las siguientes secciones de este capítulo.⁴⁹

Antes de concertar una alianza: enfoque estratégico y conversaciones iniciales

Aunque hay muchos ejemplos positivos de colaboración informal entre los referentes de seguridad en los acuerdos de alianzas, a menudo no son sostenibles en la práctica. Sin un enfoque estratégico claro sobre por qué y cuándo una organización puede buscar socios o cómo abordará la gestión de riesgos de seguridad en las alianzas, las disposiciones de seguridad pueden estar sujetas a los sesgos y las preferencias individuales de los miembros del personal, con el riesgo de que cualquier resultado positivo se pierda cuando el personal cambie de funciones.

Las organizaciones que han elaborado políticas respecto a la firma de acuerdos de alianzas y sus responsabilidades para con sus socios, así como acuerdos de seguridad claramente definidos, se benefician de acuerdos de alianzas más estratégicos y mejor equilibrados, más favorables a debates constructivos sobre la gestión de riesgos de seguridad y al apoyo mutuo. Este enfoque estratégico aumenta la probabilidad de que ambos socios se beneficien de la alianza y reduce la probabilidad de una transferencia de riesgos inadvertida y no abordada.

En la práctica, esto incluye garantizar que las consideraciones de seguridad de los referentes se incorporen a la documentación estratégica de las alianzas y a las políticas conexas. Las conversaciones iniciales pueden incorporarse a los procesos de diligencia debida. Si se plantean adecuadamente, estos debates brindan a los socios la oportunidad de abordar en colaboración las preocupaciones sobre la transferencia de riesgos, evaluar la capacidad y la preparación en materia de seguridad, y explorar formas de apoyarse mutuamente en cuestiones relacionadas con la seguridad.

Ejemplo: Más allá de los procesos unilaterales de diligencia debida

Una ONG internacional ha empezado a incorporar a su personal de seguridad local en los procesos de identificación y contratación de los socios locales en la ejecución. Esto ha permitido a la organización debatir cuestiones de seguridad al iniciar una alianza y ha dado lugar a que la seguridad se convierta en algo más que una “revisión de sistemas” de diligencia debida en la alianza.

49 Global Interagency Security Forum (2021).

Durante esta fase, los socios deben tratar de evaluar cómo se transfieren los riesgos entre las organizaciones y encontrar conjuntamente formas de abordar los retos que surjan, incluidos los riesgos relacionados con la identidad derivados de las percepciones externas de la organización y su personal. Por ejemplo, si resulta que una comunidad local tiene percepciones negativas sobre cierto trabajo que se espera que un socio en la ejecución haga para su socio en la financiación, ambos socios pueden discutir medidas de mitigación. Esto podría implicar reducir la visibilidad de esas actividades del programa o modificar el proyecto para mejorar la seguridad del personal encargado de su ejecución. Véanse algunas preguntas clave que figuran en la tabla 3.

Inicio de la alianza: acordar un enfoque de gestión de riesgos de seguridad

Poco después de establecer una alianza o, si es factible y apropiado, antes de firmar el contrato, las organizaciones deben tratar de acordar cómo cada socio puede apoyar al otro en las cuestiones relacionadas con la seguridad que surjan en la alianza y en la ejecución del programa.

La guía del GISF *Partenariados y gestión de riesgos de seguridad* proporciona una lista de preguntas que pueden servir de apoyo a estas conversaciones y ofrece algunas ideas sobre la gestión conjunta de riesgos de seguridad entre socios. En la tabla 3 se resumen las preguntas clave.

Tabla 3 Preguntas preliminares sobre gestión de riesgos de seguridad

Ámbito	Preguntas
Deber de cuidado	• ¿Cuáles son las respectivas obligaciones jurídicas y éticas del deber de cuidado de cada socio? • ¿Se explican claramente en la documentación de la alianza?
Gobernanza y rendición de cuentas	• ¿Han contribuido ambos socios en las oportunidades clave de toma de decisiones sobre el programa, el proyecto, la alianza y/o la seguridad? • ¿Disponen ambos socios de estructuras adecuadas de gestión de riesgos de seguridad (incluidas funciones y responsabilidades) que permitan cumplir los objetivos de la alianza? • ¿Se mencionan en el acuerdo de la alianza los riesgos de seguridad y su gestión? • ¿Pueden los socios apoyarse mutuamente, por ejemplo, mediante la selección de personal de seguridad especializado?

Ámbito	Preguntas
Transferencia de riesgos	• ¿Cómo perciben las partes interesadas pertinentes a cada socio? • ¿Podría la identidad organizativa de un socio afectar al otro socio? • ¿Supone la alianza nuevas amenazas para alguna de las dos organizaciones? • ¿Cambia la alianza el impacto o la probabilidad de alguna amenaza? En caso afirmativo, ¿es positivo o negativo? • A la hora de explorar medidas de mitigación, ¿puede una de las organizaciones adoptar medidas concretas para reducir el riesgo al que se enfrenta su socio? • En entornos conflictivos, ¿cómo interactúa la alianza con las dinámicas del conflicto? y ¿pueden adoptarse medidas para ser más sensibles al conflicto?
Políticas y principios	• ¿Comprenden ambos socios el mandato, la misión, los valores y los principios de cada organización? ¿Se sienten cómodas ambas organizaciones con el trabajo y el enfoque de las operaciones y la seguridad de la otra (por ejemplo, están de acuerdo ambos socios con la postura del otro en cuanto a principios humanitarios y salvaguardia)?
Operaciones y programas	• ¿Cuáles son las necesidades y las expectativas de seguridad de cada socio? • ¿Disponen los socios de un sistema acordado para detectar y supervisar los riesgos de seguridad a los que se enfrenta el personal? • ¿Disponen los socios de referentes de seguridad que puedan hablar entre sí sobre cuestiones de seguridad? • ¿Están de acuerdo los socios sobre quién es responsable de gestionar los riesgos detectados y cómo deben gestionarse y financiarse estos puestos? • ¿Existe un sistema para que ambos socios estén informados de los riesgos de seguridad y de los cambios en el entorno del riesgo (físico y en línea)? • ¿Dispone cada socio de recursos suficientes (por ejemplo, financiación, tiempo y personal) para gestionar los riesgos de seguridad?
Enfoques inclusivos de gestión de riesgos de seguridad	• El enfoque de la gestión de riesgos de seguridad de ambas organizaciones, ¿tiene en cuenta cómo la identidad de los miembros del personal puede afectar su vulnerabilidad ante las amenazas? • ¿Cómo deben tratar los socios los temas sensibles relacionados con la identidad, como las amenazas internas y externas por motivos de orientación sexual o género? ¿Cuáles son los niveles de comodidad (teniendo en cuenta las sensibilidades culturales)? • ¿Cómo pueden los socios apoyarse mutuamente para salir de su zona de comodidad y garantizar una gestión de riesgos de seguridad eficaz para todo el personal?

Ámbito	Preguntas
Amenazas internas y salvaguardia	• ¿Cómo gestionarán los socios las amenazas a la seguridad que puedan surgir dentro de sus propias organizaciones? • ¿Cómo se abordan los problemas de salvaguardia en la alianza? • ¿Existen mecanismos de reporte de incidentes de salvaguardia adecuados?
Viajes	• ¿Cómo deben gestionarse los riesgos de seguridad que se deriven de los viajes relacionados con la alianza?
Concienciación e intercambio de capacidades	• ¿Cómo identificarán los socios las necesidades de concienciación y de fortalecimiento de las capacidades de seguridad y cómo las abordarán conjuntamente (tanto en términos de seguridad personal como de gestión de riesgos de seguridad)? • ¿Puede el personal de seguridad de uno de los socios ofrecer asesoramiento, tutoría y apoyo técnico a los referentes de seguridad de la otra organización, si es necesario? • ¿Puede el personal del socio acceder a una capacitación en seguridad adecuada (interna y externa a las organizaciones socias)?
Monitoreo de incidentes	• ¿Cómo deben los socios compartir entre sí la información sobre incidentes?
Gestión de incidentes y crisis	• ¿Cómo colaborarán o se coordinarán los socios si se produce una crisis o un incidente crítico que afecte a cualquiera de las dos organizaciones en el lugar en el que actúa la alianza?
Cuidado del personal	• ¿Tienen ambos socios acceso a pólizas de seguro pertinentes? Si no es así, ¿puede uno de los socios ayudar al otro a acceder al seguro pertinente? • ¿Disponen ambos socios de políticas y procedimientos de cuidado del personal que incluyan atención médica, de salud mental y posterior a incidentes? • ¿Pueden los socios apoyarse mutuamente con recursos y actividades pertinentes destinados al cuidado del personal (como realizar cambios en la alianza para mejorar el bienestar del personal, por ejemplo, reduciendo la carga de trabajo, incorporando horarios de trabajo flexibles y reduciendo las expectativas administrativas)?
Redes y colaboración de seguridad	• ¿Existen plataformas en el contexto pertinente en las que se debatan cuestiones de seguridad? En caso afirmativo, ¿tienen ambos socios acceso y la misma capacidad para expresarse en estas plataformas y redes en sus áreas operacionales, incluidas las plataformas de intercambio de información sobre seguridad? • ¿Puede mejorarse el acceso de alguno de los socios a los mecanismos de coordinación existentes?

Ámbito	Preguntas
Monitoreo del cumplimiento y la eficacia	• ¿Cómo deben revisar ambos socios las medidas de gestión de riesgos de seguridad durante la alianza?
Recursos	• Los socios, ¿han intercambiado entre ellos sus respectivos recursos de gestión de riesgos de seguridad? • ¿Puede mejorarse el acceso a los recursos existentes para alguno de los socios?
Fin de la alianza	• ¿Tendrá consecuencias para la seguridad de alguno de los socios el hecho de poner fin a la alianza conforme al contrato (y el calendario financiero)? En caso afirmativo, ¿cómo debe abordarse este problema?

Adaptado de GISF (2021) *Partenariados y gestión de riesgos de seguridad: Guía de acción conjunta para organizaciones de ayuda locales e internacionales* (<https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/>).

Por último, para que una alianza sea equitativa, es crucial que ambos socios comprendan claramente la actitud y la tolerancia al riesgo de la otra parte. Los socios se benefician de debatir abiertamente sus respectivos apetitos de riesgo y de encontrar formas de armonizarlos cuando existen grandes diferencias, que pueden ser bastante marcadas en muchos de los contextos en los que se ejecutan los programas humanitarios. Lo ideal sería que la actitud de cada socio ante el riesgo se debatiera al inicio de la alianza y se revisara periódicamente mientras esta siga vigente (lo que podría coincidir con el calendario de hitos de la alianza). En algunos casos, quizás no se pueda llegar a un acuerdo sobre los umbrales de riesgo o no se puedan mitigar los riesgos adecuadamente, y esto puede informar debates más estratégicos sobre si la alianza debe seguir adelante o si debe modificarse el trabajo programático.

► Para obtener más información sobre los umbrales de riesgo y la criticidad de los programas, véase el capítulo 1.1.

Durante las alianzas: detectar y abordar necesidades, carencias y retos

Reforzar la comunicación y hacer operativos los principios

Se puede trabajar proactivamente para mejorar la comunicación entre los socios. Esto puede significar garantizar que las personas adecuadas estén en la cadena de comunicación (que normalmente debería incluir a los referentes de seguridad designados de cada socio), que la frecuencia y el método de comunicación sean los más apropiados y convenientes para ambos socios, que la comunicación sea transparente, honesta y clara y que el personal se adhiera a los principios clave, que tienen por objeto abordar y superar los sesgos inherentes y fomentar la confianza.

Principios de partenariado

Para que las alianzas sean más equitativas, eficaces y seguras, el personal encargado de establecerlas y mantenerlas puede tener en cuenta los principios básicos de buenas prácticas que se mencionan a continuación.

- **Equidad:** los socios tienen los mismos derechos, independientemente de cualquier desequilibrio de poder.
- **Transparencia:** existe una interacción abierta y honesta entre los socios.
- **Beneficio mutuo:** ambos socios deben beneficiarse de la alianza, idealmente esto supera el simple cumplimiento de los objetivos.
- **Complementariedad:** cada socio aporta a la alianza sus propias fortalezas y debilidades, se complementan y reconocen que la diversidad puede ser una ventaja.
- **Enfoque hacia los resultados:** las acciones que se esperan de los socios deben ser realistas y deben centrarse en los resultados.
- **Responsabilidad:** los socios deben asumir la responsabilidad de sus acciones y evitar comprometerse o prometer en exceso.

Fuente: Global Interagency Security Forum (2021) *Partenariados y gestión de riesgos de seguridad: Guía de acción conjunta para organizaciones de ayuda locales e internacionales* (<https://gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/>).

Ejemplo: Compartir riesgos en la práctica

Una ONG local nigeriana solicitó a sus socios, dos ONG internacionales, financiación para contratar a un agente de seguridad. Además de acordar la financiación de dos nuevos puestos de seguridad en la ONG local, el personal de seguridad de los socios internacionales apoyó el proceso de selección y proporcionó al personal nuevo formación inicial, apoyo quincenal y reuniones mensuales de puesta al día. Al debatir las ventajas y los retos, el personal de seguridad de las ONG internacionales que participó en el proceso coincidió en que la implicación de todos los socios era esencial y garantizaba que la titularidad de las funciones y las decisiones en materia de seguridad siguiera correspondiendo a cada organización. Coincidieron en que, para compartir el riesgo de forma eficaz, un reto fundamental es garantizar que el personal de seguridad de las ONG internacionales tenga la capacidad de establecer relaciones y proporcionar el nivel adecuado de tutoría a los referentes de seguridad de las ONG locales.

Fuente: Christian Blind Mission y Sight Savers International (2022) *Sharing risk – a good practice example in the INGO sector* (www.gisf.ngo/resource/sharing-risk-a-good-practice-example-in-the-ingo-sector/).

Diagnósticos de riesgos conjuntos y planes de seguridad adaptados

Aunque todavía son poco frecuentes en el sector humanitario, los diagnósticos de riesgos conjuntos de las actividades del programa proporcionan a los socios una imagen clara de los riesgos probables y permiten al socio en la ejecución (y a su personal) expresar sus preocupaciones antes de llevar a cabo el trabajo. Un diagnóstico de riesgos conjunto también permite un mayor debate sobre las posibles medidas de mitigación y las formas en que cada socio puede apoyar al otro para satisfacer las necesidades de seguridad y los objetivos programáticos. Este proceso permite entablar debates más claros sobre la propiedad del riesgo y las responsabilidades dentro de la alianza, así como establecer expectativas claras desde el principio sobre lo que cada organización puede aportar a la alianza. También es aconsejable realizar periódicamente una revisión conjunta de la evolución del panorama de riesgos. El ejercicio puede ser una oportunidad para que los socios se beneficien de la exposición a las perspectivas de la otra organización y ayuda a identificar dónde puede ser necesario realizar adaptaciones. Por ejemplo, esto podría incluir la conciliación del énfasis de una organización en la documentación y las políticas escritas con la dependencia de la otra en la comunicación verbal.

En función de las circunstancias, este diagnóstico de riesgos conjunto puede culminar en protocolos de seguridad compartidos. Como mínimo, estos diagnósticos deben servir para informar los planes y los procedimientos de seguridad de cada organización. La comunicación periódica entre los socios puede ayudar a abordar rápidamente los problemas de seguridad.

Los socios deben estar preparados para las crisis y los incidentes críticos y deberían acordar de antemano la mejor manera de gestionarlos. Asimismo, pueden considerar qué organización estaría en mejores condiciones para responder si se produce una crisis o un incidente crítico (por ejemplo, logística, acceso y conocimientos especializados). Por lo general, cualquier ayuda que se preste en estas circunstancias deberá decidirse a nivel estratégico, teniendo en cuenta las implicaciones jurídicas y financieras pertinentes. Sin embargo, ser reactivo al riesgo en este sentido puede no ser necesariamente la mejor opción, ya que el costo reputacional de no prestar apoyo durante un acontecimiento de este tipo (en el que una intervención sería beneficiosa y no causaría más daño que beneficio) puede ser más perjudicial que la posibilidad de incurrir en una responsabilidad legal. Una organización internacional que ha reconocido este hecho ha adoptado medidas proactivas para ayudar a sus socios locales a obtener los seguros pertinentes, algo que puede resultar muy difícil para las organizaciones locales.

Ejemplo: Gestión de riesgos de seguridad en las alianzas

Una organización internacional ha puesto en marcha varias iniciativas para abordar mejor los problemas y las necesidades de gestión de riesgos de seguridad cuando trabaja con socios. Entre ellas figuran las siguientes:

- Aumentar la participación del personal de seguridad en las interacciones con los socios desde las primeras conversaciones.
- Sensibilizar al personal de seguridad sobre lo que significa el partenariado y cómo trabajar juntos para obtener resultados comunes de forma segura.
- Crear (y a veces cocrear) y compartir orientaciones, incluyendo herramientas.
- Ofrecer un “menú” de capacitación a los socios.
- Aumentar la cantidad de miembros del personal del socio en las sesiones de capacitación en seguridad de la organización.
- Apoyar a los socios en la gestión de incidentes (en la forma de asesoramiento técnico).

Compartir la capacidad

Los socios aportan sus propios conocimientos y fortalezas a una alianza, y un debate sobre ellos, así como sobre los puntos débiles y las deficiencias, puede sentar las bases de un acuerdo más sólido y beneficioso para ambas partes. Las diferencias de enfoque no deben considerarse una falta de capacidad. Los socios deben tratar de llegar a un acuerdo sobre las necesidades más urgentes en materia de apoyo, por ejemplo, capacitación en seguridad, y sobre los formatos más funcionales. Una organización internacional creó un sitio web en línea al que pueden acceder sus socios para recibir formación sobre temas concretos, incluidos los relacionados con la seguridad. Otras organizaciones también han promovido plataformas y formación en línea con sus socios. Algunas organizaciones internacionales han diseñado cursos de capacitación en seguridad específicos para sus socios locales, mientras que otras los invitan a participar en los cursos que imparten a su propio personal. Es importante que todo el fortalecimiento de capacidades sea pertinente y beneficioso para cada socio, acordado conjuntamente según sea necesario y que sea sostenible, para poder apoyar la capacidad a largo plazo del personal y las organizaciones.

► *Para obtener más información sobre capacitación en seguridad, véase el capítulo 5.2.*

Financiación

Los socios deben tratar de discutir los costos de seguridad lo antes posible, incluida la financiación necesaria para reforzar los sistemas de seguridad internos. Por lo general, los presupuestos de las alianzas deben contener partidas presupuestarias relativas a la seguridad, mientras que los socios pueden garantizar la adecuación de los requisitos de los costos de seguridad a los riesgos de seguridad diagnosticados. Las necesidades de financiación a largo plazo también deben considerarse y debatirse en el marco de la alianza, como la financiación de la capacitación y la cobertura del seguro médico y contra daños causados por actos intencionales para el personal que corre mayores riesgos. Los socios internacionales pueden abogar ante los donantes por una financiación adecuada para sus socios en la ejecución, mientras que los propios donantes pueden exigir una mayor consideración de las necesidades de seguridad de los socios en la ejecución.

► *Para obtener más información sobre la financiación de la seguridad, véase el capítulo 3.3.*

Intercambio de recursos

En una alianza, los socios se benefician de intercambiar proactivamente recursos e información sobre gestión de riesgos de seguridad. Los socios en la ejecución pueden tener un mayor conocimiento de las condiciones de seguridad locales, que pueden compartir, mientras que los socios internacionales pueden tener un mayor acceso a los mecanismos de coordinación e intercambio de información, a los que pueden facilitar el acceso. Aunque a menudo esto se hace informalmente, lo ideal sería que los recursos de seguridad se compartieran de forma activa y periódica, estuvieran disponibles en línea y fuera de línea (en diversos formatos, siempre que sea posible) y se tradujeran a los idiomas pertinentes. Los socios pueden apoyarse mutuamente para participar en redes de seguridad y foros de intercambio de información a nivel local, nacional, regional e internacional.

Ejemplo: Mecanismos de coordinación de seguridad

Los actores locales están muy infrarrepresentados en los mecanismos de coordinación dirigidos por los agentes humanitarios internacionales. A menudo, los actores locales desconocen los mecanismos o no participan debido a obstáculos como la ubicación y el idioma. Organizaciones como la INSO están adoptando medidas para solucionar este problema, ofreciendo la afiliación a ONG nacionales registradas y permitiendo así a estos actores el acceso libre a mecanismos para hacer contactos, intercambiar información y capacitarse. Sin embargo, los agentes humanitarios locales no registrados siguen teniendo grandes dificultades para unirse a las redes.

Incidencia y alianzas

Las alianzas presentan tanto oportunidades como riesgos en lo que respecta a la incidencia. Las iniciativas conjuntas de incidencia entre los socios pueden contribuir a amplificar el mensaje, lo que puede ser útil para la incidencia relativa a la gestión de riesgos de seguridad (por ejemplo, los socios internacionales que abogan ante los Gobiernos donantes por una mayor financiación de la seguridad para los actores locales). Sin embargo, la labor de incidencia de una organización puede presentar riesgos de seguridad para sus socios, por ejemplo, cuando un Gobierno local responsabiliza a los socios locales en el país de los esfuerzos de incidencia de un socio internacional hacia él. Es una buena práctica considerar el impacto que pueden tener las iniciativas de incidencia fuera de la organización, especialmente en los socios, antes de emprenderlas. Una organización internacional en Myanmar ha debatido activamente los mensajes de incidencia con sus socios en la ejecución antes de difundirlos, con el fin de cerciorarse de que sus socios no solo están informados al respecto, sino también que pueden debatir sobre las posibles consecuencias de estos mensajes y las medidas de mitigación necesarias.

► Para obtener más información, véase el capítulo 2.2 sobre incidencia y seguridad.

Más información

Investigación y análisis

Christian Blind Mission y Sight Savers International. (2022). *Sharing risk – a good practice example in the INGO sector* (www.gisf.ngo/resource/sharing-risk-a-good-practice-example-in-the-ingo-sector/).

Foro Europeo Interinstitucional para la Seguridad. (2012). *Security management and capacity development: international agencies working with local partners* (<https://gisfprod.wpengine.com/resource/international-agencies-working-with-local-partners/>).

Global Interagency Security Forum. (2020). *Partenariado y gestión de riesgos para la seguridad: desde la perspectiva de la coparte local* (www.gisf.ngo/resource/partnerships-and-security-risk-management-from-the-local-partners-perspective/).

Global Interagency Security Forum y Humanitarian Outcomes. (2024). *State of practice: the evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Humanitarian Outcomes. (2019). *NGOs & risk: managing uncertainty in local-International partnerships (global report)* (www.humanitarianoutcomes.org/publications/ngos-risk2-partnerships).

Kemp, E. y Merkelbach, M. (2016). *Duty of care: a review of the Dennis v Norwegian Refugee Council ruling and its implications*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

Orientación y recursos

Global Database of Humanitarian Organisations (s.f.) (<https://humanitarianoutcomes.org/projects/gdho>).

Global Interagency Security Forum. (2021). *Partenariados y gestión de riesgos de seguridad: Guía de acción conjunta para organizaciones de ayuda locales e internacionales* (www.gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/).

4 Elementos operativos: procesos y herramientas

4.1 Elementos analíticos

Una buena gestión de riesgos de seguridad se basa en un análisis sólido, y las buenas prácticas sostienen que las organizaciones operan con mayor eficacia y seguridad cuando evalúan sistemáticamente los riesgos. Este capítulo trata de las metodologías y las herramientas utilizadas para llevar a cabo un análisis de riesgos exhaustivo, que sirva de base para una toma de decisiones y una planificación estratégica informadas. Subraya la importancia de la comprensión del contexto, reforzada por el análisis basado en datos, para desarrollar medidas sólidas de mitigación de riesgos de seguridad.

Los análisis del contexto y de los riesgos no son una ciencia exacta. Más bien, son un medio para ayudar a las organizaciones a comprender mejor y tomar mejores decisiones, definiendo las preguntas clave que deben plantearse.

4.1.1 Descripción general

Abajo se enumeran los pasos básicos de un proceso analítico que el personal de seguridad y de programas ha considerado útil (véase también la figura 7). Las actividades específicas realizadas en cada paso, que se detallan en las secciones siguientes, pueden variar en complejidad y sofisticación de una organización a otra, en función de su capacidad y recursos. Es importante recordar que no existe un modelo universal y que el más adecuado es el que el personal de todos los niveles comprende fácilmente y aplica consistentemente. En general, las organizaciones que optan por la simplicidad frente a la complejidad tienen más posibilidades de que el personal utilice sus herramientas.

Primer paso: Contexto, amenazas y análisis de vulnerabilidad

- **Análisis del macrocontexto.** Examinar el contexto más amplio en el que tendrá lugar la programación, las dinámicas del conflicto (si procede) y los actores principales.
- **Análisis interno.** Revisar los objetivos del programa de la organización, las prioridades, las estructuras, la presencia geográfica del personal, las capacidades de gestión de riesgos de seguridad y las modalidades operacionales.
- **Detección de amenazas.** Detectar los posibles peligros para los activos básicos de la organización (es decir, las personas), los programas, los procesos, los bienes y la reputación.
- **Vulnerabilidades.** Detectar las vulnerabilidades específicas (y las fortalezas) de la organización y su personal en relación con su programación y nivel de aceptación en la zona.

Segundo paso: Detección y evaluación de riesgos (diagnóstico de riesgos)

- **Detección de riesgos.** Enumerar los riesgos posibles de trabajar en el contexto a partir de las amenazas detectadas y las vulnerabilidades específicas de la organización y su personal.
- **Análisis y diagnóstico de riesgos.** Analizar la probabilidad y las posibles repercusiones de los riesgos detectados. Clasificarlos en consecuencia, de bajo a alto, para determinar las prioridades de las medidas de mitigación y la planificación de la gestión.

Tercer paso: Mitigación de riesgos y planificación de la gestión

- **Mitigar los riesgos detectados.** Determinar las medidas necesarias para reducir la probabilidad y/o las repercusiones de cada uno de los riesgos. Estas suelen estar influenciadas por la estrategia de seguridad de la organización (*analizada en el capítulo 4.2*).
- **Abordar el riesgo residual.** Reflexionar sobre cualquier riesgo residual que pueda quedar después de aplicar todas las medidas de mitigación. Decidir si se acepta, se evita o se comparte. Esto se basará en los objetivos de la organización, el apetito de riesgo y la criticidad del programa.

Cuarto paso: Monitoreo y revisión

- **Monitoreo y revisión.** Controlar, revisar y adaptar continuamente el diagnóstico de riesgos según sea necesario para garantizar que sigue siendo pertinente y eficaz.

Este proceso puede documentarse y formar parte de los planes de seguridad.

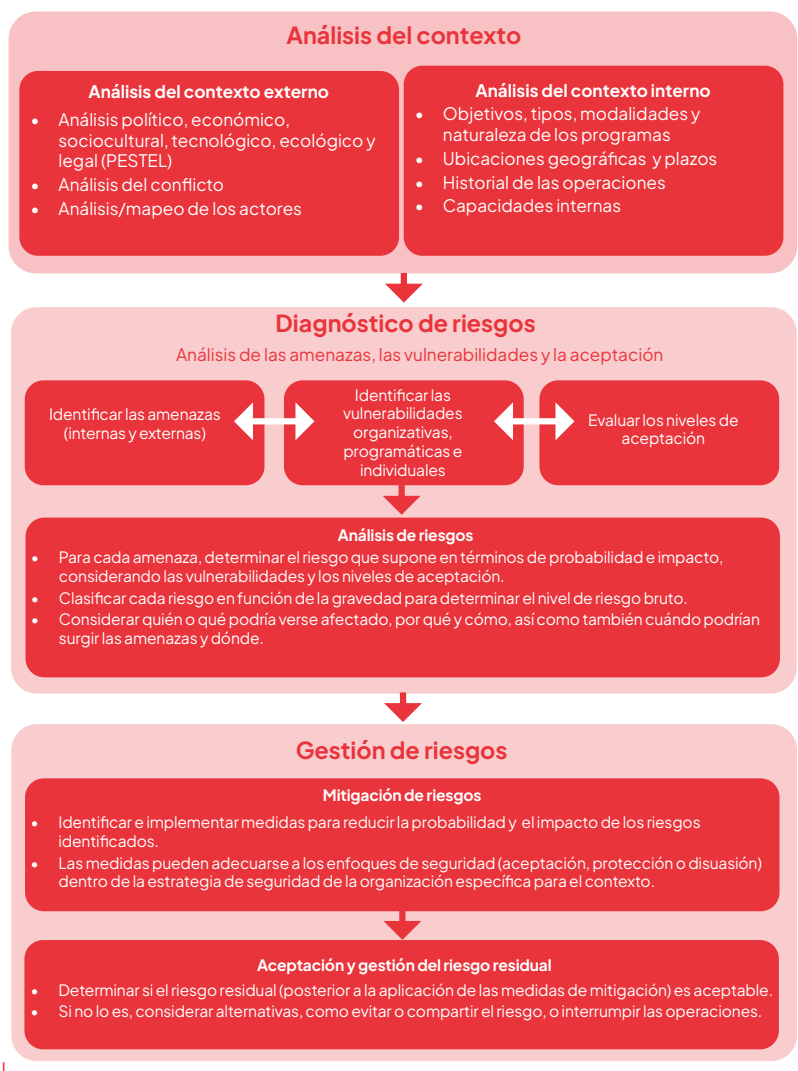
► *Para obtener más información sobre los planes de seguridad, véase el capítulo 4.3.*

Para apoyar este proceso, es esencial comunicar continuamente los riesgos, las medidas de mitigación y su impacto operacional a todas las partes interesadas, al tiempo que se mantiene informado al personal de los cambios en materia de seguridad y se recaba la opinión de las partes interesadas. También es importante evaluar y actualizar periódicamente el enfoque de seguridad de la organización, para garantizar que sigue siendo pertinente, que refleja las buenas prácticas y que apoya la capacidad de la organización para cumplir sus objetivos en medio de condiciones cambiantes.

► *Para obtener más información sobre la comunicación con el personal, véase el capítulo 5.3.*

► *Para obtener más información sobre el monitoreo de la eficacia, véase el capítulo 3.4.*

Figura 7 Proceso analítico



Consultar, compartir, evaluar, mejorar y actualizar según sea necesario.

Es importante adoptar un enfoque sistemático en el diagnóstico de riesgos porque, aunque la experiencia y la intuición pueden desempeñar un papel fundamental a la hora de comprender y responder a los riesgos, no es aconsejable depender únicamente del instinto. Las experiencias aisladas de las personas, los sesgos invisibles, las percepciones individuales y otros factores subjetivos a menudo pueden distorsionar la visión. En concreto, la gente tiende a exagerar los riesgos raros y espectaculares y a restar importancia a los frecuentes, a reaccionar de forma exagerada ante las amenazas inmediatas y a descartar los peligros a largo plazo, y a responder rápidamente a los cambios drásticos, pero a adaptarse lentamente a los cambios graduales (el síndrome de la “rana hervida”). También pueden tener dificultades para evaluar riesgos desconocidos y sobrestimar peligros ampliamente discutidos.

Un enfoque estructurado y disciplinado puede ayudar a separar los hechos de las percepciones y las emociones, lo que permite que el analista absorba más información para obtener una imagen más completa. También puede ayudar a los equipos a llegar a un consenso basado en las pruebas disponibles. La(s) persona(s) que dirige(n) o coordina(n) el proceso de diagnóstico de riesgos, normalmente el personal de seguridad, debe(n) tratar de garantizar la inclusividad. Ello implica recabar puntos de vista e información de todo el personal y considerar los riesgos desde distintos ángulos. Este enfoque fomenta una comprensión común de los riesgos y una responsabilidad compartida de las medidas de protección. Un ejemplo sería un taller de diagnóstico de riesgos en el que personas con diversas funciones y perfiles individuales se reúnen para debatir las amenazas y las vulnerabilidades que experimentan personalmente.

Además de permitir una mejor comprensión de los riesgos como base para la toma de decisiones, un diagnóstico de riesgos bien documentado puede servir como una importante herramienta de gestión para hacer un seguimiento de los cambios en el entorno operacional y proporcionar una justificación clara para la inversión en seguridad. También puede proporcionar un indicador clave de rendimiento para las actividades del programa, ya que confirma que se están detectando y gestionando los riesgos durante la ejecución.

4.1.2 Análisis del contexto, las amenazas y la vulnerabilidad

Análisis del contexto externo

Marco PESTEL

El análisis del contexto externo suele comenzar con el examen de los factores que configuran el entorno de las operaciones. Adoptar el marco PESTEL puede ser una herramienta útil para ello. En la práctica, esto implica evaluar sistemáticamente cada categoría para determinar los riesgos y las oportunidades relevantes y cómo pueden afectar a la organización y a su personal. Las categorías son las siguientes.

- **Política.** El entorno político, la estabilidad del Gobierno, la dinámica de los conflictos, los principales titulares y contendientes del poder, la violencia política y las políticas gubernamentales.
- **Económica.** Pobreza, inflación, tasas de empleo, estabilidad monetaria, crecimiento económico y desigualdad.
- **Sociocultural.** Tendencias demográficas, índices de criminalidad, actitudes de la comunidad, normas, relaciones de género y dinámicas intergrupales que pueden influir en la aceptación y en los riesgos basados en la identidad. Esto puede incluir la historia de la asistencia humanitaria en la zona y la manera en que la población local ha percibido a la comunidad humanitaria y a la organización (si procede).
- **Tecnológica.** Tecnología, seguridad digital y estabilidad de las infraestructuras, incluida la cobertura de telefonía móvil e Internet, la alfabetización digital y las limitaciones tecnológicas.
- **Ecológica.** Fenómenos climáticos y peligros naturales, escasez de recursos, y competencia y normativa medioambiental.
- **Legal.** Leyes y normas relacionadas con las operaciones humanitarias, incluida la legislación laboral y los requisitos de cumplimiento. Esto puede abarcar el impacto de factores jurídicos en los riesgos basados en la identidad.

Gracias a este marco, los equipos pueden evaluar mejor cómo interactúan los factores externos e influyen en sus operaciones, lo que les permite realizar esfuerzos más informados de mitigación de riesgos.

Análisis de conflictos

Además del marco PESTEL, un análisis más detallado de los conflictos y la violencia puede ayudar a esclarecer las fuentes de amenazas en los lugares donde hay conflictos armados. Un buen análisis de los conflictos no se centra únicamente en los lugares donde la violencia es visible. La violencia puede ir precedida de tensiones menos evidentes: las “divisiones profundas” y las “líneas divisorias” de una sociedad. Esto también debe explorarse y comprenderse. A veces se entrecruzan múltiples conflictos. Las tensiones y los estallidos de violencia en Irak, por ejemplo, pueden girar en torno a la dinámica suní-chií, la influencia del ISIS, la competencia por los recursos, las tensiones kurdo-árabes o el legado de la invasión estadounidense. Todos y cada uno de ellos pueden ser una fuente de amenazas.

Varios marcos pueden servir de apoyo al análisis de conflictos. Sin embargo, este análisis no tiene por qué ser excesivamente complejo y puede centrarse en responder a algunas preguntas clave, como las siguientes.

- **¿Cuáles son las causas visibles y subyacentes del conflicto?**
 - ¿Existen divisiones o injusticias profundamente arraigadas que provoquen tensiones (por ejemplo, económicas, políticas, sociales, históricas)?
 - ¿Cómo contribuyen al conflicto las estructuras políticas, los sistemas de gobernanza y las condiciones económicas? ¿Existen instituciones que perpetúan la exclusión o la desigualdad?
- **¿Quiénes son los principales actores y partes interesadas y cuáles son sus intereses?**
 - ¿Cómo configuran el conflicto las dinámicas de poder y las relaciones entre estos actores?
 - ¿Qué papel desempeñan las instituciones externas en la dinámica de los conflictos (por ejemplo, Gobiernos extranjeros y organismos internacionales)?
- **¿Cuáles son los posibles riesgos y factores de división que contribuyen a la escalada del conflicto?**
 - ¿Existen acontecimientos o factores desencadenantes específicos que pueden empeorar la situación?
 - ¿Cuáles son las señales de alarma de una posible escalada?
- **¿Qué conectores u oportunidades de consolidación de la paz existen?**
 - ¿Existen intereses compartidos, lazos culturales o mecanismos locales que pueden reducir las tensiones?
 - ¿Qué oportunidades existen para consolidar la paz o mitigar los conflictos mediante la colaboración con los actores locales?
- **¿Qué impacto podrían tener las intervenciones de la organización en el conflicto?**
 - ¿Podrían las acciones de la organización avivar involuntariamente las tensiones y cómo puede el personal garantizar la sensibilidad al conflicto?
 - ¿Cómo puede la organización mantenerse flexible y reaccionar ante los cambios en el entorno del conflicto, como alianzas nuevas o acciones violentas inesperadas?

Una buena práctica consiste en actualizar periódicamente el análisis del conflicto para reflejar los cambios en la situación, lo que garantiza que las estrategias sigan siendo pertinentes y respondan a los cambios en las dinámicas del conflicto.

Análisis de actores

El análisis o mapeo de los actores se centra en los principales individuos y grupos que pueden afectar la seguridad de una organización y su personal, incluidos los propios miembros del personal. Para mantener su pertinencia, este análisis debe ser continuo, y es probable que al principio arroje más preguntas que respuestas. Se trata de un ejercicio exploratorio que puede realizarse en tres etapas:

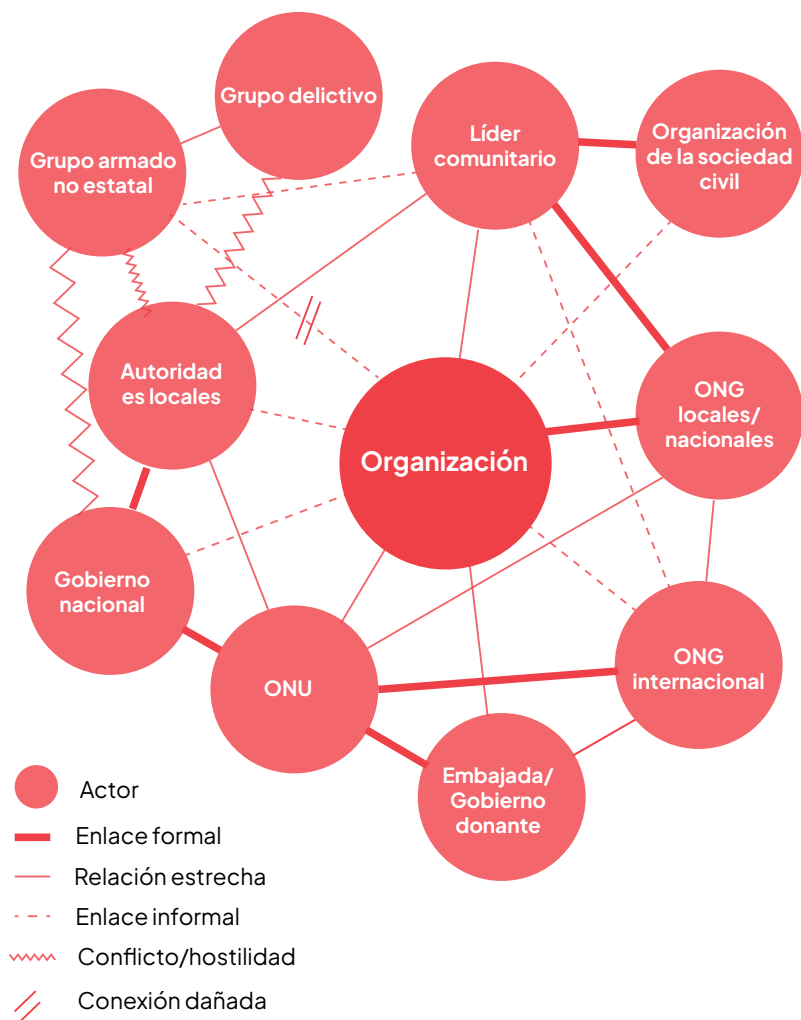
- determinar y enumerar a todos los actores pertinentes;
- comprender sus identidades, motivos, objetivos y posiciones políticas y sociales, y
- analizar sus relaciones mutuas.

En una situación de conflicto, los actores pertinentes serían los grupos armados y los actores nacionales e internacionales que participan en el conflicto o intentan influir en él (incluidas las fuerzas de mantenimiento de la paz). Entre los actores locales también pueden figurar empresarios, grupos de estudiantes, sindicatos, terratenientes, facciones de militantes religiosos o nacionalistas, medios de comunicación locales, organizaciones locales y líderes tradicionales. Los posibles actores regionales e internacionales relevantes podrían ser las potencias vecinas, las organizaciones intergubernamentales, las empresas transnacionales, los diplomáticos, las organizaciones de derechos humanos y los grupos de la diáspora.

Las interacciones entre los distintos actores pueden ilustrarse con líneas trazadas entre ellos, que representan diferentes relaciones, por ejemplo, ¿quién lucha, coopera o compite con quién? y ¿qué grupos financian o dirigen a qué otros grupos? Una matriz puede ayudar al personal a visualizar las relaciones, actualizadas a medida que cambia la dinámica (véase la figura 8). Las relaciones pueden clasificarse, por ejemplo, en “aliadas”, “amigas”, “enemigas”, “complicadas” o “en desarrollo”. Diferentes personas pueden interpretar de diferente manera estas relaciones, lo que debe tenerse en cuenta en la elaboración de la matriz. Este ejercicio también puede ser una herramienta útil para informar al personal recién incorporado. A medida que se profundiza en el análisis, puede resultar evidente que los grupos no son tan homogéneos como parecían en un principio.

Los posibles actores que representan una amenaza y que deben tenerse en cuenta en el análisis incluyen grupos armados no estatales, actores delictivos, actores económicos y actores gubernamentales. Es importante reconocer que estas etiquetas no siempre se aplican con distinciones tajantes; los grupos pueden solaparse en cuanto a objetivos y motivaciones, y los actores que representan una amenaza pueden cambiar con el tiempo.

Figura 8 Ejemplo simplificado de mapeo de los actores



Grupos armados

Los grupos armados pueden englobar un gran número de entidades con diferentes identidades, motivos e intenciones; entre ellos, grupos extremistas, grupos delictivos organizados y grupos rebeldes con motivaciones políticas que luchan contra un Gobierno. Es de vital importancia comprender a los grupos armados para entender cómo y por qué la presencia y los programas de una organización pueden verse manipulados o amenazados. En función de su dinámica de poder y de su ideología, los grupos armados pueden ver a las organizaciones humanitarias como amenazas, objetivos indirectos, herramientas políticas o fuentes de recursos que explotar. Una vez más, es posible que las percepciones solo lleguen gradualmente. Respecto a cada grupo armado identificable, las organizaciones podrían evaluar los aspectos que se mencionan a continuación.

- Estructura de mando y control: ¿Qué tan organizados y cohesionados están los líderes y los combatientes?
- Puntos de contacto: ¿Quiénes son las personas adecuadas para la comunicación o la negociación?
- Ideología y visión del mundo: ¿Cuáles son sus actitudes, creencias y objetivos, si se conocen?
- Declaraciones públicas: ¿Han hecho algún comentario sobre las operaciones o las organizaciones humanitarias?
- Acciones pasadas: ¿Qué han hecho y cómo lo han justificado?
- Símbolos o mitología: ¿Utilizan algún símbolo o narrativa distintivos?
- Relación con la población local: ¿Son grupos internos o externos? ¿Gobiernan o prestan servicios? Cuanto más abusivos sean con los civiles, mayor será el peligro potencial para las organizaciones humanitarias.

► *Para obtener más información sobre cómo dialogar con los actores armados, véanse los capítulos 2.1 y 4.2.*

Actores delictivos

Los actores delictivos pueden considerar a las organizaciones humanitarias como objetivos lucrativos de extorsión, hurto o secuestro extorsivo, o como obstáculos para sus operaciones. Para comprender mejor a estos actores, las organizaciones pueden considerar los aspectos que se mencionan a continuación.

- Estructura organizativa y jerarquía: ¿Quiénes son los líderes y los miembros principales?
- Motivaciones y objetivos: ¿Están motivados por el beneficio económico, el control territorial o las actividades ilícitas?
- Tácticas: ¿Qué métodos utilizan (por ejemplo, extorsión, secuestro, delitos cibernéticos)?

- Relaciones: ¿Cómo interactúan con las autoridades locales y las comunidades?
- Incidentes pasados: ¿Qué pautas de comportamiento existen, especialmente hacia los activos y los trabajadores humanitarios?
- Impacto: ¿Cuáles son los efectos económicos y sociales de sus actividades en la economía y en la sociedad locales?
- Canales de comunicación: ¿Existen interlocutores potenciales para la negociación, en caso necesario?

Actores de la economía de guerra

Muchos conflictos modernos han sido impulsados por “economías de guerra”, que incluyen el comercio ilegal y cuasilegal de armas, drogas, diamantes, petróleo, minerales y otros materiales. En las zonas donde existen economías de guerra, las organizaciones humanitarias podrían examinar los siguientes aspectos.

- Importancia de los recursos: ¿Hasta qué punto son cruciales los recursos locales para la economía de guerra? ¿Son limitados los recursos alternativos (lo que hace que las organizaciones humanitarias sean más importantes y vulnerables)?
- Sensibilidad geográfica: ¿Es importante la zona por sus recursos naturales o sus rutas comerciales estratégicas?
- Impacto en el reclutamiento: ¿Ofrecen los programas humanitarios medios de subsistencia alternativos que puedan afectar el reclutamiento por parte de los grupos armados o empresas delictivas?
- Impacto económico de la ayuda: La ayuda, ¿genera tensiones o dependencias que los actores del conflicto podrían explotar?
- Impacto medioambiental: ¿Podrían los programas humanitarios agravar las tensiones existentes o crear conflictos nuevos debido a los efectos medioambientales?

Actores gubernamentales

Los Gobiernos pueden tener un impacto profundo en la prestación de ayuda a través de sus estructuras, dinámicas políticas, marcos jurídicos y relaciones tanto con la población local como con las organizaciones humanitarias. Es conveniente examinar la estabilidad, las condiciones jurídicas y las oportunidades de colaboración con el Gobierno en distintos niveles, así como la comprensión de los aspectos que se mencionan a continuación.

- Estructura gubernamental: ¿Cuál es la jerarquía y quiénes son los principales responsables de la toma de decisiones en los ministerios u organismos pertinentes en las distintas localidades?
- Dinámicas políticas: ¿Hasta qué punto es estable el Gobierno y cuáles son los intereses políticos que podrían afectar a la programación?

- Marcos jurídicos: ¿Qué leyes y reglamentos se aplican a las operaciones humanitarias y cómo se hacen cumplir?
- Postura ante la ayuda: ¿Apoya o se opone el Gobierno a los esfuerzos de ayuda? ¿Se imponen restricciones o condiciones?
- Corrupción y rendición de cuentas: ¿Hay problemas de corrupción en el Gobierno?
- Coordinación: ¿Cómo se coordina el Gobierno con las organizaciones humanitarias? ¿Existen mecanismos formales de coordinación?
- Percepción pública: ¿Cómo percibe la población local al Gobierno?
- Cooperación en materia de seguridad: ¿Proporciona el Gobierno seguridad para las operaciones humanitarias? En caso afirmativo, ¿cómo?

► *Para obtener más información sobre la interacción con las autoridades, véase el capítulo 2.1.*

Contexto interno

El análisis del contexto interno examina el interior de la organización, sus actividades, activos y personas. La evaluación del contexto interno puede ayudar al personal a comprender mejor la organización en su conjunto, la forma en que las actividades de sus programas benefician a la población local y el nivel de aceptación del que goza en una zona determinada, todo lo cual contribuye a comprender las vulnerabilidades y las fortalezas de la organización. A continuación se enumeran algunas consideraciones clave.

- La misión de la organización y los objetivos del programa.
- El tipo y la naturaleza de las intervenciones del programa.
- Localización geográfica de los equipos y los activos del proyecto.
- Historial de las operaciones en la zona, si existiera.
- Modalidades de aplicación.
- Calendario de actividades.
- Capacidades organizativas internas para gestionar los riesgos.

Al analizar el contexto interno, el personal de seguridad puede colaborar con el personal del programa encargado de gestionar y ejecutar las actividades del programa, el equipo de operaciones y los trabajadores de las suboficinas para obtener la mayor información posible.

Detección y evaluación de amenazas

Tras el análisis del contexto, el siguiente paso es detectar las amenazas específicas en el entorno operacional y las vulnerabilidades particulares de la organización y su personal.

Una amenaza es cualquier acontecimiento, acción o entidad con potencial para causar daño al personal, a los programas o a los activos o para obstaculizar la consecución de los objetivos humanitarios. Las amenazas a la seguridad del personal surgen de diversas fuentes, entre ellas, la criminalidad, los conflictos y la violencia, mientras que otras proceden de causas fortuitas como accidentes, enfermedades y peligros naturales.

Fuentes de amenazas internas

Las amenazas pueden originarse tanto dentro como fuera de la organización. Los incidentes de seguridad perpetrados por trabajadores humanitarios contra colegas pueden adoptar diversas formas, como acoso, discriminación, intimidación y violencia sexual. El hurto, el fraude y la violación de confidencialidad de la información pueden poner en peligro la integridad y los recursos de la organización y generar inseguridad para el personal. La violencia física y el maltrato psicológico por parte de los compañeros, incluidas tácticas como hacer luz de gas y la manipulación, también son riesgos. Los agresores internos pueden estar motivados a causar daño por diversas razones, entre ellas, las siguientes:

- La identidad del objetivo (por ejemplo, su género, grupo étnico u orientación sexual).
- Las circunstancias personales del agresor, incluidos sus agravios personales, sus antecedentes familiares, su personalidad y su comportamiento.
- Entornos permisivos en la organización.
- Factores culturales y sociales externos.

► Véase el capítulo 1.2 para conocer más detalles sobre las amenazas internas.

► Véase el capítulo 7.7 para obtener más información sobre los riesgos de violencia sexual y consultar un debate más profundo sobre cómo tratar a los agresores internos.

Fuentes de amenazas externas

Al examinar las fuentes de amenazas externas, puede ser útil elaborar descriptores de amenazas basados en diversos actores y categorías de sucesos. Los ejemplos pueden incluir amenazas relacionadas con:

- Criminalidad (homicidio, hurto, robo de vehículos, allanamiento, agresión).
- Violencia sexual (violación, agresión, abuso).
- Detención y arresto (barricadas, puestos de control).
- Rapto (secuestro extorsivo, situaciones de rehenes, extorsión).
- Combate y restos de material de guerra (tiroteos, bombardeos, ataques aéreos, bombas).
- Información, comunicaciones y tecnología (delitos cibernéticos, acoso en línea, desinformación, filtración de datos, vigilancia hostil).
- Disturbios civiles (manifestaciones, protestas, violencia de pandillas).

Las amenazas también pueden provenir de factores ambientales, como los económicos (recesión, inflación, interrupción de la cadena de suministro) y los peligros naturales (inundaciones, terremotos, epidemias).

► *Para consultar un análisis más detallado de algunos tipos de amenazas, véase la séptima parte.*

Una vez detectadas las amenazas, es importante comprender cómo, cuándo y por qué puede producirse cada una de ellas y a quién o qué puede afectar (en términos de personas, programas, activos, bienes y reputación, por ejemplo).

Recopilación de información sobre amenazas

La información utilizada para el análisis de amenazas puede proceder de diversas fuentes, como autoridades locales, miembros del personal, líderes comunitarios, propietarios de empresas, taxistas, medios de comunicación locales e internacionales y observadores de los derechos humanos. Algunas de estas fuentes pueden estar bien informadas y dispuestas a compartir lo que saben, mientras que otras pueden estar mal informadas o brindar deliberadamente una imagen distorsionada. Las empresas de seguridad privada también pueden proporcionar información y análisis sobre las condiciones de seguridad y las posibles amenazas. Esto puede ser útil para un macroanálisis, aunque suele no ofrecer el tipo de detalles cotidianos que las organizaciones pueden necesitar a nivel local.

Existen diversos métodos para recopilar información sobre posibles amenazas en el entorno operacional, entre ellos, entrevistas directas con las partes interesadas y un análisis de la documentación, como una revisión de informes organizativos anteriores (incluidos los de organizaciones homólogas), bases de datos de las ONG, foros de coordinación, organismos de la ONU y la policía local. Las fuentes abiertas, como las redes sociales y los principales medios de comunicación, también pueden ser valiosas. El análisis cuantitativo de incidentes pasados puede ayudar a determinar tendencias y zonas de alto riesgo. Las visitas también pueden ofrecer la oportunidad de recoger observaciones de primera mano sobre la situación en el lugar.

Debe evaluarse la fiabilidad de la información (autenticidad y confiabilidad de la fuente) y su validez (coherencia y confirmación por otras fuentes independientes). El uso de una matriz para clasificar la fiabilidad y la validez de las fuentes puede mejorar la calidad del análisis de las amenazas.⁵⁰

En cualquier entorno, es posible que distintas personas y grupos vean las amenazas de forma diferente en función de sus experiencias cotidianas y sus interacciones con los actores que representan una amenaza. Los grupos de discusión, las entrevistas y las evaluaciones participativas pueden ayudar a las organizaciones a recopilar información más matizada.

Análisis de vulnerabilidad y aceptación

Una vez finalizada la evaluación de amenazas, el siguiente paso es evaluar las vulnerabilidades de la organización: el grado de exposición del personal, las propiedades y los activos a las amenazas.

La vulnerabilidad de una organización puede verse influida por los siguientes factores:

- Imagen y nivel de aceptación de la organización.
- Tipo y naturaleza de la programación.
- Ubicación del personal y de los bienes.
- Nivel de exposición del personal y los bienes.
- Valor de los activos/bienes.
- Impacto de las intervenciones del programa en la zona.
- La capacidad interna de la organización para gestionar los riesgos de seguridad.
- Capacitación del personal, concienciación y cumplimiento de las medidas de protección.

Comprender las vulnerabilidades individuales del personal

Las vulnerabilidades personales, que abarcan los aspectos inmutables de la identidad y los factores manejables, como el comportamiento, forman colectivamente el perfil de riesgo personal de un individuo. No todas las características identitarias o vulnerabilidades son visibles, por ejemplo, la salud, la orientación sexual o la estabilidad financiera. Las vulnerabilidades solo son relevantes cuando se solapan con una amenaza específica, y el personal de seguridad debe tratar de comprender y abordar las vulnerabilidades en este contexto.

Como parte de un enfoque de la gestión de riesgos de seguridad centrado en la persona, las organizaciones pueden evaluar sistemáticamente cómo los distintos factores de identidad, como el género, la orientación sexual y el grupo étnico, afectan

50 Como ejemplo, véase RedR UK, Insecurity Insight y Foro Europeo Interinstitucional para la Seguridad (2017) *Manual de gestión de la información sobre incidentes de seguridad* (<https://siim.insecurityinsight.org/tools-and-resources/handbook-guide-and-tools>).

la vulnerabilidad de un individuo ante amenazas internas y externas. Un diagnóstico de riesgos inclusivo puede abarcar una serie de factores que influyen en las vulnerabilidades individuales vinculadas a la interacción entre las identidades interseccionales de los miembros del personal, sus funciones dentro de la organización, el contexto y los factores de amenaza internos y externos. Esto garantiza que los diagnósticos de riesgos sean inclusivos, y lo ideal sería que incluyeran aportaciones de diversos miembros del personal para captar un espectro amplio de experiencias y perspectivas.

Ejemplo: Diagnósticos de riesgos inclusivos

Una organización divide su evaluación de los riesgos para la seguridad en amenazas indirectas (“dónde estás”) y amenazas directas (“quiénes somos, qué hacemos”). Esto permite al personal utilizar datos externos para determinar un nivel de seguridad de referencia, que luego se complementa con un análisis más profundo de los riesgos que el personal puede experimentar al realizar su trabajo. En este marco, un país considerado de bajo riesgo en función del contexto, puede revelarse como un lugar de alto riesgo interno debido a factores como la baja aceptación de la comunidad.

► *Para obtener más información sobre el enfoque centrado en la persona, véase el capítulo 1.2.*

Comprender la vulnerabilidad de las organizaciones y los programas

El análisis del contexto interno puede ayudar a detectar las vulnerabilidades específicas de la organización y del programa. Las percepciones de la organización, su papel, mandato y misión pueden afectar su vulnerabilidad ante las amenazas. Las organizaciones confesionales, hagan o no proselitismo como parte de su misión, pueden correr riesgos diferentes en contextos religiosos en comparación con las organizaciones seculares. Del mismo modo, las organizaciones internacionales asociadas a determinados países o las organizaciones nacionales asociadas a determinadas zonas o grupos étnicos, pueden ser blanco de ataques por motivos políticos. A los organismos de la ONU les puede resultar difícil evitar que se los identifique con la ONU como actor político, a pesar de su misión humanitaria. Determinadas actividades de los programas, como los servicios de salud reproductiva o la ayuda centrada en las comunidades marginadas, pueden suponer riesgos debido a la forma en que las comunidades locales pueden percibir estos programas. Los Gobiernos pueden tener una opinión negativa sobre el lugar y las personas con las que trabajan las organizaciones si consideran que ello va en contra de sus intereses, especialmente si lo ven como un apoyo directo o indirecto a los grupos de la oposición.

Las organizaciones cuyos programas abarcan el “nexo” de las actividades humanitarias, de desarrollo y de consolidación de la paz probablemente se enfrentarán a un panorama de amenazas más complejo, ya que sus programas se extienden más allá de la prestación de servicios humanitarios y se adentran en ámbitos potencialmente sensibles de interés político y social.

El análisis de programas implica comprender la organización, lo que pretende hacer, dónde y cuándo y, lo más importante, por qué.

- **Por qué.** ¿Por qué es necesario el programa y qué importancia tiene para las personas a las que presta asistencia? ¿Qué importancia tiene para la misión y la identidad de la organización?
- **Qué.** ¿Cuáles son las actividades fundamentales y qué modalidades operacionales implican (por ejemplo, viajes, distribuciones, cadena logística, trabajo en instalaciones locales, trabajo en la comunidad)? ¿Cómo han sido percibidas y recibidas las actividades por la comunidad en el pasado?
- **Quién.** ¿Quiénes son la población destinataria, los donantes y las partes interesadas en el ámbito local y en general? ¿Quién es el personal del programa y qué identidades interseccionales habrá que considerar?
- **Dónde.** ¿Cuáles son las localidades del programa y otras zonas en las que estará o por las que pasará el personal?
- **Cuándo.** ¿Cuáles son los calendarios de los programas? ¿Coinciden con los periodos previstos de mayor inseguridad?

Las preguntas anteriores pueden ayudar a revelar áreas de vulnerabilidad e indicar el nivel de aceptación que ha obtenido la organización.

Es crucial evaluar el nivel de aceptación de la organización en la comunidad y entre las partes interesadas, ya que la falta de aceptación puede aumentar los riesgos y dificultar el éxito del programa. Este análisis puede examinar la influencia de las partes interesadas, su percepción de la organización y su personal, así como los niveles actuales de participación, e identificar riesgos y acciones para mantener o reforzar la aceptación según sea necesario.⁵¹

► *Para obtener más información sobre el análisis de aceptación, véase el capítulo 4.2.*

⁵¹ Para consultar un ejemplo de una plantilla de un análisis de aceptación, véase Global Interagency Security Forum (s.f.) “Acceptance analysis template - xlsx”, 2. *Acceptance analysis*, NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/>).

4.1.3 **Análisis de riesgos**

Una vez que una organización ha detectado las amenazas y las vulnerabilidades en un contexto concreto, el análisis puede pasar a los riesgos. El riesgo es un tema multidisciplinario con diferentes significados en distintas situaciones, que implica una amplia gama de posibilidades conocidas y desconocidas. En materia de seguridad, el riesgo es una combinación de dos factores:

- la probabilidad de encontrarse con una amenaza, y
- las consecuencias que se derivarían de ello.

Los riesgos más críticos que hay que abordar son los que es probable que se produzcan o los que pueden causar daños graves, mientras que los acontecimientos altamente improbables o de bajo impacto suelen tener una prioridad inferior.

Los diagnósticos de riesgos deben ser colectivos y colaborativos, y reunir a personal diverso, incluido el personal de programas y operaciones, para garantizar la consideración de una diversidad de perspectivas, realidades vividas y perfiles de identidad.

Evaluar la probabilidad

La evaluación de la probabilidad calcula la probabilidad de que se produzca un acontecimiento adverso.

La estimación de la probabilidad de una amenaza a la seguridad suele guiarse por el análisis de tendencias y la información procedente de fuentes internas y externas. Esta información se utiliza para determinar la posible frecuencia del suceso. La probabilidad puede evaluarse utilizando una escala de cinco puntos, como se ilustra en la tabla 4.

Tabla 4 Evaluación cualitativa de la probabilidad

Descriptor de calificación	Descriptor de probabilidad
Cierto/inminente (5)	El acontecimiento se produce con regularidad, es seguro que se producirá o ya se está produciendo.
Muy probable (4)	La probabilidad de que se produzca el acontecimiento o la amenaza es muy alta.
Probable (3)	El acontecimiento ya ha ocurrido antes y puede ocurrir otra vez.
Moderadamente probable (2)	El acontecimiento rara vez se produce.
Improbable (1)	Es improbable que se produzca el acontecimiento

Evaluar el impacto

Evaluar el impacto implica comprender las posibles consecuencias para las personas, los programas, los procesos, los bienes y la reputación. En otras palabras, es la estimación del daño que podría causar una amenaza. El impacto puede clasificarse de dos maneras:

- Pérdida directa. El daño inmediato causado por el suceso, como la muerte o lesiones del personal, daños a vehículos o pérdida de activos.
- Pérdidas consecuentes. Repercusiones de gran alcance, como retrasos, tiempo perdido, costo de tratamientos médicos y de apoyo psicosocial prestado al personal afectado, interrupción de las operaciones y cierre de oficinas.

Un solo incidente puede tener pérdidas tanto directas como consecuentes.

Al igual que en el caso de la probabilidad, la evaluación del impacto puede utilizar una escala de cinco puntos (véase la tabla 5).

Tabla 5 Evaluación de impacto

Clasificación de impacto	Descriptor de impacto
Extremo (5)	Impacto excepcionalmente grave, como muerte, múltiple víctimas, pérdida de operaciones, suspensión de programas, cierre de oficinas.
Alto (4)	Impacto grave, como lesiones físicas o psicológicas graves al personal, pérdida de acceso humanitario, pérdidas financieras significativas o daños a la reputación.
Moderado (3)	Impacto moderado, como lesiones que no ponen en peligro la vida, pérdida de activos, restricciones de personal y programas, pérdidas financieras, algunos daños a la reputación, enfermedades no graves.
Bajo (2)	Impacto bajo, como pérdida o daños a los activos de una organización, lesiones leves, interrupciones mínimas.
Insignificante (1)	Impacto insignificante.

Matriz de riesgos

Para determinar el nivel de riesgo de cada amenaza detectada, la organización puede realizar lo siguiente:

- Tomar la lista de amenazas detectadas durante la evaluación de amenazas.
- Estimar el impacto probable si las amenazas llegaran a producirse y la probabilidad de que estas amenazas se produzcan.
- Definir el nivel de riesgo global bruto (es decir, aún no mitigado).
- Trazar las amenazas según su nivel de riesgo (probabilidad por impacto) en una matriz o mapa de análisis de riesgos.

La figura 9 presenta una matriz sencilla de cuatro niveles utilizada en el diagnóstico de riesgos para evaluar y priorizar los riesgos en función de su probabilidad e impacto. Cada combinación de probabilidad y consecuencia corresponde a una clasificación de riesgo, que puede ayudar a las organizaciones a visualizar y priorizar los riesgos en función de su gravedad. El sombreado representa los niveles generales de riesgo, que van de bajo (claro) a extremo (oscuro).

Figura 9 Ejemplo de una matriz de riesgos

Impacto <i>Probabilidad</i>	Insignificante (1)	Bajo (2)	Moderado (3)	Alto (4)	Muy alto (5)
Cierto/ inminente (5)	Medio	Alto	Alto	Extremo	Extremo
Muy probable (4)	Medio	Medio	Alto	Extremo	Extremo
Probable (3)	Bajo	Medio	Alto	Alto	Extremo
Moderadamente probable (2)	Bajo	Bajo	Medio	Alto	Alto
Improbable (1)	Bajo	Bajo	Bajo	Medio	Medio

Los riesgos pueden clasificarse en orden numérico o simplemente como “alto”, “medio” o “bajo”. Los riesgos altos suelen exigir atención inmediata y medidas de mitigación contundentes. Los riesgos moderados pueden requerir un monitoreo regular y medidas de mitigación específicas. Los riesgos bajos podrían gestionarse quizás con medidas básicas, como procedimientos operativos estándar y revisiones ocasionales. Este proceso detallado de análisis y evaluación puede ayudar a una organización a priorizar eficazmente sus recursos y esfuerzos, centrándose en los riesgos más importantes y garantizando que todas las posibles amenazas se gestionan adecuadamente.⁵²

52 Para obtener ejemplos de plantillas, véase Global Interagency Security Forum (s.f.) 3. *Risk assessments*, NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/risk-assessments-2/>).

Clasificaciones del riesgo contextual

Muchas organizaciones gestionan la seguridad sobre la base de “clasificaciones de riesgo” o “niveles de seguridad” asignados a lugares específicos. Normalmente hay de tres a cinco niveles, que van de riesgo bajo a alto. Dentro de un país, o incluso de una ciudad, pueden existir muchos niveles diferentes. Los niveles informan muchas decisiones administrativas y operativas, como la criticidad de los programas, las medidas de protección, la supervisión de la gestión de riesgos de viajes, la dotación de personal de seguridad, la presupuestación de la seguridad y las políticas de recursos humanos.

Al establecer estas clasificaciones de riesgo contextual, un proceso similar de diagnóstico de riesgos puede considerar el entorno de amenazas, la vulnerabilidad de la organización y su personal en ese lugar y la importancia de ese lugar para cumplir los objetivos generales del programa.

Este enfoque por niveles ayuda a establecer los requisitos de seguridad para las distintas localidades y garantiza que los recursos se asignen de forma eficaz y que las zonas más críticas reciban la atención necesaria para mitigar las posibles amenazas. Aunque este enfoque suele utilizarse para las localidades, también podría aplicarse a otras categorías pertinentes. Por ejemplo, puede ser útil determinar qué funciones de la organización son las de mayor riesgo y esbozar los requisitos de seguridad para esos miembros del personal (por ejemplo, formación especializada).

► *Para obtener más información sobre los requisitos de seguridad, véase el capítulo 3.1.*

Mitigación de riesgos

El diagnóstico de riesgos puede proporcionar una hoja de ruta para que la organización asigne recursos suficientes y elabore medidas de mitigación de riesgos específicas que se correspondan con los riesgos identificados.

Las medidas de protección utilizadas para mitigar los riesgos suelen incluir, y verse influidas por, una combinación de enfoques que conforman una estrategia de seguridad global para una organización en un contexto específico.

► *Para obtener más información sobre los distintos enfoques de seguridad y el desarrollo de una estrategia de seguridad, véase el capítulo 4.2.*

Las medidas de mitigación (o el tratamiento) de riesgos están diseñadas para reducir los riesgos, disminuyendo las vulnerabilidades y mejorando las capacidades mediante la reducción de la probabilidad y el impacto.

- **Reducir la probabilidad.** Determinar y aplicar medidas concretas para reducir la probabilidad de que se produzcan incidentes, como establecer procedimientos

operativos estándar, fijar normas como toques de queda y límites de velocidad, utilizar convoyes y sistemas de camaradas de apoyo y formar al personal en técnicas para evitar amenazas.

- **Reducir el impacto.** Una vez que se ha producido un incidente, el impacto puede reducirse con medidas de protección y preparación, como tener acceso a refugios reforzados o habitaciones blindadas, equipar las instalaciones y los vehículos con botiquines de primeros auxilios y extintores, preparar planes de gestión de incidentes críticos y de contingencia y disponer de seguros y recursos de cuidado del personal, como servicios de asesoramiento.

Las medidas de mitigación deben reflejar los diagnósticos de riesgos por lo que respecta a probabilidad e impacto. Si una amenaza es de alto impacto pero de baja probabilidad, puede ser más adecuado centrarse en los esfuerzos para reducir el impacto en lugar de invertir más en reducir la probabilidad. Dicho esto, es aconsejable abordar ambos aspectos siempre que sea posible. Una vez determinadas las medidas de mitigación de riesgos, habrá que aplicarlas y financiarlas.

Por último, tal como ocurre con el análisis del contexto, el diagnóstico de riesgos deberá ser un documento vivo si ha de conservar su pertinencia y utilidad. Un aspecto clave de este proceso es el monitoreo y el análisis de los incidentes de seguridad y otra información pertinente para detectar patrones o tendencias que puedan indicar modificaciones en los riesgos. El diagnóstico de riesgos y las medidas de mitigación se incorporan a los planes de seguridad y suelen estar documentados en ellos.

► Véase el capítulo 4.3 sobre planes y disposiciones de seguridad.

4.1.4 Después de diagnosticar y mitigar los riesgos

Una vez que se ha “tratado” un riesgo con medidas de mitigación, la gestión continua de riesgos implica determinar cómo tratar el riesgo residual, ya que a menudo seguirá habiendo cierto riesgo incluso después de aplicar las medidas para reducirlo. El modo en que una organización aborda el riesgo residual suele estar determinado por su mandato y sus objetivos, la criticidad de su programación y el apetito de riesgo definido por la organización. Hay al menos tres vías posibles que una organización puede seguir.

- **Aceptar el riesgo residual.** Decidir aceptar determinados niveles de riesgo si caen dentro de la tolerancia al riesgo de la organización. Esto suele ser adecuado para trabajos esenciales de la misión o que salvan vidas, en los que los beneficios potenciales superan a los riesgos.

- **Evitar el riesgo residual.** Tomar medidas para evitar el riesgo modificando planes, procesos o comportamientos para eliminar la amenaza por completo: por ejemplo, reubicar las operaciones fuera de las zonas de alto riesgo o interrumpir las actividades no críticas.
- **Compartir el riesgo residual.** Contratar a un tercero, como una organización socia, para que comparta el riesgo asumiendo las actividades de programación, de modo que se optimice la eficacia y la seguridad para ambas, y se respete el deber de cuidado.

En los casos de riesgo muy elevado, la cuestión fundamental es decidir si se debe permanecer presente y operativo, o cesar la actividad y retirarse. Esto puede desglosarse del siguiente modo:

- ¿Es necesario y conveniente que la organización permanezca? ¿Dispone de la capacidad (financiera y de competencias) para gestionar los riesgos de seguridad?
- Si no es así, ¿pueden desarrollarse o incorporarse estas capacidades con la suficiente rapidez?
- Una vez establecidos los recursos financieros y humanos, ¿se puede dedicar suficiente personal y tiempo de gestión a la gestión de riesgos de seguridad?

Si la respuesta a alguna de las preguntas anteriores es “no”, las organizaciones deben reflexionar seriamente antes de decidir seguir adelante, al menos hasta que la situación mejore o se disponga de las capacidades adecuadas para gestionar los riesgos. Existen alternativas válidas a la presencia física de los programas, como canalizar la financiación u otros recursos a través de organizaciones mejor situadas para operar con seguridad en el entorno en cuestión.

4.1.5 Pensar más allá de la matriz de riesgos

El pensamiento actual en torno al análisis de riesgos cuestiona si algunas organizaciones han llevado el enfoque sistemático demasiado lejos, sugiriendo que se ha vuelto excesivamente complejo, arcano y reglamentado hasta el punto de divorciarse de la intuición y la experiencia. Como ocurre con cualquier procedimiento, también existe el peligro de que se convierta en un ejercicio de marcar casillas en lugar de una herramienta de apoyo a la toma de decisiones.

Como ya se ha mencionado, una de las ventajas de trabajar dentro de un marco de evaluación de riesgos de seguridad es que aporta coherencia organizativa a la respuesta al riesgo y puede utilizarse para poner en marcha una serie de acciones sin vacilaciones ni largas discusiones. Sin embargo, como herramienta de gestión también puede dar una impresión engañosa de solidez y previsibilidad, y es importante comprender las limitaciones de este enfoque:

- La información incompleta y las dificultades que entraña interpretar correctamente una realidad compleja pueden dificultar la decisión de pasar a un estado de alerta diferente y, en cualquier caso, determinar la clasificación de seguridad adecuada no es lo mismo que aplicar el plan.
- En ocasiones, las clasificaciones del nivel de riesgo pueden ser demasiado amplias para captar los grados de amenaza o las categorías de las personas en riesgo en un mismo lugar.
- Las situaciones de la vida real no siempre empeoran o mejoran gradualmente; una situación puede deteriorarse de repente, saltando a través de múltiples niveles.
- Es posible que organizaciones diferentes que operan en un mismo lugar interpreten la misma situación de manera diferente y, en consecuencia, se incluyan en diferentes clasificaciones de seguridad y, por lo tanto, apliquen medidas de seguridad también diferentes.
- Las evacuaciones y las reubicaciones en momentos de crisis suelen exigir una colaboración interinstitucional, que puede complicarse por las diferentes apreciaciones del riesgo, mientras que el hecho de que algunas organizaciones se reubiquen o evacúen y otras no lo hagan puede modificar el riesgo y aumentar la vulnerabilidad de quienes se quedan.

La otra preocupación es que centrar la atención y los recursos en los riesgos de alto impacto más probables, que es el punto final lógico del ejercicio, puede obstaculizar la capacidad de las personas para visualizar y tener en cuenta riesgos mucho menos probables, pero potencialmente catastróficos. Una organización que solo esté preparada para hacer frente a una lista de los riesgos más probables, según este argumento, puede ser menos flexible y resiliente ante acontecimientos que nunca podrían predecirse. Algunas organizaciones están adoptando un proceso denominado *exploración de horizontes*, que consiste esencialmente en proponer ideas en grupo sobre acontecimientos improbables que, de producirse, tendrían un impacto grave. Este ejercicio puede incitar al personal a pensar de forma creativa en una gama más amplia de escenarios de amenaza y a concebir estrategias de respuesta que podrían hacer frente a diversos sucesos.⁵³

La toma de decisiones en condiciones de incertidumbre es una constante en los entornos humanitarios complejos, en los que la información es escasa y la situación es dinámica e imprevisible. Una toma de decisiones eficaz requiere un equilibrio entre una respuesta rápida y un análisis exhaustivo, a menudo empleando enfoques de toma de decisiones tanto analíticos como naturalistas (intuitivos y empíricos).⁵⁴ La

53 Global Interagency Security Forum y Humanitarian Outcomes (2024) *State of practice: The evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

54 Para consultar un análisis más detallado, véase Cole, A. y Olympiou, P. (2022) *Risk management & decision making under uncertainty during the Afghanistan crisis 2021*, Global Interagency Security Forum (<https://gisfprod.wpengine.com/resource/risk-management-under-uncertainty-during-the-afghanistan-crisis-2021/>).

incorporación de ejercicios de exploración de horizontes como parte de la evaluación de amenazas puede evitar enfoques basados en fórmulas que, en el peor de los casos, reducen los procesos de diagnóstico de riesgos a meras herramientas presupuestarias.

Sin embargo, disponer de un método sistemático y estructurado para el análisis de riesgos no requiere necesariamente un proceso burocrático pesado o un ejercicio técnicamente complejo. Por el contrario, debe ser lo suficientemente sencillo como para que todo el personal pueda participar de forma significativa y lo suficientemente ligero como para que pueda realizarse (y rehacerse si es necesario) en un breve periodo de tiempo. Es importante que las organizaciones adapten el proceso de análisis de riesgos a su organización, teniendo en cuenta sus necesidades y capacidades.

4.1.6 Un enfoque simplificado

A menudo, los procesos de diagnóstico de riesgos pueden parecer complejos y abrumadores. Aunque en este capítulo se han proporcionado metodologías detalladas y buenas prácticas para el análisis de riesgos, para las organizaciones con tiempo o capacidad de personal limitados puede parecer poco realista aplicar sistemáticamente todos los pasos descritos.

En tales casos, una simple revisión y reflexión sobre las siguientes preguntas clave puede ayudar a orientar el análisis y la mitigación de riesgos. El objetivo, por supuesto, no es lograr un proceso de análisis de riesgos perfecto, sino maximizar la comprensión de la situación y la toma de decisiones basada en pruebas tanto como sea posible.

Preguntas clave de análisis de riesgos

- **¿Cuál es el contexto externo?**
 - ¿Qué factores políticos, económicos, socioculturales, tecnológicos, medioambientales y jurídicos son relevantes?
 - ¿Quiénes son los actores principales (grupos armados, actores delictivos, agentes gubernamentales) que afectan a la seguridad y cómo se interrelacionan?
 - ¿Hay un conflicto activo y, en caso afirmativo, cuáles son las causas? ¿Quiénes son los actores y cuál es su relación con la organización y entre sí?
- **¿Cuál es el contexto organizativo interno?**
 - ¿Cuáles son los objetivos, la estructura, las capacidades, los programas, el personal y la ubicación de la organización, y cómo se relacionan estos elementos con el contexto externo?

- **¿Cuáles son las amenazas principales en el entorno operacional?**
 - ¿Cuáles son las amenazas internas y externas para la organización?
 - ¿Cómo, cuándo y por qué podría producirse cada amenaza y a quién o qué afectaría?
- **¿Hasta qué punto es vulnerable la organización a las amenazas detectadas?**
 - ¿Qué vulnerabilidades existen para el personal y la organización, en especial teniendo en cuenta los factores de identidad interseccional, las evaluaciones del programa y los niveles de aceptación?
- **¿Cuál es la probabilidad de que se produzcan las amenazas?**
 - ¿Cuál es la probabilidad de que se produzcan las amenazas detectadas?
 - ¿Cuáles son las amenazas más probables?
- **¿Cuáles son las posibles repercusiones de las amenazas detectadas?**
 - ¿Cuál es el posible impacto de cada amenaza detectada?
 - ¿Qué amenazas tienen consecuencias más importantes y quién o qué podría verse más afectado?
- **¿Qué medidas de mitigación pueden aplicarse?**
 - ¿Qué amenazas son las más preocupantes y exigen medidas de mitigación de riesgos (normalmente las más probables o las que tienen repercusiones más graves)?
 - ¿Qué acciones pueden reducir la probabilidad y/o el impacto de las amenazas detectadas?
- **¿Qué hará la organización con los riesgos residuales?**
 - ¿Evitará o aceptará y/o compartirá la organización cualquier riesgo residual que quede una vez aplicadas las medidas de mitigación?
- **¿Qué riesgos de baja probabilidad pero alto impacto necesitan más atención?**
 - ¿Qué riesgos exigen una planificación de escenarios o un debate más profundo debido a sus consecuencias potencialmente graves a pesar de su baja probabilidad?

Al evaluar los riesgos, es útil considerar quién o qué puede verse afectado (teniendo en cuenta los factores basados en la identidad), por qué y cómo, así como cuándo y dónde pueden surgir las amenazas (considerando tanto la esfera física como la digital).

Más información

Investigación y análisis

Cole, A. y Olympiou, P. (2022). *Risk management & decision making under uncertainty during the Afghanistan crisis 2021*. Global Interagency Security Forum (<https://gisfprod.wpengine.com/resource/risk-management-under-uncertainty-during-the-afghanistan-crisis-2021/>).

Global Interagency Security Forum y Humanitarian Outcomes. (2024). *State of practice: the evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Orientación y recursos

Bickley, S. (2017). *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*. Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Davis, J. et al. (2020). *Security to go: a risk management toolkit for humanitarian aid agencies*. 4.ª edición. Global Interagency Security Forum (<https://gisf.ngo/resource/security-to-go/>).

Global Interagency Security Forum. (s.f.a). 1. *Context analysis*. NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/1-context-analysis/>).

Global Interagency Security Forum. (s.f.b). 2. *Acceptance analysis*. NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/>).

Global Interagency Security Forum. (s.f.c). 3. *Risk assessments*. NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/risk-assessments-2/>).

RedR UK, Insecurity Insight y Foro Europeo Interinstitucional para la Seguridad (2017). *Manual de gestión de la información sobre incidentes de seguridad* (<https://siim.insecurityinsight.org/tools-and-resources/handbook-guide-and-tools>).

4.2 Elaborar una estrategia de seguridad

La estrategia de seguridad de una organización en un contexto operacional concreto comprende un equilibrio de enfoques y las medidas específicas que decida adoptar. Estas se basan en el proceso de diagnóstico de riesgos, junto con los principios y los valores de la organización. En este capítulo se presentan los tres enfoques de seguridad generales y superpuestos que pueden conformar una estrategia de seguridad: aceptación, protección y disuasión.

4.2.1 Enfoques de seguridad

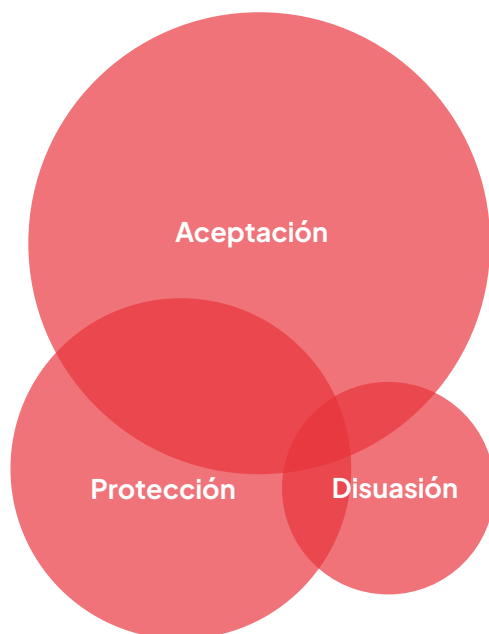
Los conceptos de aceptación, protección y disuasión constituyen cada uno un conjunto de opciones y acciones de seguridad, desde “blandas” hasta “duras”. Como ya se ha mencionado:

- El propósito de las medidas de aceptación es reducir o eliminar las amenazas al aumentar la aceptación (la tolerancia política y social) de la presencia de una organización y su trabajo en un contexto determinado.
- Las medidas de protección tienen como objetivo reducir la vulnerabilidad a la amenaza, pero no afectan a la amenaza en sí;⁵⁵ esto se denomina a menudo *endurecer el objetivo*.
- Las medidas de disuasión intentan disuadir una amenaza con una contraamenaza, como el uso de la fuerza (el ejemplo clásico son los guardias armados).

Aunque a veces se considera que la aceptación, la protección y la disuasión son estrategias separadas —cada una en su propia esquina del *triángulo de la seguridad*—, en la práctica, una organización suele elegir una combinación de opciones de cada una, dependiendo del entorno operacional. En diferentes contextos y a medida que evolucionan los riesgos, puede ser conveniente cambiar el énfasis de un tipo de medida (o enfoque global) a otro. Por tanto, en lugar de un triángulo estático, puede ser más útil imaginar esferas superpuestas e interactivas, cuyo énfasis puede variar en función del contexto, los riesgos y la estrategia organizativa (véase la figura 10).

55 Muchos profesionales de la seguridad, y ediciones anteriores de este informe, utilizaban la palabra *protección* (*protection*). Nótese, sin embargo, que algunos profesionales de la seguridad utilizan el término *protective* en inglés (como en “enfoque de protección” para “*protective approach*” y “medidas de protección” para “*protective measures*”) para hacer una clara distinción entre las medidas de gestión de riesgos de seguridad para el personal y la protección como un tipo de intervención humanitaria centrada en las comunidades en riesgo.

Figura 10 Ejemplo de combinación de medidas en una estrategia de seguridad



Teniendo en cuenta sus principios y valores, muchas organizaciones humanitarias consideran que la aceptación es el enfoque general más adecuado y eficaz y lo convierten en la base de su estrategia de seguridad en un lugar determinado (es decir, la mayoría de las medidas de mitigación de riesgos se diseñan para aumentar la aceptación, al tiempo que se evita activamente cualquier medida que pueda afectar negativamente las percepciones y la aceptación). Esto puede significar, en algunos contextos, que una organización decida abstenerse por completo de utilizar medidas de disuasión si se percibe que estas no se corresponden con los principios, los valores y el enfoque de aceptación de la organización.

Las medidas de aceptación no son eficaces contra todas las amenazas, por lo que a menudo se necesita una combinación de medidas. En entornos en los que predominan la anarquía o la violencia o en los que los actores armados tienen pocos incentivos para negociar, las medidas de aceptación pueden tener una eficacia limitada por sí solas.

Sin embargo, añadir otros tipos de medidas no significa necesariamente abandonar un enfoque basado en la aceptación. Por el contrario, la opinión de incorporar medidas de protección visibles, por ejemplo, puede requerir más divulgación y otras medidas de aceptación activa. La eficacia de cualquier enfoque también se verá influida por lo que hagan otras organizaciones humanitarias.

Las medidas de protección y disuasión no son necesariamente más eficaces en todos los casos y pueden acarrear sus propios problemas. Las medidas de protección se centran en la organización como blanco potencial y, a diferencia de la aceptación, no se dirigen a quienes representan la amenaza. También puede llevar a una “mentalidad de búnker”, que puede dar lugar a un modelo operacional restrictivo y a un mayor distanciamiento de las comunidades destinatarias, todo ello con el fin de reducir el riesgo aislando a la organización, su personal y sus activos. Esto hace que sea más difícil entablar relaciones con los demás, lo que a su vez dificulta la recopilación de información sobre el entorno y la comunicación eficaz con los interlocutores locales.

Las medidas de disuasión —las menos utilizadas entre las organizaciones humanitarias— presentan inconvenientes evidentes. Si las organizaciones exhiben su uso de la fuerza, por ejemplo conduciendo con escoltas armadas o contratando guardias armados para sus oficinas, es más difícil transmitir una imagen de neutralidad y no violencia.

Una buena estrategia de seguridad necesita una combinación flexible de estas medidas, lo que puede significar elegir un enfoque general que sirva de guía para decidir qué medidas priorizar. Como base para cualquier actividad de programación, una buena práctica es cultivar la aceptación y las buenas relaciones con la población local y sus líderes, así como con los agentes estatales y no estatales pertinentes. En entornos más inseguros en los que se han detectado riesgos generales para las organizaciones humanitarias, suele ser recomendable adoptar ciertas medidas de protección, sobre todo contra la criminalidad. En contextos altamente inseguros en los que existen riesgos considerables para la organización, puede ser necesario adoptar medidas de disuasión si esta es la única manera de proteger al personal y seguir prestando ayuda vital. Esto a veces se denomina *principio de último recurso*. Si la aceptación es el enfoque principal, las medidas de protección y disuasión pueden adaptarse para mantener la aceptación. Las medidas de aceptación pueden utilizarse para complementar las medidas de mitigación de riesgos de protección y disuasión.

Las diferentes medidas tienen diferentes implicaciones en cuanto a recursos. Todas conllevan un costo financiero. La aceptación es quizás la más difícil de medir desde el punto de vista financiero, pero puede demandar mucho tiempo del personal y posiblemente nuevas iniciativas del programa, como la difusión mediática. El equipamiento de protección conlleva un costo financiero directo, mientras que los procedimientos de protección (por ejemplo, los toques de queda o conducir siempre con dos vehículos) pueden aumentar el presupuesto al restringir la capacidad operacional. Un enfoque de disuasión puede tener implicaciones de recursos tanto

pequeñas como grandes, de las que puede ser difícil o imposible retractarse a largo plazo (por ejemplo, invertir en protección armada).

4.2.2 Aceptación

La aceptación suele ser un enfoque organizativo más amplio que se centra en fomentar relaciones genuinas con las comunidades afectadas y las partes interesadas, al tiempo que defiende los principios humanitarios básicos. Este enfoque se considera a menudo fundamental para dar legitimidad y consentimiento a la ejecución eficaz de los programas. También permite a las organizaciones humanitarias distinguirse de otros actores, como las fuerzas militares o los proveedores de servicios del sector privado.

En la gestión de riesgos de seguridad, la aceptación suele entenderse como la reducción o la eliminación de amenazas potenciales mediante el cultivo y el mantenimiento de relaciones con las partes interesadas pertinentes y la obtención de su “consentimiento” para operar en un lugar determinado. En realidad, el “consentimiento” puede no ser el concepto más adecuado para medir la aceptación. En la práctica, la aceptación puede entenderse mejor como un continuo que va de ser aceptado (más seguro) a ser atacado (más inseguro):⁵⁶

- aceptado
- tolerado
- rechazado
- atacado

Retos de la aceptación

Los retos y las limitaciones de la aceptación son numerosos. A continuación se enumeran algunos de los más destacados.

- **Financiación.** La forma como se percibe una organización puede estar vinculada a su fuente financiación. La sospecha de que los que aportan el dinero controlan la organización humanitaria puede crear serios problemas, sobre todo si el donante en cuestión es parte en el conflicto o si se considera que tiene una agenda política.

⁵⁶ Para obtener más información, véase Fast, L. et al. (2011) *The acceptance toolkit: a practical guide to understanding, assess, and strengthening your organization's acceptance approach to NGO security management*, Save the Children Federation (<https://acceptanceresearch.wordpress.com/acceptance-toolkit/>).

- **Acción humanitaria basada en principios.** En algunos contextos, tanto los Gobiernos nacionales como los extranjeros pueden no querer que las organizaciones humanitarias negocien o incluso se comuniquen con actores armados no estatales, aun cuando esto sea necesario para llevar a cabo una acción humanitaria basada en principios y para acceder a las poblaciones afectadas por la crisis. Los Gobiernos pueden penalizar estas negociaciones, por ejemplo, utilizando la legislación antiterrorista. Las organizaciones que acepten financiación con cláusulas antiterroristas deberán asegurarse de que se adopten todas las medidas razonables para garantizar su cumplimiento sin comprometer la misión humanitaria.
- **Incidencia.** La búsqueda y la preservación de la aceptación puede hacer que a las organizaciones les resulte difícil denunciar las violaciones del derecho internacional humanitario o los abusos contra los derechos humanos, ya que esto puede afectar negativamente las relaciones con diversas partes interesadas. El equipo directivo de las organizaciones se beneficia de contar con un enfoque estructurado para equilibrar los esfuerzos de incidencia con las cuestiones relacionadas con la gestión de riesgos de seguridad. *(Véase el capítulo 2.2 sobre incidencia para obtener un análisis más detallado).*
- **Información perjudicial.** Las implicaciones de la información errónea, la desinformación, la información manipulada y el discurso de odio para la seguridad de los trabajadores humanitarios son un tema de creciente preocupación y estudio. *(Véase el capítulo 6.2 para obtener un análisis más detallado de los retos que plantea la información perjudicial).*⁵⁷
- **Proliferación y fragmentación de los grupos armados.** En muchos contextos, la proliferación y la fragmentación de los grupos armados están haciendo que sea más complejo determinar quién controla qué territorio, así como quién está al mando en una organización (es decir, si las negociaciones con un representante serán respetadas por el resto del grupo). Algunas organizaciones han invertido recursos considerables en el monitoreo de los grupos armados para comprender sus estructuras internas y sus patrones cambiantes de control territorial.

Componentes clave de la aceptación activa

La aceptación no puede darse por cierta; debe forjarse activamente y mantenerse con diligencia. Las medidas de “aceptación activa” incluyen la divulgación estratégica entre un amplio abanico de partes interesadas, el desarrollo de las capacidades del personal en comunicación y en relaciones sociales, políticas e interpersonales, y el diseño y la difusión de mensajes básicos sobre la misión, los objetivos y los programas de la organización. Algunos de los componentes clave de un enfoque de aceptación activa son los siguientes:

- Trabajar con el personal del programa para integrar la gestión de riesgos de seguridad en el diseño del programa.

57 Para saber cómo puede repercutir la tecnología en la aceptación, véase Al Achkar, Z. (2021) “Digital risk: How new technologies impact acceptance and raise new challenges for NGOs” en Global Interagency Security Forum (Ed.) *Achieving safe operations through acceptance: Challenges and opportunities for security risk management* (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

- Establecer y mantener relaciones con las principales partes interesadas, incluidos los actores armados. Esto puede incluir interactuar con agentes nacionales, regionales e internacionales, cuando proceda.
- Conseguir la aceptación de la población local (por ejemplo, mediante reuniones y encuentros sociales).
- Gestionar las comunicaciones.
- Monitorear las percepciones y la opinión pública.
- Gestionar las percepciones del personal y de la organización.

En la sección siguiente se analizan estos puntos con más detalle.⁵⁸

Integración del programa

La capacidad de una organización para satisfacer las necesidades de las personas de forma transparente y responsable suele ser fundamental para la percepción que se tiene de ella. Se reconoce ampliamente que la aceptación está relacionada con una programación eficaz y con la capacidad de respuesta, que satisface las necesidades de una comunidad. La participación de la comunidad, las consultas y las alianzas locales suelen ser elementos clave de una programación eficaz. Sin embargo, aunque los programas satisfagan las necesidades de las personas afectadas, pueden afectar negativamente a determinados actores o cambiar las estructuras de poder político, económico y social. Aunque una buena programación es un componente esencial de la aceptación, esta no puede presuponerse únicamente a partir de una programación de buena calidad.

Debe procurarse que la conexión entre una programación eficaz y la obtención y el mantenimiento de la aceptación se mencione explícitamente en las actividades de planificación de programas, se incluya en los planes de programas, las evaluaciones de necesidades y los presupuestos y se incorpore a las herramientas de monitoreo y evaluación de programas.

Interacción con las principales partes interesadas

Una vez identificadas las principales partes interesadas y analizadas sus respectivas posiciones, influencia y disposición, las organizaciones pueden dirigirse a quienes, formal o informalmente, ejercen una influencia significativa sobre la posibilidad de que una organización pueda operar con seguridad en un entorno determinado. Estas podrían ser amistosas, hostiles o neutrales hacia la organización y pueden identificarse en el análisis de actores. Se debe tener en cuenta a los actores nacionales, regionales e internacionales junto con las partes interesadas locales, ya que tener su aceptación es cada vez más importante para una acción humanitaria eficaz.

► *Para obtener más información sobre el análisis de actores, véase el capítulo 4.1.*

⁵⁸ Para obtener un análisis más detallado de un enfoque de aceptación activa, véase Fast *et al.* (2011).

Es importante evaluar la influencia que tiene cada parte; en algunas situaciones, puede ser suficiente contar con la aceptación de agentes influyentes clave si no es posible conseguir la aceptación de todos. Algo que puede favorecer la aceptación es recurrir a personal de la zona o a un intermediario respetado (como un líder religioso o comunitario) a fin de llegar a otras partes interesadas en nombre de una organización.

Para entablar una relación con las principales partes interesadas no basta con celebrar reuniones formales breves y poco frecuentes. Los mensajes pueden transmitirse no solo en las reuniones, sino también a través del tipo de reunión y de cómo se celebra. Hay que seguir y respetar las costumbres culturales. Ir más despacio, tomarse tiempo para conocer y hablar con la gente, explicar, escuchar, socializar y, en general, mostrar una actitud cortés y respetuosa: todo ello puede ser importante para conseguir la aceptación.

Los acuerdos formales, como, por ejemplo, con el Gobierno o con grupos influyentes, pueden ser útiles porque aportan reconocimiento oficial y un acuerdo explícito sobre cuestiones concretas. En lo referente a la seguridad, los acuerdos pueden detallar las responsabilidades, incluidos los procedimientos que seguir y un punto de contacto en caso de que surjan problemas de seguridad. El personal operativo puede llevar consigo una copia del acuerdo (en el idioma correspondiente) para facilitar el acceso o el diálogo. Es importante tener en cuenta que los acuerdos por escrito no tienen el mismo valor en todos los entornos sociales y que otras prácticas culturales pueden ser más apropiadas. Los acuerdos formales también pueden ser problemáticos, por ejemplo, si solo son válidos durante un periodo limitado, si llaman la atención sobre ámbitos en los que las autoridades pueden estar tratando indebidamente de regular o impedir las actividades de las organizaciones humanitarias, o si consumen más tiempo del personal de lo que valen. Asimismo, es posible que estos acuerdos no sean reconocidos en todos los niveles de un grupo o entidad. Estos factores deben tenerse en cuenta antes de firmar acuerdos formales.

Agentes armados no estatales

Es probable que las organizaciones que trabajan en una zona bajo el control *de facto* de un grupo armado tengan que señalarle su presencia y obtener garantías de que su trabajo es aceptable y de que no se hará daño al personal. A continuación se enumeran algunas preguntas que hay que tener en cuenta a la hora de interactuar (o plantearse interactuar) con estos actores:

- ¿Cuál es la relación entre el grupo armado y la población local?
- ¿Cuál es la relación del grupo armado con el personal de la organización?
- ¿Cuál es la estructura de mando y la situación de disciplina? ¿Cuáles son los fines y objetivos del grupo armado?

- ¿Cómo podrían afectar el diálogo y las negociaciones con el grupo armado a las relaciones con los demás (incluidas las autoridades)?
- ¿Qué peticiones o exigencias (por ejemplo, pagar “impuestos” u obtener un “permiso” diario para operar) podrían plantearse y cómo debería responder la organización?

Para comprender estas dinámicas y riesgos se requiere una capacidad proactiva de análisis. A menudo tendrá sentido trabajar con otras organizaciones humanitarias para aunar capacidades y posibilitar un enfoque común y unas líneas rojas comunes (límites no negociables) a la hora de interactuar con actores armados no estatales.

► Véase el capítulo 4.1 para obtener más información sobre los grupos armados como parte de un análisis de actores.

Población local

Si hay un nivel de aceptación alto, los miembros de la comunidad local pueden hacer sugerencias sobre cómo reducir el riesgo y, en algunos casos, pueden proporcionar información crítica y avisos a la organización. Su influencia, sin embargo, no debe sobrestimarse; en algunas circunstancias, las comunidades pueden no estar en absoluto en condiciones de reducir significativamente los riesgos de seguridad. Es posible que no tengan poder para influir en otros actores, pueden pasar por alto o juzgar erróneamente las amenazas nuevas o pueden beneficiarse más de brindar apoyo a otro actor.

Existe una diferencia entre la mera tolerancia de la presencia y el programa de una organización y la verdadera aceptación. Las personas pueden aceptar la presencia de una organización solo porque la necesitan desesperadamente o pueden utilizar la ayuda como una fuente de apoyo, pero no sentir una responsabilidad activa por el bienestar de la organización. Escuchar y responder a lo que la gente quiere, tratarla con respeto, actuar con transparencia y rendir cuentas puede profundizar las relaciones y fomentar un mayor nivel de aceptación. Estas relaciones pueden prevalecer incluso sobre la dimensión material. Una organización humanitaria puede verse incapacitada de proporcionar un nivel adecuado de asistencia o incluso, con cierta frecuencia, ninguna asistencia en absoluto, y aun así seguir siendo aceptada por la calidad de la relación.

Gestión de la comunicación

Para todas las partes interesadas, las comunicaciones deben ser claras y coherentes. Una organización y su personal deben saber y poder explicar, de manera breve y fácil de entender, quiénes son, por qué están ahí, qué quieren hacer y cómo se relacionan con los demás. Puede ser útil preparar una simple hoja de preguntas y respuestas para el personal.

En el caso de las organizaciones internacionales y federadas, la necesidad de coherencia se extiende a la armonización de los mensajes a nivel mundial. Aunque algunas comunicaciones pueden ajustarse ligeramente para dirigir las a públicos diferentes, el mensaje general debe ser el mismo, ya sea desde la oficina central o en el lugar donde se ejecuta un proyecto.

Las declaraciones públicas deben reflejar los valores, los principios y el mandato de la organización y estar contextualizadas para facilitar su comprensión local, así como tener en cuenta el impacto en las percepciones locales.

Las declaraciones públicas de carácter crítico sobre las autoridades locales exigen una consideración cuidadosa. Entre los factores clave que hay que sopesar figuran la necesidad de divulgación pública, el momento de informar el tema, la redacción y la fundamentación de las afirmaciones y el método de publicación.

► *Para obtener un análisis más detallado, véase el capítulo 2.2 sobre incidencia y seguridad.*

Gestión de las percepciones del personal

La forma en que se percibe al personal puede influir en la percepción de la organización en su conjunto. Las características identitarias desempeñan un papel en este sentido y pueden presentar tanto puntos fuertes como vulnerabilidades, dependiendo de la percepción local de dichas características.⁵⁹

► *Véase el capítulo 1.2 para obtener más información sobre los factores y las percepciones basados en la identidad.*

La apariencia y el comportamiento también son importantes. La apariencia personal puede conllevar importantes significados sociales y políticos, y un comportamiento inapropiado puede causar resentimiento y agravar las sospechas y tensiones existentes.

El respeto de las normas sociales y culturales (por ejemplo, las costumbres referidas a la vestimenta, el alcohol y las relaciones interpersonales) puede mejorar la percepción del personal y de la organización. Es posible que quienes son nuevos en el contexto no conozcan o respeten todas las costumbres, pero los errores pueden perdonarse más fácilmente si van acompañados de una actitud educada, serena y respetuosa o si se explica claramente por qué no se siguen ciertas costumbres.

59 Para consultar un análisis de las ventajas de contratar personal diverso e inclusivo para favorecer la aceptación, véase Williams, C., Kinch, P. y Herman, L. (2021) “Promoting a blended risk management approach: the place of programming and diversity within a SRM strategy” en Global Interagency Security Forum (Ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

También deben tenerse en cuenta las normas religiosas y respetarse siempre que sea posible; es posible que las organizaciones confesionales tengan que ser especialmente cuidadosas con su imagen y sus actividades.

Gestión de la percepción de la organización

Es importante tener en cuenta cómo es percibida la organización y sus actividades. ¿Son los programas lo que la comunidad local más desea y necesita? Algunos programas pueden no ser considerados prioritarios o quizás sean percibidos negativamente por determinados segmentos de la comunidad. ¿Qué opinión tienen de la organización y su personal las partes interesadas que no se benefician del programa? ¿Están estas partes interesadas en condiciones de influir negativamente en la aceptación, entre otras cosas, obstruir los programas o hacer daño al personal?

Comprender estas cuestiones implica escuchar a las personas y adaptarse en consecuencia. Incluso un programa que goce de amplia aceptación en una comunidad, puede aún irritar a otras partes interesadas. Esto ocurre en prácticamente todos los sectores: un programa de ayuda alimentaria puede enfadar a los comerciantes locales al reducir sus beneficios; ofrecer servicios de salud gratuitos puede alejar a los pacientes de las clínicas de pago, lo que puede causar frustración entre los funcionarios de salud locales, y registrar las amenazas a la protección de la población puede enfadar a los responsables de la violencia.

Otra consideración es la estrategia de salida. Las organizaciones pueden llevar a cabo buenos programas, pero darse cuenta luego de que las estrategias de salida mal ejecutadas socavan la buena reputación generada durante el programa. Esto significa que podrían tener dificultades para conseguir aceptación en el futuro.

Capacidades y competencias relativas a la aceptación

La aceptación tiene implicaciones prácticas en lo que respecta a recursos humanos, financieros y administrativos. Un enfoque de aceptación activa exige que el personal cuente con algunas competencias clave. Estas pueden incluir las siguientes:

- Capacidad para hacer un mapeo de los actores principales y establecer una red amplia con las partes interesadas.
- Conocimiento exhaustivo de la misión y de los valores de la organización.
- Capacidad para establecer relaciones sólidas y habilidades de negociación.
- Dominio de la lengua local y excelentes habilidades de comunicación.
- Capacidad para analizar las cambiantes condiciones políticas y de seguridad.

Para aplicar eficazmente un enfoque de aceptación se necesita el liderazgo del personal superior, que deberá tener no solo las competencias necesarias, sino también tiempo suficiente en relación con sus otras responsabilidades.

La aceptación no es gratuita. Hay costos operativos, entre los que se incluyen los siguientes:

- Tiempo del personal, incluida la contratación de personal adicional con responsabilidades en materia de seguridad, difusión o medios de comunicación.
- Capacitación del personal sobre cómo comunicar la misión y los valores de la organización, así como en comunicación intercultural y habilidades diplomáticas y de negociación.
- Viajes extras (vehículos, combustible, tiempo del personal) posiblemente necesarios para reunirse con las partes interesadas.
- Traducción de materiales o mensajes de la organización a idiomas y formatos adecuados a la localidad.
- Pago por el uso de la radio, la televisión y otros medios de comunicación, cuando sea necesario.
- Tiempo adicional necesario durante la fase de diseño de un programa.
- Material de comunicación, como folletos.

Estos costos deben determinarse en el diseño del programa e integrarse en el proceso de presupuestación.

► *Para obtener más información sobre la financiación de la seguridad, véase el capítulo 3.3.*

Para aplicar un enfoque de aceptación también puede ser necesario realizar modificaciones en las normas administrativas o jurídicas de la organización, como se muestra en los siguientes ejemplos.

- Aunque los proveedores suelen elegirse en función del precio y la calidad, un enfoque de aceptación puede requerir la distribución de los contratos entre distintos sectores de la población local para que los habitantes sientan que los beneficios se reparten equitativamente. Del mismo modo, puede ser una buena idea comprar localmente, incluso si un proveedor de otro lugar ofrece una mejor relación calidad-precio.
- La organización puede optar por ajustar sus procedimientos de selección para contratar una combinación equilibrada de perfiles diversos (por ejemplo, teniendo en cuenta el grupo étnico y si las personas proceden de la localidad).

Monitoreo de las percepciones y medición de la aceptación

No hay una forma sencilla de saber cómo se percibe una organización y si es aceptada (y por qué). Puede ser un signo positivo de aceptación si las partes interesadas pertinentes:

- Se comprometen públicamente a aceptar la responsabilidad de la seguridad del personal.
- Comparten con la organización información precisa relacionada con la seguridad (por ejemplo, advierten de que alguien ha estado preguntando por la organización o de que es probable que se produzca una determinada amenaza).
- Cooperan activamente con las actividades de la organización o las apoyan.
- Permiten el acceso (por ejemplo, los grupos armados permiten que el personal de la organización atraviese los puestos de control para llegar a las zonas del programa).
- Ayudan a conseguir la liberación de un miembro del personal secuestrado o a recuperar activos robados.
- Reconocen que la organización ha logrado un cambio positivo en la vida de las personas.
- Ofrecen una disculpa si los miembros de un grupo perjudican a la organización.

La aceptación puede ser el resultado de las relaciones sólidas de un miembro del personal en un determinado lugar o entorno. Las organizaciones deben ser conscientes de ello y de las posibles implicaciones si este miembro del personal deja la organización o si cambia la percepción de esa persona.

La aceptación también puede disminuir con el tiempo, a medida que evolucionan las necesidades y las expectativas de las personas. Una vez estabilizada la situación, pueden surgir nuevas aspiraciones. Las organizaciones deben esforzarse por hacer un monitoreo continuo de las actitudes de la población local y de las principales partes interesadas para medir los niveles de aceptación y cualquier cambio que pueda interferir con el acceso y la seguridad.

Sin embargo, la falta de aceptación puede no tener nada que ver con la propia organización y no necesariamente puede mejorarse con sus esfuerzos; puede ser, por ejemplo, un rechazo del concepto de acción humanitaria en su conjunto.⁶⁰

60 Para consultar un análisis más detallado sobre las limitaciones de la aceptación, véase Daudin, P. (2021) “Acceptance under stress: old recipes for new problems” en Global Interagency Security Forum (Ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Cómo controlar y medir la aceptación: algunas ideas

- Un elemento fundamental del monitoreo de la aceptación es una buena comprensión del contexto y de las partes interesadas.
- Introducir el análisis de la aceptación como parte de los métodos de trabajo existentes. Este documento lo presenta como un paso del proceso de análisis de la seguridad. Las evaluaciones de la aceptación también podrían integrarse en auditorías de seguridad o en foros comunitarios.
- Los niveles de aceptación pueden medirse en función de criterios o indicadores objetivos, como la frecuencia de las reuniones con las principales partes interesadas y el nivel y la naturaleza de la interacción con los actores principales. Los datos sobre incidentes pueden ser útiles, pero no deben ser el único indicador.ⁱ
- Puede ser conveniente desglosar las partes interesadas pertinentes y determinar el nivel de aceptación de cada una, así como destacar la información útil y las principales acciones de monitoreo.ⁱⁱ También puede ser útil desglosar los niveles de aceptación de los diferentes actores en el lugar en cuestión: el sector humanitario en su conjunto, la organización y los programas y equipos específicos.ⁱⁱⁱ
- Entre las formas de recabar información para este análisis figuran las siguientes:
 - Hacer un monitoreo de los mensajes publicados en las redes sociales y en los principales medios de comunicación.
 - Organizar grupos de discusión y consultas.
 - Realizar periódicamente encuestas de percepción.
 - Establecer mecanismos de retroalimentación.
 - Documentar la naturaleza de las conversaciones informales.
- Una vez determinados los niveles de aceptación, pueden incorporarse a un plan de acción específico o a las medidas de mitigación de riesgos y otras actividades. Examinar los diferentes factores que pueden influir en las percepciones y establecer el grado de control que la organización tiene sobre ellos puede orientar la acción (por ejemplo, la conducta del personal frente a las motivaciones políticas de los grupos armados).

ⁱ Para consultar más ejemplos de indicadores, véase Fast *et al.* (2011).

ⁱⁱ Véase, por ejemplo, Global Interagency Security Forum (s.f.) 2. *Acceptance analysis*, NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/>).

ⁱⁱⁱ Véase, por ejemplo, Billaudel, R. (2021) “Measuring and improving acceptance: ACF’s experience and perspectives” en Global Interagency Security Forum (Ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

El monitoreo y análisis de los niveles de aceptación es un ejercicio en gran medida subjetivo. Una forma de gestionar esta subjetividad es animando a distintas personas a participar en el proceso de evaluación y pedirles que compartan ejemplos concretos para explicar sus opiniones, recurriendo a diversas fuentes de información y utilizando indicadores objetivos y normalizados en todos los equipos y lugares.

4.2.3 Protección

El objetivo de las medidas de protección es reducir la vulnerabilidad. Esto puede lograrse endureciendo el objetivo o aumentando o reduciendo su visibilidad.

Endurecimiento del objetivo

Mediante procedimientos y activos físicos se puede reducir la probabilidad de que una amenaza se acerque al objetivo o las posibles repercusiones negativas en el objetivo. En la práctica, esto podría significar:

- Equipamiento de seguridad del sitio, como sistemas de iluminación y alarma, muros perimetrales, verjas metálicas y rejas metálicas en las ventanas (*para conocer más detalles, véase el capítulo 7.2*).
- Protección de activos, como cajas fuertes para efectivo y equipamiento valioso, y alarmas para los vehículos.
- Procedimientos de protección, como controlar el acceso de los visitantes, el acceso de vehículos y las disposiciones de estacionamiento, y contratar guardias que patrullen las instalaciones y adviertan de la presencia de intrusos.
- Uso de vehículos blindados, equipos de protección personal y películas de protección en las ventanas.
- Capacitación del personal en materia de seguridad digital (*para conocer más detalles, véase el capítulo 6.2*).
- Conducir en convoyes u organizar el alojamiento del personal de modo que las residencias estén agrupadas unas cerca de otras.

La fuerza de los grupos numerosos puede ser eficaz, pero no necesariamente detendrá a un agresor decidido y podría ser contraproducente si el objetivo es un mayor número de víctimas o si el objetivo es otra organización y otros se convierten en víctimas colaterales. Asimismo, aunque los equipos de comunicación suelen ser necesarios, los equipos visibles y caros pueden atraer una atención no deseada. La luz y el sonido (por ejemplo, focos sensibles al movimiento en el exterior de un edificio) pueden avisar con cierta antelación de un ataque, lo que le permitiría al personal tomar medidas de evasión (entrar en una habitación segura o escabullirse) o pedir ayuda. Una vez más, sin embargo, estos dispositivos pueden no prevenir un incidente.

Programas de baja visibilidad o perfil bajo

Los programas de baja visibilidad se han vuelto cada vez más comunes entre las organizaciones de ayuda, especialmente cuando se determina que la aceptación no es un enfoque viable. Consiste en eliminar la marca organizacional de los edificios de oficinas, del personal, de los vehículos y de las residencias. También puede implicar el uso de vehículos particulares o taxis. En entornos de muy alto riesgo, cualquier cosa que pueda vincular al personal con una organización (documentos de identidad de la organización, teléfonos móviles, computadoras) puede ser “esterilizada”. El personal que pueda destacarse de la población local podrá ser trasladado a otro lugar. En posturas de perfil extremadamente bajo, los receptores de la ayuda pueden no ser conscientes de la fuente de la asistencia.

Otra táctica del enfoque de baja visibilidad es utilizar logotipos removibles para los vehículos en zonas donde la visibilidad no es recomendable. Saber cuándo exhibir un logotipo y cuándo retirarlo exige un diagnóstico de riesgos muy bueno, localizado y dinámico. Sin embargo, es importante tener en cuenta que las pegatinas magnéticas removibles pueden ser robadas fácilmente y utilizadas por otros para suplantar la identidad de la organización.

Un enfoque de perfil y visibilidad bajos puede hacer que la programación sea más complicada y distanciar a la organización de fuentes de información que, de otro modo, podrían mejorar su seguridad. También puede dar lugar a sospechas y percepciones erróneas acerca de lo que hace la organización, lo que socaba la aceptación. Es un enfoque difícil de mantener si la organización busca un reconocimiento amplio de su trabajo por parte del público o de los donantes. Por lo general, las organizaciones no consideran que un enfoque de bajo perfil sea una forma permanente de operar, sino más bien excepcional y limitada en el tiempo. También puede adoptarse al inicio de un programa, y luego moderarse gradualmente a medida que aumentan las operaciones.

4.2.4 Disuasión

La disuasión consiste en plantear una contraamenaza: esencialmente se trata de desalentar a los posibles atacantes infundiéndoles miedo al uso de una contrafuerza o a otras consecuencias graves. La protección armada es la forma más poderosa de disuasión utilizada por las organizaciones humanitarias. Sin embargo, existen otros factores disuasorios, y esta sección los aborda brevemente antes de pasar a un análisis en profundidad de la protección armada en las operaciones humanitarias.

Formas de disuasión

Influencia jurídica y diplomática

Existen protecciones legales para los trabajadores humanitarios bajo el derecho nacional e internacional. Por desgracia, los elementos disuasorios jurídicos no siempre son eficaces. Algunas organizaciones humanitarias pueden obtener cierta influencia del respaldo de gobiernos donantes extranjeros, en particular al negociar el acceso o al resolver problemas administrativos con los Gobiernos nacionales, pero su influencia será limitada y la interacción estrecha con los Gobiernos donantes puede socavar la apariencia de independencia y neutralidad.

Suspensión de las operaciones o retirada

Ante ciertas amenazas o tras incidentes de seguridad, las organizaciones han suspendido temporalmente sus programas de ayuda o han amenazado con hacerlo. La continuación o la reanudación del programa queda entonces sujeta a la resolución del problema o a la mejora de la situación. La evidencia anecdótica sugiere que esta táctica no siempre funciona muy bien y que las organizaciones suelen reanudar sus programas a pesar de no notar ninguna mejora, lo que puede socavar su credibilidad y cualquier amenaza similar en el futuro.

Las siguientes son circunstancias en las que una suspensión o amenaza de suspensión puede ser efectiva:

- Si no se percibe como un castigo a personas que no están vinculadas a las causas de la inseguridad y que no están en una posición de mejorar la seguridad.
- Si se puede movilizar a un sector influyente de la población o a los líderes o autoridades locales en nombre de la organización.
- Cuando las organizaciones están preparadas para mantener la suspensión hasta que la situación sea resuelta satisfactoriamente y no anularán la decisión demasiado rápido debido a presiones internas o externas.
- Si otras organizaciones no debilitan la acción interviniendo para llenar el vacío; lo ideal es establecer un frente común antes de suspender las operaciones.

A menos que el incidente sea muy grave, una suspensión selectiva (p. ej., en un lugar determinado o durante un periodo determinado) o la reintroducción gradual de los servicios puede dar más espacio de maniobra. Una suspensión total tiende a crear una situación difícil de todo o nada.

► Véase el capítulo 4.3 para consultar un análisis práctico de las implicancias de seguridad de las suspensiones y las retiradas.

Afiliación informal

Otra opción de disuasión es afiliarse informalmente con actores locales influyentes. En este escenario, un ataque a la organización podría percibirse implícitamente como un agravio a estos actores. Esta opción debe abordarse con mucha cautela ya que podría socavar los principios humanitarios de la organización y su aceptación entre otras partes interesadas e incluso podría dar lugar a que la organización se convirtiera en rehén de la protección de la persona influyente en cuestión.

Protección armada

Las organizaciones humanitarias no suelen recurrir a la protección armada. Sin embargo, puede haber circunstancias excepcionales en las que sea necesario para posibilitar la acción humanitaria, como en el caso de los convoyes humanitarios que entran en importantes zonas de combate o cuando las autoridades lo exigen como condición para el acceso. Dicho esto, si bien la protección armada puede brindar una medida de seguridad y protección a los trabajadores humanitarios en el momento (aunque también pueden hacer lo contrario y atraer disparos), también puede complicar los esfuerzos para mantener el acceso humanitario a largo plazo. En otras palabras, la práctica socava la acción humanitaria basada en principios. Las directrices del IASC ofrecen varias razones para evitar el uso de escoltas armadas en los convoyes humanitarios debido a sus implicaciones contraproducentes a largo plazo.⁶¹

La relación entre la protección armada y la acción humanitaria es complicada. Aunque prácticamente todas las organizaciones humanitarias han utilizado en algún momento alguna forma de protección armada, a menudo se la considera un anatema y los debates al respecto son muy delicados. La cooperación con un actor armado, incluida una fuerza bajo mandato de las Naciones Unidas, puede llevar a que los actores locales, nacionales e internacionales, así como la población, asocien a las organizaciones humanitarias y a los receptores de la ayuda con los objetivos políticos y/o militares de ese actor armado. Esto podría potencialmente socavar la neutralidad, la imparcialidad y la independencia reales y percibidas de la organización humanitaria y de la comunidad humanitaria en general, así como su aceptación. El impacto de la protección armada en la aceptación no siempre es directo y puede variar según el contexto y otros factores influyentes.⁶²

Si bien esta sección proporciona un marco más sistemático para considerar el asunto, no pretende ser un argumento a favor del uso de la protección armada, sino más bien una exploración de sus posibles beneficios, riesgos y desafíos. Antes de decidir si se recurre a la protección armada, es aconsejable considerar los pros y los contras en la situación específica y explorar todas las alternativas posibles.

61 Inter-Agency Standing Committee (2013) *IASC non-binding guidelines on the use of armed escorts for humanitarian convoys* (<https://reliefweb.int/report/world/iasc-non-binding-guidelines-use-armed-escorts-humanitarian-convoys>).

62 Para consultar un análisis sobre este tema, véase Jourde, J. (2021) "Private security contracting and acceptance: a dangerous match?" en Global Interagency Security Forum (Ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Las siguientes preguntas se pueden tener en cuenta a la hora de decidir si se recurre a la protección armada:

- ¿En qué circunstancias la organización permite, en principio, el uso de protección armada?
- ¿Los beneficios de utilizar protección armada en este contexto compensan los riesgos?
- ¿Existen preocupaciones serias sobre cómo gestionar la protección armada?, ¿es posible superarlas?
- ¿Cómo afectará el uso de la protección armada las percepciones de la organización en particular y de las organizaciones humanitarias en general y cómo impactará en los niveles de aceptación entre las partes interesadas clave?
- ¿Cuáles son la cultura y las prácticas locales en relación con el uso de protección armada? (Esto puede afectar cómo se percibe y acepta su uso).

En cada paso de la línea de razonamiento es posible llegar a la conclusión de que la protección armada puede no ser apropiada. También hay que tener en cuenta que la necesidad de considerar la protección armada puede indicar que ya se ha superado el umbral de riesgo aceptable y que la verdadera decisión que hay que tomar puede ser retirarse o no iniciar la programación. Si aún no se ha alcanzado este umbral o si la protección armada pudiera reducir el riesgo a un nivel más aceptable, entonces hay tres áreas importantes que considerar para tomar una decisión: principios y ética, contexto y gestión.

Cuestiones relativas a los principios y la ética

Algunos sostienen que la protección armada va en contra de los principios básicos de la acción humanitaria. Esta posición tiende a basarse en consideraciones éticas u operacionales a largo plazo. El argumento ético sostiene que la acción humanitaria nunca es compatible con el uso de la fuerza. Desde una perspectiva ideológica, una organización puede rechazar la protección armada porque su uso, por principio, contribuye a la producción y a la distribución continuas de armas.

La consideración operacional a largo plazo es que, si bien la protección armada puede ser justificable en un contexto determinado, también puede erosionar la imagen general de la acción humanitaria en todo el mundo y, por tanto, puede conducir a una mayor inseguridad en otros lugares o en el futuro. Según esta línea de razonamiento, recurrir con demasiada rapidez o frecuencia a la protección armada socava los esfuerzos globales por aumentar el respeto del derecho internacional humanitario y la acción humanitaria independiente.

También hay consideraciones prácticas. Las escoltas armadas hacen que el trabajo humanitario sea mucho menos flexible en términos de movimientos, ya que los permisos y las escoltas a menudo tienen que organizarse con antelación. Hacer que los movimientos sean más predecibles puede aumentar la vulnerabilidad de una organización a los ataques, en particular si los escoltas no son de plena confianza.

Los argumentos a favor del uso de la protección armada sostienen que puede ser aceptable como último recurso y cuando la supervivencia de las personas estuviera en riesgo si se redujera la asistencia humanitaria y de otro tipo.⁶³ En algunos contextos, el uso de protección armada para facilitar la prestación de ayuda puede ser una función del Estado en el ejercicio de sus obligaciones en virtud del derecho nacional e internacional o de las políticas gubernamentales.

Otra consideración importante se refiere a quién se beneficia de la protección armada:

- ¿Se trata solo de la organización humanitaria y su personal, o puede la protección brindar beneficios públicos más amplios y mejorar la seguridad pública?
- El uso de armas y guardias armados, reclutados quizás localmente, ¿tendrá un efecto pacificador sobre la situación local o aumentará las tensiones?
- ¿Está contribuyendo a la “privatización” de la seguridad, por lo que solo quienes pueden pagar pueden obtener seguridad?
- ¿Pone indirectamente en riesgo a otros al convertirlos en blancos fáciles en comparación? Es importante considerar qué efecto tiene, si lo hay, en el entorno de seguridad más amplio.

Incluso si el uso de protección armada se considera necesario y legítimo, puede que no sea ético o práctico pagar por el servicio a contratistas privados, grupos o individuos. En algunos contextos, la protección brindada por un Estado o por fuerzas policiales o militares con mandato internacional puede ser gratuita, pero no siempre es así. A raíz de los casos de fraude relacionados con la protección entre los guardias de la milicia somalí en la década de 1990, algunos trabajadores humanitarios argumentaron que las organizaciones humanitarias nunca deberían pagar por protección armada. La realidad es que la mayoría lo ha hecho cuando ha considerado que las circunstancias lo requerían. A veces también es una obligación legal en algunos contextos.⁶⁴

La dependencia del apoyo de un actor armado también puede hacer que sea extremadamente difícil o imposible operar sin dicho apoyo en el futuro, lo que socava la sostenibilidad de las operaciones humanitarias. El proveedor de protección armada

63 Naciones Unidas y IASC (2008) *Civil-military guidelines & reference for complex emergencies*, Oficina de Coordinación de Asuntos Humanitarios de las Naciones Unidas (<https://digitallibrary.un.org/record/697614?ln=en&v=pdf>).

64 Stoddard, A., Harmer, A. y DiDomenico, V. (2008) *The use of private security providers and services in humanitarian operations*, HPG Report 27, Londres, ODI (<https://odi.org/en/publications/private-security-providers-and-services-in-humanitarian-operations-2/>).

puede desarrollar un interés financiero en mantener el servicio. Además, el cese repentino de la protección armada puede exponer a una organización humanitaria como un blanco fácil.

La decisión de una organización de utilizar protección armada tiene consecuencias para las demás, ya que puede influir en la imagen y en la percepción de todas las organizaciones humanitarias y, por tanto, afectar potencialmente la aceptación y las relaciones de manera más amplia. Este es un tema que merece una reflexión y un análisis interinstitucional estructurado. Si bien es un recurso poco común entre las ONG, los guardias armados y/o las escoltas armadas son utilizados habitualmente por los organismos de las Naciones Unidas que operan en contextos considerados de alto riesgo, como Afganistán, Irak y Yemen. En muchos contextos, esto ha dado lugar a posturas de seguridad divergentes entre los actores humanitarios de las Naciones Unidas y de las ONG. Durante los enfrentamientos en la región de Gambella en Etiopía en 2022, el UNDSS recomendó el uso de escoltas armadas para las entregas humanitarias. Algunas ONG internacionales se alarmaron más tarde al descubrir que sus equipos locales en Gambella habían actuado conforme a esta recomendación.

Cuestiones relativas al contexto

Más allá de las cuestiones de principios, ética y riesgos para la aceptación de una organización, se puede plantear un conjunto de preguntas adicionales, específicas del contexto, a la hora de decidir sobre el uso de protección armada.

► *¿Cuáles son las amenazas y quiénes son los objetivos?*

Un análisis más profundo puede arrojar luz sobre el origen de la amenaza, el objetivo y los motivos de los posibles agresores. Se pueden hacer distinciones importantes entre las amenazas relacionadas con la seguridad del sitio y de los traslados y las amenazas específicas a la organización humanitaria (su personal y activos) y, más general, a las poblaciones afectadas. Incluso cuando la protección armada parezca justificada, puede que no proporcione un efecto disuasorio razonable o que aumente el riesgo. Por ejemplo, si los ladrones sospechan que un residente tiene un arma de fuego, pueden volverse violentos si son sorprendidos en el acto. Si los bandidos que atacan en las carreteras ven un convoy armado, es posible que disparen antes de robarlo. También es importante considerar quién es el objetivo. Si las fuerzas gubernamentales o una facción determinada proporcionan la protección armada, la organización puede convertirse en un objetivo legítimo a los ojos de la oposición armada. También existe el riesgo de accidentes por “fuego amigo” o por un mal manejo o fallas de las armas.

Mantener la distinción entre la organización y su protección armada

Las organizaciones humanitarias pueden considerar las siguientes acciones para distinguirse o distanciarse de la protección armada:

- Asegurarse de que los actores armados que protegen los convoyes viajen en vehículos separados.
- Prohibir las armas dentro de las instalaciones o los vehículos de la organización.
- Evitar usar ropa (incluidos los colores) que se parezca a la de las fuerzas armadas.
- Abstenerse de utilizar activos militares (p.ej., camiones o helicópteros); repintar y marcar de nuevo si es inevitable.
- Excluir a los guardias armados de los recintos a menos que sea absolutamente necesario.
- Utilizar guardaespaldas armados solo para amenazas selectivas como secuestros o asesinatos, aplicando la “protección cercana” cuando sea necesario.

El hecho de que estas medidas realmente ayuden a mantener una distinción perceptiva y permitan a la organización conservar alguna parte de su imagen civil y de no combatiente depende a menudo del contexto local específico.

► ¿A quién se está protegiendo?

En entornos peligrosos, las organizaciones tienden a pensar en medidas que mejoren su propia seguridad. Puede ser útil considerar si se podría mejorar la seguridad en la zona en general y de qué manera. Por ejemplo, en un campamento de refugiados se podrían desplegar guardias armados de manera que protejan no solo al personal de la organización, sino también a las mujeres refugiadas que corren el riesgo de sufrir agresiones sexuales cuando recolectan agua y leña. Se podría desarrollar un sistema mediante el cual los guardias armados de varias organizaciones individuales patrullaran el vecindario y aumentarían así la seguridad de todos. Cuando hay una operación de paz de las Naciones Unidas presente y tiene el mandato de proteger a los civiles, se pueden desplegar tropas en zonas que son peligrosas tanto para los trabajadores humanitarios como para la comunidad local.

► *¿Quién brinda protección?*

También es importante considerar quién proporciona la protección armada. Las fuentes potenciales incluyen a actores militares nacionales, la policía nacional, un grupo de resistencia armada, fuerzas de mantenimiento de la paz o la policía de las Naciones Unidas, milicias locales, empresas de seguridad privada y guardias armados directamente en nómina de la organización. En algunas circunstancias, una organización que no se opone en principio al uso de la fuerza puede concluir que ninguno de los posibles proveedores es aceptable y eficaz, por lo que tendría que optar entre operar sin protección armada o retirarse.

Ejemplos de preguntas al elegir un proveedor de protección armada

- ¿Cuál es la posición política del proveedor en un conflicto determinado? ¿Puede considerarse que la organización toma partido si se asocia a un actor en particular?
- ¿Cuál es la imagen pública y la reputación del proveedor?
- ¿Qué importancia tiene para el proveedor la extensión de la protección a una organización humanitaria en comparación con sus otros objetivos? El proveedor puede tener otros planes (por ejemplo, enfrentar al enemigo o capturar a un delincuente) que en momentos críticos puede anular la preocupación por la seguridad de la organización o incluso ponerla en peligro.
- ¿Qué tan profesional es el proveedor? Los guardias, ¿están bien capacitados, reciben una remuneración razonable, cuentan con equipo que funciona, están bien instruidos, supervisados y disciplinados?
- ¿Cuánto control de gestión necesita o desea la organización? Tener más autoridad directa sobre los proveedores de protección armada permite un mayor control, pero también hace que la organización sea directamente responsable de su comportamiento y acciones.
- ¿Cuáles son las “reglas de intervención” del proveedor sobre el uso de la fuerza y dónde recae la responsabilidad en caso de que se ejerza la fuerza y se produzcan lesiones?

► Véase el capítulo 2.1 para un análisis más amplio sobre los servicios de seguridad privada, incluidas algunas preguntas más detalladas sobre el código de conducta.

Cuestiones relativas a la gestión

Una cuestión clave relativa a la gestión se refiere a las reglas de intervención (es decir, cuándo se puede usar la fuerza y en qué grado). La norma básica suele ser que la fuerza solo puede utilizarse para proteger la vida cuando está claramente amenazada y mientras la amenaza persiste. En otras palabras, la fuerza letal solo puede emplearse en defensa y no, por ejemplo, para disparar a un ladrón, aunque esté armado, que está huyendo y ya no constituye una amenaza inmediata. Lo que constituye una amenaza inmediata a la vida y al bienestar debe analizarse en términos concretos, imaginando diferentes escenarios.

También deben aclararse las reglas de intervención para la protección de los activos. Si bien la preferencia instintiva de una organización puede ser que no se use la fuerza cuando solo están en riesgo los activos, ¿es aceptable no hacer nada mientras un almacén se vacía o todos los alimentos de un convoy son robados por actores armados, especialmente si hay personas que realmente necesitan esos suministros y dependen de ellos? Las organizaciones deben tener muy claro en qué momento y en qué situación es aceptable la intervención.

Ejemplo: Reglas de intervención en la práctica

Una organización internacional ha utilizado guardias desarmados de una empresa de seguridad privada en la República Democrática del Congo y en Sudán del Sur. La empresa también cuenta con una unidad de respuesta armada con su propio guardia armado o un oficial de policía armado incorporado. Si bien la organización utiliza principalmente guardias desarmados, las conversaciones con la empresa de seguridad privada también cubrieron cuestiones clave como las reglas de intervención en caso de que se convocara a esta unidad de respuesta armada.

Otro aspecto importante de la gestión es acordar procedimientos y enfoques para una serie de escenarios posibles, incluyendo qué hacer cuando un visitante se niega a ser registrado o insiste en traer a sus propios guardias armados, y hasta dónde llegar en la persecución de ladrones o asaltantes que huyen.

En los casos en que se solicite protección armada, puede ser necesario llegar a un acuerdo sobre los siguientes aspectos:

- Quién proporciona las armas (normalmente es el proveedor del personal).
- Qué tipo de armas utilizarán los guardias (p.ej., pistolas, escopetas o ametralladoras).
- Quién es responsable de proporcionar la munición y de comprobar que las armas están bien mantenidas y debidamente registradas.
- Quién es responsable de proporcionar equipo adicional, como ropa y linternas para los guardias.
- A qué vehículos, si hay alguno, tienen acceso los guardias armados: los guardias armados no siempre cuentan con vehículos y posiblemente sea necesario determinar si pueden utilizar los de la organización y cuándo.

El mando y el control funcionan en ambos sentidos: si una organización se pone bajo la protección de un actor armado, se espera que cumpla las reglas de dicho actor. Por ejemplo, abandonar repentinamente un convoy, irse a toda prisa o alejarse puede no ser aceptado por el proveedor de seguridad.

En una fuerza multinacional de mantenimiento de la paz, las fuerzas armadas de los distintos países tienden a tener tradiciones y culturas diferentes, incluso con respecto al mando y el control, las reglas de intervención y lo que se considera un uso apropiado o excesivo de la fuerza. Puede ser necesaria una consulta detallada y en profundidad con los comandantes de diferentes niveles para garantizar un entendimiento común. Diferentes comandantes pueden tener diferentes puntos de vista, y puede ser útil tener un acuerdo detallado por escrito con un comandante superior para gestionar las relaciones entre los diferentes niveles. Es aconsejable supervisar los cambios para asegurarse de que todos los reemplazos estén completamente informados.

► Para obtener más información sobre la coordinación civil-militar, véase el capítulo 2.1.

Resumen de preguntas clave relativas a la gestión

A continuación se enumeran las preguntas clave relativas a la gestión que deben considerarse:

- ¿Están disponibles dentro de la organización y el lugar en cuestión las políticas, los procedimientos y las competencias de gestión necesarias para manejar esta relación?
- ¿Cuáles son las disposiciones contractuales necesarias?
- ¿Quién mantiene el mando y el control y quién tiene la autoridad y la responsabilidad sobre qué?
- ¿Quién en la organización humanitaria decide o aprueba el uso de protección armada?

- Los guardias armados, ¿estarán siempre presentes o solo en determinados momentos o lugares?
- ¿Cómo se elaboran las licitaciones y se evalúan las ofertas de los servicios de seguridad privada?
- ¿Qué preguntas se pueden plantear sobre la profesionalidad e integridad de un posible proveedor de servicios?
- ¿Ante quién responden los guardias, quién tiene la autoridad de mando y quién está a cargo de la disciplina?
- Cuando las fuerzas de seguridad externas brindan protección armada, ¿cuál es la autoridad de su comandante en comparación con la de la organización?
- ¿Quién determina las reglas que rigen el uso de la fuerza letal y quién garantiza que los guardias las hayan comprendido plenamente?

Política

Las organizaciones se benefician de tener una política a nivel de toda la organización sobre el uso de protección armada. Los puntos importantes que considerar incluyen los siguientes:

- Aclaración de la posición de la organización, en principio, respecto al uso de protección armada.
- Las condiciones que podrían justificar el uso de protección armada, por ejemplo, durante la evacuación o reubicación del personal en periodos de inseguridad extrema (esto puede incluir referencias a la criticidad del programa y a las consecuencias del uso de protección armada).
- Qué alternativas se han considerado para abordar los riesgos y si la protección armada es realmente el último recurso.
- Las consideraciones y los riesgos principales (legales, de reputación y físicos), tanto para la organización en cuestión como para otros, al elegir proveedores potenciales, y cómo serán evaluados.
- Los términos que deben convenirse entre la organización y el proveedor.
- El procedimiento organizativo para la toma de decisiones y la revisión periódica.

- La obligación de acompañar el uso de la protección armada con mayores esfuerzos de comunicación para explicar su justificación, es decir, cómo puede respaldar otros enfoques de seguridad, especialmente la aceptación.

Política de muestra

Según la política de una organización, se puede considerar la protección armada cuando:

- un gran número de vidas están en peligro;
- la amenaza está relacionada con el vandalismo generalizado, no con cuestiones políticas;
- el proveedor cumple con los estándares pertinentes;
- la disuasión puede ser eficaz, y
- el uso de protección armada está autorizado en el nivel organizativo apropiado.

Una política sobre protección armada no es lo mismo que una política sobre empresas de seguridad privada, aunque estas empresas sean a menudo las proveedoras de protección armada. Una organización puede contratar empresas de seguridad privada para otros fines (p.ej., diagnósticos de riesgos o auditorías de seguridad) y otros tipos de actores también pueden proporcionar protección armada. El uso de cualquiera de ellos debe guiarse por la política establecida.

- *Para obtener más información sobre los servicios de seguridad privada, véase el capítulo 2.1.*

Más información

Investigación y análisis

Al Achkar, Z. (2021). Digital risk: How new technologies impact acceptance and raise new challenges for NGOs” en Global Interagency Security Forum (Ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Bamber-Zyrd, M. (2023). ICRC engagement with armed groups in 2023. *Humanitarian Law & Policy*. Comité Internacional de la Cruz Roja (<https://blogs.icrc.org/law-and-policy/2023/10/10/icrc-engagement-with-armed-groups-in-2023/>).

Daudin, P. (2021). Acceptance under stress: old recipes for new problems. En Global Interagency Security Forum (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Global Interagency Security Forum. (2021). *Achieving safe operations through acceptance* (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Stoddard, A., Harmer, A. y DiDomenico, V. (2008). *The use of private security providers and services in humanitarian operations*. HPG Report 27. Londres, ODI Global (<https://odi.org/en/publications/private-security-providers-and-services-in-humanitarian-operations-2/>).

Williams, C., Kinch, P. y Herman, L. (2021). Promoting a blended risk management approach: the place of programming and diversity within a SRM strategy. En Global Interagency Security Forum (Ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Orientación y recursos

Fast, L. et al. (2011). *The acceptance toolkit: a practical guide to understanding, assessing, and strengthening your organization's acceptance approach to NGO security management*. Save the Children Federation (<https://acceptanceresearch.wordpress.com/acceptance-toolkit/>).

Global Interagency Security Forum. (s.f.). Acceptance analysis template - xlsx. 2. *Acceptance analysis*. NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/>).

Naciones Unidas y Comité Permanente entre Organismos. (2008). *Civil-military guidelines & reference for complex emergencies*. Oficina de Coordinación de Asuntos Humanitarios de las Naciones Unidas (<https://digitallibrary.un.org/record/697614?ln=en&v=pdf>).

4.3 Planes y disposiciones de seguridad

Una vez que una organización ha identificado y evaluado los riesgos, puede elaborar planes para gestionarlos. Un plan de seguridad es el lugar donde se documentan estos riesgos junto con las medidas de mitigación correspondientes. En este capítulo se exponen las buenas prácticas relacionadas con la creación de planes de seguridad, prestando especial atención a dos elementos principales: los procedimientos operativos estándar (cómo la organización mitigará las amenazas identificadas en el diagnóstico de riesgos) y los planes de contingencia (cómo la organización responderá a eventos y situaciones disruptivos y potencialmente de alto riesgo).

4.3.1 Planes de seguridad

El plan de seguridad sirve como base de la gestión de riesgos de seguridad a nivel de implementación del programa. Dependiendo del contexto y de los riesgos, un plan de seguridad puede aplicarse a un país entero, a una zona geográfica específica o incluso, ocasionalmente, a un proyecto individual.

La inclusión en el proceso de planificación, involucrando a un grupo diverso de miembros del personal con diferentes funciones, procedencias y perfiles personales, es preferible a la planificación individual, ya que aporta conocimientos y experiencia colectivos y promueve una amplia apropiación del producto final. Las buenas prácticas en la planificación también incluyen el monitoreo mediante revisiones periódicas para adaptar el plan a medida que cambia el entorno.

Componentes de un plan de seguridad

Los planes de seguridad difieren entre las organizaciones, lo que refleja necesidades y políticas organizacionales específicas y el contexto. Los componentes principales de un plan de seguridad pueden incluir los siguientes aspectos (adaptado de Foro Europeo Interinstitucional para la Seguridad [ahora Global Interagency Security Forum] *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*).⁶⁵

- 1. Resumen de información crítica.** Un resumen de una página con detalles clave para una referencia rápida, que incluye números de emergencia y procedimientos o reglas importantes, como toque de queda u horario de presentación.
- 2. Visión general.** El propósito y el alcance del plan, la parte responsable, una declaración de la misión de la organización y la política de seguridad (incluido el umbral y el apetito de riesgo) y las fechas de creación del plan, la última revisión y la próxima revisión.

65 Bickley, S. (2017) *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*, Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

3. **Contexto actual y diagnóstico de riesgos.** Una sinopsis del entorno operacional en un periodo definido, que incluye la dinámica del conflicto, si es relevante, y las amenazas, los riesgos y las calificaciones de riesgo identificados.
4. **Niveles de seguridad.** Fases basadas en indicadores de riesgo y acciones necesarias.
5. **Funciones y responsabilidades.** Los nombres de las personas y cargos con responsabilidades en la gestión de riesgos de seguridad.
6. **Procedimientos operativos estándar.** Procedimientos de seguridad claros y concisos para la prevención y la respuesta basados en los riesgos evaluados y que cubran áreas clave como el manejo de efectivo, las comunicaciones, la seguridad del sitio, la salud y la seguridad, la seguridad de la información, la conducta personal, la seguridad en los viajes y la seguridad de los vehículos.
7. **Medidas de salud y seguridad.** Procedimientos operativos estándar específicos y otras medidas para proteger al personal de amenazas a la salud, accidentes y estrés.
8. **Recursos humanos.** Resúmenes de políticas de selección, verificación de antecedentes, contratos, confidencialidad, inducciones y diagnósticos de riesgos de funciones.
9. **Sesiones informativas sobre seguridad.** Una lista de los temas tratados y la información proporcionada al personal nuevo o a los visitantes y los requisitos y expectativas de capacitación.
10. **Denuncia del incidente.** Definiciones, procedimientos, responsabilidades, estructura y formato de informes.
11. **Gestión de crisis y planes de contingencia.** Estructura de gestión de crisis, planes, equipos y reglas de activación para crisis e incidentes críticos, así como planes de contingencia para reubicación, hibernación, evacuación, desastres y emergencias médicas, entre otros.
12. **Anexos.** Documentos y plantillas de apoyo, incluidos mapas del entorno operacional, listas de contactos, listas de verificación y formularios.

Hay una serie de cuestiones que tener en cuenta en relación con los planes de seguridad:

- Compartir los planes en formatos accesibles apropiados y explicarlos claramente al personal ayudará a garantizar su implementación exitosa.
- El personal que comprende el razonamiento que hay detrás de los procedimientos es más propenso a seguirlos: desarrollar el plan colectivamente con un grupo diverso de miembros del personal aumenta la probabilidad de que se cumpla.
- Una buena práctica es revisar los planes a medida que cambian las condiciones y ocurren los eventos, independientemente de la fecha ya programada para la próxima revisión.
- Algunos aspectos del plan pueden requerir conocimientos o habilidades especializados para su implementación.
- La gestión eficaz de los riesgos de seguridad depende de la práctica, mediante simulaciones y capacitación.

Revisión y actualización de los planes de seguridad

Incluso en un entorno estable y seguro, los planes de seguridad deben revisarse anualmente. En entornos de alto riesgo, se recomiendan revisiones más frecuentes para garantizar que el plan refleje los riesgos prevalentes y que la información esté actualizada. Algunos ejemplos de factores desencadenantes de una revisión pueden ser los siguientes:

- Cuando se producen cambios significativos en el contexto externo, especialmente como resultado de las acciones de cualquier actor importante en el lugar.
- Cuando se producen cambios significativos en la organización, como en el enfoque operacional, el personal o las relaciones con actores clave.
- Cuando la organización, u otra organización en la misma zona operacional o cerca de ella, experimenta un incidente de seguridad.

En las secciones siguientes se analizan dos de los elementos principales de un plan de seguridad: los procedimientos operativos estándar y los planes de contingencia. Otras secciones de un plan de seguridad, como el diagnóstico de riesgos y la gestión de crisis, se tratan con más detalle en otros capítulos de este informe.

- *Para obtener más información sobre los diagnósticos de riesgos, consulte el capítulo 4.1.*
- *Para más información sobre la respuesta a incidentes y la gestión de crisis, véase el capítulo 4.4.*

4.3.2 Procedimientos operativos estándar

Los procedimientos operativos estándar (POE) proporcionan instrucciones detalladas sobre cómo llevar a cabo las tareas o los procesos específicos necesarios para implementar el plan de seguridad, esencialmente, las instrucciones operativas para mitigar cada uno de los riesgos evaluados.

Una buena práctica requeriría POE independientes, redactados idealmente en un lenguaje claro y simple, para cubrir todas las áreas de las operaciones diarias en las que se han detectado riesgos. Estos procedimientos pueden referirse a una amplia variedad de actividades, desde rutinas diarias hasta procedimientos de respuesta a emergencias, y adaptarse para abordar los riesgos y los desafíos específicos presentes en el entorno operacional. Por ejemplo, en zonas donde viajar por carretera implica un riesgo de seguridad, generalmente la organización establecerá POE respecto a la evaluación de la seguridad de las rutas planificadas, las autorizaciones de viaje, los controles de seguridad de los vehículos, los registros a intervalos regulares, los límites de velocidad y el comportamiento en los puestos de control.

Lo ideal es que los POE estén redactados en un lenguaje claro y conciso, y que se evite el uso de jerga técnica, acrónimos y abreviaturas. A continuación se enumeran los elementos clave de un POE.

- **Título/encabezado:** indicación clara del nombre del procedimiento, que incluye el número de documento y la versión.
- **Propósito:** explicación breve de la intención y los objetivos del POE.
- **Alcance:** definición de lo que cubre el POE y a quién se aplica.
- **Responsabilidades:** descripción de las funciones y las responsabilidades de las personas involucradas en la ejecución del procedimiento.
- **Definiciones:** aclaración de términos o referencias que puedan resultar desconocidos.
- **Procedimiento:** instrucciones paso a paso para el personal que realiza la tarea o el proceso (la sustancia principal del POE).
- **Control de calidad:** especificación sobre cualquier control de calidad o inspección requerida.
- **Aprobación/autoría firma(s).**
- **Historial de revisiones:** registro de los cambios realizados en el POE a lo largo del tiempo.
- **Anexos:** cualquier material suplementario, formularios o listas de verificación.

Contar con POE bien desarrollados ayudará a garantizar la coherencia y a reducir el error humano. Cuando una organización define algo como un POE, generalmente se entiende como un requisito y no como una guía o un consejo. Dado que estos términos a veces se confunden o se utilizan indistintamente, es útil que la organización aclare al personal el nivel de cumplimiento esperado. Al mismo tiempo, sin embargo, *estándar* significa “la mayoría de las veces en la mayoría de los casos”, no que necesariamente deba prevalecer sobre el juicio profesional o el pensamiento crítico en circunstancias excepcionales. Lo ideal es que el personal evalúe la situación y pueda desviarse de los POE cuando sea necesario para la seguridad o para alcanzar objetivos críticos, documentando y justificando dichas desviaciones.

- *Para obtener información que podría ser útil para orientar el desarrollo de POE específicos, consulte la séptima parte, que cubre actividades organizacionales específicas y riesgos asociados, así como tipos particulares de amenazas.*

4.3.3 Planes de contingencia y continuidad

Planes de contingencia

Los planes de contingencia ayudan a una organización a gestionar eventos y situaciones de alto riesgo previstos, que interrumpen o hacen insostenibles las operaciones normales.

Las preguntas clave que guían el desarrollo de planes de contingencia son las siguientes:

- ¿Qué podría pasar?
- ¿Quién podría verse afectado?
- ¿Qué se necesita para responder?
- ¿Quién necesita estar informado?
- ¿Quién toma qué decisiones?
- ¿Qué se puede hacer para estar mejor preparado?

Los planes de contingencia y de gestión de crisis son conceptos relacionados pero distintos de la preparación organizacional. Las crisis requieren una respuesta organizacional que va más allá de las estructuras de gestión normales. No todas las contingencias califican como crisis; por ejemplo, algunas interrupciones, como la hibernación, pueden gestionarse dentro de los marcos operacionales normales sin necesidad de una gestión de crisis. La planificación para contingencias implica prepararse para posibles perturbaciones, y su gestión eficaz puede requerir una gestión de crisis.

► *Para obtener más información sobre la gestión de crisis, véase el capítulo 4.4.*

En la gestión de riesgos de seguridad, los planes de contingencia suelen centrarse en situaciones en las que la inseguridad aumenta repentina o drásticamente, lo que obliga a tomar decisiones sobre si se debe continuar con la programación y cómo hacerlo. En tales casos, una organización puede enfrentarse a las opciones de hibernación, reubicación o evacuación (en el caso de organizaciones internacionales) y puede abordarlas como fases progresivas y escalonadas a medida que empeoran las condiciones de seguridad. Los planes de contingencia pueden incluir factores desencadenantes específicos para cada fase o pueden ser un proceso caso por caso. Una buena práctica recomendaría establecer criterios objetivos para orientar la decisión a fin de eludir la tendencia natural a retrasar las decisiones difíciles.

La hibernación es a menudo la primera medida que se adopta cuando las circunstancias indican una mayor inseguridad. Si la situación se agrava, puede ser aconsejable trasladar al personal a un lugar más seguro. En circunstancias extremas, las organizaciones internacionales pueden decidir retirar del país a parte o a todo su personal (generalmente extranjeros), mientras continúan apoyando a los miembros del personal no evacuados. Las organizaciones nacionales generalmente no podrán evacuar a su personal y tendrán que recurrir al trabajo remoto, reubicarse en zonas más seguras o suspender las operaciones hasta que sea seguro reanudarlas. Se debe realizar un diagnóstico de riesgos antes de regresar al lugar y reanudar las actividades.

Hibernación

La hibernación implica detener el movimiento del personal y de los programas en un lugar determinado, pidiéndole al personal que se quede en casa o se refugie en una oficina o en otro edificio de la organización. Esto puede deberse a que abandonar la zona es imposible o demasiado peligroso, o porque se espera que la situación mejore en un futuro próximo. La hibernación puede ser una buena opción cuando quedarse en un lugar es más seguro que trasladarse o durante periodos temporales de mayor riesgo, como cuando hay elecciones. La conectividad a Internet ha introducido la posibilidad de que algunos funcionarios trabajen desde casa, lo que ha ampliado la definición tradicional de hibernación. La pandemia de COVID-19 demostró la viabilidad del trabajo remoto durante periodos prolongados para el personal con funciones que no requieren presencia física. En Afganistán, después de que los talibanes regresaran al poder en el 2021 y prohibieran a las mujeres afganas trabajar para organizaciones humanitarias, los acuerdos tácitos de “trabajo desde casa” permitieron a algunas organizaciones mantener el empleo de muchos miembros del personal mientras intentaban negociar exenciones o rebatir la prohibición.

Es conveniente para las organizaciones identificar una instalación de retiro o hibernación (y, si es posible, más de una) y equiparla con los siguientes elementos para posibles estancias prolongadas:

- alimentos, agua, botiquines de primeros auxilios y medicamentos esenciales;
- instalaciones para dormir, lavarse y usar el baño y ventilación;
- iluminación, fuentes de energía y cargadores;
- combustible y utensilios de cocina;
- equipo de comunicación;
- libros, juegos, vídeos u otros objetos de entretenimiento, y
- equipo de ejercicio y espacio para entrenamiento y recreación.

Si existe riesgo de bombardeo o ataque con artillería, las organizaciones podrían tener que montar habitaciones o búnkeres seguros o identificar refugios cercanos.

► *Para obtener más información sobre las habitaciones seguras y los refugios, consulte el capítulo 7.10, “Amenazas relacionadas con el combate y restos de material de guerra” y el capítulo 7.2, “Seguridad del sitio”.*

Evacuación y reubicación

La evacuación o la reubicación se refieren al retiro físico del personal (y, cuando sea posible y esté previsto, de sus familias) y los bienes de un entorno inseguro. La evacuación generalmente se refiere al traslado a otro país, mientras que la reubicación se refiere al desplazamiento dentro de un país. Esta situación puede ser precipitada por conflictos o eventos de peligro extremo, pero también puede ser forzada, como,

por ejemplo, en el caso de expulsión por parte del Gobierno. En algunas circunstancias puede ser prudente planificar una retirada temporal y preventiva, por ejemplo, retirando al personal de ciertos lugares previo a posibles acontecimientos políticos explosivos.

Es importante ser consciente de cuatro suposiciones comunes, pero a menudo erróneas, en relación con la evacuación y la reubicación:

- **El deterioro será gradual:** hay que tener en cuenta que los acontecimientos pueden adelantar los planes. La planificación por fases según niveles de seguridad, aunque útil, puede crear expectativas de una progresión lineal, cuando no siempre es así.
- **La evacuación y la reubicación se realizarán exactamente según el plan:** el personal no suele consultar el plan en una crisis repentina y aguda, es posible que hayan pasado por alto elementos importantes y no se hayan planificado, algunos miembros del personal pueden negarse a irse y factores externos pueden sustituir los planes anteriores y forzar ciertos resultados.
- **Salir será posible:** en muchas situaciones las rutas de evacuación pueden estar bloqueadas, la capacidad logística para la evacuación puede ser insuficiente o simplemente puede ser demasiado peligroso salir, y el personal tendrá que permanecer en el lugar y resistir la crisis.
- **Regresar será posible:** es posible que el personal evacuado y reubicado no pueda regresar rápidamente y que la organización deba retirarse del contexto o gestionar de manera remota el programa durante semanas, meses o incluso años.

La decisión de retirarse

La reubicación, y en especial la evacuación, es una decisión difícil tanto desde el punto de vista moral como operacional. En casi todos los casos, irse supondrá peores resultados para la población que necesita la asistencia y quedarse puede constituir una medida de protección para una población en peligro o al menos una presencia que sirva como testigo.

La decisión también puede verse influida por la presión de los donantes o el miedo a perder la financiación en el futuro, los desacuerdos del personal sobre la gravedad del riesgo, las conexiones familiares en la zona y la preocupación por perder la aceptación y la confianza de la comunidad.

El plan de contingencia deberá establecer claramente quién tiene la autoridad para tomar decisiones sobre la hibernación, la reubicación y la evacuación, y sobre qué hacer si hay opiniones divergentes.

Consideraciones interinstitucionales

En momentos de crisis grave, las reubicaciones (y en especial las evacuaciones) suelen requerir colaboración interinstitucional. Esto puede ser complicado debido a las diferentes valoraciones del riesgo. El hecho de que algunas organizaciones se marchen y otras no puede aumentar la vulnerabilidad de las que optan por quedarse. Es posible que ya no haya una masa crítica de organizaciones presentes, lo que puede fomentar el saqueo, los hurtos y los ataques. Además, no es viable ni práctico que una organización dependa de una entidad externa, como las Naciones Unidas o un Gobierno extranjero, para recibir apoyo en caso de evacuación o reubicación. Es aconsejable que las organizaciones estén preparadas para gestionar este tipo de situaciones de forma independiente.

Planificación y gestión de la retirada del personal

La política organizacional en relación con la reubicación y la evacuación debe documentarse y comunicarse claramente al personal y a los socios con antelación, como parte del deber de cuidado. Si las expectativas del personal difieren de la política, las consecuencias para cada miembro del personal, y para la moral general, podrían ser devastadoras. En la medida de lo posible, los derechos y las responsabilidades de los empleadores y los trabajadores en caso de evacuaciones y reubicaciones deben establecerse en los contratos de trabajo o en la política de seguridad, incluyendo las disposiciones que la organización adoptará respecto a los familiares que residan en el país. Las directrices pueden estipular, por ejemplo, que en los momentos de mayor riesgo para la seguridad, el personal que no participe en actividades críticas para el programa será reubicado o evacuado de la zona.

En el caso del personal nacional del país, debe quedar claro cuáles son sus derechos y los de sus dependientes en relación con la reubicación (dentro del país) y la evacuación (internacionalmente). Si esto se discute durante el proceso de elaboración de los planes de contingencia, estos miembros del personal pueden evaluar sus opciones con anticipación para optimizar su propia seguridad y la de sus dependientes. Es poco probable que las organizaciones internacionales puedan evacuar grandes cantidades de personal nacional a través de fronteras internacionales, pero en el caso de los miembros del personal que se enfrentan a riesgos especialmente elevados, la organización posiblemente tenga la responsabilidad ética de ayudar, por ejemplo, mediante instrumentos jurídicos internacionales y procedimientos nacionales de asilo. El apoyo al personal que se queda puede incluir el pago adelantado de varios meses de salario, teléfonos móviles, tarjetas telefónicas prepagadas, acceso a los edificios de la organización para ellos y sus familias o cartas de empleo o referencias.

En algunas circunstancias, puede ser apropiado que solo se retire una parte del equipo. La reubicación preventiva de parte del personal en momentos de tensión creciente, o como parte del procedimiento asociado a una fase de seguridad específica, puede disminuir la vulnerabilidad general al reducir el número de personas en situación de riesgo y hacer que una posible reubicación o evacuación de emergencia futura sea más manejable.

El personal que podría ser reubicado provechosamente en estos escenarios puede incluir cualquier puesto que no sea vital para la continuidad del programa. Las organizaciones también pueden considerar retirar al personal que se enfrenta a un riesgo particularmente alto, independientemente de si desempeñan funciones críticas para el programa. Por ejemplo, personas de determinadas nacionalidades o grupos étnicos o religiosos pueden ser un objetivo potencial.

A un miembro del personal puede resultarle psicológicamente difícil lidiar con la creciente inseguridad o puede percibirse como alguien que corre un riesgo alto. Debido a que los niveles inmanejables de estrés pueden provocar que se tomen decisiones equivocadas, es aconsejable retirar al individuo incluso si ocupa un puesto operacional clave.

Cuando las organizaciones internacionales evacúan al personal extranjero y suspenden la programación, las organizaciones locales pueden enfrentar mayores desafíos, riesgos y responsabilidades. A continuación se presentan algunas consideraciones que tener en cuenta.

- **Aumento de los riesgos de seguridad.** Las suspensiones, las evacuaciones o las reubicaciones por parte de las organizaciones internacionales pueden cambiar la dinámica local y exponer potencialmente a las organizaciones locales a mayores amenazas, por lo que es aconsejable que dichas organizaciones reevalúen sus riesgos y sus estrategias de mitigación en estos casos.
- **Continuidad operacional.** Es posible que las organizaciones locales necesiten adaptarse rápidamente para llenar los vacíos que dejan sus contrapartes internacionales cuando se retiran. Esto podría implicar asumir responsabilidades programáticas adicionales o funciones de liderazgo para mantener servicios críticos.
- **Limitaciones de recursos.** La evacuación de ciudadanos extranjeros suele coincidir con una reducción de la financiación y el apoyo material. Las organizaciones locales pueden necesitar comunicarse de manera proactiva con los donantes acerca de las necesidades financieras que siguen existiendo y explorar fuentes de financiación alternativas.
- **Oportunidades de partenariado.** Por el contrario, dado que posiblemente las organizaciones internacionales no puedan seguir ejecutando los programas debido a la reducción del personal, quizás recurran a las organizaciones locales para continuar los proyectos. Estas organizaciones querrán sopesar estas nuevas oportunidades frente a sus riesgos potenciales, como el aumento o la variación de las amenazas a la seguridad y las exigencias de cumplimiento, así como la presión adicional sobre la capacidad del personal en entornos ya caracterizados por amenazas elevadas.
- **Cuidado y apoyo del personal.** El personal puede experimentar un mayor miedo, estrés y ansiedad tras la evacuación y la reubicación de otras organizaciones. Las organizaciones pueden ayudar al bienestar de su personal brindándole apoyo psicosocial, comunicación clara y acuerdos de trabajo flexibles cuando sea posible.

Prepararse para una expulsión gubernamental: un caso especial

En el caso de expulsión gubernamental, muchos de los preparativos serán similares a una evacuación en respuesta a la inseguridad. Sin embargo, las organizaciones también podrían considerar lo siguiente:

- ¿Tratará la organización de apelar la decisión y, si es así, a través de qué medios (judicial, conversaciones directas con las autoridades, incidencia o presión como parte de un consorcio, campañas en los medios de comunicación, conversaciones con donantes o embajadas)?
- ¿Qué medidas se han tomado para proteger la información potencialmente sensible, confidencial o personal contra su divulgación involuntaria?
- ¿La expulsión pondrá al personal que permanezca en el país ante un riesgo específico?
- ¿Pueden tomarse medidas para evitar que el personal (especialmente el personal que se queda en el lugar) sea acosado o amenazado por las autoridades gubernamentales?
- ¿Se pagarán salarios o indemnizaciones al personal que permanezca en el lugar y durante cuánto tiempo? (Esto puede ser requerido por el gobierno).
- ¿Es posible minimizar el riesgo de que los activos sean embargados permanentemente?
- ¿Qué papel podrían desempeñar cualquier donante gubernamental u otros actores (como las Naciones Unidas) para anular la decisión o apelar ante las autoridades nacionales por un trato más tolerante?
- ¿Cuál será la reacción de los medios de comunicación (local e internacionalmente) y cómo se manejará?

Planificar y llevar a cabo una evacuación o reubicación

Es una buena práctica que las organizaciones revisen periódicamente los planes de evacuación y reubicación con el personal, especialmente si cada vez es más probable que sea necesaria una retirada. Esto puede hacerse mediante ejercicios de simulación o una reunión de equipo para revisar políticas, procedimientos y planes.

Logística y planificación de rutas

Al planificar una ruta de evacuación o reubicación, las organizaciones pueden considerar lo siguiente:

- ¿Qué rutas y medios de transporte son más viables en diferentes escenarios? Se recomienda planificar la ruta de manera detallada con antelación e incluir rutas alternativas.

- ¿Qué opción es más probable que reduzca el riesgo: moverse de forma llamativa (perfil alto) con logotipos y otras marcas identificables o de manera discreta sin nada de lo anterior?
- ¿Qué cantidad de transporte hay disponible y para cuántas personas? ¿Qué tipo de bienes o efectos personales se pueden llevar consigo?
- ¿Cuál es el medio de transporte más adecuado y apto para todo el personal? Por ejemplo, el personal con problemas de movilidad puede no ser capaz de caminar largas distancias.
- ¿Hay alojamiento o campamentos seguros a lo largo del camino si las rutas se vuelven inseguras?
- ¿Funcionarán las comunicaciones a lo largo de toda la ruta? y ¿en qué puntos debe el personal ponerse en contacto con sus colegas?
- ¿Quién proporcionará el transporte? Si no es la propia organización, es importante conocer la capacidad, los requisitos de procedimiento y los límites de la responsabilidad de la entidad transportista.
- ¿La reubicación o evacuación se realizará en colaboración con otras organizaciones? Si bien puede ser más seguro viajar en un convoy de vehículos con otras organizaciones, también puede significar menos control sobre cómo se lleva a cabo la salida. Puede ser útil que las organizaciones discutan de antemano cómo se tratarán estas cuestiones.

Preparativos

Los planes deben tener como objetivo identificar los sitios que se puedan utilizar como puntos de reunión, donde el personal debe reunirse antes de partir. Estos puntos deben ser accesibles, seguros, lo suficientemente grandes para acomodar a un gran número de personas y varios vehículos y disponer de comunicaciones fiables y existencias de emergencia.

Se debe disponer de información precisa y actualizada sobre cuántos miembros del personal (y sus dependientes) califican para una evacuación internacional. En general, es útil tener información clave sobre todo el personal que pueda ser evacuado o reubicado, incluido cualquier requisito especial, como necesidades médicas o si algún miembro del personal viajará con niños pequeños. Las personas que vayan a marcharse deberán estar preparadas con la documentación personal pertinente para facilitar el viaje. Tener documentos organizacionales esenciales almacenados electrónicamente (especialmente en la nube) puede ayudar a garantizar que no se pierdan datos y facilitar el acceso por parte del personal ubicado fuera de la zona de reubicación o evacuación.

► *Para obtener más información sobre la protección de información sensible, véase el capítulo 6.1.*

Cierre de oficinas

Al desarrollar planes de contingencia para el cierre de una oficina debido a una emergencia, las organizaciones quizás deseen considerar tanto la gestión de activos

como el cumplimiento legal. Es aconsejable identificar los activos que posiblemente deban protegerse o transferirse, garantizando que las disposiciones se correspondan con los requisitos de los donantes, la organización y el gobierno local. También deben preverse las obligaciones legales con propietarios, proveedores y autoridades para evitar retrasos o disputas. Se deben evaluar los riesgos de seguridad asociados con las transferencias de activos a socios o comunidades. Los planes de contingencia también pueden incluir la protección de activos clave como vehículos y equipos de comunicación, que podrían reubicarse o desactivarse para evitar su uso indebido. Es posible que el personal desee destruir información sensible antes de la salida.⁶⁶

Destino

Al seleccionar un destino para el personal que se traslada, cuando este no sea su lugar de residencia, las organizaciones deben asegurarse de que el sitio brinde la seguridad y la comodidad adecuadas, así como acceso a los servicios esenciales. El alojamiento elegido, por ejemplo, un hotel, debe ser seguro y capaz de satisfacer cualquier necesidad médica, dietética o de comunicación.

Después de la evacuación o la reubicación

Se pueden tomar una serie de medidas prácticas e inmediatas después de una reubicación o evacuación:

- En cuanto tenga la oportunidad, comuníquese con el equipo directivo de la organización para brindarles una actualización.
- Si la evacuación fue internacional, comuníquese con los funcionarios del país de llegada (si aún no lo ha hecho), así como con las embajadas pertinentes y las autoridades locales si es probable que la estadía se prolongue.
- Establezca o restablezca el contacto y la comunicación con el personal que quedó en el lugar (ver abajo).
- Prepare un informe para la oficina central y los donantes, con actualizaciones detalladas sobre el personal, los activos, las existencias, las finanzas y las obligaciones pendientes en el momento de la evacuación o de la reubicación.
- Informe al personal evacuado o reubicado y brinde apoyo psicosocial, ya que este cambio puede provocar una variedad de sentimientos difíciles, como agotamiento emocional y sensación de fracaso, enojo o culpa por los que quedaron en el lugar.

66 Para obtener orientaciones más detalladas, consulte Safer Edge (2014) *Office closure*, Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/office-closure/>).

Consideraciones sobre el cuidado del personal después de la reubicación o la evacuación

Preparativos previos a la llegada

- Kit de bienvenida (incluye agua embotellada, comida, artículos de aseo, batería externa cargada y cables de carga, tarjeta SIM local con plan de datos y botiquín de primeros auxilios).
- Identificar el hospital o instalación sanitaria más cercana en el destino en caso de que el personal necesite atención médica a su llegada.

Al llegar

- Proporcionar al personal un kit de bienvenida.
- Ayudar al personal a comunicarse con sus seres queridos.
- Identificar cualquier necesidad médica urgente o inmediata, como lesiones o medicamentos que necesiten ser renovados.
- Proporcionar al personal una sesión informativa de seguridad sobre el lugar.
- Ayudar al personal a obtener moneda local.
- Proporcionar al personal la información de contacto del personal de apoyo relevante y su disponibilidad.
- Para el primer día de llegada, se recomienda que el equipo de apoyo permanezca en un área pública o visible (p. ej., el vestíbulo del hotel o una cafetería) que sea de fácil acceso para que el personal pueda acudir en busca de asistencia.
- Es probable que el personal esté agotado por el viaje y quiera descansar en sus habitaciones. Pídeles que se pongan en contacto con el equipo de asistencia para saber que están bien. Por ejemplo, invite a las personas a reunirse para cenar y pídeles que envíen un mensaje de texto si no desean asistir o pídeles que envíen un mensaje de texto a una hora determinada para poder comprobar rápidamente cómo se encuentran.

Durante la estancia

- Asegurarse de que algún miembro del equipo de apoyo se ponga en contacto al menos una vez al día con el personal afectado. Puede ser una comunicación breve, como un mensaje o una llamada, o un encuentro social informal.
- Ayudar al personal a continuar su viaje hacia sus hogares, según sea necesario.
- Asegurarse que el personal sepa si reúne los requisitos para recibir comidas y compensaciones por otros gastos (viáticos) durante la reubicación o la evacuación.

- Ayudar al personal a encontrar proveedores de servicios médicos o farmacias locales para renovar recetas.
- Conectarlos con su seguro de salud y su proveedor de asistencia médica o apoyo psicológico según sea necesario.

► Véase el capítulo 5.4 para obtener más información sobre el cuidado del personal.

Planes y enfoques de continuidad

Algunas organizaciones pueden no estar en condiciones de reubicarse, como es el caso, por ejemplo, de las organizaciones locales que solo operan en un único lugar. La hibernación puede consistir en cerrar las oficinas y desvincular al personal, “reintegrarse” en la comunidad y esperar a que se den condiciones más favorables para reiniciar los programas. Varias organizaciones locales de algunas partes de Afganistán utilizaron esta estrategia durante años, entre 2001 y 2021, interrumpiendo y reanudando repetidamente sus actividades según lo dictaban los acontecimientos políticos y las condiciones de seguridad.

Gestión remota de programas

Cuando las reubicaciones o las evacuaciones duran mucho más de lo planeado originalmente, los planes de continuidad pueden evolucionar hacia una programación remota extendida a través de socios o una gestión remota de programas. El cambio a la gestión remota de programas puede incluir uno o más de los siguientes aspectos:

- Retirar del lugar donde se ejecuta el programa a determinadas categorías de personal (por ejemplo, no residentes en la zona en cuestión), en particular a quienes se considera que corren un riesgo especialmente elevado.
- Alterar las estructuras de gestión para dar más responsabilidad al personal que permanece en el lugar.
- Establecer acuerdos operacionales nuevos, o modificar los existentes, con socios, incluidas las organizaciones y las autoridades locales.
- Contratar supervisores externos para garantizar el cumplimiento de los objetivos del programa en ausencia de una gestión presencial.

Cuando se utiliza como último recurso y como adaptación *ad hoc*, la gestión remota de programas suele presentar serios desafíos. A continuación se mencionan algunos de ellos:

- Problemas éticos derivados de la transferencia de riesgos, en especial si se pide —y se incentiva fuertemente— a los miembros del personal o a los socios que asumen las responsabilidades del programa que acepten mayores niveles de riesgo.
- Dificultades para evaluar los riesgos de seguridad cambiantes y el entorno en general, ya que el personal y los socios en el lugar pueden ser menos sensibles a los cambios sutiles.
- Dificultades en las comunicaciones y la logística.
- Implicaciones de seguridad al entregar dinero o suministros al personal y a los socios.
- Dependencia excesiva de unos pocos miembros del personal en entornos de estrés elevado, lo que conduce al agotamiento.
- Dificultad para garantizar una supervisión programática y financiera adecuada.
- Dificultades para satisfacer los requerimientos de los donantes respecto al monitoreo y a la presentación de informes.

Las lecciones prácticas de la COVID-19 han mitigado algunas de estas dificultades, especialmente las relacionadas con las comunicaciones remotas continuas, la supervisión remota y las capacidades de capacitación remota, pero no todas.⁶⁷

Gestión de riesgos de seguridad durante la gestión remota de los programas

La gestión remota de los programas plantea una nueva serie de consideraciones financieras, de seguridad y contractuales, lo que implica un nuevo análisis de beneficios y riesgos. Continuar con los programas bajo gestión remota puede ser más arriesgado que cerrarlos por completo, y puede haber riesgos asociados con el cierre de un programa que se ha gestionado de forma remota si ello provoca el descontento del personal afectado.

Si es posible seguir operando bajo un enfoque de gestión remota, probablemente se requerirán cambios en la estructura, el estilo y el enfoque de gestión. Los procedimientos de gestión pueden llegar a ser más complejos y onerosos, con controles o informes frecuentes sobre cuestiones financieras, programáticas o de personal. Es posible que sea necesario desarrollar nuevas formas de monitorear los programas, como tomar fotos de los resultados del proyecto (p.ej., fuentes de agua o escuelas construidas) acompañadas de las coordenadas GPS.

Las condiciones de seguridad pueden cambiar rápidamente, por lo que es importante encontrar formas de supervisar la situación cambiante y reevaluar las disposiciones si los riesgos para el personal que permanece en el lugar se vuelven inaceptablemente altos. Además del personal en el lugar, se puede reunir información relevante para los diagnósticos de riesgos a través de contactos locales (p.ej., comerciantes y autoridades locales) y compartiendo información y análisis con otras organizaciones que operan en la zona.

67 Global Interagency Security Forum (2020) *Keeping up with COVID-19: Essential guidance for NGO security risk managers* (www.gisf.ngo/resource/keeping-up-with-covid-19-essential-guidance-for-ngo-security-risk-managers/).

Es posible que se necesiten recursos y capacitación adicionales para apoyar al personal que sigue en el lugar o a los socios que hayan asumido responsabilidades laborales adicionales, así como financiación y apoyo material, como vehículos y equipos de comunicación, por ejemplo.

► *Para obtener más información sobre los acuerdos de partenariado, véase el capítulo 3.5.*

Otras prácticas que contribuyen al éxito de la gestión remota de programas son las siguientes:⁶⁸

- Establecer procedimientos e instrucciones claros para el personal y los socios sobre las comunicaciones y la presentación de informes sobre las actividades y su progreso.
- Incluir el escenario de gestión remota en los ejercicios de planificación de contingencia, considerando con antelación los socios potenciales, las estructuras de gestión y supervisión y las estrategias de salida y transición.
- Trasladar al personal local o a los representantes de los socios fuera del área para celebrar reuniones y debates de gestión periódicos.
- Realizar inspecciones puntuales y visitas no programadas, según sea posible.
- Utilizar supervisores externos o cotejar y verificar la información de monitoreo con otras organizaciones y contactos locales.
- Establecer y mantener una red local de proveedores de información, intermediarios y facilitadores dentro de la comunidad local.

Retorno

Una diagnóstico de riesgos puede indicar si es lo suficientemente seguro regresar o aumentar la presencia del personal y quién en la organización debe asumir la responsabilidad de la decisión. En ausencia de un cambio bastante radical en el lugar (p. ej., un cambio en el control territorial de un actor a otro), el retorno también puede ser gradual y por etapas. En primer lugar, podrían realizarse algunas misiones exploratorias breves para reevaluar la situación; después, posiblemente, una presencia más permanente de algunos miembros clave del personal en una base de operaciones, seguida del regreso gradual de más personal a más bases de operaciones.

68 Stoddard, A., Harmer, A. y Renouf, J. S. (2010) *Once removed: lessons and challenges in remote management of humanitarian operations for insecure areas*, Humanitarian Outcomes (<https://humanitarianoutcomes.org/publications/once-removed-lessons-and-challenges-remote-management-humanitarian-operations-insecure>).

Ejemplo: Consideraciones sobre el retorno

Después de que la guerra civil se intensificara en Sudán del Sur en el 2016, muchas organizaciones humanitarias redujeron sus operaciones y evacuaron al personal extranjero del país. Al reiniciar sus operaciones, una organización internacional enfrentó desafíos importantes al implementar programas en zonas rurales relacionados con la inseguridad, el acceso y las comunicaciones. Después de varios meses, el director de seguridad organizó una reunión en la que participaron representantes de varios departamentos en el país, incluidos los de Programas, Finanzas, Recursos Humanos, Subvenciones, Respuesta a Emergencias y Educación.

A las reuniones de planificación asistieron colegas de la oficina central, de la oficina regional y del personal nacional. Durante la sesión que duró una semana, el equipo identificó riesgos y elaboró estrategias de mitigación, creó programas de bienestar para el personal nacional y determinó los recursos de seguridad necesarios. El personal nacional dirigió debates sobre riesgo y bienestar, lo que dio como resultado cambios significativos, como la concesión a todo el personal nacional de licencia de descanso y recuperación remunerada cada dos meses.

Como resultado de esta planificación de contingencia interfuncional iniciada por el personal de seguridad, los programas se reanudaron, los donantes aumentaron su financiación y se cumplieron los objetivos programáticos de la organización.

La información clave para evaluar la situación de seguridad para una misión exploratoria puede incluir:

- La situación real sobre el terreno (seguridad, militar, política), así como los perfiles personales de los empleados que regresan y los posibles riesgos asociados.
- Los posibles cambios en los tres o seis meses siguientes y sus implicancias en materia de seguridad.
- El estado de las infraestructuras locales (aeropuertos y carreteras), las comunicaciones y los servicios (p.ej., los bancos).
- El paradero y las condiciones del personal no evacuado.

- El estado de los bienes, los activos y las existencias que quedaron.
- La disponibilidad de suministros esenciales, especialmente alimentos, agua y combustible.
- La imagen o reputación de la organización a nivel local y cómo gestionar las percepciones.
- El nivel de ataques directos contra las organizaciones humanitarias y, en el caso de organizaciones internacionales o aquellas con vínculos extranjeros, contra elementos extranjeros.
- Capacidad organizativa para gestionar la seguridad en el contexto actual.
- Un análisis de los riesgos y los beneficios generales.

Más información

Orientación y recursos

Bickley, S. (2017). *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*. Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>)

Davis, J. et al. (2020). *Security to go: a risk management toolkit for humanitarian aid agencies*. 4.ª edición. Global Interagency Security Forum (<https://gisf.ngo/resource/security-to-go/>).

Global Interagency Security Forum. (2020). *Keeping up with COVID-19: Essential guidance for NGO security risk managers* (www.gisf.ngo/resource/keeping-up-with-covid-19-essential-guidance-for-ngo-security-risk-managers/).

Global Interagency Security Forum. (s.f.a). 1. *Security plans*. NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/1-security-plans/>).

Global Interagency Security Forum. (s.f.b). 5. *Contingency plans*. NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/5-contingency-plans/>).

Safer Edge. (2014). *Office closure*. Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/office-closure/>).

Investigación y análisis

Donini, A. y Maxwell, D. (2013). From face-to-face to face-to-screen: remote management effectiveness and accountability of humanitarian action in insecure environments. *International Review of the Red Cross* 95(890) (<https://doi.org/10.1017/S1816383114000265>).

Stoddard, A., Harmer, A. y Renouf, J. S. (2010). *Once removed: lessons and challenges in remote management of humanitarian operations for insecure areas*. Humanitarian Outcomes (<https://humanitarianoutcomes.org/publications/once-removed-lessons-and-challenges-remote-management-humanitarian-operations-insecure>).

4.4 Respuesta a incidentes y gestión de crisis

Cuando se produce un incidente de seguridad o una crisis, responder eficazmente implica tomar medidas para gestionar y mitigar los impactos, así como gestionar y aprender de la información relacionada con el incidente. Este capítulo comienza con los componentes informativos y luego se describen los elementos clave de la respuesta y del seguimiento posterior al incidente. También se presenta una serie de estructuras y enfoques para la gestión de incidentes y de crisis considerados generalmente buenas prácticas. Sin embargo, cada evento y organización será diferente, por lo que es importante su adaptación a las circunstancias individuales, incluidas las estructuras organizativas.

4.4.1 Informes y análisis de incidentes

La gestión de información sobre incidentes de seguridad es el proceso de recopilación y uso de información relacionada con incidentes de seguridad y protección para respaldar la toma de decisiones, las políticas y los procedimientos dentro de una organización. Es un componente esencial del aprendizaje dentro de una organización y garantiza que las experiencias relacionadas con la seguridad se registren y analicen para mejorar los procesos organizacionales. Esto lo convierte en un elemento importante para cumplir con el deber de cuidado de una organización. Los informes de incidentes respaldan la seguridad del personal y la seguridad operativa de cuatro maneras principales:⁶⁹

- **Informe de incidentes y respuesta inmediata.** Alertar a los equipos pertinentes para que estén al tanto y para que, si es necesario, puedan brindar ayuda a cualquier persona afectada durante un incidente. También se puede alertar a otros actores humanitarios que operen en la zona para reforzar la seguridad de la comunidad en general.
- **Análisis de incidentes y lecciones aprendidas.** Analizar el incidente e implementar las lecciones aprendidas para evitar que ocurran incidentes similares en el futuro y responder de manera más efectiva si ocurren.
- **Análisis del contexto.** El monitoreo de incidentes y el análisis de tendencias y patrones informan los análisis del contexto y las evaluaciones de los riesgos para la seguridad. El análisis de datos agregados de incidentes procedentes tanto del interior como del exterior de la organización ayuda a la toma de decisiones e indica si es necesario adaptar los procedimientos.
- **Toma de decisiones estratégicas y políticas informadas.** Permitir el intercambio de información sobre incidentes de seguridad internamente dentro de una organización para fundamentar acciones y decisiones para mejorar las formas de trabajar.

⁶⁹ Estos puntos se extrajeron y adaptaron del *Manual de gestión de la información sobre incidentes de seguridad*, disponible en: <https://siim.insecurityinsight.org/tools-and-resources/handbook-guide-and-tools>.

Una gestión sólida de la información sobre incidentes de seguridad también puede ayudar a las organizaciones a cumplir con cualquier requisito de notificación legal o reglamentario tras un incidente.

Informe de incidentes y socios

Algunas organizaciones pueden tener acuerdos de партнериario que incluyan la recopilación de informes de incidentes de sus organizaciones socias (aunque esto todavía es poco común). Los socios pueden utilizar esta información para apoyarse mutuamente a la hora de aprender de los incidentes y para ayudarse a satisfacer colectivamente cualquier necesidad de gestión de riesgos de seguridad identificada. Lo ideal es que el intercambio de información sobre incidentes entre socios se base en el apoyo mutuo como un medio para mejorar de manera colaborativa la seguridad del personal, más que como una expectativa de cumplimiento, incluso si por razones legales o reglamentarias esto puede ser un requisito.

► Véase el capítulo 3,5 para obtener más información sobre buenas prácticas al trabajar con socios.

Informe de incidentes y respuesta inmediata

Las organizaciones se benefician de poseer procedimientos de denuncia de incidentes bien establecidos y de garantizar que el personal esté capacitado sobre cómo informar un incidente y buscar ayuda. Los incidentes graves deben notificarse inmediatamente por los medios más eficaces, por ejemplo, por teléfono o radio, y los informes deben cubrir solo la información más esencial (véase el recuadro abajo). Los incidentes en curso requieren actualizaciones periódicas.

El informe inicial puede ir seguido de un reporte una vez que el personal haya superado la situación inmediata y haya recibido toda la ayuda médica y psicosocial urgente que necesite (esto es diferente de un informe psicológico, que se analiza con más detalle en el capítulo 5.4). Puede ser útil conceder un tiempo a las personas implicadas en un incidente para que lo comenten antes de recopilar sus ideas para elaborar un informe más formal sobre el incidente. En el caso de un incidente grave que pueda afectar a otras personas que viven o trabajan en la zona, la organización podría preferir alertar a las personas de otras organizaciones (y, cuando corresponda, a las autoridades locales y a la población) para que puedan tomar precauciones. Esto debe hacerse de manera que se garantice la confidencialidad de las personas afectadas y sin poner al personal en mayor riesgo.

Información clave al reportar inicialmente un incidente

- ¿Quién está involucrado? ¿Quiénes son las víctimas (si las hay)?
¿Se trata de personal de la organización, personal del socios o consultores? ¿Cuál es su género y grupo étnico?
- ¿Qué pasó?
- ¿Dónde (lo más preciso posible) ocurrió el incidente?
- ¿Cuándo ocurrió el incidente?
- ¿Qué se ha hecho hasta ahora al respecto? ¿Qué medidas de respuesta a emergencias se han adoptado?
- ¿Qué ayuda se necesita? ¿Se requiere una respuesta inmediata adicional? ¿La situación continúa?

Es importante alertar a los colegas y a los asociados sobre un incidente lo antes posible, cuando sea seguro hacerlo, incluso si aún no se ha obtenido toda la información. Generalmente se redacta un informe más completo después del incidente y de la respuesta inmediata, aunque en situaciones prolongadas (p.ej., un secuestro) es posible que se elabore un informe antes de que finalice el incidente.

► *Para obtener más información sobre situaciones de secuestro y rapto, véase el capítulo 7.9.*

Es una buena práctica que las organizaciones tengan un formulario de informe de incidentes estándar que sea familiar y fácilmente accesible tanto en línea como por otros medios. Algunas organizaciones han invertido en programas informáticos que permiten realizar informes mediante un portal o una aplicación en dispositivos móviles. Cualquiera que sea el formato utilizado, lo importante es que se proporcione toda la información clave y sea accesible para todo el personal pertinente. Elaborar plantillas sencillas y fáciles de usar puede incentivar la elaboración de informes.

El informe de incidentes puede centrarse en algunas preguntas básicas: ¿Qué pasó? ¿Quién hizo qué? ¿A quién? ¿Cuándo? ¿Dónde? (Es posible que parte de esta información no se incluya por ser confidencial). Es importante que el personal competente verifique toda esta información en la medida de lo posible. Puede o no ser relevante agregar algo sobre el “por qué” y “por qué esta organización o este miembro del personal”. A veces es obvio porque lo dicen los agresores, pero en otros casos puede ser solo una especulación. Es importante saber si la organización y su personal fueron el objeto específico del ataque y, de ser así, por qué, sobre la base de la información disponible. El informe puede indicar el grado de confianza en las respuestas a estas preguntas y ser transparente sobre cuánto es especulación.

El subregistro es uno de los elementos más desafiantes en la gestión de información sobre incidentes de seguridad. Esto a menudo se debe a una falta de comprensión o familiaridad con el proceso de denuncia de incidentes, incluyendo cómo y quién utilizará la información. Esto se puede solucionar estableciendo un proceso de denuncia sencillo con plantillas fáciles de usar y capacitando al personal sobre cómo y por qué reportar.⁷⁰ Otro desafío importante puede ser la falta de acceso a los mecanismos de reporte. Esto puede deberse a barreras lingüísticas (p.ej., cuando los reportes se hacen en inglés) u otros factores, incluida la cultura organizacional (p.ej., si existe una cultura de culpar o avergonzar o si reportar se considera una carga burocrática en lugar de una oportunidad para aprender y mejorar). Otros desafíos comunes con los informes de incidentes son los siguientes:

- Falta de tiempo y de recursos para reportar o gestionar información de incidentes; en lugares con una frecuencia alta de incidentes puede resultar difícil para los referentes o puntos focales procesar grandes volúmenes de informes de incidentes de manera eficiente.
- Formatos o procedimientos para reportar incidentes inconsistentes en los diferentes departamentos u oficinas.
- Sesgo y subjetividad; los informes pueden estar influenciados por sesgos, percepciones o interpretaciones personales. Por ejemplo, el personal puede no ser sensible a ciertos tipos de incidentes y quizás no considere relevante reportarlos.
- Desconocer la identidad de los agresores o sus motivos hasta mucho tiempo después o, en algunos casos, nunca llegar a conocerlos. Es importante indicar el grado de confianza sobre las declaraciones y cambiar los registros organizacionales internos si surgen detalles nuevos.
- Una reticencia natural a reconocer que los actos u omisiones de la organización o de parte de su personal han contribuido a que se produzca un incidente. El personal puede temer medidas disciplinarias u otras represalias por no cumplir los requisitos organizacionales.

⁷⁰ Insecurity Insight y DisasterReady han elaborado conjuntamente una guía móvil para el personal sobre cómo gestionar y reportar incidentes. Véase: <https://siim.insecurityinsight.org/tools-and-resources/siim-app-and-short-guides>.

- Dificultades de clasificación, por ejemplo, para distinguir entre hurto, allanamiento y robo a mano armada, y entre secuestro y rapto. Todas las personas que reporten incidentes deben entender claramente la definición de estas diferentes categorías. Puede ser útil contar con sistemas de clasificación organizacional, y también hay orientación externa disponible.⁷¹

Es importante evitar que estos desafíos y la confusión o desacuerdo sobre las clasificaciones y la terminología obstaculicen el establecimiento de un sistema para reportar incidentes. Si los miembros del personal no pueden aplicar las clasificaciones de manera consistente, si hay barreras idiomáticas o si el personal encuentra que el proceso es abrumador o desalentador, el personal de seguridad debe tratar de asegurarse de que la información quede registrada. Algunas organizaciones y plataformas de seguridad centralizan la clasificación de los incidentes, de modo que el personal solo tiene que transmitir la información de que dispone lo más rápido posible, y los referentes de seguridad hacen luego un seguimiento con ellos para que respondan a las preguntas que sean necesarias y realizan la clasificación y el registro formal de forma centralizada.

¿Qué incidentes se considera que deben reportarse?

Se requiere orientación gerencial para garantizar que las personas comprendan qué se espera que informen y cómo se puede utilizar esa información. Incluso en caso de duda, se debe alentar al personal a informar.

Un incidente de seguridad es cualquier cosa que cause daño al personal o a personas asociadas, o pérdida o daño a los activos. Un *cuasiincidente* o *cuasiaccidente* es algo que casi causó tal daño, perjuicio o pérdida. Es una buena práctica incluir incidentes que tengan el potencial de causar daño (es decir, una amenaza). Una acción amenazante puede manifestarse por escrito, verbalmente o mediante un gesto físico, siempre que indique de forma creíble la intención de un actor de causar daño. Es importante incluir incluso los incidentes menores y los cuasiincidentes.

La mayoría de las organizaciones registran los incidentes de seguridad tanto accidentales como intencionales, como, por ejemplo, los accidentes de tráfico y los ataques deliberados contra el personal.

⁷¹ Véase, por ejemplo, la clasificación de incidentes de Insecurity Insight: <https://siim.insecurityinsight.org/tools-and-resources/classification-of-incidents>.

Los informes también pueden incluir incidentes o cuasiincidentes que afecten a otras entidades involucradas en el programa, como las organizaciones socias y los contratistas. También puede ser útil incluir en los requisitos de notificación cualquier incidente en el que un miembro del personal haya causado daño a un tercero, o pérdida o daño a la propiedad o los activos de un tercero. Pueden incluirse otros tipos de incidentes si indican tendencias en el entorno operacional, como disturbios en la comunidad o casos de violencia cerca de los lugares de ejecución de los proyectos.

En determinadas circunstancias, como en los casos de acoso y violencia sexual y cuando el incidente es perpetrado por un empleado (es decir, incidentes de salvaguardia), algunas organizaciones pueden tener mecanismos de reporte separados. El motivo puede ser que estos incidentes normalmente no forman parte de las responsabilidades de la función de seguridad y también porque es sumamente importante garantizar la confidencialidad y la seguridad del informante. Si es posible garantizar la confidencialidad, las organizaciones también se beneficiarían de elaborar un informe de incidentes de seguridad. Registrar los incidentes en un sistema central ayuda a trazar las tendencias e implementar medidas de mitigación adecuadas.

Análisis de incidentes y lecciones aprendidas

El contacto de seguimiento con el personal afectado puede tener lugar en diferentes momentos, dependiendo de la gravedad del incidente y de la forma como se haya informado. Una buena práctica es que los miembros del personal responsables, como los referentes de seguridad, busquen cualquier información adicional no incluida en el informe del incidente y organicen una reunión informativa sobre los hechos con las personas afectadas para identificar lecciones. Estas se centran en los hechos del incidente en lugar de en las respuestas emocionales al evento. Al planificar estas reuniones, se deben tener en cuenta las cuestiones de confidencialidad, si la sesión informativa debe estar a cargo de profesionales capacitados (no necesariamente el personal de seguridad) y las necesidades individuales del personal afectado (como el idioma) y cómo pueden adaptarse. En el caso de que el incidente se haya producido porque el personal no siguió los procedimientos, la organización tendrá que considerar la necesidad de aplicar medidas disciplinarias y de alentar al personal a notificar los incidentes.

Una vez recopilada la información sobre el incidente, el personal pertinente puede analizar con más profundidad qué sucedió y por qué. Las preguntas clave que considerar durante el análisis del incidente incluyen las siguientes:

- ¿Cuál fue la causa y el impacto del incidente? Se deben considerar las características identitarias y las percepciones de la organización y de los individuos afectados, y si estas influyeron en la motivación del incidente. Por ejemplo, ¿se atacó deliberadamente a un miembro del personal en particular debido a su grupo étnico?
- ¿Han ocurrido incidentes similares en el pasado (incluso en otras organizaciones que trabajan en la misma zona)?
- ¿Se siguieron los procedimientos de la organización?
- ¿Se gestionó adecuadamente la respuesta al incidente, incluido el proceso de denuncia? ¿Qué se podría haber hecho de manera diferente?

Los informes de incidentes transparentes y consistentes ayudan a mantener la confianza entre el personal, las partes interesadas y el público. Demuestra que la organización se toma en serio la seguridad y es proactiva a la hora de abordar las inquietudes. Comunicar al personal y a otras personas involucradas las lecciones aprendidas, las decisiones tomadas y las medidas adoptadas puede mejorar la comprensión y la confianza de los miembros del personal en la gestión de la información de incidentes y puede alentar la presentación de denuncias.

Análisis del contexto

Los informes de incidentes pueden ayudar en gran medida al personal de seguridad a comprender el contexto operacional y a predecir el tipo de incidentes o amenazas que pueden ocurrir en el futuro. Una visión general fiable de los incidentes notificables en todo el mundo, elaborada a partir de una base de datos, permite realizar un análisis más exhaustivo de la seguridad a nivel nacional, regional y mundial, así como en relación con programas y perfiles organizacionales o de personal específicos.

Muchas organizaciones humanitarias cuentan con sistemas internos de reporte de incidentes, desde simples hojas de cálculo de Excel hasta portales o aplicaciones que muestran los datos en tableros.

► *Para obtener más información sobre los tableros de información, véase el capítulo 3.4.*

Tener un sistema para gestionar y registrar los datos sobre los incidentes estandariza el tipo de incidentes que se informa, el tipo de información que se recopila y la clasificación de los incidentes, lo que permite un análisis más profundo de las tendencias y los patrones. Estos datos pueden revelar la concentración geográfica de los incidentes, proporcionar información sobre los tipos de incidentes y mostrar si el número total de incidentes está aumentando o disminuyendo. Este tipo de información puede a su vez ayudar a decidir dónde asignar recursos de seguridad (humanos y financieros) y dónde

se necesita más inversión, por ejemplo, en capacitación, tecnología o actualizaciones de infraestructura. El análisis de la información sobre los incidentes puede ayudar a garantizar que los recursos se destinen a donde más se necesitan para mejorar la seguridad y la resiliencia de las operaciones.

El análisis de incidentes individuales y de datos agregados sobre incidentes también es clave para el aprendizaje y el desarrollo organizacional. Este análisis ayuda a las organizaciones a identificar las tendencias, el origen y los problemas sistémicos que deben abordarse y permite realizar mejoras específicas en los protocolos de seguridad, en los programas de capacitación y en los procedimientos operacionales. La información también puede utilizarse para determinar y estructurar la orientación y la formación del personal, los visitantes y los viajeros, así como los protocolos correspondientes.

Las organizaciones querrán gestionar quién tiene acceso a las bases de datos de incidentes para proteger la privacidad de las personas afectadas. Sin embargo, es importante que se comparta la información, y las organizaciones deben permitir a los usuarios ver patrones y tendencias agregados sin revelar información sensible sobre incidentes específicos. Esto se puede lograr estableciendo restricciones de acceso en las bases de datos o elaborando informes a partir de datos que puedan compartirse más ampliamente.

Comparar los datos sobre incidentes con los de otros agentes en los mismos lugares puede facilitar un análisis más objetivo de los patrones de incidentes y ayudar a determinar tendencias si los datos se analizan a lo largo del tiempo. Es posible acceder a datos de incidentes externos a través de foros de seguridad interinstitucionales y de bases de datos de código abierto (consulte la sección “Más información” para ver ejemplos). Algunas organizaciones también pueden tener acuerdos de intercambio de datos sobre incidentes entre sí, por ejemplo, entre organizaciones socias. Todos los datos externos deben analizarse considerando la validez y la fiabilidad de los datos sobre incidentes compartidos. Las organizaciones deben procurar compartir datos para la gestión de riesgos de seguridad de una manera que garantice la confidencialidad y promueva la colaboración.⁷²

Toma de decisiones estratégicas y políticas informadas

Los datos sobre incidentes de seguridad pueden fundamentar la toma de decisiones en toda la organización, dentro y fuera de las funciones de seguridad, y las organizaciones deben tener procedimientos para compartir y utilizar los datos sobre incidentes internamente.

72 Insecurity Insight y GISF han desarrollado una guía y herramientas sobre cómo compartir información sobre incidentes de seguridad entre organizaciones, que se pueden consultar aquí: <https://gisf.ngo/long-read/ngo-security-collaboration-guide/> y <https://siim.insecurityinsight.org/tools-and-resources/siim-in-ngo-security-collaboration>.

La información obtenida del análisis de incidentes puede orientar la planificación de programas, las propuestas de financiación, las descripciones de puestos de trabajo y las políticas de RR. HH., así como los diagnósticos de riesgos y el análisis del contexto. El equipo directivo puede utilizar los datos de incidentes para decidir qué actividades y recursos financiar, qué medidas de gestión de riesgos de seguridad implementar y dónde y cómo operar en determinados lugares. Este análisis también puede ayudar a orientar las decisiones estratégicas sobre en qué contextos trabajar, qué enfoques de seguridad priorizar y cómo comunicarse con las diferentes partes interesadas (incluidos los donantes, los grupos locales y las autoridades). Los datos sobre incidentes también pueden ser útiles para las campañas de incidencia relativas a la violencia contra los trabajadores humanitarios y las restricciones de acceso humanitario.

► Para obtener más información sobre la incidencia, véase el capítulo 2.2.

4.4.2 Respuesta a incidentes y gestión de crisis

Todos los incidentes requieren una respuesta, pero es su gravedad la que determina el tipo de respuesta. Un incidente no crítico puede resolverse utilizando los procedimientos y la capacidad organizativa existentes en el lugar donde se produjo el incidente. Para este tipo de incidente, el referente de seguridad y otros miembros del personal pertinentes pueden aplicar los POE y los planes de la organización para garantizar que el personal afectado sea atendido y que se gestione el impacto más amplio del incidente. Lo que se considera un incidente no crítico varía según la organización. Algunos ejemplos pueden ser el acoso no verbal de bajo nivel, daños materiales al equipo, detenciones de corta duración o un accidente de tráfico menor que no haya provocado lesiones graves. Los incidentes no críticos generalmente se tratan a través de la estructura directiva, con medidas adicionales que pueden incluir conversaciones con partes interesadas externas, el intercambio de información con el personal y el cumplimiento de cualquier requisito legal o de seguro (p. ej., al denunciar un robo). El personal de respuesta debe tener siempre en cuenta cualquier circunstancia personal (p. ej., grupo étnico, situación personal o género) que pueda requerir un enfoque específico.

Los incidentes críticos son eventos que amenazan seriamente la vida o la salud del personal. Un incidente de este tipo tiende a ser demasiado grave para ser manejado a través de estructuras de gestión estándar, requiere apoyo adicional (financiero, de personal, administrativo y técnico) y a menudo involucrará al personal de varias oficinas, incluida la oficina central. La mayoría de los incidentes críticos requieren una respuesta a la crisis, lo que significa que será necesario activar la estructura de gestión de crisis de la organización.

Una crisis es un acontecimiento altamente perturbador que interrumpe gravemente las operaciones normales, provoca o amenaza con provocar consecuencias graves y requiere medidas extraordinarias y la intervención inmediata del equipo directivo. Las crisis pueden adoptar diversas formas y amenazar la reputación, los programas, los

activos, las finanzas y la seguridad del personal de una organización. Aunque pueden ser desencadenadas por un incidente crítico, no todas las crisis están relacionadas con un incidente de este tipo.

Lo que se considera una crisis o un incidente crítico varía según la organización, pero los ejemplos más comunes son las situaciones de rehenes o los secuestros, la muerte de un miembro del personal, un ataque grave que afecte a la organización directa o indirectamente (p.ej., un ataque dirigido contra el personal o un ataque con bomba cerca de las instalaciones de la organización, un golpe de Estado o un peligro natural, como un terremoto).

La respuesta del equipo directivo de una organización a un incidente crítico o a una crisis se puede dividir en varios pasos.⁷³

- Planificación y preparación
 - Elaboración de un plan y una estructura de gestión de crisis.
 - Capacitación y sensibilización en gestión de crisis.
- Gestión de incidentes y crisis
 - La respuesta inicial, como brindar apoyo médico e informar a las partes interesadas clave.
 - Gestionar la situación, como desarrollar e implementar una estrategia para apoyar a los afectados, así como gestionar las comunicaciones, las partes interesadas y la información.
 - Resolución de la situación, como la liberación exitosa del personal secuestrado.
- Acciones posteriores al incidente
 - Una revisión del acontecimiento, de las políticas y los procedimientos de respuesta y gestión de riesgos de seguridad de la organización, así como del apoyo a largo plazo para las personas afectadas.

Estos pasos pueden variar en la práctica según el tipo de incidente y su duración.

Planificación y preparación para la gestión de crisis

Una gestión de crisis eficaz implica contar con la estructura adecuada, planes integrales, capacitación y ejercicios. Para tomar decisiones y adoptar las medidas correspondientes en respuesta a un incidente crítico o a una crisis, las organizaciones pueden necesitar activar su plan de gestión de crisis y movilizar o constituir la estructura de gestión de crisis (un marco dentro de una organización para lidiar con una crisis o un incidente crítico).

Un plan de gestión de crisis puede incluir los siguientes elementos:

73 En adelante nos referiremos a ello como *gestión de crisis*, un término genérico que engloba tanto los incidentes críticos como las crisis. Algunas organizaciones utilizan el término *gestión de incidentes críticos* para las respuestas a este tipo de incidentes.

- Definiciones de los tipos de incidentes críticos y las crisis.
- Cuándo activar y finalizar la estructura de gestión de crisis, incluido quién decide esto en última instancia.
- La delimitación de funciones y responsabilidades de los actores clave, incluida la composición de los equipos de gestión de crisis y de gestión de incidentes.⁷⁴
- Protocolos y plantillas relevantes, como protocolos de evacuación médica y plantillas de denuncia de incidentes.

Estos planes pueden probarse periódicamente e incorporarse a ejercicios de capacitación y simulación. Requieren revisión y (posiblemente) actualización después de una crisis o una respuesta a un incidente crítico.

La estructura de gestión de crisis variará según la organización y la situación, pero puede incluir lo siguiente:

- Una **autoridad decisoria**, un individuo o un grupo con la máxima autoridad decisoria con respecto a la crisis o al incidente crítico, que normalmente no forma parte de la gestión diaria de la crisis, pero que se informa regularmente y que, a su vez, mantiene informadas a otras personas del equipo directivo y a los miembros de la junta sobre las acciones del equipo de respuesta. La autoridad decisoria generalmente se encarga de evaluar la gravedad y el impacto de un acontecimiento o situación frente a criterios o umbrales predeterminados que definen qué constituye un incidente crítico o una crisis que requiere una respuesta de gestión de crisis.
- Un **equipo de gestión de crisis** en la oficina central o regional, y posiblemente otro en la oficina en el país (para las organizaciones internacionales). Este equipo es responsable de todos los aspectos de la respuesta a la crisis. Los equipos virtuales de gestión de crisis, con personal que participa desde diferentes lugares, se han vuelto más comunes a medida que la tecnología se vuelve más confiable.
- Un **equipo de gestión de incidentes** a nivel local donde se produce el incidente, que es responsable de implementar la estrategia de gestión de incidentes bajo la dirección del equipo de gestión de crisis.
- **Equipos de apoyo a la respuesta a crisis**, como el personal de seguridad, salud, informática y comunicaciones, que pueden brindar apoyo adicional sin ser miembros oficiales de los equipos de gestión de crisis o de gestión de incidentes.

74 De aquí en adelante, la mención a los equipos de gestión de crisis incluye a cualquier equipo de gestión de crisis y de gestión de incidentes activados en diferentes lugares.

- También puede haber funciones **de enlace y apoyo familiar y de comunicaciones para situaciones de crisis**, que si bien están vinculadas a los equipos de gestión de crisis y de gestión de incidentes, suelen mantenerse separadas. Las organizaciones pueden asegurarse de que formen parte de sus planes de preparación (véanse las secciones posteriores).

El equipo de gestión de crisis puede establecer responsabilidades jerárquicas y distinguir claramente las funciones desempeñadas en las diferentes oficinas (p. ej., oficinas del proyecto, regional o central). Se puede elaborar un organigrama claro y mantenerlo actualizado, con responsabilidades definidas y una lista de contactos. Todos los involucrados deben saber cuál es su lugar. En algunos incidentes, un equipo de gestión de incidentes puede operar solo a nivel local, pero es necesario que comprenda claramente cuándo debe involucrar a la oficina central (incluidos los equipos de respuesta a crisis regionales cuando corresponda). Los incidentes graves o prolongados (un asesinato, un ataque con explosivos, un secuestro o una hibernación forzada, por ejemplo) o cambios importantes (como una reubicación o evacuación) normalmente requerirán un equipo de gestión de crisis específico, respaldado por un equipo de gestión de incidentes. La distribución exacta de las responsabilidades entre estos equipos dependerá del contexto y de la situación. Por ejemplo, la designación de oficiales de enlace familiar capacitados para apoyar al personal afectado y a sus familias se puede realizar tanto a nivel del equipo de gestión de crisis como del de gestión de incidentes, según la situación.

Lo ideal es que los equipos de gestión de crisis sean pequeños para agilizar y acelerar la toma de decisiones. Estos equipos pueden incluir a representantes de varias funciones básicas (véase el recuadro más abajo). También se podrá designar a un gestor de crisis con autoridad para comprometer al personal, el equipo, los fondos y otros recursos adecuados para garantizar una respuesta eficaz y oportuna. La gestión de la información debe considerarse cuidadosamente dentro del equipo de gestión de crisis y las funciones de apoyo, en particular porque aquellas personas encargadas de interactuar con las partes interesadas externas (como el personal de enlace familiar y de comunicaciones) pueden verse en una posición incómoda si tienen acceso a toda la información.

La gestión de crisis es desafiante y requiere un conjunto de competencias y conocimientos (jurídicos, médicos, psicológicos y de negociación de rehenes, por ejemplo), algunos de los cuales puede ser necesario buscar fuera de la organización. Lo ideal es que cualquier requerimiento de apoyo externo se identifique y obtenga lo antes posible, y que se utilice durante el tiempo que sea necesario (que puede variar desde una consulta inicial hasta un aporte regular durante el periodo de respuesta). Algunas organizaciones recurren a exempleados que conocen la organización y cuyas competencias y experiencia son reconocidas y confiables. También pueden participar miembros del personal externos a los equipos de gestión de crisis y de gestión de incidentes que tengan conocimientos, contactos y habilidades relevantes.

Funciones del equipo de gestión de crisis

La composición de los equipos de gestión de crisis y de gestión de incidentes variará en función de la organización y del evento al que se responda. Algunas funciones que las organizaciones podrían considerar son las siguientes:

- Líder de equipo o gestor de crisis.
- Recursos humanos
 - Apoyo administrativo (p. ej., expedientes del personal y enlace con seguros).
 - Apoyo familiar (coordinación de contactos y apoyo familiar, gestión de los oficiales de enlace familiar).
 - Apoyo al personal (atención psicosocial para el personal afectado, incluido el personal de respuesta).
- Medios y comunicaciones (generalmente implementados por un equipo de comunicaciones para situaciones de crisis independiente).
- Asistente para apoyar tareas administrativas, incluyendo tomar notas y organizar reuniones.
- Según la naturaleza del incidente o evento, referentes de seguridad, director nacional, jefe de operaciones en el lugar, expertos en el contexto, médicos, legal, logística y TI.

No todas las personas que responden a un incidente crítico o a una crisis se encontrarán necesariamente en el mismo lugar. La gestión de crisis puede implicar la colaboración y la coordinación remotas y virtuales entre los miembros del equipo.

La gestión de crisis puede ser inicialmente un trabajo a tiempo completo. El personal involucrado debe ser liberado de sus otras tareas y protegido de intrusiones innecesarias para que pueda concentrarse en la tarea en cuestión. Es conveniente que tengan su propio espacio de trabajo e instalaciones, incluida una sala de crisis temporal. Deben procurar monitorear la situación a diario y decidir y revisar periódicamente las políticas respecto a las diferentes partes interesadas. Los miembros del equipo pueden necesitar descanso y relajación regulares, así como apoyo durante y después de la crisis.

Archivo de información personal

El personal de Recursos Humanos puede apoyar la gestión de crisis asegurándose de tener a mano la información y la documentación adecuadas de todos los empleados en caso de que se produzca una crisis o un incidente crítico. Algunas organizaciones mantienen un archivo de información personal con datos clave como los siguientes:

- Información de prueba de vida.
- Contactos de emergencia (que pueden ser diferentes según las circunstancias).
- Información médica.
- Información de redes sociales.
- Datos adicionales que pueden ser relevantes al comunicarse con la familia o prestar apoyo de emergencia al miembro del personal.

Este archivo deberá manejarse con la máxima confidencialidad, pero deberá ser rápidamente accesible en caso de emergencia.

Si la crisis continúa durante un periodo prolongado, puede ser necesario rotar a los miembros de los equipos de gestión de crisis y de gestión de incidentes. Las licencias, los viajes y otros compromisos laborales también pueden afectar el tiempo durante el cual las personas pueden dedicarse a las funciones de gestión de crisis. Se puede facilitar una transición sin inconvenientes manteniendo actualizado un archivo de traspaso con informes y análisis y planificando el traspaso de manera que los miembros del equipo coincidan. Una buena práctica consiste en tener uno o dos empleados de respaldo para cada puesto, todos capacitados y preparados para intervenir si fuera necesario.

La capacitación en gestión de crisis es uno de los componentes más importantes de la preparación para una crisis o un incidente crítico. Todo el personal identificado para un puesto de gestión de crisis o incidentes necesita estar capacitado y sentirse cómodo trabajando en equipo. Se necesita financiación para la capacitación en preparación, que incluya ejercicios de simulación.

Capacitación en gestión de crisis

Los ejercicios y la capacitación en gestión de crisis pueden adoptar distintas formas: desde ejercicios de simulación hasta un simulacro general. En los ejercicios iniciales basados en debates se identifican al personal de respuesta, las capacidades y las deficiencias clave. Los ejercicios de simulación más avanzados ponen a prueba los planes para crisis en escenarios realistas. La capacitación y los ejercicios periódicos en respuesta a crisis y comunicación mejoran la toma de decisiones, la conciencia y la confianza en la capacidad de una organización para gestionar eficazmente las crisis y los incidentes críticos.

Respuesta inicial y estrategia

El primer paso para afrontar un incidente crítico o una crisis es decidir si se requiere una acción inmediata para preservar la vida o garantizar la seguridad. Se debe establecer información verificable que describa los detalles del evento. Esto puede formar parte del informe inicial. También se deberá comunicar cualquier información adicional o cambio a medida que se produzca.

Lo ideal es que se inicie un registro inmediatamente después de la notificación de un incidente y que se mantenga regularmente para registrar la cronología de los eventos, las llamadas telefónicas y las notas de las reuniones, y para garantizar que todos los documentos se registran y archivan.

Al recibir un informe de un incidente, la primera decisión es determinar si una situación particular califica como una crisis o un incidente crítico y si se debe activar la estructura de gestión de crisis de la organización. Dado que a menudo es más fácil suspender una respuesta de gestión de crisis que esforzarse por ponerse al día, las organizaciones pueden considerar la posibilidad de operar sobre la base de una “sobre-reacción prudente”. Si se activa la función de gestión de crisis, el equipo tiene que tomar decisiones respecto a las siguientes cuestiones:

- Si se deben suspender las actividades del programa o retirar al personal a un lugar más seguro.
- Si es necesario desplegar personal de apoyo adicional para ayudar.
- Qué información debe circular interna y externamente y cualquier limitación o cuestión de confidencialidad.
- El objetivo final (p.ej., persona herida evacuada, cuerpo repatriado, miembro del personal secuestrado liberado).

La importancia de los registros

Un elemento importante de la gestión de incidentes y crisis es la apertura y el mantenimiento de un registro para anotar las decisiones tomadas, las razones de esas decisiones, quién las tomó, cuándo y las acciones resultantes. Algunos beneficios de hacerlo son los siguientes:

- Proporciona un registro completo para facilitar el traspaso a nuevos miembros del equipo de gestión de crisis en una respuesta prolongada.
- Puede ayudar a fundamentar las acciones posteriores a un incidente o crisis.
- Proporciona una prueba documental de que la organización ha hecho todo lo posible para cumplir con su deber de cuidado hacia el personal afectado.
- Los registros pueden demostrar que la organización utilizó un enfoque considerado y sistemático para decidir qué medidas adoptar, incluso si estas no tuvieron los resultados previstos.

La información en el registro debe gestionarse con cuidado y conservarse de forma segura, manteniendo y respetando la confidencialidad.

Una función clave del equipo de gestión de crisis es elaborar una estrategia de gestión de crisis o incidentes que informe el enfoque de la organización ante el evento e incluya los siguientes elementos:

- Gestión de las partes interesadas, incluido el apoyo familiar y el enlace con las autoridades, los medios de comunicación, las comunidades y otras organizaciones.
- Comunicaciones.
- Negociaciones y comunicación con los agresores, si corresponde.
- Gestión de la información, incluida la recopilación y el análisis de información, el resguardo de la seguridad de la información, el mantenimiento de registros y la documentación.
- Asignación de recursos (materiales y humanos).

La estrategia debe contar con el asesoramiento de expertos pertinentes, como asesores jurídicos, para garantizar que contemple los marcos jurídicos y las jurisdicciones

aplicables. Cada incidente debe tener su propia estrategia, que debe revisarse periódicamente.

En general, el equipo de gestión de crisis tiene que considerar cuestiones médicas y de seguridad, el apoyo logístico y la capacidad de respuesta, así como cuestiones relacionadas con la reputación, los aspectos legales, las comunicaciones y los medios de comunicación. Es posible que este equipo tenga que ponerse en contacto con los proveedores de seguros y garantizar una cobertura, desembolsos y apoyo adecuados. Puede haber personas lesionadas que requieran atención inmediata o a largo plazo. Si se pierden vidas, será necesario informar a los familiares y tomar medidas para cubrir los gastos del funeral y el entierro, entre otros. La seguridad puede seguir siendo un problema si las personas que no estuvieron involucradas en el incidente aún están en riesgo, y puede necesitarse apoyo logístico para organizar evacuaciones médicas, la repatriación o el retorno de los cuerpos a sus familias. Según la situación, se puede enviar personal especializado al lugar afectado, por ejemplo, para proporcionar capacidad de búsqueda y salvamento, asistencia médica o forense y apoyo psicológico y asesoramiento. Otras oficinas, a nivel regional y/o la oficina central, también pueden requerir dicha experiencia.

El equipo de gestión de incidentes desempeña un papel clave en la implementación de las directrices del equipo de gestión de crisis, que puede incluir las siguientes responsabilidades:

- Gestión de la crisis a nivel local.
- Comunicación con las partes interesadas locales, entre ellas, la familia, las autoridades locales (incluida la policía), las embajadas y otros representantes gubernamentales, las Naciones Unidas, las ONG y los medios de comunicación locales.
- Asistencia a la familia, si está presente en el lugar, y apoyo moral y material a las personas afectadas, si es posible.
- Intercambio de información y evaluación de riesgos para el equipo de gestión de crisis de la oficina central.

Gestión de la comunicación y los medios

La gestión de las comunicaciones es un componente crucial de la gestión de una crisis o de un incidente crítico. Dados los riesgos asociados a la filtración de información, se considera una buena práctica mantener la confidencialidad y adoptar un enfoque basado en la “necesidad de saber”. En la guía *Managing the message* del GISF se comparten pautas y herramientas detalladas sobre cómo gestionar las comunicaciones con las partes interesadas internas y externas durante una crisis o un incidente crítico.⁷⁵

75 Davidson, S. (2013) *Managing the message: communication and media management in a security crisis*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/managing-the-message/).

Coordinación en tiempos de crisis o incidentes críticos

Algunos eventos pueden requerir la coordinación entre múltiples organizaciones, como un ataque a un convoy o un secuestro grupal. En estas circunstancias, el equipo de gestión de crisis de la organización se comunicaría con las partes interesadas clave y posiblemente compartiría información, asesoramiento, conocimientos del contexto y recursos con otras organizaciones.

Cuando varias organizaciones deciden reubicar o evacuar al personal debido a una crisis importante, como un conflicto civil, las organizaciones pueden depender en gran medida de los mismos recursos o de las Naciones Unidas para recibir apoyo. La coordinación en estas circunstancias es fundamental, pero en la práctica puede ser un desafío, ya que los recursos pueden verse superados y el acceso limitado. Es esencial que todas las organizaciones tengan claro qué apoyo necesitan durante este tipo de situaciones y confirmen que disponen de dicho apoyo antes de que se produzcan los hechos.

Siempre es una buena práctica establecer relaciones con las partes interesadas externas antes de que ocurra un evento, y que todos los actores tengan claro qué apoyo pueden esperar de los demás y cuáles son los mecanismos de coordinación. Un buen punto de partida es que las organizaciones se pongan en contacto con actores pertinentes, incluidas otras organizaciones humanitarias y las Naciones Unidas, al ingresar a una zona nueva y pregunten cuál sería la modalidad de coordinación en caso de producirse una crisis grave.

► *Para obtener más información sobre los mecanismos de coordinación interinstitucional, véase el capítulo 2.1.*

Los planes de gestión de crisis en materia de comunicación y medios forman una parte importante de la preparación para la gestión de crisis y deben establecerse antes de que se produzca un incidente crítico o una crisis. Si bien las comunicaciones con las partes interesadas internas y externas deben ser dirigidas por el equipo de gestión de crisis con el apoyo de un equipo de comunicaciones para situaciones de crisis, este último es el principal responsable de tratar con los medios de comunicación, desarrollar e implementar la estrategia de comunicación y medios, preparar y redactar las

comunicaciones para audiencias externas e internas, monitorear los medios (incluidas las redes sociales) y designar un portavoz.

El equipo de comunicación para situaciones de crisis podría incluir un jefe de equipo, un portavoz, un supervisor de medios de comunicación y personal de apoyo. Al igual que con el equipo de gestión de crisis, es una buena práctica que este equipo esté capacitado adecuadamente y practique regularmente la implementación del plan de comunicación y medios de difusión para situaciones de crisis de la organización.

El equipo de comunicación para situaciones de crisis asume la responsabilidad de las actividades relacionadas con las comunicaciones, a menudo bajo la dirección, en conjunto con o con la aprobación final del equipo de gestión de crisis, como, por ejemplo, la redacción de mensajes clave para diferentes grupos (internos y externos) y la definición de una estrategia de medios.

Comunicaciones a nivel del proyecto y del país

Es posible que durante una crisis sea necesario informar rápidamente a muchas personas y organizaciones. En lugar de que una sola persona intente hacer esto, las organizaciones pueden establecer una cadena o red de comunicación en el que cada “nodo” tiene la responsabilidad de transmitir la información a otros tres o cuatro nodos. Una forma sencilla de hacerlo es utilizando el organigrama del personal. Esto se puede actualizar periódicamente a intervalos preestablecidos para que los nombres y la información de contacto sean precisos y se actualicen inmediatamente si hay cambios de personal. También se puede aclarar previamente si se utilizarán llamadas telefónicas, mensajes de texto o la radio. Esto se puede integrar a un sistema de guardias, si ya existe. En las situaciones de emergencia, las redes de comunicaciones nacionales suelen fallar o sobrecargarse: si es posible, la organización debe asegurar medios de comunicación alternativos independientes de la infraestructura nacional.

Si el incidente pone en duda la continuidad de las actividades del programa o incluso de la presencia de la organización en el lugar, puede ser necesario comunicarse con las comunidades afectadas, las partes interesadas clave (p.ej., las autoridades), el público en general y los donantes clave.

Comunicación entre equipos y oficinas de la organización

A menudo se necesitan comunicaciones fiables, especializadas, con suficientes recursos, seguras y disponibles las 24 horas entre el lugar afectado y los diferentes equipos de gestión de crisis. Es aconsejable prever una pérdida temporal de la comunicación y prepararse en consecuencia. Es posible que se necesite servicio de traducción si las partes interesadas y los equipos hablan diferentes idiomas. El control de rumores dentro de la organización es importante, ya que es probable que la especulación abunde y se exprese de múltiples maneras, como a través de las redes sociales, las aplicaciones de mensajería y el correo electrónico. La comunicación interna eficaz con otros miembros del personal de la organización debe ser proactiva y estar bien gestionada.

Es aconsejable que las organizaciones anticipen las preguntas y mantengan la moral y la confianza del personal en la organización, mientras que al mismo tiempo deben intentar mantener al personal no esencial a una distancia segura de la labor de gestión de la crisis.

La comunicación puede implicar los siguientes elementos:

- Sesiones informativas periódicas o según sea necesario para todo el personal, impartidas por el jefe del equipo de gestión de crisis.
- Un folleto informativo accesible a todo el personal (en varios idiomas si es necesario) y publicado en la intranet o por otro medio de comunicación.
- Brindar al personal oportunidades para sentirse involucrado y mostrar su apoyo a los colegas afectados, por ejemplo, escribiendo mensajes de apoyo: el personal afectado parece apreciar dichos esfuerzos una vez que se han resuelto los incidentes.

En caso de incidentes o crisis graves, puede ser necesario mantener informados a los miembros de la junta directiva de la organización y consultarlos sobre decisiones críticas.

Comunicación con los medios de comunicación

Los incidentes graves que afectan a un miembro del personal (como fallecimiento o lesiones) generalmente requerirán una notificación inmediata a la familia, seguida de una declaración o un comunicado de prensa del equipo directivo. En ocasiones son otras entidades, como la embajada o las autoridades locales, las que se encargan de la notificación, y en estas circunstancias la organización debe intentar ponerse en contacto con la familia lo antes posible. También se puede convocar una conferencia de prensa o emitir un comunicado de prensa.

Las organizaciones deben tener un plan de medios preparado que respalde la estrategia de medios adoptada para una crisis o un incidente crítico en particular. Las organizaciones pueden identificar con antelación a las personas encargadas de hablar con los medios de comunicación (se puede designar un portavoz) y brindarles capacitación. El portavoz está estrechamente vinculado al equipo de gestión de crisis, aunque normalmente no forma parte oficialmente de este equipo. No obstante, es aconsejable que estas personas participen en la capacitación del equipo de gestión de crisis.

Es posible que sea necesario comunicarse con los medios de comunicación locales, nacionales e internacionales y estar preparado cuando se pongan en contacto con la organización. Es importante que las organizaciones estén al tanto de las discusiones sobre los incidentes y el personal afectado en las redes sociales. Los *influencers* de las redes sociales pueden crear contenido sobre los casos de alto perfil, y el equipo de medios de comunicación de la organización posiblemente deba supervisar estas plataformas y estar preparado para responder si es necesario. Las organizaciones

que no cuentan con profesionales de comunicación en su personal pueden buscar asesoramiento profesional externo.

En determinadas circunstancias, puede ser apropiado publicar una declaración en el sitio web de la organización, la intranet y las plataformas de redes sociales pertinentes. Dada la proliferación de información, cabe señalar que cualquier declaración pública puede tener un alcance global. Las comunicaciones compartidas con el personal pueden filtrarse a los medios de comunicación. Como regla general, la identidad del personal afectado siempre debe mantenerse confidencial. Dentro de la organización, debe ser claro qué información debe permanecer confidencial, quién está incluido en el círculo de información y cómo se protegerá la confidencialidad.

Consideraciones sobre las redes sociales

La comunicación a través de las plataformas de las redes sociales puede desencadenar sentimientos muy negativos después de un incidente. Por ejemplo, tras un ataque mortal contra dos empleados de una ONG internacional en Burkina Faso en 2023, un análisis de las reacciones en las redes sociales reveló una incompreensión generalizada y sentimientos negativos hacia la organización y el trabajo humanitario en general. Varios comentaristas acusaron a la organización de colaborar con los grupos armados y de actuar como representante de los Gobiernos occidentales. La intención declarada públicamente por la organización (el día del incidente) de iniciar un diálogo con todas las partes en el conflicto provocó una fuerte reacción negativa en las redes sociales, con muchos comentarios en los que esto se interpretó como un intento de legitimar a los grupos armados islamistas.

El monitoreo de las redes sociales para evaluar el sentimiento local hacia las organizaciones humanitarias es un aspecto cada vez más importante para medir las percepciones locales, la aceptación del trabajo humanitario en contextos operacionales y la gestión de riesgos de seguridad. Este tipo de monitoreo se vuelve aún más importante durante las crisis y los incidentes críticos. Algunas organizaciones invierten directamente en este trabajo de monitoreo, mientras que otras dependen de fuentes públicas (por ejemplo, los informes de supervisión de redes sociales de Insecurity Insight: <https://insecurityinsight.org/projects/aid-in-danger/social-media-monitoring>).

Fuente: Insecurity Insight (2023) “MSF ambush in Burkina Faso” (<https://insecurityinsight.org/wp-content/uploads/2023/03/MSF-attack-Burkina-Faso-Social-Media-Monitoring-March-2023.pdf>).

El objetivo principal de todas las actividades relativas a los medios de comunicación debe ser proteger al personal afectado; en algunos casos de incidentes críticos esto puede significar mantener un perfil bajo, pero en otros puede significar aumentar su presencia mediática de una manera cuidadosamente gestionada. En algunos casos de incidentes críticos, como los raptos, el objetivo principal del agresor puede ser conseguir la atención de los medios de comunicación. En algunos contextos, los medios de comunicación no pueden publicar detalles sobre casos de violencia sexual, e incluso en lugares donde esto no está prohibido las personas supervivientes corren el riesgo de sufrir estigmatización o mayor victimización si se filtra su identidad.

Comunicación con los vecinos y otras organizaciones

Si, por ejemplo, la oficina de la organización ha sido atacada, es aconsejable hablar con los vecinos, cuya sensación de inseguridad probablemente se haya acentuado. También puede ser necesario alertar a otras organizaciones humanitarias sobre un incidente de seguridad importante para que puedan tomar medidas de precaución.

Enlace y apoyo familiar

Apoyar y establecer vínculos con las familias de los miembros del personal afectados es una parte fundamental de la gestión de un incidente. En esencia, esto implica garantizar que la familia se sienta segura de que la organización está gestionando de manera adecuada la situación que afecta a su ser querido. No se trata solo de un aspecto importante del deber de cuidado: no hacerlo también podría socavar los esfuerzos de gestión de crisis de la organización. Los familiares que no confíen en la respuesta de la organización pueden, por ejemplo, acudir a los medios de comunicación o ir a la zona afectada por la crisis con sus propios planes. Si bien estas acciones en sí mismas no son problemáticas (a veces puede ser aconsejable que los familiares hagan declaraciones o que la organización facilite su presencia en el lugar), las acciones no coordinadas pueden interferir con el plan de gestión de crisis de la organización. En 2017 el EISF (ahora GISF) elaboró *Family First*, una guía detallada sobre el enlace y apoyo familiar durante incidentes críticos y crisis.⁷⁶ La siguiente sección cubre algunas consideraciones básicas.

En primera instancia, una organización debe comunicarse con las familias del personal y de otras personas afectadas por un incidente. Se debe hacer todo lo posible para garantizar que los familiares sean los primeros en ser informados sobre un incidente. Es una buena práctica no difundir ningún mensaje o declaración hasta que los familiares hayan sido informados directamente por el personal de la organización.

El equipo de comunicación para situaciones de crisis puede trabajar junto con el oficial de enlace familiar para apoyar a los familiares que puedan sufrir la intrusión de los medios de comunicación, lo que puede incluir el cierre de las cuentas de redes sociales del personal y de los familiares afectados. Esta acción también puede impedir que grupos hostiles, incluidos los agresores, accedan a información personal y la utilicen

76 Davidson, S. (2013) *Family first: liaison and support during crisis*, Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/family-first/).

de forma malintencionada. Para ello, lo ideal es que las organizaciones cuenten con planes y, cuando sea posible, vías de comunicación establecidas con las redes sociales y otras plataformas para cerrar cuentas o eliminar artículos que puedan comprometer la seguridad y la privacidad del personal o los familiares afectados.

El apoyo a las familias puede requerir un compromiso más activo según la naturaleza y la duración del incidente. También es importante que las organizaciones sean conscientes de que las familias pueden tomar iniciativas por sí mismas, especialmente si el incidente dura mucho tiempo. Es importante que se sientan capacitadas para hacerlo, a la vez que sus planes y acciones se coordinen con el plan de gestión de crisis de la organización tanto como sea posible. Para apoyar a los familiares del personal afectado, las organizaciones deben considerar las siguientes medidas:

- Identificar el contacto de emergencia y tomar nota de cualquier circunstancia personal que deba guiar la interacción con la familia.
- Seleccionar al portador de noticias y al referente de enlace familiar. Por lo general, la persona que hace el primer contacto con el miembro de la familia será un miembro del equipo directivo de la organización, y luego será el referente de enlace familiar quien se encargará de brindar apoyo.
- Dar la noticia sin demora, con franqueza y compasión.
- Presentar a la persona designada como referente para la familia y explicar su función y cómo contactarla.
- Evaluar y satisfacer las necesidades inmediatas de la familia.
- Garantizar la confidencialidad y establecer una confianza bidireccional entre la familia y la organización.
- Establecer un horario de contacto regular con la familia.
- Gestionar el flujo de información entre la organización, los equipos de gestión de crisis y la familia.
- Incorporar servicios y asesores externos para apoyar a la familia.
- Mantener registros escritos de las comunicaciones mantenidas y de las decisiones tomadas.
- Desarrollar una estrategia de salida, por ejemplo, después de la resolución del incidente o si el incidente nunca se resuelve.

Se puede designar a un miembro del personal capacitado y con buenas habilidades interpersonales como referente para la familia. La persona seleccionada debe ser capaz de conversar con la familia en su idioma y ser de confianza y aceptada por la familia. Algunas organizaciones tienen un oficial de enlace familiar expresamente para circunstancias como estas, mientras que en otras ocasiones puede ser una persona

ya conocida por la familia, como el supervisor del miembro del personal afectado, quien a su vez recibe el apoyo de un oficial de enlace familiar capacitado. Cuando las organizaciones no tienen un puesto específico para esto, una buena práctica es tener al menos uno o dos miembros del personal capacitados en enlace familiar que puedan asumir esta función en caso de un incidente. Una de las funciones de este puesto es actuar como la persona de contacto designada para la familia (cuando varias personas han sido raptadas, puede ser necesario identificar a varias personas para que actúen como interlocutores con las familias afectadas). Lo ideal es que la misma persona desempeñe este papel durante todo el incidente, aunque en la práctica esto puede resultar difícil en incidentes de larga duración. Se trata de una responsabilidad exigente y a menudo requerirá el apoyo de la organización.

El oficial de enlace familiar no suele formar parte de un equipo de gestión de crisis, aunque debe conocer la estructura del equipo y sus formas de trabajar y mantener un contacto regular con él. Sin embargo, no debe participar en la gestión operacional diaria del incidente o crisis; esto le permite centrarse en apoyar plenamente a la familia. Las tareas de un referente de enlace familiar son, entre otras, las siguientes:

- Actuar como único canal de comunicación entre la organización y la familia.
- Establecer y mantener contacto regular con la familia, lo que incluye estar disponible en todo momento en caso de secuestro o rapto.
- Orientar a la familia sobre qué hacer si son abordados por los medios de comunicación o por los agresores (p.ej., los secuestradores).
- Compartir información, orientación y apoyo de otros equipos, como el equipo de comunicación para situaciones de crisis.
- Organizar el pago de salarios y otros apoyos a la familia.
- Establecer vínculos con otros según sea necesario.

Las circunstancias personales pueden requerir mayor tacto y sensibilidad al comunicarse con miembros de la familia. Las unidades familiares pueden adoptar diversas formas y estructuras. En determinadas situaciones, una familia puede estar dividida o separada. Además, hay casos en los que los familiares de un miembro del personal afectado no conoce o no reconoce a su pareja. Las relaciones y las dinámicas familiares pueden ser complejas y no tradicionales, y desviarse por tanto de las normas convencionales. Es imprescindible que el personal de enlace familiar considere los deseos y las necesidades del personal afectado. Algunos miembros del personal, por ejemplo, quizás no deseen que sus familias se enteren de determinados incidentes, como la violencia sexual. Otros quizás prefieran mantener la confidencialidad de su información personal, como su orientación sexual o historial médico, frente a sus familias. Las organizaciones deben tener información de contacto de emergencia en los archivos del personal, en los que pueden indicarse además circunstancias especiales

que pueden incorporarse al trabajo de enlace familiar, como diferentes contactos de emergencia para distintas situaciones.

Relaciones con las autoridades

Las organizaciones pueden necesitar coordinarse con las autoridades, incluido el Gobierno del país donde se produjo el incidente o la crisis y, si es diferente, el Gobierno del país de origen del personal afectado. Tampoco es inusual que los trabajadores humanitarios sean ciudadanos de diferentes países, lo que significa que puede haber varios “países de origen” que considerar. También podría ser necesario involucrar diversos departamentos e instituciones gubernamentales.

Posiblemente se necesiten acuerdos y la colaboración de las autoridades para procesar rápidamente las solicitudes de visa para el personal de apoyo en situaciones de crisis u otro personal de refuerzo. Los Gobiernos pueden movilizar a sus propios expertos de acuerdo con el tipo de incidente y las nacionalidades de los afectados. Esto puede generar una situación difícil en términos de responsabilidad y deber de cuidado. Si otra entidad toma la iniciativa, las organizaciones pueden defender lo que consideran que es mejor para las personas afectadas, con suerte en consonancia con los deseos de la familia. Puede ser posible anticiparse preguntando a los funcionarios gubernamentales pertinentes qué medidas tomarían en caso de producirse un incidente específico.

Consideraciones administrativas, jurídicas y financieras

Algunas situaciones pueden requerir asesoramiento jurídico. Este asesoramiento puede referirse a las condiciones de los contratos, las prestaciones de los empleados, cuestiones relacionadas con los seguros, los derechos legales en virtud de la legislación laboral aplicable, la representación legal ante el Gobierno anfitrión o el de origen, o la gestión de problemas jurídicos y reclamaciones por daños y perjuicios.

La gestión de incidentes críticos o crisis, en especial si son prolongados, también requiere apoyo administrativo y recursos humanos especializados. Puede haber otros gastos urgentes de viaje, equipamiento o servicios externos. El personal afectado puede no estar en condiciones de trabajar temporalmente debido a lesiones físicas o estrés psicológico, y puede ser necesario traer reemplazos temporales y brindar apoyo para su bienestar. Las organizaciones pueden requerir efectivo adicional debido a gastos no planificados y no presupuestados, incluidos los gastos relativos a la implementación de la estrategia de respuesta a la crisis. Parte de estos gastos puede estar cubierto por el seguro de la organización.

- Para obtener más información sobre seguros y cuidado del personal, véase el capítulo 5.4.

Gestión después de un incidente

Desactivación de la respuesta de gestión de crisis

Llegará un momento en que la estructura de gestión de crisis se desactivará, a menudo cuando el incidente se considere “resuelto”, por ejemplo, cuando las personas afectadas por un evento ya no estén en peligro y hayan recibido el apoyo necesario. Sin embargo, es posible que no haya una resolución clara, como en el caso del personal desaparecido o raptado. Este tipo de incidentes pueden durar muchos años y una organización puede decidir finalizar la respuesta a la crisis incluso en ausencia de una resolución. Las organizaciones deben tener un proceso claro para decidir cuándo y cómo desactivar y disolver los equipos de gestión de crisis.

Atención del personal tras un incidente

Es posible que el cuidado de las personas afectadas dure más que la respuesta de la organización a la crisis. Las organizaciones posiblemente tengan que estar preparadas para brindar apoyo a largo plazo al personal y a otras personas afectadas por un incidente.

Después de un evento, el personal afectado puede requerir apoyo de diversas maneras, como las siguientes:

- Acogida bajo el cuidado de la organización tras la liberación (en caso de detención, arresto o rapto).
- Atención médica y psicológica inmediata.
- Apoyo material inmediato, como alojamiento y otros materiales para su comodidad y bienestar.
- Apoyo en caso de reubicación o evacuación.
- Apoyo para reunirse con la familia.
- Gestión de las comunicaciones tras la resolución del incidente, de acuerdo con los deseos del miembro del personal afectado, que puede incluir orientación sobre cómo afrontar las solicitudes de los medios de comunicación.
- Plan de reincorporación al trabajo.
- Orientación sobre el acceso a servicios de apoyo, incluidos seguros y atención médica y psicosocial a largo plazo.
- Orientación sobre cómo buscar justicia contra los agresores.

Las personas involucradas en la gestión del incidente o afectadas por él (por ejemplo, los miembros del equipo de la persona afectada), incluida la familia, también pueden requerir apoyo después de un incidente grave.

Un enfoque centrado en el superviviente ayudará a garantizar que el miembro del personal afectado se sienta capacitado para tomar sus propias decisiones con respecto a su recuperación e implicará ser cuidadoso de no abrumarlo con demasiada información o demasiadas opciones y trabajar respetando sus deseos y dentro de sus capacidades (que pueden cambiar con el tiempo).

► *Para obtener más información sobre el enfoque centrado en el superviviente, la atención del personal después de un incidente y los seguros, véase el capítulo 5.4 sobre cuidado del personal.*

Informe y revisión posterior a la acción

Toda persona que haya estado directamente involucrada en la gestión del incidente o la crisis debe tener la oportunidad de recibir un informe sobre los hechos. Esto también puede incluir a personas cercanas a la situación aunque no hayan estado directamente involucradas en su gestión. Cualquier crisis, incidente o cuasiincidente que afecte a la organización, sus programas, sus socios o sus contratistas merece un análisis, y en general se considera una buena práctica realizar una revisión posterior a la acción (denominada a veces revisión posterior al incidente). En el caso de eventos graves, las organizaciones pueden considerar una evaluación más exhaustiva e idealmente independiente de por qué ocurrió la situación, cómo se gestionó y por qué tuvo el impacto que tuvo. Después de cualquier incidente de seguridad grave, es necesario revisar las políticas y los procedimientos de seguridad existentes.

Entre las preguntas clave que considerar figuran las siguientes:

- ¿Se implementaron medidas de protección?, ¿el personal las comprendió?
- ¿Se siguieron las medidas de protección?
- ¿Las medidas de protección fueron apropiadas de acuerdo con la amenaza?
- ¿Se observaron señales de advertencia de una amenaza inminente específica y, de ser así, se actuó en consecuencia y con anticipación?
- Por el contrario, ¿se trató de un evento imprevisto puesto que no hubo señales de advertencia?
- ¿Se evaluó con precisión el riesgo de que ocurriera una amenaza específica y se implementaron las medidas de protección adecuadas, pero el evento ocurrió de todos modos?
- ¿Estaban los equipos de gestión de crisis previamente identificados y preparados?

Esencialmente, las organizaciones deben procurar evaluar si hubo deficiencias o problemas de cumplimiento relacionados con el análisis de riesgos y las estrategias de mitigación de riesgos empleadas. Una revisión del mecanismo de respuesta a crisis constituye también una buena práctica que le permite a la organización realizar los ajustes necesarios en la preparación para incidentes críticos o crisis futuros.

Es importante que los informes y las revisiones posteriores a la acción se realicen con sensibilidad y se centren en los supervivientes. Esto implica considerar qué información puede revelarse, incluida, por ejemplo, la violencia física y sexual, y cómo debe gestionarse y reportarse este tipo de información.

Cualquier incidente grave que afecte a otra organización que opere en el mismo entorno también merece atención y análisis. Ese análisis no necesariamente concluirá que la organización corre un riesgo mayor. Puede haber varias razones por las que lo que le ocurrió a una organización es poco probable que le ocurra a otra. La capacidad de realizar un análisis razonable de un incidente que afecta a otra organización puede depender de cuánta información fiable se pueda obtener.

Es fundamental que, si el análisis posterior a la crisis indica que deben adoptarse medidas de seguimiento (como brindar una capacitación adicional o introducir modificaciones en los análisis de riesgos y en los procedimientos de seguridad), se desarrolle un plan de acción y se establezca un mecanismo de implementación (con responsabilidades claras) para garantizar que se realicen los cambios señalados. En muchos casos, el plan de acción no se implementa adecuadamente después de que un equipo de gestión de crisis se disuelve y sus miembros regresan a su trabajo habitual. Lo ideal sería compartir las conclusiones de la revisión posterior a la acción con el personal, posiblemente con diferentes niveles de detalle según el grado de participación en el incidente. La información puede presentarse a otras organizaciones si les concierne, y esta información debe compartirse de una manera que no comprometa al miembro del personal afectado.

Revisar el umbral de riesgo aceptable

Cualquier evento de seguridad grave, ya sea que afecte directamente a una organización o no, normalmente debería desencadenar una revisión del umbral de riesgo aceptable de la organización. Si el incidente involucró a socios, una organización puede considerar si su exposición al riesgo es aceptable. ¿Señala este evento que el análisis inicial fue erróneo? ¿Indica esto que la organización ha cruzado el umbral de riesgo aceptable? ¿Cuáles son las consecuencias prácticas? ¿Se pueden reforzar las medidas de protección para reducir el riesgo? ¿Debería introducirse algún cambio en la estrategia de seguridad operacional?, ¿serán efectivos estos cambios? ¿Debe reubicarse al personal lejos de las zonas de alto riesgo? Si se requieren ajustes o cambios, se debe asignar personal para garantizar que se estos cambios implementen y se debe establecer un plazo. Esto puede requerir capacitación nueva o adicional.

Este es un momento apropiado para compartir con todo el personal la nueva evaluación de la situación de seguridad y de la naturaleza y el nivel de riesgo, así como la eficacia probable de las medidas de protección de la organización. También representa una oportunidad para que el personal esté informado de cualquier cambio en la situación o contexto y revise su umbral de riesgo individual.

Más información

Orientación y recursos

Bickley, S. (2017). *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*. Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Buth, P. (2010). *Crisis management of critical incidents*. Foro Europeo Interinstitucional para la Seguridad (<https://gisfprod.wpengine.com/resource/crisis-management-of-critical-incidents/>).

Davidson, S. (2013a). *Family first: liaison and support during crisis*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/family-first/).

Davidson, S. (2013b). *Managing the message: communication and media management in a security crisis*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/managing-the-message/).

Foro Europeo Interinstitucional para la Seguridad. (2017). *Abduction and kidnap risk management* (www.gisf.ngo/resource/abduction-and-kidnap-risk-management-guide/).

Global Interagency Security Forum. (2021). *GISF – Remote crisis management course* (www.gisf.ngo/resource/gisf-remote-field-crisis-management-course/).

Global Interagency Security Forum. (2022). *NGO security collaboration guide* (<https://gisf.ngo/long-read/ngo-security-collaboration-guide/>).

Global Interagency Security Forum y Overseas Security Advisory Council. (2023). *Manual de ejercicios de gestión de crisis para ONG: Una guía para desarrollar y facilitar ejercicios eficaces* (<https://gisf.ngo/resource/ngo-crisis-management-exercise-manual-a-guide-to-developing-and-facilitating-effective-exercises/>).

Insecurity Insight. (s.f. a). *La gestión de la información sobre incidentes de seguridad* (<https://siim.insecurityinsight.org/>).

RedR UK, Insecurity Insight y Foro Europeo Interinstitucional para la Seguridad. (2017). *Manual de gestión de la información sobre incidentes de seguridad* (<https://siim.insecurityinsight.org/tools-and-resources/handbook-guide-and-tools>).

Bases de datos sobre incidentes de seguridad de código abierto

Humanitarian Outcomes. (s.f.). *Aid Worker Security Database* (www.aidworkersecurity.org/).

Insecurity Insight. (s.f.b). *Aid in danger* (<https://insecurityinsight.org/projects/aid-in-danger>).

Insecurity Insight. (s.f.c). *Social media monitoring* (<https://insecurityinsight.org/projects/aid-in-danger/social-media-monitoring>).

International NGO Safety Organisation. (s.f.). *Humanitarian Data Dashboard* (<https://ngosafety.org/ngo-data-dashboard/>).

5 Personas en la gestión de riesgos de seguridad

5.1 Recursos humanos

La gestión de riesgos de seguridad en el sector humanitario es una función multifacética que implica una gran variedad de interacciones en múltiples niveles y requiere una variedad de habilidades técnicas, interpersonales y analíticas. Este capítulo describe los perfiles, cualificaciones, competencias y funciones cambiantes de aquellas personas que gestionan la seguridad de una organización y la manera en que la seguridad puede y debe impactar en la gestión de las personas, desde la selección hasta la finalización de los contratos.

5.1.1 Evoluciones en la función de gestión de riesgos de seguridad

A medida que la gestión de riesgos de seguridad en el sector humanitario ha evolucionado a lo largo de las décadas, también lo ha hecho el grupo de profesionales que ahora desempeña funciones de gestión de riesgos de seguridad. El cambio de enfoques altamente protectores basados en modelos militares y de las fuerzas del orden a enfoques más integrados y centrados en posibilitar la acción humanitaria ha dado lugar a un nuevo campo profesional: la seguridad humanitaria. En esta disciplina emergente, los profesionales son cada vez más valorados por su combinación de habilidades de seguridad tradicionales y su comprensión de la programación y los principios humanitarios.

Otros avances que han afectado los perfiles y las habilidades requeridas del personal de seguridad humanitaria son los desafíos que plantean niveles más altos de apetito y de umbral de riesgo entre algunas organizaciones, y la necesidad de desarrollar habilidades internas para permitir el trabajo en entornos de alto riesgo y múltiples amenazas y para gestionar situaciones de crisis. Alianzas más frecuentes con otras organizaciones, así como una mayor colaboración en materia de seguridad en entornos de respuesta, requieren la capacidad de coordinar y establecer enlaces entre una amplia variedad de entidades. Además, el personal de seguridad humanitaria interactúa continuamente con tecnologías emergentes como posibles amenazas a la seguridad y como herramientas para la gestión de riesgos de seguridad.

Por último, en las funciones de gestión de riesgos de seguridad se pone cada vez más énfasis en las habilidades interpersonales y en el liderazgo adaptativo, a medida que los equipos se vuelven más diversos e inclusivos y que las estrategias de seguridad se enfocan cada vez más en la seguridad centrada en la persona y en los factores de riesgo basados en la identidad.

► *Para obtener más información sobre cómo crear una cultura de seguridad positiva, consulte el capítulo 1.1.*

5.1.2 Funciones de las personas en la gestión de riesgos de seguridad

La gestión de los riesgos de seguridad está determinada por las estructuras más amplias y las políticas de toma de decisiones de la organización. Una organización pequeña que opera en una sola localidad podría tener un único referente de seguridad. Por el contrario, una organización internacional grande puede disponer de equipos de seguridad multinacionales a nivel mundial, regional, nacional y subnacional. Las funciones y las responsabilidades de estos profesionales pueden variar, pero la mayoría desempeña funciones técnicas y de asesoramiento centradas en apoyar al equipo directivo, con una autoridad decisoria limitada. Por ejemplo:

- Para las organizaciones internacionales, un director superior de seguridad a nivel global que asesora al equipo ejecutivo de la organización y supervisa el desarrollo y la implementación de las políticas de seguridad en toda la organización.
- Para las organizaciones internacionales, un asesor y/o un equipo de seguridad a nivel regional que brinda apoyo a la gestión de los riesgos de seguridad operacional, asesoramiento técnico y supervisión de los programas nacionales.
- Un referente y/o equipo de seguridad a nivel nacional que asesora al equipo directivo en el país y supervisa la gestión de riesgos de seguridad; para las organizaciones nacionales, esta sería su oficina central y el personal de seguridad de mayor jerarquía.
- Referentes de seguridad a nivel local en los diferentes lugares donde se ejecuta el programa que gestionan los incidentes de seguridad y realizan actividades diarias de gestión de riesgos de seguridad.

Según la organización, estos puestos pueden tener diferentes títulos, entre ellos, director de seguridad, asesor, gerente, coordinador, oficial o referente.

Es importante destacar que las organizaciones estructuran e implementan la gestión de riesgos de seguridad de diversas maneras. En algunos casos, la responsabilidad está incluida en las funciones de gestión habituales y no existe una función de seguridad separada. En otros, la autoridad decisoria en materia de seguridad recae en las funciones de seguridad. Otras organizaciones pueden tener, complementaria o alternatively, grupos de trabajo de seguridad, en los que diferentes funciones comparten responsabilidades de gestión de riesgos de seguridad.

A la hora de estructurar las funciones del personal, puede ser útil recurrir al modelo RACI,⁷⁷ que identifica, para cada área de actividad, a la persona o personas:

⁷⁷ Para consultar un análisis más detallado sobre cómo se puede utilizar el modelo RACI en la gestión de riesgos de seguridad, véase GISF (2024) *Estrategia de gestión de riesgos de seguridad (GRS) y desarrollo de políticas: Una guía interfuncional* (<https://gisf.ngo/resource/srm-strategy-and-policy-guide/>).

- **Responsables:** ejecutan el trabajo.
- **Aprobadoras:** responsables en última instancia de la tarea o decisión.
- **Consultadas:** aportan información y asesoramiento.
- **Informadas:** se mantienen informadas sobre el progreso o las decisiones, pero no están directamente involucradas en el trabajo.

En esta sección se describe un modelo de gestión de riesgos de seguridad consultivo, que es uno de los más comunes en el sector humanitario. En este modelo, el personal de seguridad generalmente es responsable de la gestión de riesgos de seguridad, mientras que la rendición de cuentas recae en el equipo directivo. Nota: aunque aquí se hace referencia únicamente a la seguridad frente a incidentes deliberados, en la práctica muchas de las funciones y responsabilidades laborales abarcan la seguridad frente a actos tanto intencionados como accidentales.

► *Para obtener más detalles sobre las estructuras de gobernanza y seguridad, véase el capítulo 3.1.*

Personal superior de seguridad

Los puestos superiores de seguridad en el nivel directivo de la organización están idealmente ocupados por profesionales de gestión de riesgos de seguridad altamente calificados y con experiencia, que ejercen el liderazgo y desempeñan varias funciones críticas, entre las que figuran las siguientes:

- Comunicar la visión, elaborar políticas, estándares y estrategias relacionadas con la seguridad y crear planes de gestión de riesgos de seguridad.
- Liderar al personal y los equipos de seguridad.
- Contribuir al desarrollo de programas de capacitación en seguridad a varios niveles.
- Realizar proyectos de investigación y de desarrollo sobre tendencias y buenas prácticas, e integrarlas en los procesos y procedimientos organizacionales.
- Elaborar presupuestos básicos de seguridad.
- Desarrollar y controlar los esfuerzos de monitoreo del cumplimiento y la eficacia de la seguridad.
- Representar a la organización en foros interinstitucionales globales y participar en debates de alto nivel sobre gestión de riesgos de seguridad dentro del sector humanitario.
- Redactar políticas de gestión de crisis y participar en los equipos de gestión de crisis.
- Asociarse con las partes interesadas de la organización para integrar la seguridad a un enfoque más amplio de gestión de riesgos organizacionales.
- Revisar y mejorar las actividades de seguridad para reflejar los cambios en los contextos operacionales, incluidas las tendencias de los datos de incidentes.

Algunas organizaciones internacionales más grandes han establecido equipos de seguridad globales, liderados por un director de seguridad mundial. Para distribuir las responsabilidades entre todo el equipo, estas personas pueden cubrir diferentes regiones o aportar experiencia específica y liderar actividades relacionadas con esa área, por ejemplo, capacitación o seguridad de la información.

Personal y equipos de seguridad a nivel regional y nacional

En muchas organizaciones, si bien la responsabilidad principal de la toma de decisiones de seguridad a nivel nacional recae normalmente en el gerente superior de esa oficina (p.ej., el director de país o el director ejecutivo), los profesionales de gestión de riesgos de seguridad desempeñan una importante función de asesoramiento y realizan muchas tareas de gestión y apoyo, como las siguientes:

- Asesorar al equipo directivo superior respecto a las mejores prácticas de gestión de riesgos de seguridad e introducir lecciones y prácticas de otros entornos.
- Gestionar y enseñar al personal subalterno de seguridad.
- Identificar las metas y los objetivos de la gestión de riesgos de seguridad y desarrollar planes de acción en consonancia con los planes estratégicos de la organización o del programa del país.
- Implementar la política, las normas, las pautas y los procedimientos de seguridad y garantizar su revisión y cumplimiento.
- Recopilar y analizar información para detectar tendencias, adaptar las medidas de gestión de riesgos de seguridad y prepararse para posibles escenarios futuros.
- Establecer y supervisar sistemas para registrar, analizar y difundir información de seguridad o incidentes que afecten al personal y a las operaciones.
- Realizar y revisar evaluaciones de los riesgos para la seguridad.
- Concebir planes, protocolos, procedimientos y medidas para mitigar los riesgos detectados.
- Apoyar a los equipos de gestión de crisis en el manejo de incidentes críticos y crisis.
- Recomendar y adquirir equipos de seguridad.
- Realizar sesiones informativas y capacitaciones sobre seguridad.
- Representar a la organización en foros de seguridad interinstitucionales y reuniones de coordinación a nivel regional y nacional.

Algunas organizaciones han adoptado un enfoque integrado de gestión de la seguridad y el acceso combinando ambos puestos.

- *Para consultar un análisis más detallado del vínculo entre la gestión de riesgos de seguridad y las funciones de acceso, véase el capítulo 3.2.*

En algunas organizaciones internacionales, hay asesores o equipos de seguridad adicionales a nivel regional. Estos puestos realizan actividades similares a las mencionadas anteriormente y se centran en asesorar al equipo directivo regional y en apoyar los esfuerzos de gestión de riesgos de seguridad de los equipos nacionales en la región.

Referentes de seguridad en la oficina local

En las oficinas locales, los entornos de seguridad de alto riesgo generalmente ameritan un miembro del personal de seguridad a tiempo completo. En entornos de riesgo bajo y moderado, un referente de seguridad sin dedicación exclusiva puede cumplir esta función junto con otras responsabilidades (p.ej., administrativas, logísticas o de RR.HH.). Esta persona normalmente se encarga del trabajo diario relacionado con la seguridad. A nivel nacional y local, las responsabilidades de seguridad ante incidentes no deliberados por lo general recaen también en los referentes de seguridad.

La descripción del puesto de un referente de seguridad local podría incluir las siguientes tareas:

- Realizar análisis de riesgos del entorno operacional y enviar alertas de seguridad al personal pertinente.
- Ayudar a desarrollar estrategias de mitigación de riesgos de seguridad, incluidos POE, pautas y planes de contingencia.
- Informar al personal nuevo.
- Asegurarse de que todo el personal del lugar esté informado sobre los cambios en las condiciones de seguridad.
- Reportar los incidentes de seguridad.
- Asesorar y gestionar los equipos y los suministros de seguridad y comunicaciones.
- Supervisar el cumplimiento de los procedimientos y los planes, y reportar las infracciones o desviaciones de seguridad.
- Gestionar al personal relacionado con la seguridad, como guardias, operadores de radio y otros referentes de seguridad.
- Capacitar y asesorar a colegas para desarrollar competencias relacionadas con la seguridad.
- Participar en la presupuestación de los gastos de seguridad operacional.
- Participar en la gestión de la respuesta a incidentes y de crisis, así como en las revisiones y evaluaciones posteriores a la acción.
- Establecer vínculos e intercambiar información con otras organizaciones humanitarias y con las autoridades.

El referente de seguridad no necesita ser el único responsable de la gestión de riesgos de seguridad. Un enfoque de equipo para gestionar la seguridad suele ser beneficioso. Esto permite que un grupo de referentes gestione la carga de trabajo, codirija los planes y los procedimientos de seguridad y construya una cultura de seguridad positiva en el lugar. En algunas organizaciones, un comité de seguridad local apoya al referente, y la seguridad es un tema permanente en la agenda de las reuniones programáticas y operacionales.

5.1.3 Atributos y competencias clave

Perfiles, habilidades y cualificaciones

Las habilidades de seguridad se pueden clasificar en términos generales como “duras” y “blandas”. Las primeras se refieren a los aspectos más técnicos y operacionales de la seguridad, como el manejo de equipos de seguridad, la protección física y las tácticas. Suelen estar asociadas con una experiencia en las fuerzas armadas, la policía o los servicios de inteligencia, donde los individuos pueden haber adquirido conocimientos sobre armas, tácticas militares, operaciones policiales y medidas antiterroristas. También pueden incluir habilidades de investigación, así como análisis de amenazas y riesgos.

Las habilidades blandas se relacionan con capacidades interpersonales, como comprender las dinámicas sociales y culturales, y trabajar con un equipo multicultural, así como con habilidades de liderazgo, tutoría, capacitación, construcción de relaciones, comunicación y gestión. En la gestión de riesgos de seguridad humanitaria, también incluyen una buena comprensión de los objetivos del programa, los mandatos organizacionales y los principios humanitarios. Dada la complejidad de los actores y las partes interesadas en los entornos humanitarios, también es necesario construir y mantener redes con diversas comunidades y ser capaz de comprender y analizar diferentes contextos culturales, sociales, geopolíticos y ambientales, incluidas las zonas afectadas por conflictos violentos.

En los últimos años, a medida que el valor de las habilidades blandas y la apreciación de los enfoques de seguridad basados en la aceptación han ganado fuerza, ha habido un cambio en el perfil y en las habilidades del personal de seguridad. El perfil elegido con mayor frecuencia es un profesional en gestión de riesgos de seguridad con habilidades tanto técnicas como interpersonales y con una sólida experiencia en el sector humanitario. Aun así la disponibilidad de estas personas puede ser limitada en muchos lugares. Para abordar este problema, algunas organizaciones buscan desarrollar la capacidad de seguridad internamente capacitando al personal existente para funciones de seguridad. Cada vez más personal recurre a la capacitación, los títulos y las certificaciones para desarrollar sus habilidades y conocimientos y demostrar sus competencias.

► Para ver algunos ejemplos de recursos de capacitación y certificaciones, véase el capítulo 5.2.

Las habilidades y las competencias requeridas de un profesional en gestión de riesgos de seguridad pueden depender del tipo y del mandato de la organización, así como del trabajo a realizar. También puede variar en función del contexto en el que opera la organización. Por ejemplo, en un entorno con un conflicto activo y presencia de múltiples actores militares donde se requieren más medidas de protección y disuasión, pueden resultar más beneficiosas las habilidades duras y los conocimientos relacionados con lo militar. En un entorno caracterizado por problemas socioeconómicos y dinámicas tribales, donde la negociación del acceso y la aceptación son los enfoques clave de la gestión de riesgos de seguridad, puede ser necesario un conocimiento más profundo del contexto y sólidas habilidades interpersonales. Los contextos con niveles altos de criminalidad pueden exigir un espectro completo de habilidades y competencias, incluidos conocimientos en sociología, criminología y gestión del delito. En las oficinas o en los lugares donde resulta especialmente difícil lograr que el personal aplique los procedimientos de seguridad, puede ser conveniente contratar a una persona con la que el personal pueda identificarse (por su carácter, trayectoria y atributos personales) y con sólidas habilidades interpersonales, que le permita fomentar un mayor cumplimiento de los protocolos de seguridad.

Para las organizaciones internacionales, una consideración clave es si un puesto de seguridad debe ser ocupado por un ciudadano del país o por un extranjero. El personal de la zona generalmente tendrá un mejor conocimiento del entorno social, cultural y político y mayores redes de contactos. Sin embargo, también pueden enfrentar dificultades si ciertos actores creen que están alineados con una de las partes en conflicto o afiliados a grupos locales en disputa. Dados sus vínculos con las comunidades locales, pueden ser más vulnerables a las presiones de los agentes locales. El personal que no es del lugar puede tener una posición y una perspectiva diferentes y puede estar en mejores condiciones para colaborar con todas las partes interesadas. También puede carecer de conocimientos locales, tener poca conciencia cultural y contextual y tener sesgos arraigados. Contratar a un miembro del personal de un país cercano puede conllevar beneficios y desafíos, e incluso el personal de otras partes del país puede ser visto y tratado como extranjero en determinados lugares.

La selección del personal de seguridad debe estar guiada por el contexto y las necesidades específicos del puesto, en lugar de depender de perfiles o estructuras predeterminados. A medida que las situaciones evolucionan y el personal de seguridad de diversos orígenes adquiere nuevas habilidades, las organizaciones deben permanecer flexibles y abiertas a considerar una variedad más amplia de candidatos. Este enfoque permite una mejor correspondencia entre los requisitos del puesto y las crecientes competencias de la reserva de talentos, lo que garantiza una dotación de personal más inclusiva, eficaz y adaptable.

Muchas organizaciones se esfuerzan por lograr una mayor diversidad en sus equipos de seguridad, puesto que reconocen que esto puede mejorar las percepciones del personal y el compromiso con la seguridad. Una representación equilibrada de géneros, grupos

étnicos y otros atributos identitarios entre el personal de seguridad puede conducir a resultados positivos, como una mejor comprensión de las experiencias de vida de una fuerza laboral diversa, menos sesgos en los diagnósticos de riesgos y en los acuerdos de seguridad, y una resolución de problemas más innovadora.

Mujeres en seguridad

Las mujeres rara vez han ocupado puestos de seguridad en las organizaciones humanitarias, al menos hasta hace poco. La subrepresentación de las mujeres se debe a una serie de factores, incluidas las barreras sociales y culturales, así como percepciones negativas sobre las aptitudes y las habilidades de las mujeres. Estas percepciones se derivan en gran medida de los estereotipos de género y de opiniones rígidas sobre lo que es un referente de seguridad eficaz. Sin embargo, la cantidad de personal femenino con funciones de gestión de riesgos de seguridad en organizaciones humanitarias ha aumentado significativamente en los últimos años, gracias a políticas más amplias que promueven el equilibrio entre géneros y una representación igualitaria. Esto ha tenido numerosos beneficios, entre ellos, mayor credibilidad, ideas y enfoques nuevos y una mayor representación y comprensión de las necesidades de seguridad de las trabajadoras humanitarias.

Competencias clave

Las habilidades y las competencias específicas de las personas en puestos de seguridad dependerán de la organización y el contexto, pero pueden incluir las que se enumeran en la tabla 6.⁷⁸

Es poco probable que un solo individuo posea todas las competencias mencionadas aquí. Por lo tanto, muchas organizaciones forman equipos de seguridad con personas con experiencia diversa en distintas áreas.

78 La INSSA ha elaborado una lista de competencias básicas para el personal de seguridad: <https://inssa.org/certification>.

Tabla 6 Competencias clave del personal de seguridad

Competencia	Descripción
Resolución de problemas, pensamiento analítico, crítico y adaptativo	La capacidad de analizar situaciones complejas, prever riesgos potenciales y concebir soluciones efectivas para tomar decisiones informadas en entornos dinámicos. A esto se vinculan las habilidades para gestionar el cambio a fin de adaptar los enfoques y los planes de seguridad a las amenazas cambiantes y a los cambios organizacionales, lo que garantiza una adaptación continua y la mitigación de riesgos.
Diagnóstico y mitigación de riesgos	La capacidad de identificar y analizar riesgos de seguridad y elaborar estrategias de mitigación de riesgos.
Planificación de seguridad	La capacidad de desarrollar planes de seguridad, incluidos los planes de contingencia.
Respuesta a incidentes y gestión de crisis	Competencia en el manejo de incidentes y crisis.
Medidas de seguridad	Conocimiento y capacidad para implementar medidas de seguridad para amenazas específicas o entornos de amenaza. Esto dependerá del contexto pero puede incluir, por ejemplo, medidas relacionadas con la seguridad del sitio, amenazas relacionadas con el combate y riesgos de rapto. En algunos casos, puede ser relevante contar con conocimientos de primeros auxilios y respuesta a traumas, seguridad digital o habilidades para detectar y mitigar la vigilancia hostil.
Habilidades de negociación y resolución de conflictos	Habilidades de negociación transaccional y resolución de conflictos con colegas y partes interesadas externas.
Comunicación efectiva y habilidades de persuasión	Comunicación clara y persuasiva para transmitir políticas de seguridad, coordinar con equipos y establecer vínculos con el equipo directivo y con las autoridades y las partes interesadas externas.
Trabajo en equipo y colaboración	Capacidad para trabajar bien en equipo y en colaboración en diferentes departamentos de la organización.
Gestión financiera y presupuestaria	Habilidades para la gestión de presupuestos a fin de garantizar que los recursos se asignen de manera eficiente a la mitigación de riesgos.
Habilidades de presentación	Capacidad de presentar información de forma clara y eficaz a diversos públicos, incluido el personal, las partes interesadas y los donantes.

Competencia	Descripción
Gestión del ciclo del proyecto	Comprender las fases de la gestión de proyectos, desde la planificación hasta la evaluación, para implementar medidas de protección que se correspondan con los objetivos y el cronograma del proyecto.
Conocimientos jurídicos y regulatorios	Conocimiento de la legislación y las normas pertinentes para garantizar su cumplimiento y para ayudar a los colegas a enfrentar los problemas jurídicos en diferentes jurisdicciones.
Conciencia cultural	Capacidad de comprender y respetar las costumbres y las normas locales y de adaptar las medidas de seguridad según corresponda.
Tecnologías de la información y la comunicación	Competencia en el uso de las herramientas tecnológicas para garantizar la seguridad de las comunicaciones, la gestión de datos y la denuncia de incidentes.
Alfabetización en el uso de datos/análisis de datos	Capacidad de recopilar, analizar y visualizar datos utilizando herramientas informáticas y tecnologías, lo que puede ayudar, por ejemplo, a extraer información de conjuntos de datos para detectar tendencias y tomar decisiones basadas en evidencia.
Gestión de los riesgos institucionales	Conocimiento exhaustivo de los marcos y las prácticas de gestión de riesgos de toda la organización.
Habilidades de capacitación	Capacidad de desarrollar competencias y enseñar al personal los protocolos de seguridad, los procedimientos de emergencia, el uso de equipos de protección y otros temas relevantes.

Buenas prácticas de comunicación interna

La comunicación efectiva es una habilidad blanda crucial necesaria para una gestión exitosa de los riesgos de seguridad en las organizaciones. Sin embargo, los profesionales de seguridad suelen tener dificultades para comunicar eficazmente su mensaje a otros miembros de la organización e impulsar el cambio. La jerga técnica, las explicaciones complejas sobre los riesgos y las fórmulas, así como las diferentes prioridades, pueden crear barreras para la comprensión y la aceptación por parte del personal no relacionado con la seguridad. La falta de empatía y comprensión de la perspectiva, las motivaciones y los desafíos que afrontan las partes interesadas internas también puede ser una barrera para una colaboración eficaz. Es probable que el equipo directivo de las organizaciones y el personal no relacionado con la seguridad interactúen más con el personal de seguridad que escucha atentamente y comunica soluciones adaptadas a sus requisitos de una manera comprensible.

El personal de seguridad puede abordar los problemas de comunicación mediante las acciones mencionadas a continuación.

- **Simplificar el lenguaje técnico:** evitar la jerga y las explicaciones complejas, haciendo que la información sea más fácil de entender.
- **Adaptar los mensajes a la audiencia:** personalizar la comunicación en función del nivel de comprensión de la audiencia y de sus preocupaciones específicas.
- **Proporcionar contexto a través de ejemplos e historias:** utilizar ejemplos con los que pueden identificarse o historias personales para ayudar al personal a comprender por qué la seguridad es importante para ellos de forma personal y para su trabajo.
- **Ofrecer capacitación y sensibilización:** organizar sesiones de capacitación o iniciativas de concienciación que aclaren la visión y los objetivos de la gestión de riesgos de seguridad dentro de la organización.
- **Mantener una comunicación regular y variada:** utilizar diferentes métodos de comunicación y compartir actualizaciones constantes, destacando los éxitos para levantar la moral.
- **Ser empático:** iniciar conversaciones mostrando empatía, generando confianza a través del diálogo abierto y la escucha activa.
- **Fomentar la comunicación bidireccional:** invitar a los colegas y a las partes interesadas a ofrecer retroalimentación para garantizar que se sientan escuchados y adaptar las estrategias en función de sus aportes.
- **Utilizar la comunicación no verbal:** ser consciente del lenguaje corporal, el tono y las expresiones faciales, ya que pueden mejorar o dificultar la comunicación del mensaje.

► *Para obtener más información sobre la comunicación en materia de seguridad dentro de una organización, véase el capítulo 5.3.*

Valores, principios y habilidades sociales

Además de las competencias mencionadas, el personal que desempeña funciones de seguridad puede apoyarse en los valores y atributos que se mencionan a continuación.

- **Aprendizaje continuo:** actualizar activamente los conocimientos y las habilidades para mantenerse actualizado y relevante.

- **Profesionalismo:** apreciación y deseo de dominar un ámbito profesional y cumplir los estándares de competencia, diligencia y ética.
- **Inteligencia emocional:** la capacidad de identificar y gestionar las propias emociones, empatizar con los demás, comunicarse eficazmente, reconocer diferentes perspectivas y distender los conflictos.
- **Construcción de relaciones:** interactuar eficazmente con colegas y una amplia variedad de redes externas, incluidas las Naciones Unidas, otras organizaciones humanitarias, empresas privadas, autoridades locales y la comunidad empresarial, como fuentes de información y experiencia.
- **Resiliencia personal:** la capacidad física, mental y emocional para resistir problemas y dificultades y superar situaciones de estrés en entornos cambiantes.

► *Para obtener más información sobre la resiliencia y el manejo del estrés, véase el capítulo 5.4.*

Nota sobre los principios humanitarios

Cada vez más se considera que creer en los principios y los valores humanitarios y respetarlos es una característica importante de un profesional eficaz en la gestión de riesgos de seguridad. Comprender estos principios y valores y comprometerse con ellos permite que los referentes de seguridad se comuniquen de manera más eficaz con el personal del programa y ajusten las medidas de gestión de riesgos de seguridad a los objetivos estratégicos generales de una organización humanitaria. Por lo tanto, es aconsejable asegurarse de que el personal de seguridad recién contratado, en particular si no tiene experiencia en el sector humanitario, comprenda, acepte y pueda aplicar y comunicar eficazmente estos valores y principios.

Habilidades de gestión y liderazgo adaptativo

El conocimiento, la experiencia y las habilidades interpersonales y sociales de un gerente son fundamentales para dar forma a la experiencia colectiva de un equipo e influir en su éxito. Esto también es cierto para el personal de seguridad. Un referente de seguridad que intenta hacer cambios o alcanzar objetivos de seguridad avasallando, en lugar de adaptándose y colaborando, puede generar más problemas que soluciones. Es aconsejable que el personal de seguridad adopte enfoques colaborativos para ganar

aceptación y construir una cultura de seguridad positiva, que garantice que el objetivo general sea permitir que los colegas realicen su trabajo de la manera más segura posible.

El modelo de liderazgo adaptativo ha ganado atención en los últimos años y puede resultar especialmente útil para puestos de gestión de riesgos de seguridad. Este enfoque utiliza el diagnóstico de problemas, la interrupción y la innovación para abordar los problemas y los obstáculos a medida que surgen, lo que es directamente relevante para la gestión de riesgos en entornos internos y externos en constante cambio. Si una técnica o proceso no produce los resultados deseados, un líder adaptativo busca estrategias nuevas que puedan funcionar. El cambio adaptativo requiere que los líderes se comuniquen eficazmente con la gente sobre lo que permanece igual (continuidad) y lo que debe cambiar. El liderazgo adaptativo supone estrategias como las siguientes:

- Diagnosticar e interpretar problemas desde una perspectiva amplia.
- Reconocer y lamentar colectivamente las pérdidas.
- Monitorear los niveles de estrés para prevenir daños al trabajo en equipo y a la salud mental de las personas.
- Despersonalizar los conflictos para comprender las distintas perspectivas.
- Determinar activamente qué conservar o descartar dentro de los sistemas organizacionales.
- Fomentar la experimentación y la toma de riesgos inteligente.
- Realizar evaluaciones disciplinadas para refinar los sistemas y los procesos.

5.1.4 Seguridad y gestión de personas

La gestión de las personas es una parte fundamental de la gestión de riesgos de seguridad de una organización. Los empleados contentos y motivados tienen más probabilidades de estar comprometidos y ser productivos. Por el contrario, los empleados poco motivados y descontentos no solo tienen un rendimiento inferior en el lugar de trabajo, sino que también es probable que se conviertan en una fuente de riesgo para la organización. Una de las muchas maneras de establecer un equipo saludable y que funcione bien es garantizar el liderazgo y la claridad respecto a la identidad organizacional, las funciones, la comunicación, la toma de decisiones, la gestión de conflictos y la formación de equipos, y crear un entorno de trabajo en el que los miembros del equipo se sientan cómodos y valorados. Esto comienza con la claridad en los manuales y en los contratos de los empleados y continúa durante cada fase del empleo de un miembro del personal: selección, incorporación, desempeño, desarrollo y finalización del contrato.⁷⁹

79 Para obtener más información sobre la manera en que la seguridad puede contribuir en estas diferentes fases, consulte Davis, J. *et al.* (2020) “Module 13, People management” en *Security to go: a risk management toolkit for humanitarian aid agencies*, 4.^a edición, Global Interagency Security Forum (<https://gisf.ngo/resource/security-to-go/>).

La transparencia y la claridad en los acuerdos contractuales (p. ej., la terminación anticipada de los contratos) pueden reducir las preocupaciones y las reclamaciones del personal. También es un mecanismo importante a través del cual la organización puede aclarar el papel de cada miembro del personal en el seguimiento de las normas y las orientaciones de seguridad. A través del proceso de RR.HH., se puede informar al personal sobre las políticas, la estrategia y la estructura de la organización relacionadas con la seguridad, dónde se ubican las responsabilidades de seguridad y a quién recurrir para obtener apoyo. La claridad y la transparencia respecto a los procedimientos disciplinarios, como las advertencias y los despidos, son fundamentales en caso de incumplimiento de las normas y expectativas de seguridad.

Seleccionar a las personas adecuadas es especialmente importante para las organizaciones humanitarias. Las habilidades inadecuadas o el mal criterio pueden afectar no solo la eficacia operacional en general, sino que también pueden aumentar la vulnerabilidad a los riesgos externos. Asimismo, es importante que los perfiles de riesgo personales se consideren de forma proactiva en las decisiones de selección con el fin de proteger al personal, sin ser indebidamente discriminatorio. Los anuncios de empleo deben redactarse de manera no discriminatoria, considerando cuestiones de identidad y de inclusión. Cuando ciertos perfiles personales puedan correr mayor riesgo que otros debido al contexto y otras circunstancias, esto se puede discutir durante el proceso de selección.

► *Para obtener más información sobre cómo se pueden considerar los perfiles de riesgo personales durante el proceso de selección, véase el capítulo 1.2.*

La investigación previa al empleo es crucial. Esta debe incluir, como mínimo, la verificación de los antecedentes penales, el historial o presencia en línea, la verificación de las certificaciones declaradas, el historial laboral y la investigación de los periodos de inactividad laboral superiores a un mes. Muchos donantes internacionales exigen que se compruebe si los nombres de los miembros del personal figuran en una lista de personas y entidades sancionadas y que se guarde en los archivos una prueba de esta verificación.

Los procesos de incorporación pueden preparar a los empleados nuevos para el entorno de seguridad al que ingresan. Un buen proceso de incorporación considera orientaciones en múltiples niveles sobre las políticas de RR.HH., la seguridad, las operaciones, los programas, la estructura organizacional, el mandato, la misión y el nivel de aceptación/apetito de riesgo, así como el comportamiento personal y cómo se relaciona con la seguridad. Esto puede incluir las posibles repercusiones de las actividades personales, incluido el uso de las redes sociales, en la seguridad. En contextos de alto riesgo es aconsejable proporcionar sesiones informativas y orientaciones exhaustivas sobre seguridad. La incorporación del personal nuevo es un momento ideal para que la organización cumpla con su deber de informar al personal sobre los riesgos que pueden enfrentar y garantizar que el personal se sienta cómodo aceptándolos.

- *Para obtener más información sobre el deber de informar y sobre los umbrales de riesgo individuales, véase el capítulo 1.1.*

Cuando los empleados se marchan de una organización, en particular en casos de cese repentino, despido o cierre de la oficina debido a problemas de inseguridad o financiación, se generan importantes implicaciones para la seguridad. Prepararse para este tipo de escenarios es esencial, no solo para tratar al personal de manera justa, sino también para garantizar que la información de seguridad se transmita de la mejor manera posible a los empleados nuevos. Los errores en la planificación, como se vio durante las evacuaciones en Afganistán en el 2021 y en Sudán en el 2023, pueden dejar al personal local especialmente vulnerable a los riesgos de seguridad, lo que resalta posibles incumplimientos éticos y de seguridad. Las conversaciones tempranas sobre la finalización de los contratos y la realización de entrevistas de fin del servicio pueden ayudar a las organizaciones a conservar conocimientos valiosos, y ofrecer apoyo a los empleados que dejan la organización puede mitigar posibles problemas futuros.

Por último, algunos incidentes de seguridad han sido el resultado de la falta de mecanismos internos de resolución de reclamos, y muchas organizaciones aún pasan por alto la necesidad de gestionar los riesgos de seguridad internos. Establecer procedimientos o mecanismos de presentación de reclamos para el personal proporciona un canal formal y seguro para reportar conductas indebidas (incluida la mala gestión, la corrupción, el acoso y el abuso) sin temor a represalias. Esto puede ayudar a identificar y abordar los problemas de forma temprana y fomenta una cultura de rendición de cuentas y confianza. También es un elemento fundamental en la gestión de incidentes de violencia sexual que afectan al personal de una organización.

Esto está estrechamente vinculado con la salvaguardia, que ha recibido mucha atención en los últimos años dentro del sector humanitario. La salvaguardia se refiere a las medidas más amplias que adoptan las organizaciones para proteger a las personas, tanto dentro como fuera de la organización, de daños, abusos, negligencia y explotación (véase el cuadro más adelante).

Elementos clave de salvaguardia

Políticas y procedimientos

- Políticas de salvaguardia sólidas que describan el compromiso de la organización para prevenir la explotación sexual, el abuso, el acoso y otras conductas indebidas por parte del personal y el personal asociado.
- Mecanismos de reporte y procedimientos de investigación claros, confidenciales y seguros para inquietudes o incidentes de salvaguardia.
- Integración de la salvaguardia a los códigos de conducta, las prácticas de recursos humanos, la gestión de riesgos de seguridad y el diseño de programas.

Prevención

- Investigación y examen exhaustivo durante los procesos de selección.
- Capacitación obligatoria sobre salvaguardia para todo el personal, los socios y los voluntarios.
- Concientizar a las comunidades afectadas sobre sus derechos y la manera de reportar sus inquietudes.
- Evaluación y mitigación de riesgos de salvaguardia en áreas programáticas.

Respuesta

- Enfoques centrados en el superviviente que priorizan sus derechos, sus necesidades y sus deseos.
- Canales de denuncia confidenciales y medidas de protección de denunciantes.
- Investigaciones justas y oportunas de las denuncias, realizadas por investigadores capacitados.
- Medidas de rendición de cuentas transparentes y acciones disciplinarias para casos comprobados de conductas indebidas.

Más información

Investigación y análisis

Foro Europeo Interinstitucional para la Seguridad. (2018). *Gestión de la seguridad del personal humanitario con perfiles diversos* (<https://gishf.ngo/resource/managing-the-security-of-aid-workers-with-diverse-profiles/>).

Global Interagency Security Forum y Humanitarian Outcomes. (2024). *State of practice: the evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Heifetz, R.A., Linsky, M. y Grashow, A. (2009). *The practice of adaptive leadership*. Harvard Business Review Press (www.hks.harvard.edu/publications/practice-adaptive-leadership-tools-and-tactics-changing-your-organization-and-world).

Partner Liaison Security Operations. United States Agency for International Development. (2022). *Women in security. A study of barriers and enablers to entering and progressing within the security field in South Sudan* (<https://gishf.ngo/resource/women-in-security-a-study-of-barriers-and-enablers-to-entering-and-progressing-within-the-security-field-in-south-sudan/>).

Orientación y herramientas

Davis, J. et al. (2020). Module 13, People management. En *Security to go: a risk management toolkit for humanitarian aid agencies*. 4.ª edición. Global Interagency Security Forum (<https://gishf.ngo/resource/security-to-go/>).

Global Interagency Security Forum. (2024). *Estrategia de gestión de riesgos de seguridad (GRS) y desarrollo de políticas: Una guía interfuncional* (<https://gishf.ngo/resource/srm-strategy-and-policy-guide/>).

International NGO Safety and Security Association. (s.f.). Certification (<https://inssa.org/certification>).

Safeguarding Resource and Support Hub. (s.f.). Safeguarding Support Hub. (<https://safeguardingsupporthub.org/>).

5.2 Capacitación en seguridad

La capacitación en seguridad en el sector humanitario ha crecido significativamente en los últimos años y, si bien se desarrolló a partir de los aprendizajes de los sectores privado y gubernamental, ha llegado a convertirse en un área de práctica única y diversa. A pesar de la realización de numerosas investigaciones, del desarrollo de pautas generales y de los esfuerzos para mejorar la calidad y la consistencia de la capacitación en seguridad en el sector,⁸⁰ todavía no existe un enfoque estándar sobre la capacitación en seguridad.

En este capítulo se cubren los enfoques existentes sobre la capacitación en seguridad, incluidos los beneficios y los desafíos de los diferentes tipos de capacitación, y consideraciones clave para las organizaciones con respecto a las necesidades básicas y la equidad en el acceso a estos recursos.

5.2.1 ¿Por qué es importante la capacitación en seguridad?

Si bien este informe de buenas prácticas se centra en el trabajo del personal de seguridad, muchas, si no la mayoría, de las decisiones de seguridad las toman miembros individuales del personal. Por esa razón, todo el personal, sin importar su puesto, debe ser capaz de tomar decisiones de seguridad informadas para evitar incidentes y responder eficazmente ante las amenazas. La capacitación en seguridad desempeña un papel fundamental en este sentido y es un aspecto clave para cumplir con el deber de cuidado y crear una cultura de seguridad positiva.

5.2.2 Tipos de capacitación en seguridad

La capacitación en seguridad se puede dividir en tres categorías:

- Concientización general sobre seguridad, brindada al personal a través de orientaciones iniciales y reuniones informativas.
- Capacitación en habilidades de seguridad personal, como la formación sobre sensibilización para entornos hostiles (HEAT, por sus siglas en inglés).
- Capacitación en gestión de riesgos de seguridad para personal con responsabilidades de seguridad, que puede incluir capacitación en gestión de crisis.

Una cuarta categoría potencial es la capacitación en gestión estratégica de riesgos de seguridad para el personal con funciones de liderazgo en las organizaciones, generalmente para el equipo directivo y los directores de seguridad. Esto abarca cuestiones como la manera en que la seguridad se relaciona con otros procesos organizacionales y con la gestión de riesgos, así como su integración en otras políticas

80 Por ejemplo, el NGO Safety and Security Training Project de EISF e InterAction (2014): <https://reliefweb.int/report/world/ngo-safety-and-security-training-project-how-create-effective-security-training-ngos>.

y áreas de trabajo, especialmente el deber de cuidado. Este nivel de capacitación es poco común.

Concientización sobre seguridad: orientaciones iniciales y sesiones informativas

Normalmente, se brinda capacitación básica en seguridad al personal recientemente incorporado a una organización o cuando llega a un lugar nuevo. Estas sesiones suelen ser breves y se centran en proporcionar al personal una descripción general de las políticas y los procedimientos de seguridad de la organización, incluidos los recursos y los puntos de contacto, así como las funciones y las responsabilidades clave (incluidas las propias responsabilidades de los miembros del personal). En este sentido, estas sesiones son diferentes de la mayoría de las capacitaciones en seguridad personal, que tienden a ser más genéricas y no siempre tratan los procedimientos organizacionales.

Las sesiones de concientización sobre seguridad pueden centrarse en tipos específicos de riesgos, a menudo relacionados con un contexto particular, y también pueden abarcar los desafíos más amplios, como cuestiones relacionadas con los riesgos basados en la identidad y otras preocupaciones, como, por ejemplo, las amenazas digitales. También pueden incluir los riesgos de seguridad derivados de hechos accidentales, como la seguridad contra incendios, en especial en los lugares donde se ejecutan los proyectos, aunque en ocasiones estos pueden tratarse por separado de las cuestiones de seguridad ante actos intencionados, sobre todo cuando en la organización hay referentes de seguridad separados para abordar estos dos tipos de situaciones. Estas sesiones pueden convertirse en ejercicios de marcar casillas, especialmente si se ofrecen en línea sin la posibilidad de plantear preguntas.

Tabla 7 Sesiones informativas de concientización sobre seguridad: contenido de ejemplo

Contenido de ejemplo	Descripción
Enfoque de seguridad	Una explicación del enfoque de la organización sobre la seguridad, el deber de cuidado del personal, los riesgos que afronta el personal y la actitud de la organización hacia el riesgo (es decir, el apetito de riesgo).
Política de seguridad	Una introducción a la política de seguridad de la organización y otras políticas pertinentes, incluidos los principios clave y los requisitos de seguridad conexos y su aplicación.
Estructura de gestión de riesgos de seguridad	Una descripción general de las funciones y las responsabilidades con respecto a la gestión de la seguridad en la organización.

Contenido de ejemplo	Descripción
Expectativas	Las expectativas de la organización respecto a cada miembro del personal, incluida su responsabilidad por su propia seguridad y la de sus colegas, y las acciones y comportamientos pertinentes. También puede abarcar lo que el personal debe esperar de la organización con respecto a la seguridad, incluido el derecho a retirarse o a decir “no” si siente que una situación es insegura.
Seguridad en los viajes	Las disposiciones de seguridad de la organización para los viajes.
Procedimientos de emergencia	Una explicación de los procedimientos de la organización en caso de emergencia, como asistencia médica. Puede incluir toda la información necesaria para que el personal reporte un incidente y busque asistencia (p. ej., cómo llamar al proveedor de seguro médico).
Denuncia de incidentes	Una explicación de qué incidentes deben reportarse y cómo hacerlo.
Recursos	Recursos pertinentes para el personal, entre ellos, documentos, recursos en línea, manuales, guías y material de capacitación.

Adaptado de Bickley, S. (2017) *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*, EISF (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Capacitación en seguridad personal

Brindar una capacitación más profunda sobre seguridad personal puede ser apropiado para el personal que trabaja en lugares de mayor riesgo. Estos cursos tienden a ser más largos (algunos duran varios días) y pueden ser impartidos por personal calificado de la organización o por proveedores de servicios externos.

Si bien las sesiones de concienciación sobre seguridad tienden a centrarse en lograr la comprensión y el cumplimiento de los protocolos de seguridad organizacional, la capacitación en seguridad personal suele ser más genérica y normalmente se centra en desarrollar comportamientos y habilidades para proteger al personal y a sus colegas. En la tabla 8 a continuación se enumeran algunos ejemplos de objetivos de aprendizaje.⁸¹

81 Para conocer más objetivos de aprendizaje relativos a la seguridad personal, consulte EISF e InterAction (2014).

Tabla 8 Ejemplos de objetivos de aprendizaje

Objetivo	Descripción
Conciencia de la situación	Consideración del entorno y las percepciones locales.
Conciencia de la seguridad	Conciencia y responsabilidad personal por las decisiones y acciones que pueden afectar la seguridad personal y organizacional.
Perfil de riesgo personal	Conciencia de cómo puede ser percibido cada miembro del personal a través de su apariencia o acciones, incluyendo cualquier exhibición de riqueza o estatus, comportamiento seguro y sereno, lenguaje diplomático y con tacto, y actitudes respetuosas hacia las culturas y costumbres locales. También es importante tener claro que, en ocasiones, los perfiles personales se perciben erróneamente o no se pueden mitigar a nivel individual (por ejemplo, cuando existe discriminación basada en el grupo étnico o actitudes negativas hacia las mujeres).
Comunicación	Mantenerse en contacto con los colegas según sea apropiado y de acuerdo con las expectativas de la organización.
Respuesta personal	Capacitar al personal sobre cómo responder eficazmente a las amenazas, la hostilidad, las crisis y el estrés.

El nivel de detalle y la duración de un curso de capacitación en seguridad personal generalmente están determinados por el nivel de riesgo al que posiblemente se enfrente el personal. Este tipo de capacitación puede adoptar muchas formas, pero lo ideal es que esté adaptada a cada organización, a las necesidades del personal y al lugar en cuestión. Lo que funciona para una organización o un lugar puede no ser adecuado para otro. Los cursos de capacitación en seguridad se han vuelto cada vez más profesionales y generalizados en los últimos años (aunque con distintos niveles de calidad y credibilidad), y muchos consideran que los cursos de HEAT son el “modelo de referencia” en la capacitación en seguridad personal para contextos de alto riesgo.⁸² Si bien no existe un formato establecido para estos cursos, normalmente duran entre 3 y 5 días e implican una combinación de aprendizaje y ejercicios en el aula con escenarios de simulación más complejos, que por lo general implican colocar a los participantes en situaciones estresantes realistas con utilería y actores.

82 La HEAT es el tipo de entrenamiento predominante, aunque existen diferentes variaciones, entre ellas, la formación en entornos hostiles y primeros auxilios (HEFAT, por sus siglas en inglés) y la formación en entornos hostiles (HET, por sus siglas en inglés).

Muchos argumentan que el componente de simulación hace que la HEAT sea diferente de los cursos generales de seguridad personal. Los cursos de HEAT de calidad se basan en los principios del entrenamiento de exposición al estrés de alta fidelidad (o entrenamiento de inoculación del estrés), desarrollado en el campo de la psicología. Las investigaciones sobre el entrenamiento de exposición al estrés de alta fidelidad en profesiones como la medicina y la aviación respaldan la eficacia de dicho entrenamiento cuando:

- transmite conocimientos y familiaridad con el entorno de estrés para formar expectativas precisas;
- transmite conocimientos sobre los efectos del estrés en el cerebro y en el comportamiento y cómo controlar estas respuestas de forma segura, y
- genera confianza en la capacidad de la persona para desempeñarse en situaciones cada vez más estresantes.

Las simulaciones de la HEAT permiten a las personas presenciar sus reacciones instintivas en situaciones altamente estresantes. Ya sea que tiendan a respuestas de “lucha”, “huida”, “parálisis” o “amistad/adulación” (es decir, capitular y obedecer), estarán mejor equipados para manejar estas reacciones en situaciones del mundo real. Al practicar habilidades bajo presión y estrés, se espera que los alumnos retengan y apliquen mejor los conocimientos cuando sea necesario.

Algunos cursos de HEAT también cubren primeros auxilios en casos de trauma. La mayoría de estos cursos son impartidos por proveedores de servicios externos especializados. En algunos contextos, algunas entidades nacionales ofrecen cursos de HEAT de acceso libre.

Además de los cursos generales de capacitación en seguridad personal y de HEAT, existen otros cursos relacionados con la seguridad personal: las Naciones Unidas, por ejemplo, ha desarrollado una capacitación en seguridad específicamente para mujeres, llamada Women’s Security Awareness Training (WSAT; Curso de concienciación sobre seguridad para mujeres).

Desde la pandemia de COVID-19, se ofrecen más cursos de seguridad y protección personal en línea y en formato modular (tanto facilitados como no facilitados), y algunos proveedores también anuncian cursos de HEAT en línea. Cada vez hay más cursos gratuitos en línea sobre seguridad personal disponibles en plataformas de capacitación dirigidas a trabajadores humanitarios.⁸³ Algunas organizaciones más grandes han desarrollado internamente capacitación en seguridad en línea.

Algunas organizaciones y proveedores de capacitación han optado por un enfoque combinado de capacitación: una parte de la capacitación se proporciona en línea y luego se realizan ejercicios y simulaciones de manera presencial.

83 Se ofrecen ejemplos en la sección “Más información” al final de este capítulo.

Capacitación en seguridad basada en simulación: posibles desventajas

Los cursos de HEAT son un área de controversia en la comunidad de seguridad humanitaria. Si bien a menudo se los describe y se los considera como “la” capacitación en seguridad para trabajar en lugares de alto riesgo —algunos empleados esperan incluso que sea incluidos como algo habitual en sus organizaciones—, su disponibilidad y accesibilidad limitadas y su alto costo hacen que solo esté disponible para unos pocos trabajadores humanitarios (aunque la expansión del sector ha aumentado su disponibilidad en los últimos años). Pese a que hasta la fecha solo se han realizado unos pocos estudios que demuestran la eficacia de las simulaciones de HEAT,ⁱ las investigaciones sobre cómo responde el cerebro a situaciones amenazantes indican que la información cognitiva previamente aprendida deja de estar disponible a menos que se consolide a través de experiencias más viscerales.ⁱⁱ

La calidad de la simulación de un curso de HEAT puede variar desde simulaciones bien gestionadas, respaldadas por psicólogos y moderadamente estresantes hasta simulaciones más extremas que pueden ser física y psicológicamente angustiantes. Los cursos de capacitación pretenden promover la retención de habilidades pero, si se llevan demasiado lejos, especialmente sin apoyo psicológico, el estrés que experimentan los participantes podría tener el efecto contrario. Más preocupante es el riesgo de traumatización o retraumatización en las simulaciones de capacitación en seguridad, dependiendo de cuán sensible pueda ser un participante a ciertos factores desencadenantes.

A pesar de que las simulaciones más extremas (por ejemplo, escenarios de toma de rehenes) son ahora menos frecuentes en el sector humanitario, el riesgo de perjudicar a los participantes al someterlos a simulaciones estresantes aún es una preocupación. Las buenas prácticas sugieren establecer niveles moderados de estrés (para estimular la memoria), garantizar que los escenarios de simulación estén claramente vinculados a objetivos de aprendizaje específicos y alentar a los participantes a centrarse en cómo reaccionan a los factores estresantes para aprender más sobre sus propias respuestas al estrés.

Si bien el riesgo de causar daño no se puede eliminar por completo, los proveedores de capacitación experimentados han implementado medidas de protección. Esto incluye que un psicólogo calificado administre cuestionarios confidenciales sobre antecedentes psicológicos y de traumas antes de la capacitación y brinde consultas a los participantes que sean motivo de preocupación antes de la capacitación. También se puede disponer de un psicólogo en el lugar para apoyar a los participantes durante las simulaciones. Todos los instructores, alumnos y actores deben sentirse capacitados para abandonar una simulación en cualquier momento si sienten que les resulta imposible manejarla. Por último, un psicólogo puede realizar un seguimiento a cualquier participante que haya tenido dificultades en la formación para garantizar su bienestar. En general, cualquier simulación que genere estrés debe procurar contar con actores bien capacitados, personal de apoyo psicológico y pautas y orientaciones claras.

- i Turner, C.R., Bosch, D. y Nolty, A.A.T. (2021) “Self-efficacy and humanitarian aid workers”, *Journal of International Humanitarian Action* 6(1), 1–12 (<https://doi.org/10.1186/s41018-021-00092-w>) y Roberts, N.T. (2021) *Hostile environment awareness training for humanitarian aid workers: an outcome evaluation*, Tesis doctoral, Fuller Theological Seminary, School of Psychology.
- ii Arnsten, A.F. (2015) “Stress weakens prefrontal networks: molecular insults to higher cognition”, *Nature Neuroscience* 18(10), 1376–1385 (<https://doi.org/10.1038/nn.4087>) y McEwen, B.S. y Akil, H. (2020) “Revisiting the stress concept: implications for affective disorders”, *Journal of Neuroscience* 40(1), 12–21 (<https://doi.org/10.1523/JNEUROSCI.0733-19.2019>).

Capacitación en gestión de riesgos de seguridad

Los cursos de capacitación presenciales y en línea sobre gestión de riesgos de seguridad para el personal humanitario cubren aspectos esenciales de la gestión de la seguridad, incluida la manera de identificar y mitigar los riesgos, así como la forma de responder a situaciones o crisis particulares, entre ellas, las detenciones y los secuestros. Cada vez más, estos cursos consideran los riesgos basados en la identidad y cómo incorporarlos a la gestión de riesgos de seguridad.

La capacitación suele ofrecerse externamente, pero algunas organizaciones han desarrollado sistemas internos para capacitar al personal para que se convierta

en referentes de seguridad. Algunos de estos cursos se han convertido en parte de un programa de certificación para reconocer formalmente las habilidades y las competencias del personal de seguridad (véase la sección “Más información” al final de este capítulo).

También se encuentra disponible capacitación específica sobre diferentes aspectos de la gestión de riesgos de seguridad, como capacitación sobre denuncia de incidentes, conducción (defensiva, segura y de vehículos blindados) y gestión de crisis; los cursos incluyen ejercicios de simulación, que pueden abarcar varias oficinas en diferentes lugares de una misma organización. Los proveedores externos de servicios también ofrecen cursos de gestión de crisis, y hay orientación disponible en línea sobre cómo desarrollar y facilitar este tipo de capacitación (se ofrecen algunos ejemplos en la sección “Más información” al final de este capítulo).

Hay ejemplos de cursos de capacitación estratégica para el personal directivo, como directores de seguridad y el equipo directivo superior con responsabilidades en materia de seguridad sobre el deber de cuidado y los marcos de gestión de riesgos de seguridad, entre otros temas. Sin embargo, los recursos de capacitación en gestión de riesgos de seguridad para el personal superior de seguridad siguen siendo poco comunes y la mayor parte del aprendizaje se comparte a través de redes de organizaciones y en eventos y talleres.

5.2.3 Dificultades

A pesar de los avances logrados en la capacitación en seguridad para los trabajadores humanitarios, aún quedan importantes dificultades por resolver, en especial respecto a la capacitación en seguridad y protección personal.

Tabla 9 Dificultades de la capacitación en seguridad

Ámbito	Dificultad
Desigualdades	Los trabajadores humanitarios nacionales, incluidos los que trabajan para organizaciones internacionales, tienen muchas menos probabilidades de recibir capacitación en seguridad personal que sus colegas internacionales.
Acceso	Existe una falta de capacitación en seguridad accesible a nivel local y en el idioma apropiado, lo que hace que sea más difícil brindar recursos a los trabajadores humanitarios nacionales. Las limitaciones relativas al lugar y el horario de los cursos también pueden impedir que el personal en general acceda a la capacitación. Además, existe la preocupación de que los cursos de HEAT se hayan convertido en el modelo de referencia en materia de capacitación en seguridad, a pesar de no ser accesibles financiera ni logísticamente para la mayoría de los trabajadores humanitarios, en especial los nacionales.

Ámbito	Dificultad
Eficacia	Pese a la dependencia de la capacitación en seguridad personal para preparar al personal para trabajar en lugares de alto riesgo (en particular los cursos de HEAT), existe poca evidencia publicada sobre la eficacia de los diferentes tipos de capacitación en seguridad personal. Aunque los estudios publicados respaldan la eficacia de este tipo de capacitación, la mayoría de los informes sobre su impacto son anecdóticos.
Costos	El costo de la capacitación en seguridad puede variar significativamente en función de lo que se brinda al personal y dónde; muchos miembros del personal de seguridad deben decidir quién recibe la capacitación y quién no, según los fondos disponibles.
Sostenibilidad	Los cursos de capacitación suelen ser experiencias puntuales. Aunque algunas organizaciones exigen actualizaciones cada pocos años, gran parte de la información impartida se olvida rápidamente si no se practica regularmente o si no hay un vínculo claro con las responsabilidades laborales.
Calidad	La ausencia de un estándar claro respecto a la capacitación en seguridad personal conlleva que exista una amplia variación entre los cursos impartidos tanto dentro de las organizaciones como por proveedores externos de servicios. Las organizaciones con menos conocimientos sobre gestión de riesgos de seguridad o menos recursos financieros tienen más probabilidades de elegir, involuntariamente, una capacitación en seguridad de peor calidad para su personal.
Pertinencia	Algunos cursos de seguridad, en particular los que se ofrecen en línea, carecen de adaptación a contextos, programas, organizaciones e individuos específicos. Si bien esto hace que la capacitación sea más accesible, también es posible que no pueda relacionarse con las necesidades y las experiencias particulares de los participantes.
Diversidad	Aunque ha habido avances en este ámbito, todavía hay una falta de diversidad entre los instructores, lo que puede afectar su capacidad para interactuar eficazmente con grupos diversos de trabajadores humanitarios y adaptar el contenido a ellos.

Adaptado de GISF y Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space* (www.humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

5.2.4 Consideraciones sobre buenas prácticas

Las organizaciones deben hacer esfuerzos especiales para garantizar que todo el personal tenga acceso a oportunidades de capacitación y aprendizaje sobre seguridad, pero en especial los miembros del personal más expuestos a los riesgos de seguridad.

Por eso es importante no limitarse a una simple evaluación de las necesidades de capacitación, y analizar los niveles de riesgo de los diferentes miembros del personal en toda la organización, su acceso a la capacitación en seguridad y las medidas para cubrir las deficiencias detectadas. Esto puede complementarse con la traducción de materiales de capacitación a los idiomas locales pertinentes. Para algunas organizaciones internacionales, esto ha significado reducir la oferta de cursos de HEAT para liberar fondos para una capacitación integral en seguridad personal para más personal, especialmente para aquellos que normalmente no recibirían capacitación.

Ejemplo: La seguridad como derecho

El equipo de seguridad de una organización se ha centrado en fomentar un entorno organizacional que considera la seguridad como un derecho. Esto implica educar al personal sobre lo que debe esperar de la organización en términos de apoyo de seguridad y cómo plantear inquietudes si lo que se proporciona en la práctica no coincide con lo que se le ha dicho al personal que espere. Esto se refuerza mediante la capacitación y la concienciación para que el personal sea capaz de ejercer su derecho a la seguridad.

La capacitación en línea se ha convertido en un recurso importante en el sector humanitario. Cada vez hay más cursos de capacitación en seguridad disponibles de forma gratuita y de pago, con distintos niveles de detalle, que cubren múltiples aspectos de la seguridad y en un número cada vez mayor de idiomas. La llegada de la inteligencia artificial (IA) ha acelerado el proceso de desarrollo y traducción de nuevos cursos en línea. Si bien la naturaleza genérica y el diseño “estandarizado” de los cursos en línea, especialmente aquellos que están disponibles gratuitamente, sigue siendo un punto débil, estos recursos pueden servir como una introducción a la seguridad que puede complementarse con una capacitación más detallada y pertinente para la organización.

Un problema que surge de determinar la capacitación en seguridad según los niveles de riesgo contextuales es que puede dar lugar a omisiones en lo que respecta a amenazas como la violencia interpersonal, que suelen tratarse en cursos de capacitación para situaciones de mayor riesgo, pero que son relevantes para la mayoría del personal, independientemente de su ubicación. Por esta razón, algunas organizaciones y proveedores de formación han adoptado un enfoque modular de capacitación, clasificando ciertos temas como “fundamentales” para todo el personal y construyendo módulos sobre la base de las necesidades individuales, la ubicación, las amenazas, la identidad organizacional y los marcos.

Algunos proveedores de formación externos ofrecen cursos personalizados adaptados a necesidades particulares. Estos pueden ser costosos. La capacitación interna, si bien

supone una inversión organizacional significativa en términos de financiación y de personal, permite que los cursos cubran circunstancias específicas de la organización, como el tipo de programación y los perfiles particulares del personal, y sean más fáciles de adaptar a contextos y desafíos particulares. Existen varios recursos para ayudar a las organizaciones a desarrollar la capacitación en seguridad internamente (véase la sección “Más información” al final de este capítulo).

Muchas organizaciones han optado por un enfoque de formación de formadores, que les permite desarrollar capacidad interna y ofrecer formación personalizada en más lugares. Estos enfoques presentan dificultades para el control de calidad y deben ser supervisados de cerca. La colaboración interinstitucional y la inversión conjunta para ofrecer cursos de capacitación en seguridad adecuados al contexto a los trabajadores humanitarios de un lugar en particular también han demostrado ser útiles y pueden reducir los costos de capacitación.

Con el fin de reforzar el aprendizaje impartido durante los cursos de capacitación, algunas organizaciones han incorporado referencias constantes a cuestiones de seguridad en el trabajo rutinario y han establecido simulacros periódicos de seguridad y protección. Para aquellos con responsabilidades de seguridad, algunas organizaciones han desarrollado un programa de tutoría y han asignado “tareas” relacionadas con las responsabilidades reales de los participantes, lo que les permite aprender mientras hacen su trabajo. Por ejemplo, un organismo de las Naciones Unidas ofrece 90 días de formación en el puesto de trabajo para el personal de seguridad después del curso sobre seguridad.

Seguridad inclusiva en la capacitación

Discutir sobre los riesgos diferenciados según los perfiles de identidad puede ser un desafío. La capacitación ofrece una oportunidad para abordar mitos y prejuicios en esta área, y varios instructores han aprovechado el espacio para alentar al personal a pensar más allá de sus propios perfiles de identidad. A continuación se expone una lista de ejemplos de cómo se ha abordado la seguridad inclusiva en la capacitación.

- Ejemplos de la vida real del grupo, anonimizados, compartidos y analizados por el facilitador. Puede ser impactante escuchar lo que los colegas afrontan a diario (incluidas las amenazas internas). Incluso si existe animosidad hacia ese perfil en particular, la mayoría de las personas no quieren que sus colegas sufran daños.
- Un ejercicio de juego de roles en el que se pide a los participantes que consideren los riesgos a los que se enfrentan personajes imaginarios con perfiles de identidad únicos en situaciones particulares.

- La selección intencional de instructores diversos, que ofrece a los participantes la oportunidad de escuchar de primera mano los problemas de seguridad que enfrentan perfiles de identidad específicos. También puede ser útil para los participantes ver perfiles similares en posiciones de influencia y respeto (p.ej., instructores). En general, una buena práctica es combinar distintos perfiles de instructores (género, grupo étnico, trayectoria y habilidades, por ejemplo). La diversidad de los instructores debe reflejar la diversidad de los participantes.

La capacitación en seguridad de una organización comprende temas como qué puede hacer el personal con movilidad limitada en los puestos de control o durante el fuego cruzado y cómo sus colegas pueden apoyarlos en estas circunstancias.

Tabla 10 Consideraciones para la selección de proveedores de formación

Consideración	Factores
Perfil	Los valores, la motivación, la ética y la cultura del proveedor de formación se corresponden con los de la organización y su personal. Lo ideal es que los equipos de capacitación se formen teniendo en cuenta todas las habilidades y la experiencia necesarios, incluida su capacidad para interactuar adecuadamente con el personal del programa humanitario.
Reputación y experiencia	Los instructores pueden proporcionar referencias y testimonios de otras organizaciones humanitarias y tienen la capacidad y la experiencia para capacitar a trabajadores humanitarios. La experiencia contextual es relevante cuando los cursos se imparten en una zona geográfica particular. También puede ser importante tener experiencia docente o conocimientos técnicos en temas específicos (p.ej., violencia sexual o trauma).

Consideración	Factores
Contenido	El contenido de la capacitación en seguridad se corresponde con los tipos de riesgos que probablemente enfrentará el personal de la organización y su enfoque general de seguridad. Puede ser adecuado buscar capacitación con ejercicios de simulación, pero estos pueden ser demasiado agresivos o inapropiados para el personal que participa en la capacitación. El contenido cubre habilidades blandas y duras relevantes. Algunos cursos pueden centrarse en riesgos de mayor impacto y menor probabilidad, como el rapto, y pueden descuidar riesgos de menor impacto pero mayor probabilidad, como los conflictos interpersonales y el estrés crónico.¹ Los cursos más avanzados pueden considerar el bienestar del personal y la gestión del estrés, así como los riesgos basados en la identidad. Muchas organizaciones incluyen capacitación en primeros auxilios. Esto debe ser apropiado al contexto y proporcionado por un instructor con la cualificación necesaria.
Costos	La comparación de los costos entre diferentes proveedores de capacitación es una buena práctica, pero también debe tener en cuenta la calidad y el contenido de la capacitación. Asimismo, se debe considerar si es más apropiado capacitar a menos personal con cursos de seguridad de mayor calidad y más completo o elegir una opción más barata que llegue a más personal, especialmente a aquellos con mayor riesgo de sufrir un incidente de seguridad.
Identidades individuales de los instructores	Es una buena práctica tener en cuenta las habilidades, los conocimientos y la experiencia individuales de los instructores y si se pueden solicitar instructores específicos. Contar con un equipo diverso de instructores que refleje los perfiles del personal que asistirá a la capacitación (p. ej., todos los géneros y grupos étnicos relevantes) puede fomentar una mayor participación y compromiso.
Lugar e idioma	El lugar y la accesibilidad de la capacitación son consideraciones particularmente importantes, incluidos los idiomas en que está disponible la capacitación y los costos relacionados con la asistencia.

¹Para obtener más información sobre las consideraciones de contenido, véase: EISF e Inter-Action (2014).

Adaptado de Bickley (2017) *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*, EISF (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Ejemplo: Principios de capacitación basados en el trauma

Una organización que ofrece capacitación interna sobre seguridad personal con componentes de simulación ha desarrollado principios de capacitación basados en el trauma para su curso. Estos son los siguientes:

- **Seguridad:** los instructores toman medidas para garantizar que los participantes se sientan psicológica y físicamente seguros durante la capacitación.
- **Confianza y transparencia:** los instructores informan a los participantes con antelación sobre lo que deben esperar del curso, las simulaciones y los instructores; no hay sorpresas y el personal es informado previamente sobre los temas que podrían ser inquietantes.
- **Apoyo y conexión:** los instructores hacen esfuerzos concertados para interactuar con los participantes de forma individual, y los participantes trabajan juntos en grupos pequeños; los asesores internos están disponibles durante el curso y hay opciones de asesoramiento externo para el personal que necesite más apoyo.
- **Colaboración y reciprocidad:** el curso está diseñado para fomentar el intercambio de experiencias entre los participantes.
- **Empoderamiento, voz y elección:** el curso abarca buenas prácticas (en lugar de “qué hacer y qué no hacer”) y alienta a los participantes a examinar lo que puede funcionar para ellos en diferentes contextos; los participantes pueden retirarse de un escenario que les parezca inseguro o que supere sus propios límites personales.
- **Justicia social:** la capacitación reconoce la dinámica de poder entre los individuos y aborda específicamente cuestiones de identidad y riesgo; para evitar perpetuar estereotipos dañinos, los lugares ficticios utilizados para la capacitación no se parecen a contextos ni personas de la vida real.
- **Resiliencia, crecimiento y cambio:** el curso procura aumentar la confianza entre los participantes haciéndolos sentir seguros, apoyados y validados; los métodos de enseñanza validan las respuestas de los participantes; después de todas las simulaciones se realizan sesiones informativas para que los participantes reflexionan sobre lo que les funcionó y lo que no.

Más información

Orientación

Comité Internacional de la Cruz Roja. (2021). *SAFE: security and safety manual for humanitarian personnel* (www.icrc.org/en/publication/4425-safe-manuel-de-securite-pour-les-humanitaires).

Foro Europeo Interinstitucional para la Seguridad e InterAction. (2014). *NGO Safety and Security Training Project: how to create effective security training for NGOs* (<https://reliefweb.int/report/world/ngo-safety-and-security-training-project-how-create-effective-security-training-ngos>).

Global Interagency Security Forum. (2022a). *Security and safety training pack* (<https://gisfprod.wpengine.com/long-read/security-safety-training-pack/>).

Global Interagency Security Forum. (2022b). *Inclusive security session plan*. Security and safety training pack (<https://gisf.ngo/long-read/security-safety-training-pack/3-training-resources/>).

Global Interagency Security Forum. (2023). *Manual de ejercicios de gestión de crisis para ONG: Una guía para desarrollar y facilitar ejercicios eficaces* (www.gisf.ngo/resource/ngo-crisis-management-exercise-manual-a-guide-to-developing-and-facilitating-effective-exercises/).

Global Interagency Security Forum. (s.f.). 1. *Security training*. NGO Security Toolbox (www.gisf.ngo/toolbox-pwa/resource/1-field-security-training/).

Investigación y análisis

Arnsten, A. F. (2015). Stress weakens prefrontal networks: molecular insults to higher cognition. *Nature Neuroscience* 18(10), 1376–1385 (<https://doi.org/10.1038/nn.4087>).

Bickley, S. (2017). *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*. Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/>).

Breckenridge, M.-J. et al. (2023) *Aid worker security report 2023 – Security training in the humanitarian sector: issues of equity and effectiveness*. Humanitarian Outcomes (www.humanitarianoutcomes.org/AWSR_2023).

Departamento de Seguridad de las Naciones Unidas. (2021). *Best practices for inclusive security training* (https://gisf.ngo/wp-content/uploads/2021/04/UNDSS_Best-Practices-for-Inclusive-Security-Training.pdf).

Global Interagency Security Forum y Humanitarian Outcomes (2024). *State of practice: the evolution of security risk management in the humanitarian space* (www.humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Headington Institute (apoyo psicológico e investigación sobre HEAT): <https://headington-institute.org/>

McEwen, B. S. y Akil, H. (2020). Revisiting the stress concept: implications for affective disorders. *Journal of Neuroscience* 40(1), 12–21 (<https://doi.org/10.1523/JNEUROSCI.0733-19.2019>).

Roberts, N. T. (2021). *Hostile environment awareness training for humanitarian aid workers: an outcome evaluation*. Tesis doctoral, Fuller Theological Seminary, School of Psychology.

Turner, C. R., Bosch, D. y Nolty, A. A. T. (2021). Self-efficacy and humanitarian aid workers. *Journal of International Humanitarian Action* 6(1), 1–12 (<https://doi.org/10.1186/s41018-021-00092-w>).

Recursos de capacitación

DisasterReady: www.disasterready.org/

Global Interagency Security Forum: <https://gisfprod.wpengine.com/training-events/>

Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja: <https://ifrcstaysafe.org/stay-safe-e-course>

International NGO Safety and Security Association: <https://inssa.org/certification>

Kaya: <https://kayaconnect.org/>

Departamento de Seguridad de las Naciones Unidas: <https://training.dss.un.org/thematicarea/category?id=6>

5.3 Comunicación sobre seguridad en la organización

En los entornos complejos en los que operan las organizaciones humanitarias, la comunicación eficaz de información de seguridad no es solo una necesidad procesal: es también un componente fundamental para proteger al personal y garantizar la continuidad del trabajo humanitario. Cuanto mejor informado esté un miembro del personal, más probabilidades tendrá de comprender y cumplir con los procesos de gestión de riesgos de seguridad de su organización. Además, una información bien difundida y de alta calidad puede ayudar a aliviar la ansiedad y la incertidumbre que a menudo acompañan al trabajo en entornos inestables o de alto riesgo.

5.3.1 Comunicación centrada en la persona

Un principio clave en la difusión de información de seguridad es adoptar un enfoque centrado en la persona y específico para la audiencia. A diferencia de los modelos tradicionales centrados en las necesidades de la organización, este método prioriza las preocupaciones, las vulnerabilidades y los requisitos específicos de las personas en riesgo, al tiempo que adapta el método de comunicación al público objetivo. Ya sea que la información se comparta individualmente mediante reuniones informativas o colectivamente por medio de páginas de la intranet o alertas de mensaje de texto, el contenido y el método de difusión deben adaptarse a los destinatarios. Este enfoque no solo garantiza el cumplimiento de los protocolos de seguridad, sino que también involucra activamente al personal haciendo que la información sea relevante respecto a sus circunstancias inmediatas y su seguridad personal.

Por ejemplo, al informar a un miembro del personal sobre los riesgos en un entorno de alto riesgo, es fundamental considerar factores como sus antecedentes, experiencia y función en la organización. Es posible que una sesión informativa genérica no aborde de manera adecuada los riesgos particulares que enfrenta una empleada que viaja sola en una región conservadora o un miembro del personal con afecciones de salud. Al dirigirse a grupos más grandes por medio de la intranet o de alertas de mensajes de texto, la información debe ser clara, accesible y adaptada a las preocupaciones comunes del grupo, permitiendo al mismo tiempo consideraciones individuales cuando sea necesario.

El personal de seguridad debe ser creativo sobre cómo comparte la información.⁸⁴ Es necesario tener en cuenta el idioma, los formatos y los canales de comunicación. Las ayudas visuales como las infografías, los mapas y los diagramas de flujo pueden ayudar a que la información compleja sea más fácil de entender, y el lenguaje sencillo, las instrucciones claras y la ausencia de jerga técnica pueden mejorar significativamente la eficacia de la comunicación.

⁸⁴ Contar historias, por ejemplo, puede ser una forma eficaz de involucrar al personal en cursos de capacitación en seguridad. Para más información, véase Persaud, C. (2022) *Storytelling for learning: using engaging, ethical stories for effective security training*, Global Interagency Security Forum (<https://gisf.ngo/blogs/storytelling-for-learning-using-engaging-ethical-stories-for-effective-security-training/>).

En última instancia, el objetivo de la comunicación sobre seguridad no es simplemente informar, sino empoderar. El personal debe ser capaz de comprender no solo lo que debe hacer, sino también por qué es importante, ya que esto aumenta la probabilidad de cumplimiento y ayuda a construir una cultura de seguridad positiva. Al brindarle al personal la información específica que necesita para comprender y abordar los riesgos que enfrenta, las organizaciones pueden ayudarlo a trabajar de manera segura y eficaz, incluso en las circunstancias más difíciles.

- *Para obtener más información sobre un enfoque de seguridad centrado en la persona, véase el capítulo 1.2.*
- *Para obtener más información sobre cómo construir una cultura de seguridad positiva, véase el capítulo 1.1.*

5.3.2 Métodos de difusión de la información

La eficacia de la difusión de la información de seguridad depende en gran medida de los canales y los métodos utilizados.

- **Páginas web de la organización para el personal (intranet).** Las intranets son una herramienta valiosa para difundir información de seguridad. Las organizaciones pueden utilizarlas para publicar actualizaciones periódicas sobre la situación de seguridad, cambios en los niveles de riesgo y actualizaciones de los protocolos de seguridad. También puede haber páginas específicas que orienten al personal con perfiles de identidad particulares. Sin embargo, la intranet depende del funcionamiento de las redes, que podrían no estar siempre disponibles para todo el personal.
- **Correo electrónico.** El correo electrónico sigue siendo un canal clave para difundir información dentro de las organizaciones humanitarias. Para ser eficaces, los correos electrónicos deben ser claros, concisos y estructurados, con la información importante visiblemente destacada. Los indicadores de urgencia, como las banderas de prioridad y las líneas de asunto claras, ayudan a garantizar que no se pasen por alto los mensajes críticos. Las actualizaciones periódicas son cruciales en las situaciones en curso, y la traducción a los idiomas principales de los miembros del personal evita malentendidos (a veces, proporcionar enlaces a traductores de IA puede ser suficiente). En algunas circunstancias puede ser conveniente solicitar que el personal confirme la recepción y comprensión de los correos electrónicos, especialmente en el caso de comunicaciones críticas.
- **Alertas de teléfonos móviles (como mensajes de texto o aplicaciones como Signal y WhatsApp).** Las alertas enviadas a teléfonos móviles constituyen un medio de comunicación directo e inmediato, que garantiza que la información crítica se transmita al personal incluso si están viajando o trabajando de forma remota. Estas alertas son particularmente útiles en escenarios donde se requiere una rápida difusión de la información, como, por ejemplo, durante un incremento repentino

de la violencia o un desastre inesperado. Sin embargo, es fundamental equilibrar la frecuencia de las alertas para evitar abrumar al personal con mensajes excesivos, ya que esto podría provocar que no se lean alertas importantes.

- **Sesiones informativas.** Las sesiones informativas relacionadas con los viajes son una parte esencial de la difusión de información de seguridad, en especial para los miembros del personal que están a punto de ingresar a un entorno inestable o desconocido. Dado que las situaciones pueden cambiar rápidamente, es importante proporcionar periódicamente información de seguridad actualizada al personal afectado. Las sesiones informativas nunca deben ser un evento único.

► *Para obtener más orientaciones sobre las sesiones informativas y los riesgos y las medidas de mitigación relacionados con los viajes, véase el capítulo 7.1.*

- **Informes sobre la situación.** Los informes sobre la situación son una herramienta crucial para mantener al personal informado sobre la situación de seguridad actual. Estos informes deben poder generarse rápidamente, ser concisos y centrarse en proporcionar información situacional actualizada que sea fácilmente entendible. Un informe sobre la situación bien elaborado no solo describe el entorno de seguridad actual, sino que también destaca las posibles implicaciones para las operaciones de la organización y cualquier cambio que pueda requerirse en los procedimientos.

Los informes sobre la situación tienen un formato bastante común, pero aún así deben adaptarse a la audiencia y al propósito específicos. Los informes dirigidos al personal del proyecto se centran en asesoramiento práctico y en los riesgos inmediatos, mientras que los escritos para el equipo directivo pueden incluir un análisis más amplio de las tendencias y los posibles escenarios futuros.

- **Informes.** Además de las actualizaciones más inmediatas proporcionadas en los informes sobre la situación, las organizaciones pueden producir informes analíticos que ofrecen un examen más profundo de las tendencias y los riesgos de seguridad. Estos reportes pueden elaborarse como consecuencia de cambios situacionales o contextuales significativos y están diseñados para informar la toma de decisiones estratégicas dentro de la organización. Los informes analíticos también pueden tener una periodicidad determinada, como evaluaciones mensuales o trimestrales y pueden incluir una variedad de medios y otros recursos.

Aunque es menos probable que estos informes den lugar a cambios procedimentales inmediatos, desempeñan un papel fundamental en la configuración de la estrategia de seguridad a largo plazo de la organización. Por ejemplo, un informe podría destacar amenazas emergentes en una región particular que podrían afectar las operaciones futuras de la organización, lo que generaría una revisión de los diagnósticos de riesgos y los planes de contingencia. Dada la naturaleza estratégica de estos informes, es esencial que se redacten teniendo en cuenta el público objetivo. El equipo directivo, por ejemplo, puede requerir un análisis más detallado del impacto potencial sobre las operaciones, mientras que el personal operacional podría beneficiarse de resúmenes centrados en las implicaciones prácticas para sus actividades diarias.

- *Para obtener más información sobre el análisis de las tendencias de incidentes de seguridad, véase el capítulo 4.4.*
- *Para obtener más información sobre los mecanismos de monitoreo de la seguridad, véase el capítulo 3.4.*

5.3.3 Gestión de la sobrecarga informativa

Uno de los desafíos más importantes en la difusión de información de seguridad es el riesgo de sobrecarga informativa, particularmente en entornos inestables donde los acontecimientos pueden desarrollarse rápidamente. En tales situaciones, el gran volumen de información puede abrumar al personal, lo que provoca que sea difícil absorber y actuar en función de las actualizaciones más críticas. Un sistema de clasificación prioriza la información según su urgencia y relevancia.

Este sistema debe guiarse por una serie de preguntas y consideraciones clave:

- **Importancia operacional.** ¿Se verá comprometida la seguridad del personal si esta información no se transmite inmediatamente? En caso afirmativo, debe compartirse inmediatamente. En caso contrario, deben considerarse los puntos siguientes.
- **Actualización de la situación.** ¿Indica la información un posible efecto sobre la seguridad, lo que posiblemente señale a su vez la necesidad de aumentar las precauciones? En caso afirmativo, debe informarse al personal pertinente de manera oportuna. En caso contrario, debe considerarse el punto siguiente.
- **Cambio en el contexto.** ¿Indica la información una tendencia u otras implicaciones a largo plazo para el contexto del programa? En caso afirmativo, debe considerarse cuándo y cómo utilizar mejor la información para respaldar la toma de decisiones estratégicas.

Cada organización deberá considerar la mejor manera de transmitir la información de seguridad para cada nivel y asegurarse de que el personal esté capacitado sobre cómo y cuándo compartir esta información y con quién.

Cuando la información tiene una importancia inmediata y representa una amenaza general para los miembros del personal, la prioridad es difundirla lo más rápida y ampliamente posible. Los métodos de comunicación sobre seguridad tradicionales, como una cadena de comunicación, pueden ser efectivos en estos escenarios, pero muchas organizaciones ahora también utilizan mensajería grupal o de difusión. Estos métodos permiten la rápida difusión de información crítica, lo que garantiza que todo el personal pertinente esté informado y pueda tomar medidas apropiadas sin demora.

Ejemplos de un sistema de clasificación para el intercambio de información

- **Importancia operacional.** Una protesta frente a los edificios del Parlamento del país se está volviendo violenta. Informe al personal que evite el área. Utilice mensajes de texto, una cadena de comunicación o mensajería de difusión o de grupos de WhatsApp/Signal para difundir rápidamente información al personal que trabaja en la zona.
- **Actualización de la situación.** Se prevén protestas en los próximos días frente a los edificios del Parlamento. Envíe un aviso por correo electrónico y/o incorpórelo en los informes sobre la situación, los informes de seguridad específicos y los POE.
- **Cambios en el contexto.** Las protestas llevaron al surgimiento de un Gobierno hostil hacia las organizaciones humanitarias. Incorpore la información pertinente en los informes de seguridad, las sesiones informativas o las capacitaciones, y utilícela en los procesos analíticos de seguridad.

Cadena de comunicación

Una cadena de comunicación es un sistema jerárquico utilizado para difundir información rápidamente a un grupo grande. Comienza con una persona que se comunica con individuos clave, que luego a su vez informan a otras personas, y se crea un efecto en cascada hasta llegar a todos. Este modelo es ideal para emergencias o actualizaciones urgentes, ya que garantiza una comunicación rápida. Las cadenas de comunicación pueden ser manuales, mediante llamadas directas, o automatizadas, utilizando un programa informático para enviar mensajes por medio de llamadas, mensajes de texto y correos electrónicos.

Para la comunicación a nivel operacional, es esencial introducir componentes de redundancia. Esto significa que el personal tiene acceso a múltiples métodos de comunicación independientes, como radios y teléfonos satelitales, de modo que la comunicación puede continuar incluso si un método falla.

► *Para obtener más información sobre los diferentes métodos de comunicación y el desarrollo de planes de comunicación que incorporen la redundancia, véase el capítulo 6.1.*

Para las actualizaciones situacionales o los cambios en el contexto que no requieren una actuación inmediata pero tienen implicaciones a largo plazo, suele ser adecuado un enfoque más moderado. Este tipo de actualizaciones aún deben comunicarse rápidamente, pero el énfasis debe estar en proporcionar un análisis exhaustivo de la situación y su impacto potencial en la gestión de riesgos de seguridad de la organización.

Las actualizaciones estratégicas de alto nivel podrían comunicarse mejor a través de informes formales o sesiones informativas ejecutivas, mientras que las actualizaciones operacionales podrían difundirse mediante canales de comunicación más informales, como reuniones de equipo o chats grupales. Se podrían compartir conceptos e información de seguridad de manera más exhaustiva en las sesiones informativas y de capacitación. La clave es garantizar que el método de comunicación se corresponda con la urgencia y la importancia de la información, así como con las preferencias y los hábitos del público destinatario.

Tableros de información y aplicaciones

Las organizaciones humanitarias utilizan cada vez más tableros de información y aplicaciones móviles personalizadas para compartir información de seguridad.

Los tableros de información proporcionan una plataforma para que el personal acceda a información relacionada con la seguridad, como los planes de seguridad, a menudo de formas visualmente llamativas mediante, por ejemplo, una matriz cromática (*véase el capítulo 3.4 para obtener más información sobre estos tableros*).

Las aplicaciones móviles pueden brindar actualizaciones de seguridad en tiempo real, permitir la denuncia rápida de incidentes y ofrecer orientación sobre situaciones de seguridad específicas (como acciones a tomar en los puestos de control). También pueden incluir información de contactos de emergencia. Las aplicaciones pueden ser especialmente útiles para el personal que necesita acceder a información de seguridad mientras se desplaza.

Verificación y sobrerreacción prudente

La precisión y la fiabilidad de la información de seguridad son de suma importancia. Naturalmente, se espera que toda la información difundida por la organización haya sido verificada en la mayor medida posible. Sin embargo, en situaciones que evolucionan rápidamente no siempre es posible verificar completamente la información

antes de que sea necesario comunicarla. En tales casos entra en juego el concepto de sobrereacción prudente.

Una sobrereacción prudente implica adoptar medidas de precaución basadas en la información disponible, incluso si no ha sido completamente verificada, siempre que los riesgos potenciales justifiquen tal enfoque. Por ejemplo, si hay un informe no verificado de una amenaza inminente a la seguridad en una zona determinada, puede ser prudente suspender temporalmente las operaciones o aconsejar al personal que se refugie hasta que haya más información disponible. La clave es comunicar la información de una manera que describa claramente las razones de las medidas adoptadas, reconociendo al mismo tiempo la incertidumbre que rodea la situación. Al transmitir dicha información, es esencial anticipar las posibles preguntas que pueda tener el personal, como “¿por qué necesito saber esto?” y “¿qué tengo que hacer?”. Al abordar estas preguntas anticipadamente, las organizaciones pueden ayudar a reducir la confusión y garantizar que el personal esté preparado para tomar las medidas necesarias en respuesta a posibles amenazas.

Revisión y adaptación continuas

La comunicación eficaz sobre seguridad en las organizaciones humanitarias depende en gran medida de la retroalimentación y la adaptación continuas. El personal de seguridad debe buscar e incorporar activamente los comentarios de sus colegas para garantizar que la información proporcionada sea clara y útil. A medida que evolucionan los entornos de seguridad y las amenazas, también deben evolucionar las estrategias y los métodos de comunicación utilizados. Es esencial realizar revisiones o auditorías periódicas de estas prácticas, en las que participen todos los niveles de la organización. Mantenerse informado sobre las nuevas tecnologías de comunicación puede ayudar a mejorar la eficiencia y el alcance de las actualizaciones sobre la seguridad.

Más información

Persaud, C. (2022). *Storytelling for learning: using engaging, ethical stories for effective security training*. Global Interagency Security Forum (<https://gisf.ngo/blogs/storytelling-for-learning-using-engaging-ethical-stories-for-effective-security-training/>).

5.4 Cuidado del personal

La resiliencia del personal y de los equipos es esencial para la resiliencia de la organización. Los entornos en los que se desarrolla el trabajo humanitario suelen ser muy estresantes, por lo que un apoyo adecuado al bienestar mental y físico del personal mejora su resiliencia y su capacidad para tomar decisiones acertadas que son fundamentales para una gestión eficaz de los riesgos de seguridad.

Este capítulo se centra en la importancia de integrar consideraciones de salud física y mental en la gestión de riesgos de seguridad y de apoyar al personal antes, durante y después de incidentes críticos. Proporciona estrategias para mantener el bienestar del personal y fortalecer la salud mental y el apoyo psicosocial con el objetivo de evitar resultados adversos a largo plazo. El enfoque descrito puede ser implementado por personal no médico, garantizando que todos los aspectos del cuidado del personal se aborden eficazmente.

► *Este capítulo se centra principalmente en la salud mental. Para consultar consideraciones médicas físicas y las preparaciones necesarias, véase el capítulo 5.5.*

5.4.1 Conceptos clave

Resiliencia y bienestar

La resiliencia es el proceso y el resultado de adaptarse con éxito a experiencias de vida difíciles o desafiantes, especialmente a través de la flexibilidad cognitiva, emocional y conductual y la adecuación a las demandas externas e internas. Abordar la resiliencia implica apoyar el bienestar general para desarrollar la capacidad individual y del equipo a fin de manejar las crisis de manera eficaz y al mismo tiempo brindar apoyo psicosocial inmediato y a largo plazo en respuesta a los incidentes (véase la figura 11).

La resiliencia de los miembros del personal frente a entornos y eventos desafiantes puede depender de varios factores, entre ellos, el poder de las redes sociales, factores culturales y otros aspectos de la identidad, la perspectiva y la disposición general y los mecanismos de afrontamiento. Las capacidades de resiliencia se pueden desarrollar y nutrir, y cada individuo tiene su propio nivel de resiliencia influenciado por sus atributos personales, expectativas, estilo de vida y autoconciencia de sus límites. El entorno laboral también influye, ya que factores como el horario laboral, las expectativas, la carga de trabajo y los posibles traumas vicarios afectan la resiliencia.

Figura 11 Factores propicios para la resiliencia



Si bien muchos factores estresantes pueden estar fuera de su control, las organizaciones aún pueden fomentar la resiliencia promoviendo una cultura laboral de apoyo.

En una respuesta humanitaria, las condiciones de vida suelen ser difíciles, ya sea que el personal resida en una zona afectada por una crisis o en tiendas de campaña o viviendas compartidas de la organización. Para el personal que trabaja lejos de su hogar y su familia, los factores estresantes fuera del horario laboral pueden ser más significativos, ya que carecen del apoyo familiar. El personal puede tener dificultades con los límites difusos entre el trabajo y el tiempo personal y puede experimentar un mayor estrés debido al acceso limitado al apoyo familiar. El personal que reside en el lugar podría enfrentar presiones adicionales como miembros de la comunidad afectada, puesto que las crisis podrían afectar a sus familias, a sus amistades y a la infraestructura circundante.

Implementar un enfoque de apoyo entre pares basado en equipos y garantizar que los gerentes comprendan la importancia del autocuidado y los riesgos para la salud mental puede mejorar significativamente la resiliencia individual y organizacional.

El bienestar general de una persona es más que su salud física y su seguridad, y el grado en que la gestión de riesgos de seguridad incluye y apoya activamente las dimensiones mentales, emocionales y sociales también puede tener un efecto crucial en la moral, el desempeño, la toma de decisiones y los resultados personales. El personal sano toma mejores decisiones de seguridad y está mejor preparado para afrontar entornos e incidentes estresantes.

Ejemplo: Centrarse en mecanismos de afrontamiento saludables

Una organización ha incluido la gestión del estrés en la capacitación sobre salud y seguridad personal para todos sus miembros. Durante esta sesión, el personal aprende a reconocer signos de estrés en ellos mismos y en los demás y a analizar sus mecanismos de afrontamiento. Cada uno de ellos se compromete a utilizar al menos un mecanismo de afrontamiento saludable en el que se centrará durante los meses posteriores a la capacitación. La sesión finaliza con los participantes acordando las medidas que la organización puede tomar para mejorar el bienestar del personal. Algunos ejemplos son colocar plantas en la oficina, disponer que haya un médico en el lugar un día al mes para consultas sin cita previa, organizar un desayuno con el equipo una vez a la semana y crear un espacio seguro para que el personal se relaje durante o al final de su jornada laboral. Las sesiones ayudan a normalizar las conversaciones sobre el bienestar y la salud, crean una mejor comprensión sobre la manera en que los equipos pueden apoyarse entre sí y aumentan la conciencia de los mecanismos de afrontamiento de los miembros del personal.

El bienestar general de una persona comprende seis dimensiones: física, emocional, social, intelectual, profesional/ocupacional y espiritual/religiosa. Estas dimensiones son interdependientes, lo que significa que si una se ve afectada, puede tener un efecto sobre las demás. El personal de seguridad debe comprender y tener en cuenta estas dimensiones y su interrelación, en especial durante eventos o periodos difíciles. También puede desempeñar un papel importante a la hora de promover la implementación en toda la organización de iniciativas de bienestar que aborden estas seis dimensiones.

Prácticas de bienestar en el lugar de trabajo

Las prácticas de bienestar en el lugar de trabajo pueden incluir la designación de un referente o comité de bienestar que organice actividades físicas, talleres y capacitación sobre manejo del estrés y salud mental. Prácticas como promover la gratitud y el reconocimiento y alentar los descansos pueden mejorar la moral y la productividad. Normas como no enviar correos electrónicos fuera del horario laboral, alentar al personal a tomar vacaciones anuales y ofrecer acuerdos de trabajo flexibles contribuyen aún más al bienestar. Proporcionar espacios para la meditación, el yoga y las actividades sociales puede ayudar a los empleados a sentirse valorados y apoyados. Brindar opciones de desarrollo profesional, programas de educación financiera y apoyo al personal en circunstancias especiales, como a quienes acaban de ser padres o tienen compromisos religiosos, pueden promover el bienestar.

Estrés y trauma

Debido a las tareas que realizan y al entorno en el que se encuentran, todos los trabajadores humanitarios son vulnerables al estrés. Esto incluye a profesionales y jefes de seguridad que deben lidiar periódicamente con incidentes que afectan a otras personas. Cada persona experimentará y manifestará el estrés de distintas maneras y desarrollará mecanismos de afrontamiento individuales, de acuerdo con sus perfiles y circunstancias personales.

Existen distintos tipos de estrés, y este puede ser saludable o no saludable. El estrés saludable ayuda a las personas a centrarse en la tarea o en la situación, moviliza la energía y las prepara para la acción. Por ejemplo, tener una fecha límite puede provocar estrés, pero también puede ayudar a completar una tarea. En situaciones de tensión o riesgo, las reacciones al estrés y al miedo pueden dar a las personas la concentración que necesitan para sobrevivir.

Sin embargo, cuando el estrés se produce con demasiada frecuencia, es demasiado intenso o dura demasiado tiempo, se vuelve perjudicial. Todo estrés utiliza energía. Una serie aparentemente interminable de plazos ajustados o la exposición continua a situaciones o experiencias de alto riesgo pueden agotar las reservas de energía. Cuando varios factores estresantes tienen lugar al mismo tiempo y especialmente cuando son prolongados, incluidos los factores corrosivos como el miedo, la incertidumbre y el conflicto persistentes, se puede generar estrés acumulativo.

Existe una diferencia entre estrés y trauma. Las respuestas habituales al estrés, llamado estrés agudo, como el mecanismo de supervivencia *luchar o huir*, se desactivan cuando la amenaza termina. Con el trauma, el cuerpo permanece en ese modo de supervivencia y continúa respondiendo como si estuviera bajo amenaza incluso después de que la amenaza haya cesado. Los eventos traumáticos superan la capacidad de las personas para afrontar y manejar el estrés.

Si una persona sufre un nivel continuo de estrés elevado, sus mecanismos de afrontamiento pueden verse superados, lo que reduce su capacidad para resistir el impacto psicológico de un evento traumático. El estrés y el trauma prolongados también afectarán la capacidad para tomar decisiones de una persona.

El trauma puede ser la consecuencia de un factor estresante agudo (como un incidente crítico o un evento potencialmente mortal), estrés acumulativo o exposición continua al trauma de otros. Aunque el trauma es común, un evento adverso solo o incluso una serie de ellos no producen inevitablemente un trauma. Depende más bien de cómo responda la persona y de cómo esté preparada para afrontar la experiencia, lo que está estrechamente vinculado con los recursos a su disposición, así como con sus experiencias pasadas.

El conjunto de factores estresantes que pueden provocar un trauma es muy amplio y este puede producirse horas, días, semanas, meses y años después (del inicio de) un suceso. Estos factores pueden variar en cuanto a su intensidad y pueden provocar un trastorno de estrés postraumático u otras formas de trauma. En todos los casos, afectan la resiliencia del personal. Es posible que las organizaciones necesiten estar preparadas para brindar apoyo mucho tiempo después de que se haya producido el incidente.

Trauma indirecto

Los trabajadores humanitarios pueden sufrir traumas indirectamente de diversas formas. El estrés traumático secundario se refiere a síntomas como pesadillas o ansiedad que surgen de la exposición indirecta de un individuo al trauma de otra persona, generalmente a través de sus interacciones con el superviviente del trauma o por prestarle asistencia. El trauma vicario implica un cambio profundo en la visión del mundo de una persona causado por la exposición indirecta repetida al trauma de otros. Afecta normalmente al equipo de respuesta inicial, como los paramédicos, pero también puede afectar a otros, por ejemplo, al personal de medios y comunicación expuesto repetidamente a contenido inquietante en línea.

5.4.2 Seguridad, salud mental y apoyo psicosocial

Los riesgos de los efectos sobre la salud mental asociados con el trabajo humanitario deben reconocerse como parte del deber de cuidado de una organización. El desarrollo de estrategias localizadas puede mejorar el entorno de trabajo y reforzar la preparación para la respuesta psicosocial (SMAPS) a fin de apoyar al personal durante y después de las emergencias y los incidentes críticos. Esto puede basarse en un enfoque de salud mental y apoyo psicosocial, que aborde tanto las necesidades de salud mental como los factores sociales que afectan el bienestar de las personas y los grupos mediante la integración de la atención psicológica con los sistemas de apoyo social. Es importante señalar que el apoyo psicológico se centra en la terapia individual y en el manejo de problemas de salud mental como la ansiedad o la depresión, mientras que el apoyo psicosocial es un enfoque más amplio que integra aspectos psicológicos y sociales del bienestar, y aborda el impacto de las relaciones, el medio ambiente y la comunidad en la salud mental.

La incorporación de los recursos de salud mental y apoyo psicosocial en los procesos de gestión de riesgos de seguridad mejora la resiliencia del personal y reduce el riesgo de incidentes relacionados con el estrés o el agotamiento. Esto puede implicar:

- Fomentar una cultura de apoyo que reduzca el estigma y aliente al personal a buscar ayuda antes de que los problemas se agraven y comprometan la seguridad.
- Identificar las necesidades y los obstáculos relativos a la salud mental y el apoyo psicosocial.
- Mapear los proveedores de servicios de salud mental y apoyo psicosocial de la organización y locales, aprobados por médicos.
- Desarrollar estrategias para el reclutamiento, la selección y la supervisión de los servicios de apoyo psicosocial.
- Contactarse con los recursos locales para mejorar la gestión de incidentes críticos proporcionando apoyo psicosocial inmediato y culturalmente adecuado.
- Incluir procedimientos de respuesta psicosocial en los planes de gestión de crisis y seguridad.
- Capacitar a jefes y a gerentes sobre cómo responder eficazmente a problemas psicosociales, incluidas estrategias de bienestar mental y desarrollo de la resiliencia.
- Preparar y capacitar al personal para dar respuestas psicosociales adaptadas al trauma ante incidentes críticos, incluida la violencia sexual.
- Incorporar consideraciones sobre la salud mental en la capacitación y las sesiones informativas sobre seguridad.

► *Para obtener más información sobre cómo incorporar consideraciones de salud mental en la capacitación en seguridad, véase el capítulo 5.2.*

Algunos expertos recomiendan un enfoque de gestión de riesgos de salud mental que aborde los riesgos psicológicos como si fueran riesgos de seguridad (utilizando las mismas herramientas y marcos), evaluando los riesgos psicológicos junto con los riesgos de seguridad física e implementando medidas de mitigación y planes de contingencia pertinentes. Al incorporar la salud mental en el marco de gestión de riesgos de seguridad, las organizaciones pueden mejorar la resiliencia en general y gestionar eficazmente los riesgos de seguridad y los psicológicos.

Esto puede respaldarse con un mapeo inicial de las necesidades y la capacidad de salud mental y apoyo psicosocial en cada lugar donde opera la organización. Este mapeo puede considerar los factores estresantes comunes del personal con diferentes perfiles, así como los problemas y las necesidades de salud mental existentes entre los miembros del personal. Puede incluir una revisión en la que se indique qué servicios, proveedores, instalaciones y programas están disponibles local o remotamente (incluidos los planes de seguro) y para quién (considerando, por ejemplo, los idiomas y las necesidades de accesibilidad del personal). Las actitudes prevalecientes, la cultura organizacional y los mecanismos de afrontamiento frente al estrés, el agotamiento, el trauma vicario y el estrés postraumático también son consideraciones importantes.

La información recopilada a partir de este mapeo se puede utilizar para informar las iniciativas de apoyo psicosocial y bienestar de una organización. A continuación se mencionan algunos ejemplos de servicios de salud mental y apoyo psicosocial, tanto formales (brindados por profesionales externos e internos) como informales (como grupos de apoyo entre pares).

Servicios de asesoramiento y terapia:

- Programas de asistencia al empleado (servicios confidenciales de apoyo y asesoramiento psicológico de terceros para cuestiones personales y relacionadas con el trabajo).
- Profesionales de salud mental en el lugar (internos o externos).
- Servicios de telesalud (internos o externos).
- Servicios especializados, como psiquiatras o terapeutas, convocados después de un incidente o una crisis.

Otras iniciativas incluyen:

- Talleres y capacitación en salud mental.
- Programas de manejo del estrés.
- Formación en primeros auxilios psicológicos.
- Programas de apoyo entre pares.
- Recursos de salud mental en línea.

Es importante revisar periódicamente las opciones de salud mental y apoyo psicosocial para garantizar que se correspondan con las necesidades y las expectativas del personal y sean pertinentes y accesibles para el personal con diversos orígenes culturales. Las buenas prácticas sugieren no depender de un solo mecanismo de apoyo, sino ofrecer una variedad de opciones pertinentes para diferentes tipos de factores y eventos estresantes, a fin de abordar eficazmente el amplio espectro de necesidades del personal. Por último, la organización debe indicar claramente por adelantado qué servicios proporciona en términos de salud mental y apoyo psicosocial, con objeto de que el personal sepa a qué servicios tiene acceso y qué tipo de apoyo puede esperar después de un incidente crítico.

Ejemplo: Jornadas de bienestar

Tras la escalada de violencia en mayo de 2023 en Gaza, cuando el personal tuvo que soportar un periodo intenso de ataques aéreos, una organización concedió dos días de bienestar a todo el personal que se encontraba allí. La mayoría del personal tenía muchos días de vacaciones para tomarse, pero la licencia por bienestar se concibió como un reconocimiento, y el personal se sintió motivado y valorado. La oficina permaneció abierta para el personal que prefirió estar con sus colegas como forma de afrontar la situación.

5.4.3 Consideraciones generales sobre la respuesta

Las buenas prácticas relativas a los enfoques de atención y seguimiento del personal tras un incidente abarcan una variedad de consideraciones prácticas.

Garantizar que el personal se sienta apoyado

Después de un incidente u otro acontecimiento estresante, es importante que el personal sienta que la organización comprende que su experiencia ha sido difícil y que tiene la intención de apoyarlo y garantizar que los próximos pasos sean lo más sencillo posible. Las organizaciones pueden lograr esto escuchando al personal afectado, atendiendo sus necesidades tras el incidente y brindando respuestas a sus preguntas iniciales, al tiempo que los conectan con los recursos necesarios. El personal puede necesitar tiempo para procesar los acontecimientos y las emociones relacionados con el incidente o la situación. Las organizaciones deben alentar a los involucrados a tomarse tiempo para descansar, practicar el autocuidado y conectarse con sus seres queridos. No es raro que el personal tenga necesidades inmediatas de salud física o mental después de un acontecimiento estresante. Una respuesta estructurada para apoyar la salud mental inmediatamente después de un incidente, que incorpore el apoyo entre pares y un liderazgo y una gestión compasivos, reducirá la probabilidad de que una persona necesite apoyo profesional para tratar el trauma más adelante.

Las consideraciones generales sobre el cuidado del personal durante o después de incidentes o acontecimientos altamente estresantes incluyen lo siguiente:

- **Mensajes de apoyo al personal.** Cuando el personal enfrenta adversidades, recibir mensajes de apoyo del equipo directivo (en su lengua materna) puede tener un gran impacto. El acercamiento personal por parte de los colegas también puede brindar consuelo. La comunicación puede realizarse por mensajes de texto, redes sociales, correo electrónico o teléfono y puede incluir la posibilidad de que el personal afectado responda a los mensajes y comparta sus experiencias.
- **Visitas al hospital.** Si un miembro del personal está hospitalizado lejos de su hogar, organizar la visita de otro miembro del personal o de una organización socia puede aliviar los sentimientos de aislamiento.
- **Paquetes de ayuda.** El personal, o los socios si la organización no puede acceder a ciertas zonas, puede entregar paquetes de provisiones personalizados para el personal afectado por incidentes o conflictos.
- **Equipo de recepción.** Contar con un equipo de recepción para dar la bienvenida al personal que llega a un lugar seguro puede marcar una diferencia significativa. Este equipo puede estar presente para ayudar al personal que se traslada tras una evacuación, un incidente crítico o una situación violenta.
- **Información posterior al incidente.** Proporcionar un resumen por escrito del apoyo, los recursos, el seguro, los beneficios y el asesoramiento jurídico disponibles para el personal afectado por un incidente. Esto puede ir acompañado de orientación personal por parte de un representante y una persona de contacto definida para preguntas de seguimiento.
- **Informe psicológico posterior al incidente.** El personal responsable puede programar una sesión informativa psicológica posterior al incidente con un psicólogo profesional autorizado u otra persona capacitada (ver abajo).

► *Para obtener más detalles sobre los informes posteriores a los incidentes, véase el capítulo 4.4.*

Durante la reubicación y la evacuación

Las organizaciones pueden tomar medidas para garantizar que el personal se sienta apoyado después de una reubicación o evacuación, por ejemplo, garantizando que se satisfagan sus necesidades inmediatas (suministros esenciales, atención médica y asistencia con la comunicación). Esto incluye apoyo continuo durante su estadía en un lugar seguro, como controles periódicos, ayuda con los preparativos para continuar su viaje y acceso a servicios médicos y psicosociales. El objetivo es garantizar que el personal se sienta seguro, apoyado y conectado durante todo el proceso de reubicación y evacuación.

Enfoque centrado en el superviviente

Ya sea que se trate de apoyar al personal involucrado en un accidente de tránsito grave, una agresión sexual, una reubicación tras una situación potencialmente mortal, un rapto u otro acontecimiento estresante, es aconsejable que las organizaciones adopten un enfoque centrado en el superviviente.

A continuación se exponen los conceptos clave de la atención centrada en el superviviente.

- **Respeto.** Respetar los deseos y las decisiones del superviviente, tratarlo con dignidad y comprender que sus reacciones pueden ser emocionales y diferir de las expectativas de los demás.
- **Confidencialidad.** Compartir información personal del superviviente solo cuando sea necesario y solicitar su consentimiento antes de revelar cualquier otro detalle.
- **Autonomía.** Reconocer el derecho del superviviente a tomar sus propias decisiones, considerando que la autonomía puede interpretarse de manera diferente en distintos contextos culturales. Brindar información clara sobre los procedimientos y los posibles resultados a fin de respaldar decisiones informadas.
- **Claridad y orientación.** El superviviente puede sentirse desorientado después del incidente y necesitar asesoramiento para comprender en qué aspectos puede necesitar ayuda y cómo acceder a ella.

También puede sentirse abrumado por la experiencia y por la expectativa de tener que tomar decisiones, por lo que es fundamental brindarle apoyo durante este proceso. Un enfoque centrado en el superviviente prioriza sus necesidades sin sobrecargarlo indebidamente con cuestiones relacionadas con el empleo, las acciones legales, los procedimientos relativos al seguro y la necesidad de transitar por mecanismos de apoyo internos y externos. Esto supone proporcionar una descripción clara y concisa de los beneficios y el apoyo disponibles y establecer una persona de contacto para todo el periodo de recuperación. En las primeras etapas, puede ser un miembro del equipo de gestión de incidentes o un acompañante de superviviente. A medio o largo plazo, este apoyo (por ejemplo, licencia de emergencia mientras no pueden trabajar, reincorporación al trabajo o cambios en la trayectoria profesional) puede delegarse a un supervisor, con el apoyo regular de un gerente de Recursos Humanos, un socio empresarial o un asesor jurídico.

El personal responsable debe reconocer que las preferencias de apoyo pueden variar. Para algunos, recibir apoyo puede significar tener a alguien con quien compartir sus experiencias. Otros pueden apreciar la oportunidad de mantenerse ocupados o concentrados en otras cosas. Algunos querrán tomar la iniciativa en todas las acciones y respuestas de seguimiento, mientras que otros pueden tener una capacidad o habilidad limitada para hacerlo y pueden necesitar más apoyo por parte de la organización. Se

puede contratar a un acompañante externo de supervivientes para apoyar al personal afectado.

Un enfoque centrado en el superviviente es distinto de un enfoque dirigido por el superviviente, ya que existe cierta supervisión para evitar decisiones que podrían suponer mayores riesgos. Un enfoque centrado en el superviviente, aunque respeta sus deseos siempre que sea posible, permite hacer excepciones cuando dichos deseos podrían ponerlo a él o a otras personas en riesgo de sufrir más daños.

5.4.4 Acciones de respuesta

Es común que los trabajadores humanitarios afectados por incidentes críticos experimenten una forma de “traición institucional” cuando su organización, a través de su acción o inacción, les causa más daño o incluso parece ponerse del lado de los agresores. Es fundamental garantizar que el personal se sienta cuidado y escuchado después de un incidente crítico.

Respuesta informada al trauma

Una respuesta informada al trauma implica comprender las consecuencias psicológicas y emocionales del trauma en las personas y garantizar que se prioriza su seguridad, bienestar y empoderamiento, como se detalla a continuación.

- **Seguridad:** garantizar la seguridad física y emocional del personal afectado.
- **Confianza:** mantener una comunicación clara y transparente para generar confianza.
- **Apoyo entre pares:** fomentar el apoyo entre colegas, familiares u otras personas que hayan compartido experiencias similares.
- **Colaboración y reciprocidad:** fomentar un sentimiento de alianza y colaboración en el proceso de recuperación, reconociendo que sanar implica un esfuerzo compartido.
- **Empoderamiento, voz y elección:** reconocer la capacidad de las personas para defenderse a sí mismas y garantizar que tengan la oportunidad de ser escuchadas.
- **Consideraciones culturales, históricas y de género:** reconocer que el perfil de riesgo de cada individuo será único y respetar las dimensiones culturales, históricas y de género que puedan afectar su recuperación.

- **Evitar la retraumatización:** ser consciente del lenguaje y de las acciones para evitar más daños.
- **Educación y concienciación:** educar al personal pertinente sobre los efectos del trauma en la salud y en el comportamiento de las personas afectadas y sobre la manera de brindar una respuesta adecuada.
- **Apoyo a los cuidadores:** proporcionar recursos y apoyo a los cuidadores, ya que corren un riesgo elevado de sufrir un trauma secundario.

► *Para obtener orientaciones generales sobre la respuesta a incidentes, véase el capítulo 4.4.*

► *Para obtener más información sobre las respuestas a incidentes de violencia sexual, véase el capítulo 7.7.*

► *Para obtener más información sobre las respuestas a los raptos, véase el capítulo 7.9.*

Consideraciones y acciones iniciales

Inmediatamente después de un incidente, una buena práctica es garantizar la seguridad física del miembro del personal trasladándolo a un entorno seguro y, si es necesario y apropiado, brindándole primeros auxilios (incluidos los primeros auxilios psicológicos) y acceso a atención médica profesional (servicios físicos y psicosociales). Esto debe ir seguido del desarrollo de un plan de seguridad personal específico.

Debido a que las consecuencias médicas y psicológicas del incidente pueden no ser inmediatamente evidentes, lo ideal sería que las opciones de apoyo permanezcan accesibles mucho tiempo después de ocurrido el incidente.

Primeros auxilios psicológicos y apoyo entre pares

El apoyo entre pares puede ser un mecanismo eficaz para ayudar al personal a atravesar periodos y eventos difíciles fomentando un sentimiento de comprensión compartida y ayuda mutua. Este enfoque permite al personal brindar apoyo emocional y práctico inmediato a colegas que se encuentran en una situación difícil. La creación de una red de apoyo puede ser especialmente valiosa en situaciones en las que el apoyo psicosocial profesional puede no estar disponible de inmediato. El apoyo entre pares no solo mejora la resiliencia, sino que también promueve una cultura de compasión y solidaridad dentro de la organización.

Las organizaciones deben asegurarse de que todo el personal de respuesta a incidentes, incluido el personal directivo superior y ejecutivo, faciliten el apoyo entre pares y un liderazgo compasivo. Todo el personal debe estar familiarizado con los principios de

primeros auxilios psicológicos (ver el cuadro más abajo), y todas las personas que probablemente interactúen con colegas durante y después de incidentes críticos deben recibir capacitación básica en primeros auxilios psicológicos.

Principios de los primeros auxilios psicológicos

A continuación se enumeran los tres principios fundamentales.

- **Observar:** buscar señales de angustia o alguien que pueda necesitar apoyo específico.
- **Escuchar:** acercarse a la persona que pueda necesitar apoyo y pedirle permiso para ayudarla; escucharla, intentar ayudarla a sentirse tranquila y ayudarla a priorizar las necesidades urgentes; respetar la confidencialidad y su autonomía.
- **Conectar:** brindar información práctica y ayudar a la persona a ponerse en contacto con los servicios de apoyo (dentro de la organización y con sus seres queridos, según corresponda).

Los primeros auxilios psicológicos se centran en abordar las necesidades inmediatas y en aliviar la angustia brindando apoyo compasivo, concebido para ayudar a las personas a afrontar el impacto emocional y psicológico de un evento traumático. No es un tratamiento para el trastorno del estrés postraumático ni para otras condiciones psicológicas. Se centra en brindar comodidad y tranquilidad, escuchar activamente las preocupaciones de las personas y ofrecer asistencia práctica para abordar las necesidades inmediatas, como encontrar un refugio seguro o atención médica. El objetivo de estos primeros auxilios es validar los sentimientos del individuo, ayudándolo a comprender que sus respuestas son típicas en las circunstancias dadas. Implica conectar a las personas con redes de apoyo, recursos adicionales y servicios de apoyo profesional según sea necesario.

Para ser eficaces, el personal de respuesta debe ser sensible a las consideraciones culturales, étnicas, religiosas, lingüísticas, de orientación sexual e identidad de género que pueden incidir en la experiencia del trauma de una persona y en sus necesidades de recuperación.

Otras formas de apoyo entre pares incluyen grupos de apoyo, tutoría, sistemas de camarada de apoyo y foros en línea para trabajadores humanitarios actuales y anteriores.

Plan de seguridad personal

Los planes de seguridad personal después de un incidente traumático establecen formas de mantenerse a salvo o de mitigar daños adicionales, adaptadas a las necesidades de seguridad física y psicológica específicas del superviviente. Los componentes de un plan de seguridad variarán según el incidente, el miembro del personal y la organización en cuestión. Sin embargo, en términos generales puede incluir lo siguiente:

- Medidas de seguridad inmediatas, como la reubicación en un lugar seguro y el establecimiento de medios de comunicación y contactos de emergencia.
- Medidas de protección física, como alojamiento seguro y otras formas de apoyo, incluida la presencia de un amigo o un colega de confianza.
- Diagnóstico de riesgos de la amenaza y cualquier vulnerabilidad actual del miembro del personal afectado.
- Medidas para mantenerse seguro en casa (p. ej., cerraduras, alarma de emergencia, código para abrir puertas).
- Medidas para mantenerse seguro en otros lugares, como en el trabajo y en público.
- Garantizar el acceso a documentos importantes como el pasaporte, el permiso de conducir, el documento de identidad y la tarjeta del cajero automático.
- Orientación sobre qué hacer si hay contacto con el agresor, si corresponde.
- Cómo afrontar los factores desencadenantes mentales y emocionales.
- Información de contacto en caso de emergencia.

A continuación, se puede poner en contacto al miembro del personal afectado con los recursos pertinentes, incluido el apoyo médico y psicosocial (interno y externo). A largo plazo, las organizaciones pueden considerar el desarrollo de un plan de apoyo con la persona afectada que le brinde claridad sobre los servicios de apoyos disponibles, los beneficios, el seguro y la atención a largo plazo.

Acciones a corto plazo

Una vez atendidas las necesidades inmediatas, puede ser conveniente realizar una evaluación más detallada de la seguridad del miembro del personal afectado, introducir modificaciones en sus tareas laborales, revisar las opciones de medidas legales y judiciales (como denunciar el incidente a la policía), informar el incidente utilizando los protocolos de la organización y realizar una sesión informativa psicológica. Es importante tener en cuenta también las necesidades de los cuidadores y de quienes brindan apoyo a la persona afectada.

Informe psicológico

Tras un incidente o acontecimiento, puede ser aconsejable organizar una sesión informativa psicológica: una discusión estructurada y guiada, concebida para ayudar a las personas a procesar lo ocurrido y comenzar a manejar sus respuestas emocionales. Por lo general, esto implica reunir a los afectados por el incidente para analizar lo sucedido y compartir sus reacciones y sentimientos, y organizar el apoyo de pares y profesionales de la salud mental. Los objetivos de la sesión informativa psicológica son los siguientes:

- ayudar a las personas a comprender el acontecimiento y sus reacciones;
- normalizar sus respuestas emocionales;
- proporcionar información sobre las reacciones al estrés y las estrategias de afrontamiento, e
- identificar a personas que puedan necesitar más apoyo.

La sesión suele ofrecerse entre 24 y 72 horas después del suceso, para que los participantes puedan expresar sus pensamientos y sentimientos iniciales mientras el acontecimiento aún está fresco en la memoria. Algunos expertos sugieren que la sesión informativa psicológica no debería ser obligatoria, ya que no todos se benefician de conversar sobre el incidente inmediatamente y para algunos podría agravar su angustia. Dicho esto, las creencias y la cultura estoica o firme que prevalece en el sector humanitario, junto con actitudes culturales específicas, a veces pueden hacer que el admitir la necesidad de apoyo psicosocial parezca una debilidad. Para abordar este problema, ofrecer una sesión informativa psicológica de carácter opcional tras un incidente, en lugar de obligatoria, puede aumentar significativamente la participación. Además, al personal le puede preocupar que reconocer lesiones psicológicas pueda afectar negativamente sus perspectivas laborales. Brindarle al personal la seguridad de que buscar apoyo no pondrá en peligro sus oportunidades laborales puede ayudar a abordar este problema.

Apoyar al acompañante de los supervivientes y a otras personas afectadas

La atención durante y después de los incidentes más críticos se centra en los supervivientes, pero el apoyo también debe extenderse más allá del miembro del personal inmediatamente afectado y puede incluir la asistencia a los testigos y al equipo en general. Aquellos que responden a un incidente (en cualquier nivel de la organización) pueden requerir apoyo específico. El estrés acumulativo y el trauma vicario son factores importantes que considerar, especialmente en el caso de quienes prestan apoyo en incidentes sucesivos.

A las personas que necesitan apoyo adicional se les puede ofrecer tiempo libre para recuperarse, acceso a apoyo psicosocial y asistencia para gestionar su carga de trabajo ajena al incidente. Otras intervenciones eficaces incluyen ofrecer acceso a recursos de

salud mental, como asesoramiento y grupos de apoyo, talleres de manejo del estrés y un entorno de trabajo de apoyo que le permita al personal hablar de sus preocupaciones abiertamente. Los controles periódicos y la creación de oportunidades para que el personal realice prácticas de *mindfulness* o técnicas de relajación pueden ayudar a manejar el estrés y a prevenir el agotamiento, lo que garantiza que todos los empleados estén preparados para afrontar las dificultades del lugar de trabajo y las presiones personales.

Atención posterior a largo plazo

A largo plazo, puede ser aconsejable seguir supervisando el bienestar del miembro del personal mediante controles regulares, adaptando el plan de seguridad según sea necesario y garantizando que tenga acceso a apoyo psicosocial y atención médica prolongados, incluida una terapia especializada en traumas si es necesario. Esto se puede documentar en un plan de apoyo detallado. En este punto, también puede ser útil brindar orientaciones más detalladas sobre las vías legales y judiciales, además de considerar las opciones para volver al trabajar.

Plan de apoyo general

Según la gravedad del incidente, el personal afectado puede requerir atención posterior a largo plazo. El personal responsable puede desarrollar un plan de apoyo integral con el miembro del personal afectado. Este debe ser flexible, centrarse en el superviviente e incorporar, por tanto, evaluaciones y tratamientos médicos y psicológicos, atención posterior al incidente, reintegración laboral y transición a servicios de largo plazo como los servicios nacionales de salud. El plan debe tener en cuenta los factores culturales y las vías de recuperación preferidas del miembro del personal afectado, que pueden incluir métodos de sanación tradicionales.

Las organizaciones deben indicar claramente el alcance, el costo y la duración del apoyo que pueden y están dispuestas a brindar tras un incidente, a fin de manejar las expectativas.

El apoyo a largo plazo a los supervivientes y al personal involucrado en incidentes graves puede requerir además lo siguiente:

- modificaciones en las obligaciones laborales;
- comunicación prudente sobre las ausencias;
- controles periódicos para abordar las inquietudes actuales;
- notificación a los proveedores de seguros, cuando sea apropiado y con consentimiento;
- ayuda financiera para las personas afectadas y el personal de apoyo (p. ej., los miembros del equipo de respuesta), y
- apoyo para lesiones de aparición tardía (p. ej., trastorno de estrés postraumático o lesiones cerebrales traumáticas).

Puede ser útil (y para algunas organizaciones esta es una política estándar) mantener la documentación de los informes médicos y de otra índole sobre el diagnóstico de lesiones para ayudar a orientar el apoyo a largo plazo.

Ejemplo: Errores en la atención posterior a un incidente

Tras un incidente crítico grave, un trabajador humanitario internacional tuvo que someterse a múltiples evaluaciones psicológicas y psiquiátricas y presentar ocho informes antes de que su empleador aceptara su diagnóstico de trastorno de estrés postraumático. Informes posteriores incluyeron diagnósticos de depresión. Además, tuvo que entregar 12 informes médicos antes de que la organización estuviera dispuesta a admitir que sus lesiones estaban relacionadas con una herida de bala sufrida durante el incidente. Este proceso no solo fue difícil para la persona, sino que también provocó que otros miembros del personal perdieran la confianza en la disposición de la organización a apoyarlos si resultaban heridos mientras trabajaban en contextos de alto riesgo.

Justicia y reparación legal

Cuando el personal que ha sufrido actos de violencia desea buscar justicia a través de mecanismos jurídicos formales, las organizaciones deben estar preparadas para brindar asesoramiento sobre las distintas opciones jurídicas, incluidas las implicaciones de denunciar a las autoridades locales y las definiciones legales del delito en ese contexto. También deben tener un conocimiento exhaustivo del entorno jurídico en el que operan, incluyendo a qué comisaría acudir en caso de incidente y los requisitos para denunciarlo (incluidos los plazos), y establecer relaciones con profesionales jurídicos locales de confianza que puedan proporcionar orientación previa y asistencia inmediata. Si un miembro del personal decide emprender acciones judiciales, una organización puede considerar en qué medida está preparada para brindar los siguientes tipos de apoyo (y cómo):

- Acompañar al personal afectado durante informes policiales, entrevistas y recolección de pruebas.
- Obtener una representación legal adecuada.
- Proporcionar información práctica sobre arrestos, procedimientos judiciales y posibles sanciones.

- Ofrecer apoyo psicosocial continuo para ayudar a afrontar el trauma de los procesos legales.
- Aclarar los procedimientos y los plazos y garantizar que el personal pueda tomar decisiones informadas sobre las acciones judiciales.
- Disponer de servicios jurídicos, médicos y psicológicos en caso de incidente, incluida la recolección de pruebas forenses.

Consideraciones cuando los presuntos agresores son miembros del personal

En los casos en que el presunto agresor es un miembro del personal (como en los casos de violencia sexual u otros daños infligidos a otro miembro del personal), una organización puede considerar las acciones que se mencionan a continuación.

- **Deber de cuidado:** definir y proporcionar apoyo jurídico, médico y psicosocial al presunto agresor, y determinar cuándo debe concluir este apoyo.
- **Investigación interna:** iniciar una investigación interna para reunir información a fin de determinar los hechos, garantizando la sensibilidad y la neutralidad, y con la participación de investigadores capacitados e independientes.
- **Procedimientos judiciales:** estar preparado para apoyar al personal durante los procedimientos judiciales y considerar las consecuencias de involucrar a las autoridades locales; estas son consideraciones especialmente importantes en contextos con castigos severos y malas condiciones de encarcelamiento.

► Véase el capítulo 7.7 para consultar más ejemplos y consideraciones en caso de un incidente de violencia sexual, así como un análisis más detallado de las investigaciones internas.

Regreso al trabajo

Regresar al trabajo después de un incidente grave puede ser difícil. Es importante reconocer que la reintegración es un proceso único para cada individuo y puede llevar mucho tiempo. La fecha de regreso al trabajo debe ser flexible, puesto que algunas personas pueden desear reanudar sus funciones inmediatamente, mientras que otras pueden necesitar más tiempo. Este proceso debe gestionarse con compasión, y quizás sea posible ofrecer puestos alternativos o analizar opciones de jubilación si la persona decide no regresar. Las organizaciones deben asegurarse de que otros miembros del personal sepan cómo apoyar a los colegas que se reincorporan y, al mismo tiempo,

brindarles apoyo ante cualquier impacto emocional que el incidente pueda haber tenido en ellos.

5.4.5 Seguros y beneficios

Descripción general de los seguros

Las organizaciones necesitan estar preparadas para cubrir los costos financieros de responder a los incidentes que afecten a su personal. Para ello, la mayoría de las organizaciones contratan pólizas de seguro que cubren una amplia variedad de riesgos. Sin embargo, algunas organizaciones han optado por esquemas de autoseguro a través de los cuales la organización asume el riesgo financiero asociado con ciertos acontecimientos, como las prestaciones sanitarias para los empleados, la indemnización por accidentes laborales o los daños a la propiedad, y utiliza sus propios recursos para pagar las reclamaciones.

Es importante recordar que la cobertura del seguro proporciona compensación, no protección. No evitará enfermedades ni lesiones, pero puede ayudar a mitigar las consecuencias financieras de un incidente. Asimismo, el seguro cubrirá únicamente las pérdidas incluidas en los términos y condiciones específicos de la aseguradora. En última instancia, lo que las compañías de seguros proporcionan es un nivel de protección económica, que mitiga las consecuencias de acontecimientos negativos al transferir el riesgo de una gran pérdida económica a la compañía de seguros, a cambio de una prima.

Los accidentes e incidentes de seguridad pueden tener importantes consecuencias financieras para el personal afectado, sus familias y la organización. Existen costos inmediatos, como la evacuación médica y los tratamientos de emergencia, que pueden ascender rápidamente a sumas de dinero muy cuantiosas. También existen posibles costos a largo plazo, como los que se derivan de la discapacidad permanente (por ejemplo, después de la pérdida de extremidades) y las necesidades de atención a largo plazo. Algunas pólizas de seguro prevén un especialista en gestión de riesgos para apoyar la respuesta, además de cubrir los costos de incidentes como una detención ilegal, una evacuación debido a la inseguridad y un rapto.

Es parte del deber de cuidado de una organización brindar una compensación financiera al personal afectado en caso de lesión, enfermedad, muerte o durante otros acontecimientos de la vida. Dado que la mayoría de las organizaciones no pueden cubrir estos costos por sí mismas, la cobertura de seguro constituye un medio para proporcionar esa compensación. Para las organizaciones internacionales, esta responsabilidad también se aplica al personal nacional. Por tanto, el hecho de que la cobertura de seguros de algunas organizaciones internacionales no cubra a todos los miembros de su personal se convierte en un grave problema operacional y ético. El seguro es una herramienta que puede ayudar a cumplir con la responsabilidad del empleador, pero normalmente no debe representar la totalidad del apoyo que una organización brinda al personal afectado.

Se debe informar a los trabajadores humanitarios sobre los detalles de la cobertura de seguro que ofrece su organización (con posibles excepciones para pólizas de contingencia especiales, como, por ejemplo, cobertura de secuestro y rescate). El personal tiene derecho a preguntar sobre la cobertura de seguro que se le proporciona y a solicitar más información. Si bien las lesiones y las afecciones psicológicas pueden incluirse en la indemnización médica y por accidentes laborales, no es un proceso automático. Es posible que la organización tenga que asegurarse de que estos aspectos están incluidos, en lugar de simplemente asumir que lo están, sobre todo si los documentos de la organización especifican el apoyo a la salud mental.⁸⁵

Ejemplo: Evaluación del acceso y la elegibilidad

Una organización ha determinado el acceso y la elegibilidad para la asistencia médica y la evacuación. Además de brindar transparencia al personal sobre la cobertura, esta descripción permite a la organización identificar carencias y superposiciones en los seguros y mejorar la equidad.

La organización identificó primero los grupos beneficiarios:

- Personal del programa de país.
- Personal internacional.
- Personal de la oficina central.
- Teletrabajadores.
- Viajeros que no son miembros del personal (p.ej., miembros de la junta).

Para cada grupo, la descripción enumera detalles sobre el acceso a un proveedor de asistencia médica y la cobertura de seguro aplicable:

- Acceso a un proveedor de asistencia médica
 - ¿Quién?
 - ¿Cuándo?
 - ¿Información, asesoramiento y derivación? Sí/No.
 - ¿Atención médica rutinaria/electiva?
 - ¿Asistencia médica en caso de accidente o enfermedad? (p.ej. Sí/Sí [mientras viaja internacionalmente por asuntos oficiales]).
 - Evacuación médica en caso de accidente o enfermedad (p.ej., Sí/Sí [mientras viaja internacionalmente por asuntos oficiales]).
 - ¿Qué cubre la organización? (Detalles sobre el apoyo brindado sin costo y el apoyo por el cual se incurrirá en costos).

85 Reilly, L. (2024) "Is your mental health covered? Insurance for psychological injury", Bond (www.bond.org.uk/news/2024/05/is-your-mental-health-covered-insurance-for-psychological-injury/).

- Cobertura de seguro vigente
 - Información general (sobre asistencia para realizar pagos y presentar reclamaciones de seguros).
 - Atención médica rutinaria/electiva en el país (p. ej., cobertura médica local, cobertura de seguro de salud internacional, ninguna proporcionada por la organización).
 - Atención médica de rutina/electiva fuera del país (según lo mencionado anteriormente).
 - Atención médica en caso de accidente o enfermedad durante un viaje internacional por asuntos oficiales (p. ej., seguro de accidentes en viajes de negocios, seguro médico internacional).
 - Evacuación médica en caso de accidente o enfermedad durante un viaje internacional por asuntos oficiales (como se indica más arriba).

Deficiencias y carencia de un seguro de salud nacional

Proporcionar un apoyo adecuado a los trabajadores humanitarios nacionales implica no solo el acceso y la elegibilidad para la asistencia médica, sino también beneficios más amplios, como la cobertura y el acceso al apoyo psicosocial, el seguro de vida, los beneficios por discapacidad, la indemnización por accidentes laborales, las capacitaciones pagas y las asignaciones por educación/desarrollo. Sin embargo, la asistencia para la evacuación de los trabajadores humanitarios nacionales sigue siendo un desafío, ya que puede implicar muchas más negociaciones con los proveedores de servicios de evacuación y requiere visas y otras aprobaciones administrativas además de los costos financieros del seguro. En algunos casos, los planes de seguro locales no están disponibles o son inasequibles. Algunas compañías internacionales pueden ofrecer cobertura a los ciudadanos nacionales, aunque esto depende del país y del proveedor de seguros.

Puesto que no tener ningún seguro no es una opción, las organizaciones pueden tomar las siguientes medidas:

- Optar por un esquema de autoseguro, si es posible, en el que la organización reserve fondos para cubrir posibles riesgos y reclamaciones en lugar de comprar un seguro de un proveedor externo.
- Negociar ampliaciones de pólizas de seguros (globales).
- Proporcionar una suma fija para la cobertura médica.

- Apoyar las solicitudes de indemnización o ayuda económica en caso de enfermedad, lesión o fallecimiento caso por caso.
- Desarrollar un sistema interno de seguro cooperativo con un fondo de seguro creado con una suma fija proveniente de la organización, más las contribuciones de los empleados participantes.
- Proporcionar asistencia médica gratuita a todo el personal como una prestación laboral (como suele ocurrir en las organizaciones de socorro médico).

Es probable que, en países propensos a sufrir peligros naturales, la cobertura del seguro médico nacional no funcione en momentos de crisis y tal vez sea necesario considerar métodos alternativos.

► *Para consultar más información relativa a las emergencias médicas, véase el capítulo 5.5.*

Pólizas de seguro comunes

Diferentes organizaciones necesitarán diferentes seguros. El seguro debe considerarse un componente de una estrategia de mitigación y, como todo lo demás, requiere una apreciación completa de los riesgos detectados en una evaluación integral. La mayoría de las organizaciones tienen pólizas de seguro con los siguientes tipos de cobertura (la lista a continuación no es exhaustiva).

- Seguro médico estándar.
- Seguro contra accidentes estándar: incluye muertes por accidente o desmembramiento.
- Seguro de discapacidad parcial o total de largo o corto plazo.
- Seguro de emergencia médica: incluye la cobertura de evacuaciones médicas y atención de emergencia en el lugar y durante los traslados.
- Seguro de riesgo de guerra: suele ser una póliza independiente o un complemento con un coste adicional que cubre lesiones o muertes causadas por “actos de guerra o terrorismo” (véase más información en el apartado “Cláusulas de exclusión” más adelante).
- Seguro de riesgos especiales: incluye conocimientos técnicos para la gestión de crisis y contingencias para facilitar la liberación segura de rehenes.
- Seguro de responsabilidad civil general/comercial: se trata de una de las pólizas de seguro más generales que protege contra los costos de reclamaciones de terceros por lesiones corporales o daños causados a la propiedad y, por ejemplo, casos de resbalones y caídas en las instalaciones de la organización.
- Seguro de responsabilidad civil de vehículos y seguro de flotas/vehículos: pólizas que cubren responsabilidades legales y financieras, como responsabilidad civil, colisión y cobertura global, además de proteger contra un conjunto más amplio de riesgos, incluidos los daños a los vehículos.

- Seguro de accidentes laborales: brinda prestaciones médicas y complementos salariales para los empleados lesionados en el trabajo. El seguro de accidentes laborales para extranjeros extiende la cobertura para los empleados que trabajan en el extranjero, incluidos los riesgos adicionales y la repatriación. Los esquemas locales garantizan el cumplimiento de las normativas locales en materia de seguros y proporcionan las protecciones necesarias a los trabajadores en países específicos.
- Seguro de responsabilidad profesional: cubre a las empresas contra reclamaciones por negligencia, errores u omisiones en los servicios o asesoramiento que brindan.
- Seguro de directores y empleados: protege a los directores y a los empleados de pérdidas financieras personales, costos legales e investigaciones regulatorias.
- Seguro de responsabilidad civil por prácticas laborales: cubre a los empleadores contra reclamaciones relacionadas con discriminación en el lugar de trabajo, acoso, despido injustificado e incumplimiento de los contratos de trabajo.
- Seguro contra delitos y deshonestidad laboral: protege a las empresas de pérdidas financieras derivadas de hurtos, fraudes o malversación de fondos por parte de empleados o terceros.
- Seguro cibernético: brinda cobertura ante pérdidas financieras causadas por violaciones de la seguridad de los datos, ciberataques y otros incidentes relacionados con la ciberseguridad.
- Seguro de propiedad: cubre daños o pérdida de activos físicos como edificios y equipos debido a incendios, hurtos u otros riesgos.
- Seguro contra la violencia política y el terrorismo: asegura contra pérdidas causadas por actos violentos motivados políticamente, como guerras, disturbios y actos de terrorismo.

Cláusulas de exclusión

Es fundamental que las organizaciones lean la letra pequeña y pregunten explícitamente qué está y qué no está cubierto, para así conocer con claridad el alcance de las omisiones en la cobertura del seguro que tendrían que cubrir ellas mismas. Las pólizas de seguro pueden no aplicarse en determinadas condiciones, y los detalles y la interpretación de estas cláusulas de exclusión pueden ser de suma importancia. Las organizaciones pueden encontrarse con un seguro insuficiente y verse obligadas a cubrir costos inesperados por su cuenta.

La cobertura del seguro puede excluir riesgos de guerra evidentes (ciertos tipos de riesgos de guerra o actos maliciosos, en particular, actos de terrorismo como un atentado con bomba en un lugar público), a menos que la organización tenga una cláusula de riesgo de guerra como complemento a su póliza de seguro o como un acuerdo separado. Incluso con una cláusula de riesgo de guerra, las compañías de seguros pueden excluir zonas de guerra específicas de la cobertura. Algunas de estas zonas están predeterminadas por el proveedor de seguros. Las aseguradoras también

pueden agregar ciertos países a la cláusula de exclusión, ya sea al momento de la renovación del contrato o incluso durante la vigencia del contrato, proporcionando una notificación por escrito (los detalles de esto estarán en el contrato y la mayoría de los agentes pueden ayudar a las organizaciones con el lenguaje específico del contrato).

El seguro en un país incluido en una cláusula de exclusión puede no cubrir lesiones, enfermedades, muerte o discapacidad como resultado directo de un acto de guerra o terrorismo. Esto significa que la muerte de un miembro del personal debido a un vehículo impactado por un dron armado no está asegurada, pero sí lo está la muerte de un miembro del personal debido a un accidente de tráfico. Las primas para añadir países a la cláusula de exclusión del seguro (“comprar otra vez este seguro”) pueden ser muy elevadas. Si la organización desea no obstante contratar personal en ese país, podría optar por autosegurarse, por ejemplo, comprometiéndose a indemnizar al personal que trabaje o viaje a ese país por el importe que la compañía de seguros cubriría si el país no estuviera excluido de la cobertura.

Otros ejemplos de exclusiones:

- La cobertura se aplica únicamente durante las asignaciones laborales (p. ej., en Somalia, pero no durante un periodo de descanso y relajación en Nairobi).
- La cobertura se aplica únicamente durante el horario laboral (p. ej., hasta las 18h pero no más tarde ni durante los fines de semana).
- La cobertura se aplica solo si la organización tiene ciertas cláusulas de seguridad por escrito, como el principio de no pagar rescates.
- La cobertura excluye al personal con contratos de corto plazo, al personal de determinados países o a los voluntarios.

También es importante identificar lo que puede considerarse una condición preexistente y, por lo tanto, no cubierta, por ejemplo, afecciones de salud mental o física. Una organización debe analizar su proceso de selección y diligencia debida con su agente/proveedor de seguros.

Consideraciones sobre seguros

- **Educar al personal.** El personal debe comprender el alcance de la cobertura de accidentes y de los seguros mientras trabaja y viaja para la organización, y el impacto potencial en cualquier seguro personal que pueda tener (p. ej., las pólizas de seguro de vida, como las adquiridas con una hipoteca, que se vuelven inválidas si se trabaja en un área de alto riesgo).
- **Cobertura al comienzo y al final del contrato de trabajo.** Las organizaciones deben saber con precisión cuándo comienza y termina la cobertura. Es importante determinar si el miembro del personal está cubierto si aún no recibe un salario o aún no ha comenzado su asignación, por ejemplo. También debe quedar claro tanto para la organización como para el individuo en qué momento, una vez finalizada la

asignación, cesa la cobertura. Esto es importante en el caso del daño psicológico, que puede manifestarse mucho tiempo después de un incidente.

- **Primas de seguro.** Las organizaciones a menudo pueden negociar primas más bajas con su agente si pueden demostrar que existen medidas adecuadas de mitigación de riesgos (p. ej., políticas, procedimientos y capacitación en seguridad). Algunos proveedores ofrecen un crédito que puede utilizarse para mejorar las medidas de gestión de riesgos de seguridad.
- **Equidad en la cobertura.** Al analizar las políticas de seguros en las organizaciones internacionales, es fundamental abordar las posibles disparidades y problemas que pueden surgir entre el personal nacional e internacional. Estas disparidades a menudo se manifiestan en el acceso a la asistencia médica y a los servicios de emergencia, como las evacuaciones médicas, y en la calidad de los servicios de salud internacionales en comparación con los nacionales.

Más información

Análisis

Barkwill, D. (2022). *Letter of recommendation: reversing the mental health pandemic amongst aid workers*. AidEx (<https://gisf.ngo/resource/letter-of-recommendation-reversing-the-mental-health-pandemic-amongst-aid-workers/>).

Reilly, L. (2024). Is your mental health covered? Insurance for psychological injury. Bond (www.bond.org.uk/news/2024/05/is-your-mental-health-covered-insurance-for-psychological-injury/).

Orientación

Foro Europeo Interinstitucional para la Seguridad. (2017). *Abduction and kidnap risk management* (<https://gisf.ngo/resource/abduction-and-kidnap-risk-management-guide/>).

Foro Europeo Interinstitucional para la Seguridad. (2019). *Gestión de la violencia sexual contra el personal humanitario: prevención, preparación, respuesta y atención posterior* (<https://gisf.ngo/resource/managing-sexual-violence-against-aid-workers/>).

Linnell, H. (2017). *Guide to selecting appropriate crisis management insurance*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/guide-to-selecting-appropriate-crisis-management-insurance).

Organización Mundial de la Salud, War Trauma Foundation y World Vision International. (2011). *Primera ayuda psicológica: guía para trabajadores de campo*. Organización Mundial de la Salud (www.who.int/publications/i/item/9789241548205).

5.5 Consideraciones médicas y de salud

Dado que los incidentes de seguridad suelen causar daños físicos al personal, la gestión de riesgos de seguridad implica necesariamente atender consideraciones médicas de emergencia, especialmente cuando se trabaja en entornos inestables o de conflicto activo. Incluso aunque no haya violencia, los problemas de salud son inevitables y van desde la exposición a enfermedades y el empeoramiento de enfermedades crónicas hasta lesiones potencialmente mortales, por lo que se requieren mecanismos claros de prevención, preparación y respuesta. En este capítulo se describen los elementos esenciales necesarios para gestionar los riesgos e incidentes médicos, incluyendo la preparación, los primeros auxilios, la respuesta de emergencia y el traslado sanitario. Las orientaciones pueden ayudar a las organizaciones a identificar las medidas necesarias para responder mejor a los problemas médicos. Sin embargo, este capítulo no es exhaustivo y se recomienda a las organizaciones consultar a los proveedores médicos para desarrollar políticas y protocolos más apropiados para su personal y contextos específicos.

5.5.1 Prevención y mitigación de riesgos

Muchos de los problemas médicos que enfrentan las organizaciones son evitables. De manera similar, la capacidad de responder eficazmente a problemas médicos y de salud a menudo depende de consideraciones no médicas, incluidas las evaluaciones de salud previas a la partida, una sólida seguridad del personal y la creación de marcos detallados para el equipo directivo sobre cómo manejar incidentes médicos.

Una respuesta rápida y apropiada a las emergencias sanitarias requiere una buena comprensión de los riesgos médicos y de salud que afectan al personal y del panorama de la atención sanitaria circundante. Esto implica incluir los riesgos médicos y de salud relevantes en los ejercicios de diagnóstico de riesgos y mapear los recursos de asistencia médica disponibles para ayudar a gestionar las emergencias médicas.

Una nota sobre salud y seguridad ocupacional

La salud y la seguridad ocupacionales se refieren a las medidas, las prácticas y las políticas dirigidas a proteger la salud, el bienestar y la seguridad de las personas en el lugar de trabajo así como del público en general. Incluye la promoción y el mantenimiento del bienestar físico y mental de los trabajadores, la prevención de enfermedades y lesiones relacionadas con el trabajo y la inspección periódica de los lugares de trabajo para detectar posibles peligros.

La salud y la seguridad ocupacionales suelen estar codificadas en la legislación gubernamental, abarcando muchas medidas diferentes que están más allá del alcance de este documento. Sin embargo, en este capítulo se analizan en profundidad algunas consideraciones sanitarias muy relevantes para la gestión de riesgos de seguridad, con especial atención a las buenas prácticas en la preparación y en la respuesta a emergencias médicas. Para obtener orientaciones más detalladas, consulte recursos específicos de salud y seguridad ocupacionales, como la norma *ISO 45001:2018 de la Organización Internacional de Normalización: Sistemas de gestión de seguridad y salud ocupacionales* (www.iso.org/iso-45001-occupational-health-and-safety.html).

Evaluación de los riesgos y de las capacidades de salud locales

Antes de iniciar las actividades del programa deben considerarse algunas cuestiones como las condiciones y las tendencias generales de salud en la zona de operaciones y los principales riesgos que pueden dar lugar a emergencias médicas. A continuación se enumeran algunas de las más comunes:

- enfermedades infecciosas (p.ej., hepatitis, malaria, cólera);
- lesiones causadas por conflictos armados (p.ej., heridas de bala y lesiones causadas por minas terrestres y ataques aéreos);
- lesiones por agresiones (p.ej., apuñalamiento, golpiza);
- lesiones por accidentes de tráfico;
- enfermedades no transmisibles o afecciones crónicas de salud entre el personal, como diabetes o hipertensión, y
- problemas de salud mental.

Los riesgos aumentarán si hay poco o ningún acceso a servicios de salud en la zona, por lo que las evaluaciones deben incluir un mapeo de los recursos médicos disponibles (p.ej., hospitales, ambulancias, proveedores de salud y medicamentos o suministros médicos) y una evaluación de su capacidad para apoyar la respuesta a incidentes y cualquier necesidad específica del personal. Estas evaluaciones también deben incluir un acceso rápido a centros de crisis por violación y otras instalaciones que ofrezcan atención especializada y profilaxis postexposición contra el VIH para supervivientes de agresiones sexuales.

► Para obtener más información sobre los riesgos de violencia sexual, véase el capítulo 7.7.

Como mínimo, las organizaciones deben tener los datos de contacto de emergencia de proveedores locales confiables, así como la ubicación de los centros de atención médica más cercanos. También es importante identificar a los proveedores que están disponibles todos los días de la semana, tanto para la atención física como psicológica. Para la asistencia de salud mental, las organizaciones pueden considerar servicios disponibles tanto localmente como remotos.

► *Para obtener más información sobre los riesgos y el apoyo para la salud mental, véase el capítulo 5.4.*

Vale la pena señalar que el proveedor de salud más cercano o más confiable puede ser una ONG médica. Es aconsejable que el personal directivo establezca relaciones con proveedores de servicios de salud clave. De esta manera se podrá agilizar la prestación de los servicios y mejorar la calidad de la atención en situaciones de emergencia.

Autorización médica

Si la organización asigna personal (y cualquier dependiente acompañante) a un lugar lejos de su hogar, tiene la responsabilidad de garantizar que sus necesidades de salud puedan ser satisfechas allí. Un proceso de autorización médica evalúa la aptitud para el puesto (es decir, una evaluación de salud ocupacional) y la aptitud para llevar a cabo la nueva asignación (es decir, las necesidades de salud existentes se pueden satisfacer en el país de la asignación). Las normas sobre qué es y qué no es aceptable preguntar a los empleados varían según las distintas jurisdicciones, y las organizaciones también deben ser claras respecto a cómo se utilizará esta información y quién la utilizará. El examen puede incluir una revisión centrada en el historial médico del individuo (salud física y mental), los planes de tratamiento actuales, los medicamentos y los factores de riesgo de enfermedades o lesiones graves. Se pueden iniciar nuevas autorizaciones antes de nuevas asignaciones o después de cambios significativos en el estado de salud de un miembro del personal o en las condiciones de riesgo del lugar. También se puede alentar al personal a actualizar su autorización médica ante cualquier cambio en su estado de salud o posibles necesidades durante la asignación. Esta evaluación deberá ser realizada por profesionales cualificados y deberá ser tratada de forma confidencial (ver abajo).

Si el historial médico de un miembro del personal requiere un plan de mitigación de riesgos, su médico puede trabajar con él para concebir un plan apropiado y factible para proponer a la organización. Como parte del proceso, se debe informar al personal sobre cualquier posible obstáculo al acceso a la asistencia médica durante el trabajo, incluida la posibilidad de una atención demorada o rudimentaria. Se puede compartir un plan general de manera confidencial con el equipo directivo del país (según la *necesidad de saber*) para garantizar que se pueda implementar sin cargas ni dificultades indebidas. A continuación se citan algunos ejemplos:

- Un miembro del personal necesita un medicamento que no está disponible en el lugar. Sin embargo, su proveedor de atención primaria de salud acepta recetarle la cantidad suficiente para un año a fin de que pueda tomarlo mientras esté en el lugar.
- El hijo de un miembro del personal, que tiene una alergia grave al maní, acompañará a la familia a un puesto internacional. La familia está capacitada en el uso de un autoinyector de epinefrina y se compromete a viajar siempre con dos. Se instruye a la familia sobre la dieta local y cómo evitar la exposición accidental al maní.

Al igual que con otros protocolos de seguridad, el personal debe tener claro que se espera que cumpla con todos los consejos médicos y de salud mientras esté asignado a una misión, incluidas, por ejemplo, las políticas que exigen la vacunación o la toma de medicamentos contra la malaria.

Es importante garantizar que toda la información médica se entregue en un documento confidencial que la organización mantendrá seguro, se ingrese directamente en un portal en línea seguro (de la organización o de un proveedor de servicios externo) o se envíe por correo electrónico cifrado con archivos protegidos con contraseña.

Confidencialidad médica

Es aconsejable que cada organización establezca pautas y expectativas en torno a la confidencialidad médica, incluyendo si pueden existir diferentes protocolos según el entorno y el acceso a los proveedores médicos. El personal debe estar informado de estas medidas y tener claridad sobre quién tiene acceso a su información médica y las circunstancias en las que esta puede divulgarse a otros.

La información médica personal debe permanecer estrictamente confidencial, excepto en circunstancias excepcionales predefinidas. Se recomienda brindar instrucciones al personal pertinente sobre la confidencialidad médica y la privacidad de datos. Nadie más debe tener acceso a la información de salud de un miembro del personal sin su consentimiento explícito.

El personal responsable de áreas como salud y seguridad puede necesitar ocasionalmente solicitar información médica adicional para respaldar la toma de decisiones. En caso de emergencia médica, el personal de apoyo puede extender la confidencialidad médica al personal directivo de la organización de forma limitada y en función de la necesidad de saber.

Capacidades y prácticas permanentes

En función de los riesgos evaluados, las medidas de mitigación pueden requerir el desarrollo o el fortalecimiento de la capacidad de la organización para responder a emergencias médicas y la elaboración de los componentes médicos de los planes de respuesta a crisis y de gestión de incidentes.

Si los riesgos médicos y de salud son elevados y la disponibilidad de los recursos sanitarios externos es baja, las organizaciones deben considerar si tienen las capacidades básicas para cuidar a su personal en caso de que ocurra un incidente. No tener tales capacidades sería un incumplimiento del deber de cuidado.

Las capacidades sanitarias y médicas pueden incluir lo siguiente:

- **Medidas preventivas.** Reducir el riesgo médico en primer lugar, por ejemplo, mediante protocolos de seguridad sólidos y coordinando con los equipos de logística y suministros para garantizar el acceso continuo a los suministros necesarios.
- **Protocolos y procedimientos.** Crear y reevaluar periódicamente los protocolos para responder a incidentes médicos, incluidos los protocolos y las responsabilidades específicos de notificación (p. ej., evacuaciones médicas, incluido el transporte y la coordinación con los servicios de evacuación locales e internacionales).
- **Capacidades de primeros auxilios.** Brindar capacitación en primeros auxilios (incluida la reanimación cardiopulmonar y cualquier necesidad específica para entornos remotos), kits (en todas las oficinas, incluidos los espacios de oficina compartidos), sitios de proyectos, (almacenes, alojamientos y vehículos) y orientación (identificar un referente de salud que sea responsable del mantenimiento de los kits y de su evaluación periódica para verificar que no falten suministros y las fechas de vencimiento).
- **Suministros médicos de emergencia y logística.** Considerar qué otros suministros médicos de emergencia se necesitan, como los kits profilaxis postexposición contra el VIH, y cómo obtenerlos o acceder a ellos (ya sea almacenándolos directamente o accediendo a ellos a través de otra entidad) y asegurar un reabastecimiento oportuno.
- **Educación sanitaria.** Brindar educación sanitaria, como seminarios web o reuniones informativas para el personal sobre brotes de enfermedades, y elaborar un plan de educación sanitaria continua sobre los riesgos detectados. Esto debe incluir los riesgos para la salud mental.
- **Prestaciones de salud.** Evaluar y optimizar las prestaciones de salud física y mental brindadas a todo el personal, para satisfacer las necesidades del personal y mejorar la equidad (en particular en el caso de los trabajadores humanitarios nacionales).
- **Asistencia médica externa.** Identificar y contratar proveedores externos de asistencia médica para proporcionar información, asesoramiento y derivaciones sobre salud física y mental, y concertar con un proveedor o clínica la atención

rutinaria o electiva, el transporte médico urgente o de emergencia y el acceso a la asistencia sanitaria (véase la sección 5.5.2 más abajo para obtener más información). Establecer y mantener relaciones con proveedores e instalaciones locales de asistencia médica para obtener apoyo y derivaciones.

- **Telesalud.** Implementar soluciones de telesalud, cuando sea apropiado y posible, para brindar consultas remotas con profesionales médicos, especialmente en zonas con acceso limitado a instalaciones de asistencia médica.

Lista de verificación de salud en el lugar de trabajo

A continuación se presentan algunos elementos clave que las organizaciones pueden implementar para proteger la salud de su personal:

- Fomentar exámenes médicos individuales periódicos/anuales.
- Botiquines de primeros auxilios en todas las oficinas, residencias y vehículos.
- Capacitación en primeros auxilios para el personal.
- Apoyo para acceder a medicamentos y medidas de contingencia en caso de pérdida.
- Autorizaciones médicas para despliegues de personal y viajes.
- Planes de mitigación de riesgos médicos para el personal con mayores riesgos de salud.
- Seminarios web sobre riesgos relevantes y de duración limitada, como brotes de enfermedades.
- Orientaciones sobre confidencialidad médica, privacidad de los datos y capacitación sobre el manejo de información personal.
- Contactos de emergencia (para el personal y sus familias).
- Controles de salud ocupacional en las oficinas en la organización o en el domicilio.
- Asesoramiento ergonómico experto sobre el equipamiento de la oficina.
- Un plan de accesibilidad e inclusión de la discapacidad.
- Adaptaciones para la inclusión y la accesibilidad en las oficinas y en otros espacios de la organización (accesibilidad física y tecnológica).
- Acceso a telesalud.
- Acceso a servicios de salud mental en general, así como asistencia especializada tras un incidente.
- Planes de seguridad, que incluyan los riesgos para la salud y su mitigación.

- Informes de salud escritos u orales previos a la partida e informes de salud específicos del lugar (internos o gestionados a través de un proveedor de asistencia médica externo).
- Un conjunto de recursos para el personal (en los idiomas pertinentes), que incluya el acceso a aplicaciones de primeros auxilios, orientación escrita y datos de contacto, y que contenga instrucciones claras sobre cómo acceder al apoyo en caso de emergencia.
- Cobertura de seguro a través de un proveedor comercial u otro tipo de acuerdo en caso de que se produzca un incidente.

Cuanto mayor sea el riesgo de una emergencia médica (p.ej., en entornos de conflicto activo o cuando se responde a brotes de enfermedades), más debe hacer una organización para apoyar y capacitar al personal, estar preparada para incidentes y contar con medidas de respuesta apropiadas y oportunas.

Ejemplo de buenas prácticas: Integración de la salud en situaciones de seguridad

Tras el inicio de los enfrentamientos violentos en Sudán en abril de 2023, que provocaron el colapso del sistema de salud en Jartum, una organización organizó consultas de telesalud para el personal. Esto incluyó asesoramiento por telesalud para la esposa embarazada de un miembro del personal antes y durante el parto, la identificación de farmacias con insulina disponible y la organización de la entrega a un miembro del personal con diabetes.

5.5.2 Preparación

Preparación para emergencias médicas

Para garantizar respuestas oportunas y apropiadas a emergencias médicas y evacuaciones, es fundamental centrarse en la preparación médica antes de que ocurran los incidentes. Igualmente importante es alentar al personal a informar sobre enfermedades o lesiones lo antes posible. Por ejemplo, para una organización es preferible que un miembro del personal informe de un dolor abdominal intenso en el momento en que se produce en lugar de enfrentar una situación en la que esta

persona se desmaya a causa de la ruptura del apéndice durante un traslado. A menudo es posible prevenir peores resultados si el personal informa a tiempo y busca ayuda. Al garantizar el respeto de la confidencialidad médica, las organizaciones pueden ayudar a mejorar las notificaciones, ya que el personal probablemente tendrá más confianza en el responsable médico designado.

En algunas circunstancias, los problemas médicos pueden abordarse con el apoyo de un proveedor externo de asistencia médica. Un proveedor de asistencia no es una compañía de seguros, aunque algunas compañías de seguros pueden proporcionar (alguna) asistencia médica y apoyo para las evacuaciones como parte de su paquete. Los proveedores pueden ser pagados por la compañía de seguros (si el proveedor de asistencia tiene un acuerdo de facturación directa con ella), por la organización (a través de una garantía de pago) o por el miembro del personal.

En el caso de que el personal se lastime o se enferme durante su trabajo, debe haber una forma de cubrir los costos conexos. Esto puede hacerse a través de las pólizas de seguro pertinentes. Sin embargo, esto puede resultar difícil para organizaciones locales más pequeñas que operan con presupuestos ajustados y en lugares con un mercado de seguros comerciales limitado (o nulo). En tales casos, las organizaciones podrían recurrir a esquemas de autoseguro o al apoyo de donantes y socios.

► *Para obtener más información sobre los seguros, véase el capítulo 5.4.*

Algunos servicios de apoyo que pueden proporcionar los proveedores de seguridad y asistencia médica son los siguientes:

- acceso todos los días de la semana al centro de asistencia más cercano, en caso de emergencia o para asesoramiento de rutina;
- asesoramiento e información especializados de salud, seguridad y viajes;
- alertas de seguridad médica y de viaje en tiempo real y específicas del lugar;
- listas de verificación de viaje, y
- datos de contacto actualizados en caso de emergencia.

Independientemente de si se dispone de asistencia médica externa, una buena práctica es que las organizaciones cuenten con un punto de contacto interno para cuestiones médicas.

Ejemplo: Atentado con bomba en un restaurante en Islamabad (Pakistán) en 2008

En 2008 unos terroristas atacaron un restaurante italiano frecuentado por extranjeros en Islamabad e hirieron a personal de al menos dos organizaciones humanitarias. Ambas organizaciones tenían proveedores de asistencia médica asociados al mismo hospital en Islamabad. Una organización había visitado el hospital, había abierto una cuenta y había establecido una relación. Su personal fue evaluado en el hospital durante la primera hora después del ataque. La segunda organización fue al hospital y solicitó que su personal fuera admitido de acuerdo con el procedimiento de su proveedor médico. El hospital quería la confirmación de la capacidad de pago de la organización. Esto demoró varias horas y el personal fue admitido en el hospital recién después de completarse este proceso.

Además de la preparación para los problemas de salud física, las organizaciones también deben implementar recursos y protocolos para la prestación de apoyo de salud mental. Esto requiere una consideración cuidadosa, dado el daño psicológico de responder en entornos violentos y el acceso limitado a proveedores de salud mental en muchos contextos.

Las necesidades de salud mental pueden adoptar diversas formas, entre ellas, las siguientes:

- Personal con necesidades de salud mental que requieren cuidados y apoyo continuos (p.ej., medicación y asesoramiento psicológico).
- Personal que experimenta problemas de salud mental, como estrés o trastorno de estrés postraumático, como consecuencia directa de experiencias relacionadas con el trabajo.
- Personal cuyas afecciones de salud mental preexistentes empeoran o se agravan por las exigencias y los desafíos de su entorno de trabajo.

Cada persona afronta el estrés y reacciona ante las crisis de manera diferente. Las personas pueden manifestar una variedad de emociones, desde extremas hasta ninguna. La expresión intermitente de emociones también son normales. El apoyo psicosocial brindado por profesionales, así como el apoyo de pares capacitados y el liderazgo compasivo, pueden reducir la probabilidad de sufrir lesiones psicológicas graves, como el trastorno de estrés postraumático.

Lo que la organización puede proporcionar en términos de apoyo de salud mental debería evaluarse minuciosamente y explicarse claramente al personal antes de un incidente, y puede variar según las necesidades y los deseos de los miembros del personal afectados.

- *Para obtener más información sobre el apoyo de salud mental para el personal, véase el capítulo 5.4.*

Capacitación en primeros auxilios

Los primeros auxilios que se brindan de manera oportuna y apropiada, con los materiales adecuados, son la mejor medida de mitigación para reducir el impacto de una emergencia médica. En entornos alejados o con recursos limitados, la capacitación en primeros auxilios debe centrarse en la atención inmediata y eficaz dado que la ayuda médica profesional puede no estar fácilmente disponible. Esto incluye capacitación en primeros auxilios centrada en el trauma sobre la manera de realizar evaluaciones rápidas de lesiones/afecciones; administrar tratamientos adecuados, como mantener las vías respiratorias, la respiración y la circulación y el control del sangrado; controlar el dolor de manera eficaz, y garantizar el transporte seguro del paciente. Comprender los impactos ambientales en la salud es fundamental, ya que factores como las temperaturas extremas y el mal de altura pueden causar y empeorar afecciones médicas y lesiones. Además, se puede capacitar a los trabajadores humanitarios sobre cómo utilizar la “adaptación ingeniosa”, improvisando soluciones con recursos mínimos y utilizando posiblemente materiales naturales para estabilizar y tratar a la persona afectada hasta que sea posible una intervención profesional. La capacitación especializada en primeros auxilios para trabajadores humanitarios (que a menudo se brinda como parte de la formación sobre sensibilización para entornos hostiles) considera el alcance (y la gravedad) de las emergencias médicas (con un enfoque particular en las lesiones) que el personal humanitario puede enfrentar, el acceso limitado a los servicios médicos y los desafíos ambientales agravados (naturales y provocados por el hombre) que dificultan el tratamiento.

- *Para obtener más información acerca de la formación sobre sensibilización para entornos hostiles, véase el capítulo 5.2.*

Equipo de primeros auxilios para entornos remotos o con recursos limitados

Además de una capacitación integral, la disponibilidad de un equipamiento de primeros auxilios adecuado (en cantidades apropiadas) es esencial para una respuesta médica eficaz en zonas apartadas con acceso limitado o nulo a servicios de salud profesionales. A continuación se muestra una lista de ejemplo. La lista no es exhaustivo y las organizaciones deben buscar asesoramiento especializado sobre los artículos que deben poseer y la capacitación adaptada al contexto y a las necesidades de su personal.

Respuesta a incidentes médicos importantes

- **Vendajes para traumatismos.** Vendajes estériles y absorbentes para cubrir heridas (incluidos sellos torácicos y vendajes triangulares para cabestrillos).
- **Férulas.** Para inmovilizar fracturas y estabilizar extremidades lesionadas.
- **Agentes hemostáticos.** Agentes especializados que contribuyen a la coagulación sanguínea y al control del sangrado.
- **Torniquetes.** Para controlar sangrados severos en las extremidades.
- **Desfibrilador.** En caso de paro cardíaco.
- **Apósito en gel para quemaduras.** Para tratar quemaduras.

Limpieza y tratamiento de heridas

- **Soluciones antisépticas.** Para limpiar heridas y prevenir infecciones.
- **Gasas estériles.** Se utiliza para el vendaje.
- **Vendajes adhesivos.** Para cubrir cortes pequeños y abrasiones.
- **Pomada antibiótica.** Para el tratamiento tópico de heridas y prevenir infecciones.
- **Envoltura de plástico.** Para la protección temporal adicional de una herida.

Evacuación y transporte

- **Camillas.** Camillas portátiles para transportar personas lesionadas por terrenos difíciles.
- **Mantas.** Para brindar calidez y comodidad a las personas heridas. Las mantas de emergencia e isotérmicas que retienen el calor corporal y brindan calor.
- **Botiquines médicos portátiles.** Kits compactos que contienen medicamentos y suministros esenciales.

Equipo de protección personal

- **Guantes.** Guantes desechables para mantener la higiene y evitar la contaminación cruzada.
- **Mascarillas.** Para proteger contra los agentes patógenos y contaminantes transportados por el aire.
- **Protección para los ojos.** Gafas o anteojos de seguridad para protegerse contra residuos y salpicaduras.

Suministros adicionales

- **Cinta médica.** Para asegurar vendajes y apósitos.
- **Tijeras.** Tijeras de uso médico para cortar vendajes y ropa.
- **Linternas.** Fuentes de luz portátiles para evaluar lesiones en condiciones de poca luz.

Garantizar la disponibilidad y el mantenimiento adecuado de los suministros de primeros auxilios es fundamental para brindar una atención rápida y eficaz en entornos difíciles. Es importante señalar que los tratamientos más complejos, en particular la administración de medicamentos, debe realizarse bajo la supervisión de un médico. En situaciones de emergencia, esto se puede proporcionar de forma remota.

5.5.3 Respuesta a emergencias médicas

Los programas de ayuda humanitaria a menudo se implementan en zonas donde el acceso a una atención médica oportuna es limitado. La respuesta rápida a las emergencias médicas es fundamental, ya que los retrasos en el tratamiento pueden tener consecuencias graves. En esta sección se proporciona orientación sobre las habilidades, el equipo y los protocolos necesarios para una respuesta eficaz. Todos los protocolos deben ser desarrollados y elaborados por personal o asesores con experiencia médica.

- *Las siguientes secciones se centran en los riesgos médicos físicos. Para obtener más información sobre los riesgos psicológicos y las buenas prácticas, véase el capítulo 5.4.*

Respuesta inmediata

Si bien la mayoría de los protocolos humanitarios de primeros auxilios y respuesta se centran en lesiones traumáticas (es decir, lesiones físicas graves que ocurren repentinamente y requieren atención médica inmediata), otros tipos de emergencias médicas también pueden requerir una respuesta inmediata, como, por ejemplo, un paro cardíaco, un ahogamiento y un golpe de calor. Las organizaciones deben considerar a qué emergencias médicas su personal debe estar preparado para responder,

dependiendo del contexto y las circunstancias del personal. Es una buena práctica que las organizaciones cuenten con planes y protocolos para gestionar crisis médicas, que incluyan procedimientos de clasificación de urgencias, evacuación de víctimas o heridos y transporte.

Los pasos clave para ayudar a una persona que sufre un trauma físico u otra emergencia médica incluyen:

- Garantizar la seguridad del lugar y utilizar el equipo de protección personal adecuado antes de comenzar cualquier evaluación o tratamiento.
- Evaluar y tratar rápidamente las amenazas inmediatas a la vida, como un sangrado grave o una obstrucción de las vías respiratorias.
- Decidir si es necesario el traslado para recibir un nivel superior de cuidado e iniciar el proceso de traslado.
- Proporcionar información sobre el estado del paciente al centro receptor.
- Elegir un modo de transporte adecuado en función de las necesidades del paciente y los recursos disponibles.
- Atención continua y supervisión durante el traslado.

El objetivo es abordar las necesidades críticas inmediatas y estabilizar al paciente para que pueda ser trasladado a un centro médico, y hacerlo dentro de la crítica “hora de oro” en el caso de que se trate de una lesión traumática.

Las consideraciones adicionales para la gestión de incidentes médicos graves incluyen las siguientes:

- **Comunicación de emergencia.** Esto implica establecer una comunicación eficaz para coordinar los esfuerzos de respuesta y buscar asistencia, utilizando radios, teléfonos satelitales y dispositivos de señalización.
- **Evacuación médica (MEDEVAC).** Las habilidades básicas de conducción y lectura de mapas pueden ayudar a facilitar el transporte rápido de pacientes a instalaciones médicas o puntos de evacuación. También es una buena práctica que los vehículos del proyecto estén equipados con suministros básicos para permitir el traslado del personal herido o enfermo.
- **Evaluación y mejora continua de los protocolos de respuesta a incidentes médicos.** Esto podría incluir la recopilación de comentarios de los equipos de respuesta para adaptar las estrategias en función de las lecciones aprendidas y los desafíos cambiantes.

- **Documentación e informes.** Documentar y reportar incidentes, incluidos los cuasiaccidentes y las lecciones aprendidas, para el seguimiento y análisis de incidentes y para el seguro, y cualquier necesidad de información externa para atención médica y seguimiento. Cuando corresponda, y siempre que se garantice la confidencialidad, esto puede vincularse a las denuncias de incidentes de seguridad de una organización.

Consideraciones para las organizaciones humanitarias que responden a una situación con múltiples víctimas

Las situaciones con múltiples víctimas, que pueden ser desde desastres relacionados con peligros hasta accidentes a gran escala o actos de violencia, exigen una acción rápida y eficaz y pueden saturar rápidamente los sistemas de salud. Esto puede significar considerar cuestiones que van más allá de la atención médica inmediata y que abarcan aspectos de gestión operacional, coordinación y ética.

- **Seguridad.** Garantizar la seguridad del personal de respuesta y proteger el lugar del incidente. Hay que tener en cuenta las posibles amenazas o peligros secundarios.
- **Evaluación rápida y clasificación.** Evaluar rápidamente la escala del incidente e implementar un sistema de clasificación para priorizar el tratamiento de las víctimas según la gravedad de las lesiones.
- **Gestión de recursos.** Asignar eficientemente al personal, los suministros y los equipos para brindar el mayor beneficio. Analizar la posibilidad de solicitar recursos adicionales con anticipación.
- **Comunicación y coordinación.** Establecer líneas de comunicación claras entre las organizaciones de respuesta, los hospitales y los centros de comando. Coordinar esfuerzos para evitar duplicaciones y deficiencias en la respuesta.
- **Información pública.** Coordinar una comunicación consistente y oportuna con el público y los medios de comunicación sobre el incidente y los esfuerzos de respuesta.
- **Documentación.** Implementar sistemas para hacer un seguimiento de los pacientes, los recursos utilizados y las acciones tomadas con vistas a su análisis posterior y posibles acciones legales.
- **Sensibilidad cultural.** Ser consciente y respetuoso de las prácticas culturales y religiosas, especialmente en lo que respecta al tratamiento de los fallecidos.

- **Toma de decisiones éticas.** Estar preparado para tomar decisiones éticas difíciles sobre la asignación de recursos limitados.
- **Apoyo psicosocial.** A largo plazo, proporcionar recursos de salud mental para las personas afectadas, las familias y el personal de respuesta.

Atención posterior

Un plan de seguridad y apoyo bien estructurado es crucial para la atención posterior a largo plazo de los trabajadores humanitarios que han sufrido un incidente médico crítico. Este plan debe priorizar la seguridad y el bienestar del individuo, garantizando que tenga acceso a apoyo médico y psicosocial continuo y adaptado a sus necesidades y deseos específicos (es aconsejable adoptar un enfoque de atención a largo plazo centrado en el superviviente). El apoyo médico a largo plazo puede incluir controles regulares y acceso a atención especializada según sea necesario, mientras que el apoyo psicosocial puede incluir asesoramiento o terapia para abordar el trauma psicológico y prevenir efectos psicológicos a largo plazo. Es esencial ser transparente con el personal afectado sobre el alcance y la duración del apoyo.

La reintegración al trabajo debe manejarse con cuidado para apoyar la recuperación del miembro del personal afectado. Esto podría implicar acuerdos de trabajo flexibles, un retorno gradual a las funciones o una reasignación a tareas menos exigentes. Mantener una comunicación regular con el individuo para evaluar su comodidad y progreso, realizando los ajustes necesarios.

► Para obtener más orientación sobre la atención posterior a largo plazo centrada en el superviviente para el personal afectado, véase el capítulo 5.4.

Más información

Orientación y recursos

Center for Substance Abuse Treatment (US, 2014). Chapter 1, Trauma-informed organizations. En *Trauma-Informed Care in Behavioral Health Services*. Treatment Improvement Protocol Series, Núm. 57 (www.ncbi.nlm.nih.gov/books/NBK207201/).

Centros para el Control y la Prevención de Enfermedades. (2024). *CDC Yellow Book: health information for international travel 2024* (www.cdc.gov/yellow-book/index.html).

Cruz Roja Americana. (s.f.). First aid training (www.redcross.org/take-a-class/first-aid/first-aid-training).

DeMers, G. y Wightman, J. (2019). Mass casualty preparedness and response. En F.G. O'Connor, E.B. Schoomaker y D.C. Smith (Eds.). *Fundamentals of military medicine*. Borden Institute (<https://medcoeckapwstorprd01.blob.core.usgovcloudapi.net/pfw-images/dbimages/Fund%20ch%2034.pdf>).

DeNolf, R.L. y Kahwaji, C.I. (2022). *EMS mass casualty management*. StatPearls (www.ncbi.nlm.nih.gov/books/NBK482373/).

Organización Internacional de Normalización. (2018). *ISO 45001:2018: Sistemas de gestión de la seguridad y salud en el trabajo — Requisitos con orientación para su uso* (www.iso.org/iso-45001-occupational-health-and-safety.html).

Organización Mundial de la Salud. (2022). *Guide: mass casualty preparedness and response in emergency units*. ReliefWeb (<https://reliefweb.int/report/world/guide-mass-casualty-preparedness-and-response-emergency-units>).

Rural Health Information Hub. (s. f. a). *Emergency preparedness and response for mass casualty incidents* (www.ruralhealthinfo.org/toolkits/emergency-preparedness/4/mass-casualty-incidents).

Rural Health Information Hub. (s. f. b). *Partners and collaborators for emergency preparedness and response* (www.ruralhealthinfo.org/toolkits/emergency-preparedness/1/partners-collaborators).

6 Tecnología y seguridad

6.1 Gestión de la seguridad de la información y las comunicaciones

Este capítulo se centra en las consideraciones para gestionar información sensible y transferir información de forma segura, así como en las medidas que tomar cuando se interrumpen los métodos habituales de comunicación. Después de una descripción general de la seguridad de la información, se analizan las comunicaciones seguras y los elementos esenciales de un plan de comunicación.

6.1.1 Seguridad de la información

La seguridad de la información se refiere a las medidas y a las prácticas dirigidas a proteger la información sensible del acceso no autorizado, las violaciones de la seguridad de los datos y el mal uso. Esto incluye garantizar la confidencialidad, la integridad y la disponibilidad de los datos, especialmente en entornos donde la información puede ser fundamental para la seguridad y la eficacia de las operaciones. Para las organizaciones humanitarias, esto suele implicar salvaguardar los datos personales, datos operacionales y otra información sensible que, de verse comprometida, podría poner en peligro a las personas o a las operaciones. La información sobre los miembros del personal, las actividades de la organización, los destinatarios previstos de la ayuda y los contactos pueden utilizarse con fines nocivos. En algunos casos, la información no está concebida para ser compartida externamente. En otros casos, la información puede simplemente malinterpretarse o sacarse de contexto.

Los registros confidenciales de las organizaciones pueden incluir:

- Documentos sobre miembros del personal, como salarios y evaluaciones de desempeño.
- Información personal confidencial, como historiales médicos.
- Información específica de la organización (p.ej., registros bancarios, documentos legales y acuerdos gubernamentales).
- Evaluaciones de las operaciones (p.ej., diagnóstico de riesgos, mapeo de los actores e informes de situación e incidentes, que pueden percibirse como espionaje).
- Información sobre movimientos del personal.
- Actas de reuniones.
- Información asociada a los programas, incluidos datos de los beneficiarios de la ayuda.

- Información sobre finanzas y manejo de efectivo.
- Inventarios de activos (vehículos, equipos de oficina, radios).

Entre los ejemplos típicos de materiales sensibles se incluyen los historiales médicos, los datos identitarios del personal y de los destinatarios de la ayuda y los planes operacionales en zonas de conflicto. La mala gestión de dicha información puede tener consecuencias graves, incluidos riesgos para la seguridad personal y la credibilidad de la organización. Los problemas más comunes son el almacenamiento inadecuado de los documentos, archivos digitales no seguros y procedimientos poco rigurosos para la eliminación de información sensible. Una mala gestión puede fácilmente dar lugar a accesos no autorizados o a fugas accidentales de datos.

En algunos entornos, también existe un alto riesgo de vigilancia por parte de actores estatales, grupos criminales u otras partes interesadas en las operaciones de las organizaciones humanitarias. Esto puede incluir el monitoreo de las comunicaciones, el hackeo de los sistemas o la vigilancia física.

Las organizaciones pueden tomar varias medidas para fortalecer la seguridad de la información.

- **Las políticas y los procedimientos operativos** de seguridad de la información son cruciales para todos los contextos operacionales. Estos documentos establecen qué se considera “información sensible”, quién está autorizado a verla y cómo debe almacenarse, comunicarse, transportarse, desensibilizarse o destruirse. Básicamente, el personal responsable debe evaluar el impacto que tendría que personal no autorizado acceda a la información. Por ejemplo, ¿cuáles serían las consecuencias si actores gubernamentales hostiles accedieran a la computadora personal de un miembro del personal al llegar al país, que contiene información personal e imágenes?
- Se pueden implementar **protocolos** para el manejo de datos, el control del acceso, la respuesta a incidentes y la planificación de contingencia. También deberían abordar desafíos específicos, como la gestión de la información en entornos de alto riesgo o durante emergencias. Estos protocolos también pueden orientar las comunicaciones externas, incluida la interacción con los medios de comunicación, las declaraciones oficiales y las publicaciones en las redes sociales.
- Una forma clave de proteger la información es mantener **copias de respaldo** en múltiples lugares. Esto brinda protección contra pérdidas (pero no hurtos). Se deben conservar copias de seguridad tanto digitales como impresas de los documentos esenciales. Las buenas prácticas para proteger la información impresa incluyen el manejo adecuado de los documentos, el almacenamiento seguro y métodos de destrucción apropiados. En algunos casos, puede ser necesario destruir rápidamente documentos sensibles (por ejemplo, triturarlos y eliminar de forma segura archivos digitales) por lo que es aconsejable minimizar la documentación

en el lugar. Restringir el acceso a la información sensible a un número limitado de personas puede proporcionar una capa adicional de seguridad.

- **La capacitación del personal** es crucial. Todo el personal debe ser consciente de la importancia de la seguridad de la información, del modo de reconocer y manejar la información sensible y de los riesgos de comunicación específicos del contexto operacional. Esto es especialmente importante para el personal con acceso a la información sensible o para quienes interactúan habitualmente con actores externos o gestionan las interacciones con los medios de comunicación, como el personal de comunicación.

Las buenas prácticas en materia de seguridad de la información también incluyen la gestión de las comunicaciones y de la seguridad digital, así como el tratamiento de los riesgos que surgen de la vigilancia hostil. La seguridad de las comunicaciones se aborda con más profundidad en las siguientes secciones de este capítulo, mientras que la seguridad digital se analiza en detalle en el capítulo 6.2. Para obtener más información sobre la vigilancia hostil, véase el capítulo 7.5.

6.1.2 Planificación de comunicación

La capacidad de comunicarse con otros es uno de los pilares fundamentales de la seguridad y es especialmente importante en entornos de alto riesgo. Los planes y los procedimientos de seguridad no se pueden implementar sin la capacidad de comunicarse y, en una emergencia, la capacidad de comunicarse rápidamente con otras partes puede implicar la diferencia entre la vida y la muerte. Por ello, un plan de comunicación es tan importante para la seguridad como un diagnóstico de riesgos, y el desarrollo de un buen plan de comunicación debe tomarse con la misma seriedad.

Un buen plan de comunicación está diseñado para adaptarse a la organización y satisfacer sus necesidades específicas en el contexto en el que opera. Los planes de comunicación deben adaptarse a cada organización, a cada oficina e incluso a cada proyecto. La integración de la seguridad de la comunicación a las políticas de seguridad más amplias de la organización ayuda a garantizar un enfoque consistente en todas las operaciones.

Consideraciones iniciales

Las siguientes consideraciones deben informar el plan de comunicación de cualquier proyecto, oficina u organización.

Tamaño y presupuesto de la organización

Si bien los planes localizados pueden ser suficientes para las organizaciones pequeñas, las entidades más grandes con múltiples oficinas requieren estrategias integrales y compatibles a fin de garantizar una comunicación eficaz entre las oficinas y eficiente en función de los costos. El objetivo es maximizar las capacidades de comunicación en toda la organización. La escalabilidad es crucial; los planes deben poder adaptarse

al crecimiento o a la contracción futuros y evolucionar a medida que cambien las necesidades de la organización.

Las consideraciones presupuestarias son cruciales. Las organizaciones más pequeñas generalmente asignan un porcentaje mayor de su presupuesto general a las comunicaciones (debido a los altos costos de la tecnología y de la infraestructura), mientras que las organizaciones más grandes gastan más por miembro del personal pero un porcentaje menor del presupuesto general de la organización. Establecer un presupuesto realista, tanto en términos de gasto por empleado como de porcentaje del presupuesto general de operación, es esencial. La escalabilidad a largo plazo justifica potencialmente mayores inversiones iniciales en soluciones sostenibles.

Contexto operacional

Es posible que se necesite un plan de comunicación distinto para cada contexto operacional. Un plan de comunicación que funciona para un entorno urbano de oficina puede no ser apropiado para una zona rural apartada, y un plan de comunicación para un entorno urbano de oficina en un país puede no funcionar en un entorno similar pero en otro país. De manera similar, un plan de comunicación concebido para una oficina fija puede no ser adecuado para un equipo móvil.

El costo y la visibilidad de los equipos de comunicación, como las radios y los teléfonos satelitales, pueden convertirlos en blancos atractivos para hurtos u otras actividades delictivas. Este riesgo debe considerarse como parte de la selección de las comunicaciones, junto con las medidas de seguridad para mitigarlos, como el almacenamiento seguro, el acceso controlado y la capacitación periódica del personal sobre el uso y manejo seguro de los equipos.

Infraestructura existente

Maximizar el uso de la infraestructura de comunicación existente puede aumentar las opciones y la flexibilidad de un plan de comunicación, y minimizar al mismo tiempo los costos. Sin embargo, se debe investigar la confiabilidad de la infraestructura existente, ya que cualquier cosa fuera del control directo de la organización puede ser susceptible a interrupciones o fallas.

- Comunicaciones móviles:
 - identificar proveedores de servicios móviles en la zona;
 - evaluar la cobertura de la torre de telefonía móvil;
 - determinar si los dispositivos móviles de comunicación deben ser parte del plan y utilizarse.

- Comunicaciones basadas en Internet:
 - identificar proveedores de servicios de Internet locales;
 - evaluar la velocidad de transferencia de datos;
 - evaluar los costos asociados a los servicios de Internet.
- Comunicaciones por radio:
 - comprobar si hay una red de radio existente disponible;
 - evaluar si la organización necesita construir su propia infraestructura.
- Infraestructura eléctrica:
 - evaluar los sistemas eléctricos existentes;
 - determinar qué voltaje está disponible y si cumple con los requisitos;
 - evaluar la necesidad de fuentes de alimentación de respaldo;
 - considerar si se necesitan baterías para energía portátil o de respaldo;
 - desarrollar un plan para cargar y mantener las baterías en caso de que se requieran.

Las comunicaciones pueden ser vigiladas por los Gobiernos, los proveedores de servicios y otros actores. La seguridad de la información (tener cuidado con quién tiene acceso a qué información y cómo se comparte) es primordial. También es un elemento importante a la hora de decidir qué equipo utilizar y cuándo.

Ejemplo: Planificación para interrupciones en la infraestructura

En 2024 Starlink (un proveedor privado de servicios de Internet por satélite) anunció que suspendería los servicios de Internet en Sudán, alegando la falta de autorización para operar allí. Esta decisión alarmó a las organizaciones humanitarias que dependían de Starlink para comunicarse en medio del conflicto y de los cortes de las telecomunicaciones. Instaron a Starlink a reconsiderar su decisión, destacando el papel vital del servicio en la coordinación de la ayuda y en la facilitación de la comunicación entre las personas necesitadas.

Consideraciones ambientales y otros tipos de emergencias

Los equipos de comunicación son susceptibles a fallas en entornos con temperaturas extremas. Tanto las condiciones de mucho calor como las de mucho frío requieren equipos de comunicación diseñados para soportar temperaturas extremas o

mecanismos de refrigeración o calefacción adicionales. En ambientes muy húmedos puede necesitarse un sistema deshumidificador. En entornos muy lluviosos, puede necesitarse protección adicional para evitar la intrusión de agua. Donde hay mucha suciedad o polvo, los dispositivos con ventiladores y partes móviles pueden funcionar mal si no se limpian y protegen adecuadamente.

Durante las emergencias, la cantidad de llamadas puede aumentar dado que las personas quieren saber cómo están sus seres queridos o buscar ayuda. Esto puede provocar la saturación de la red y dificultar la conexión de las llamadas, ya sea a través de líneas fijas o redes móviles. Si las redes de telecomunicaciones se ven comprometidas, es posible que las alertas nacionales de emergencia no se transmitan de manera eficaz, lo que complicaría aún más la comunicación durante una emergencia.

Estructura de la oficina y del personal

Las oficinas o los equipos con menos personal generalmente necesitarán menos equipos de comunicación que aquellos con más personal. También hay otros factores que son relevantes. ¿El personal trabajará únicamente desde una oficina o viajará? ¿Qué medio de transporte utilizarán? ¿Viajarán en equipos grandes o individualmente? Un equipo pequeño de cinco personas que viajan a lugares diferentes diariamente necesitará más recursos que un equipo de 20 personas que solo realiza un viaje grupal por semana a un solo lugar. Sin embargo, si el equipo de cinco personas viajara una vez por semana a un lugar en particular y cada uno pudiera viajar a un lugar nuevo en un día diferente, entonces los recursos de comunicación del viaje podrían compartirse, lo que reduciría el costo general. Esto ilustra cómo la estructura de la oficina y del personal, no simplemente la cantidad de personal, pueden determinar las necesidades de comunicación.

Consideraciones sobre el tiempo

La duración del programa es un factor crucial en el desarrollo de un plan de comunicación. Tal vez no sea aconsejable realizar grandes inversiones en una infraestructura fija de comunicación para una programación de corto plazo. Si la organización tiene intención de ocupar una oficina durante años, los costos iniciales de invertir en un plan de comunicación sólido tienen más sentido.

Consideraciones regulatorias

Es importante identificar qué equipos de comunicación están permitidos por las autoridades locales. Por ejemplo, los sistemas satelitales de comunicación pueden requerir un registro especial y pueden estar prohibidos en algunas jurisdicciones. Aunque las organizaciones humanitarias pueden solicitar una exención, especialmente si trabajan o se asocian con las Naciones Unidas, la aprobación no está garantizada y debe buscarse antes de importar los dispositivos de comunicación al país. Saber qué equipos de comunicación son legales puede evitar errores costosos.

Ejemplo: Elegir el equipo adecuado

También es importante considerar qué equipos de comunicación se utilizan normalmente en determinados contextos y quién los utiliza. En 2023 una organización humanitaria que operaba en el este de Ucrania fue atacada inadvertidamente por el ejército ruso. Una revisión posterior a la acción reveló que la organización humanitaria fue confundida con un objetivo militar ucraniano porque tenía una antena parabólica de Starlink en el techo de su edificio. Los únicos otros sistemas de Starlink en la zona estaban siendo operados por unidades militares ucranianas.

Coordinación interinstitucional

En muchas zonas operacionales de alto riesgo, los servicios de telecomunicaciones pueden ser proporcionados por el grupo temático de telecomunicaciones de emergencia (ETC, por sus siglas en inglés). Este grupo es una red global que colabora con varias organizaciones para brindar servicios de comunicación compartidos durante emergencias humanitarias. Ofrece opciones de comunicación de voz y otros servicios esenciales a organizaciones humanitarias, autoridades nacionales y comunidades afectadas, particularmente cuando la infraestructura de comunicación existente pueda estar comprometida o no estar disponible. El grupo de trabajo local ETC o el Programa Mundial de Alimentos (PMA), en cuanto organismo coordinador del ETC, pueden proporcionar información sobre los servicios disponibles en la zona de operaciones. Los riesgos para los servicios del ETC son similares a los de otras telecomunicaciones, incluidas las vulnerabilidades en la infraestructura y las interrupciones. En algunas regiones, las organizaciones pueden participar en el sistema radioeléctrico de las Naciones Unidas o es posible que se hayan asignado frecuencias específicas a las ONG.

Socios previstos en materia de comunicación

El siguiente paso en la creación de un plan de comunicación es considerar a las personas y las organizaciones que necesitan comunicarse entre sí. Cada uno de estos grupos probablemente necesite un plan de comunicación independiente, pero no necesariamente equipos de comunicación separados.

Comunicaciones internas

La comunicación interna es más sencilla ya que la organización tiene un control total sobre los equipos, los métodos y las políticas. Las comunicaciones internas también son las más fáciles de solucionar cuando surgen problemas. Las comunicaciones internas pueden ser las más costosas, ya que la organización debe cubrir todos los costos relacionados con la compra de equipos, el mantenimiento y la capacitación.

Al crear un plan de comunicación interna, la organización debe considerar primero quiénes y qué grupos necesitan estar en comunicación entre sí. Si varias personas de un equipo pequeño viajan a un lugar dentro del país por separado, se puede elaborar un plan de comunicación que indique cómo se comunicará cada miembro del equipo con los demás. Un segundo plan de comunicación podría detallar cómo ese equipo se comunicará con otros equipos, mientras que un tercero podría indicar cómo esos equipos se comunicarán con su oficina central. Un plan de comunicación independiente podría establecer cómo cada individuo o grupo se comunicará con las partes interesadas internas relevantes.

Comunicaciones externas

Las comunicaciones externas abarcan todas las interacciones con individuos o grupos que no pertenecen a la organización. Esto puede incluir a las personas que reciben la ayuda, los representantes de la comunidad local, las organizaciones socias, las entidades gubernamentales, las agencias de financiación y los organismos de las Naciones Unidas. Es recomendable que se elaboren planes de comunicación para cada entidad. En algunos contextos, puede requerirse que las organizaciones humanitarias adopten el plan o el equipo de comunicación utilizado por la entidad externa. Esto no siempre es así, pero antes de desarrollar un plan de comunicación, es recomendable identificar quiénes son las partes interesadas externas y qué sistemas utilizan ya que esto puede ahorrarle a la organización tiempo y dinero a largo plazo.

► *Para obtener más información sobre las comunicaciones durante una crisis, véase el capítulo 4.4.*

Comunicaciones de emergencia

Un plan de comunicación de emergencia debe describir múltiples métodos para que las personas y los equipos se comuniquen con los servicios de emergencia, tanto dentro del país como dentro de la organización. No todos los países y los contextos cuentan con números de teléfono nacionales estandarizados para servicios de emergencia, y se deben tomar medidas en caso de que las redes telefónicas fallen.

Generalmente, las organizaciones deben adoptar los métodos, los planes y los protocolos de comunicación determinados por los proveedores de servicios de emergencia, por lo que es aconsejable comprender estos protocolos antes de elaborar un plan de comunicaciones de emergencia organizacional.

6.1.3 Equipos de comunicación

En esta sección se describen los tipos básicos de equipos de comunicación que una organización puede tener en cuenta en su planificación.

Tipos de equipos

Radio de alta frecuencia

Las radios de alta frecuencia (HF), que operan en frecuencias de entre 3 y 30 megahercios (p. ej., equipos portátiles, de vehículos o de estaciones de base) son utilizadas normalmente por operadores de radioaficionados, personal militar y organizaciones humanitarias, entre ellas, las Naciones Unidas. Las organizaciones humanitarias recurren cada vez menos a estas radios dado que las tecnologías móviles y satelitales se han generalizado y abaritado.

La principal ventaja de estos sistemas de radio es que rebotan las señales de comunicación en la atmósfera superior, lo que permite transmisiones de mayor alcance. De esta forma, las radios de HF pueden comunicarse entre sí a cientos de kilómetros de distancia. Las principales desventajas de las comunicaciones por medio de estas radios son que las perturbaciones atmosféricas pueden interrumpir la señal (p. ej., el clima y la luz solar). Asimismo, los sistemas de radio de HF generalmente requieren un alto nivel de experiencia para su instalación, mantenimiento y operación, lo que puede suponer una inversión en capacitación (por ejemplo, en el manejo de los equipos y en el uso de un lenguaje codificado: las comunicaciones no cifradas pueden ser interceptadas por cualquiera con una radio que funcione en la misma configuración y frecuencia). Estas radios normalmente también requieren una antena grande, que puede aumentar la visibilidad del vehículo, convirtiéndolo potencialmente en un objetivo para actores hostiles o hurto o haciendo que se confunda con un activo militar.

Tabla 11 Consideraciones de seguridad para los equipos de comunicación por radio de HF

Tipo	Ventajas	Desventajas/vulnerabilidades
Radio del vehículo	● Alimentado por el vehículo (la radio está encendida cuando el vehículo también lo está). ● Puede comunicarse a distancias más largas. ● Accesible para todos en el vehículo.	● La calidad de la señal puede depender de la ubicación del vehículo. ● Requiere un nivel de conocimiento generalmente alto para poder solucionar problemas. ● Las necesidades de mantenimiento pueden ser mayores debido a las condiciones de conducción. ● Costos iniciales elevados. ● Debe estar funcionando en ambos extremos para la comunicación. ● Puede requerir una licencia para operarlo.

Tipo	Ventajas	Desventajas/vulnerabilidades
Radio portátil	• Más pequeña que una radio de vehículo. • Es portátil, es decir, no está ligada a la energía del vehículo. • Se puede utilizar sin infraestructura existente.	• Requiere un alto nivel de conocimiento para configurarla y utilizarla correctamente. • Requiere baterías, que pueden agotarse. • El equipo es pesado. • Costo inicial elevado. • Debe estar funcionando en ambos extremos para la comunicación. • Puede requerir una licencia para operarlo.
Estación de base de radio	• Utiliza la energía existente (toma de pared o generador). • Puede comunicarse a distancias muy largas. • Accesible para todos. • No depende de ninguna infraestructura existente, salvo la energía.	• Requiere un nivel muy alto de conocimiento para configurarla y mantenerla. • Debe estar funcionando en ambos extremos para que se establezca la comunicación. • Costo inicial elevado. • Puede requerir una licencia para operarlo.

Radios de frecuencia muy alta y ultraalta

Las radios de muy alta frecuencia (VHF) operan en la banda de 30 a 300 megahercios y las radios de frecuencia ultraalta (UHF) operan entre 300 megahercios y 3 gigahercios. Estas radios son utilizadas por una amplia variedad de personas, desde militares, policías y otros servicios de emergencia hasta aficionados.

La principal ventaja de las radios de VHF y UHF es la comunicación instantánea en un paquete fácil de usar y relativamente rentable. La principal desventaja es que las radios de VHF y UHF generalmente requieren una línea visual, por lo que la comunicación puede ser difícil en zonas urbanas con edificios altos, por ejemplo, o en regiones montañosas donde el terreno obstruye el camino directo entre las radios.

Aunque la distancia máxima de comunicación por radio de VHF y UHF varía según el fabricante, la potencia, la antena y otros factores, las radios portátiles de VHF y UHF deben estar a unos pocos cientos de metros o unos pocos kilómetros entre sí o no podrán comunicarse. Las radios de UHF generalmente funcionan mejor en entornos urbanos ya que la banda de frecuencia puede penetrar mejor las paredes y otros objetos que las radios de VHF. Las radios de VHF generalmente son más adecuadas para comunicaciones al aire libre de largo alcance. Las radios de VHF y UHF son una mala opción para las comunicaciones a gran distancia a menos que se utilicen repetidores.

Al igual que las radios de HF, las radios de VHF y UHF funcionan punto a punto, lo que significa que una radio se comunica directamente con otra sin necesidad de

depender de la retransmisión por parte de un intermediario. Sin embargo, los repetidores pueden utilizarse como intermediarios, aceptando la transmisión de una radio y retransmitiéndola para ampliar el alcance de la señal. Al igual que las radios de HF, las señales viajan largas distancias y, si no están cifradas, son susceptibles de ser interceptadas por cualquiera que tenga una radio que funcione con la misma configuración y frecuencia. Al igual que las radios de HF, estos sistemas requieren experiencia para su instalación, mantenimiento y funcionamiento.

Tabla 12 Consideraciones de seguridad para equipos de comunicaciones por radio de VHF y UHF

Tipo	Ventajas	Desventajas/ vulnerabilidades
Radio del vehículo	• Alimentado por el vehículo (la radio está encendida cuando el vehículo también lo está). • Puede comunicarse a varios kilómetros de distancia. • Accesible para todos en el vehículo.	• Una buena señal requerirá que el vehículo esté dentro del alcance del receptor previsto. • Requiere algunos conocimientos para su configuración (aunque no para usarla). • Las necesidades de mantenimiento pueden ser mayores debido a las condiciones de conducción. • Debe estar funcionando en ambos extremos para la comunicación. • Puede requerir una licencia para operarlo.
Radio portátil	• Más pequeña que una radio de vehículo. • Es portátil, es decir, no está ligada a la energía del vehículo. • Se puede utilizar sin infraestructura existente.	• Requiere baterías, que pueden agotarse. • Alcance limitado (aproximadamente 8 kilómetros o menos, según las condiciones) sin un repetidor. • Debe estar funcionando en ambos extremos para la comunicación. • Puede requerir una licencia para operarlo.

Tipo	Ventajas	Desventajas/ vulnerabilidades
Estación de base de radio	• Utiliza la energía existente (toma de pared o generador). • Pueden comunicarse a distancias más largas que los radios portátiles. • Accesible para todos. • No depende de ninguna infraestructura existente, salvo la energía.	• Requiere un nivel moderado de conocimientos para su configuración y mantenimiento. • Debe estar funcionando en ambos extremos para que se establezca la comunicación. • Puede requerir una licencia para operarlo.
Repetidor	• Amplía el alcance de la comunicación retransmitiendo la transmisión de radio. • Requiere energía pero ninguna otra infraestructura existente. • No requiere que nadie lo opere una vez configurado.	• Puede ser caro. • Debe tener energía y un espacio donde instalarlo. • Puede requerir muchos repetidores para establecer una gran red de comunicación. • Requiere un nivel moderado de conocimientos para su configuración y mantenimiento, pero no para operarlo. • Puede requerir una licencia para operarlo.

Dispositivos móviles

Los dispositivos móviles requieren una red móvil existente que repita la transmisión de un dispositivo móvil a otro a lo largo de la red o, según la situación, a través de Internet. Las principales ventajas de los dispositivos móviles son la presencia generalizada de los equipos, el coste relativamente bajo, la amplia infraestructura existente y la facilidad de uso. Las principales desventajas son la dependencia de la infraestructura existente (sin cobertura móvil los dispositivos no pueden comunicarse) y el hecho de que las compañías de servicios móviles actúan como intermediarias en la cadena de comunicación, lo que les permite interceptar y potencialmente vigilar las comunicaciones. Muchos Gobiernos tienen el poder de cortar las comunicaciones móviles o controlar estrictamente la actividad. Muchos también requieren el registro obligatorio de la tarjeta SIM, que generalmente implica proporcionar datos personales, incluida una identificación válida, para activar la tarjeta. Por último, aunque una gran cantidad de comunicaciones de voz y datos están cifradas, lo que impide que la mayoría de los usuarios intercepten las comunicaciones y las escuchen clandestinamente, no siempre es posible mantener la seguridad de las comunicaciones frente al proveedor de telefonía móvil o el Gobierno.

Tabla 13 Consideraciones de seguridad para equipos móviles de comunicación

Tipo	Ventajas	Desventajas/vulnerabilidades
Teléfono móvil (voz)	• El equipo es de bajo costo y de uso universal. • Las necesidades de capacitación son mínimas. • Se necesita una señal de telefonía móvil de menor intensidad para la comunicación de voz que para la de datos.	• Debe tener cobertura de red móvil y un plan activo. • Puede estar sujeto a vigilancia gubernamental. • Los Gobiernos pueden cerrarlo en cualquier momento. • Puede verse afectado por peligros naturales u otros factores ambientales. • Mayor riesgo de saturación de la red durante emergencias.
Teléfono móvil (datos)	• El equipo es de bajo costo y de uso universal. • Las necesidades de capacitación son mínimas. • El flujo de información y la velocidad de transmisión de datos pueden ser muy altos, lo que permite comunicar grandes cantidades de datos en poco tiempo.	• Debe tener cobertura de red móvil y un plan activo. • Puede estar sujeto a vigilancia gubernamental. • Los Gobiernos pueden cerrarlo en cualquier momento. • Puede verse afectado por peligros naturales u otros factores ambientales.
Punto de acceso móvil	• Los costos de los equipos son bajos. • Varios dispositivos pueden comunicarse a través de un punto de acceso. • Algunos puntos de acceso pueden utilizar varias redes móviles, lo que permite una mayor cobertura.	• Debe tener cobertura de red móvil y un plan activo. • Puede estar sujeto a vigilancia gubernamental. • Los Gobiernos pueden cerrarlo en cualquier momento. • Puede verse afectado por peligros naturales u otros factores ambientales.

Tipo	Ventajas	Desventajas/vulnerabilidades
Dispositivo inteligente	• El propio dispositivo se conecta directamente a la red móvil sin necesidad de otro dispositivo como intermediario. • Los dispositivos pueden variar de tamaño (de muy pequeños a muy grandes) • Los dispositivos pueden venir con equipamiento existente (pantalla inteligente instalada en un vehículo, por ejemplo).	• Debe tener cobertura de red móvil y un plan activo. • Puede estar sujeto a vigilancia gubernamental. • Los Gobiernos pueden cerrarlo en cualquier momento. • Puede verse afectado por peligros naturales u otros factores ambientales. • Las opciones de comunicación casi siempre están limitadas a las opciones de software instaladas en el dispositivo.

Dispositivos de línea fija

Los dispositivos de línea fija se conectan entre sí a través de una red existente de cables (subterráneos, sobre el suelo, bajo el mar). La principal ventaja de los dispositivos de línea fija es que generalmente pueden comunicar grandes cantidades de voz o datos de manera confiable y rápida. También pueden ser más confiables que los dispositivos móviles porque es necesario cortar la conexión de línea fija para interrumpir el servicio, mientras que los dispositivos móviles dependen de la intensidad de la señal de una conexión remota a una torre de telefonía móvil. Un punto débil de las conexiones de línea fija es que las conexiones en sí no se pueden mover y, por lo tanto, no son portátiles. Además, la infraestructura existente de conexiones de línea fija no está tan generalizada como las torres de telefonía móvil, y la reparación de las interrupciones puede llevar más tiempo.

Tabla 14 Consideraciones de seguridad para equipos de comunicación de línea fija

Tipo	Ventajas	Desventajas/vulnerabilidades
Teléfono fijo	• Más difícil de interceptar que las llamadas de voz de un teléfono móvil. • Fácil de usar. • Los teléfonos fijos tradicionales, especialmente los modelos analógicos, no requieren una fuente de alimentación externa para funcionar.	• Completamente sin cifrar. • Disponibilidad decreciente. • Los Gobiernos pueden cerrarlo en cualquier momento. • Puede verse afectado por peligros naturales u otros factores ambientales.

Tipo	Ventajas	Desventajas/vulnerabilidades
Conexión por línea conmutada	• Proporciona acceso a Internet.	• Solo disponible en algunos lugares más remotos. • Depende de las líneas telefónicas existentes. • Velocidad de transmisión de datos muy lenta. • Puede verse afectado por peligros naturales u otros factores ambientales.
Línea de abonado digital	• Más rápido que el acceso por línea conmutada. • Costo bajo. • Ampliamente disponible. • Se pueden usar enrutadores wifi para que varios dispositivos puedan comunicarse en una línea.	• Depende de las líneas telefónicas existentes. • Puede estar sujeto a vigilancia gubernamental. • Los Gobiernos pueden cerrarlo en cualquier momento. • Puede verse afectado por peligros naturales u otros factores ambientales.
Cable	• Velocidades de transferencia de datos muy rápidas. • Más confiable que la línea de abonado digital. • La conexión puede ralentizarse durante las horas punta de uso. • Se pueden usar enrutadores wifi para que varios dispositivos puedan comunicarse en una línea.	• Depende de líneas de cable existentes (originalmente tendidas para televisión por cable). • Puede estar sujeto a vigilancia gubernamental. • Los Gobiernos pueden cerrarlo en cualquier momento. • Puede verse afectado por peligros naturales u otros factores ambientales.
Fibra	• Velocidades de transferencia de datos muy rápidas. • La conexión es más confiable. • Puede ser caro. • Menos propensa a cortes o ralentizaciones. • Se pueden usar enrutadores wifi para que varios dispositivos puedan comunicarse en una línea.	• Depende de las líneas de fibra óptica. • Puede estar sujeto a vigilancia gubernamental. • Los Gobiernos pueden cerrarlo en cualquier momento. • Puede verse afectado por peligros naturales u otros factores ambientales.

Dispositivos de comunicación satelital

Los dispositivos de comunicación satelital se comunican a través de una red de satélites (o una constelación de satélites) en lugar de torres de telefonía móvil. La ventaja de esto es que un satélite puede proporcionar cobertura a un área terrestre mucho más grande que una torre de servicio móvil. Los dispositivos de comunicación satelital también son más difíciles de interrumpir y los Gobiernos generalmente no tienen la capacidad de cortar los servicios como pueden hacerlo con los dispositivos móviles u otras redes terrestres.

Las dos principales desventajas de los dispositivos satelitales son que la antena del dispositivo debe tener una línea de visión directa al cielo abierto (por lo que no se pueden usar desde el interior de un edificio a menos que se coloque una antena en el exterior) y los dispositivos y los servicios son más caros que con las comunicaciones móviles. También es importante reconocer que no son totalmente inmunes al control gubernamental o a otras formas de interferencia (incluidas las interrupciones selectivas). Algunos Gobiernos prohíben por completo los dispositivos de comunicación satelital, otros imponen restricciones a ciertas compañías y otros exigen que todos los dispositivos satelitales estén registrados. Por último, un riesgo importante de las comunicaciones por satélite es la dependencia de los proveedores de servicios satelitales, que pueden optar por finalizar abruptamente los servicios. Si bien esto supone una dificultad para todos los servicios de comunicación, es más notable en las comunicaciones satelitales debido a la cantidad reducida de operadores.

Tabla 15 Consideraciones de seguridad para equipos de comunicaciones por satélite

Tipo	Ventajas	Desventajas/vulnerabilidades
Teléfono satelital	● Cobertura casi universal. ● Puede llamar a cualquier teléfono.	● Algunos proveedores tienen mejor cobertura que otros. ● El servicio puede ser costoso. ● El teléfono debe tener una línea de visión directa hacia el cielo. ● Puede ser ilegal en algunas jurisdicciones o requerir una licencia/autorización.
Dispositivo “pulsar para hablar” por satélite.	● Cobertura casi universal. ● La señal puede ser más confiable que con un teléfono satelital. ● Puede hablar con varias personas a la vez (como un sistema de radio).	● Algunos proveedores tienen mejor cobertura que otros. ● El servicio puede ser costoso. ● El dispositivo debe tener una línea de visión directa hacia el cielo. ● Puede ser ilegal en algunas jurisdicciones o requerir una licencia/autorización. ● Se necesita un nivel moderado de conocimientos para configurarlo.

Tipo	Ventajas	Desventajas/vulnerabilidades
Localizador/baliza de emergencia	• Cobertura casi universal. • La señal puede ser más confiable que con un teléfono satelital o un dispositivo pulsar para hablar. • Puede cifrarse completamente. • La transmisión de microrráfagas no requiere una señal activa y continua.	• Algunos proveedores tienen mejor cobertura que otros. • El dispositivo debe tener una línea de visión directa hacia el cielo. • Puede ser ilegal en algunas jurisdicciones o requerir una licencia/autorización. • Generalmente limitado a pequeñas cantidades de datos (mensajes de texto, archivos pequeños, una sola imagen) o solo información de ubicación. • Los mensajes pueden tardar en enviarse o recibirse.
Internet por satélite.	• Cobertura en rápida expansión. • Acceso completo a Internet. • Puede conectar varios dispositivos a una sola conexión.	• Algunos proveedores tienen mejor cobertura que otros. • El servicio puede ser costoso. • El dispositivo debe tener una línea de visión directa hacia el cielo. • Puede ser ilegal en algunas jurisdicciones o requerir una licencia/autorización. • Puede requerir un nivel moderado de conocimientos para su configuración.

6.1.4 Elegir el equipo y crear un plan

Una vez que se ha alcanzado una comprensión básica de los tipos de equipos y las necesidades de comunicación de la organización, es momento de comenzar a desarrollar un plan de comunicación.

Elegir un equipo seguro

A menudo se pregunta al personal de seguridad qué métodos y equipos de comunicación son los más seguros. La respuesta depende del lugar, las circunstancias y el momento, ya que la tecnología cambia rápidamente. Las buenas prácticas recomiendan realizar un diagnóstico de riesgos exhaustivo para seleccionar las herramientas de comunicación que mejor se adecuen a las necesidades y al contexto de las operaciones, junto con la redundancia para protegerse contra las fallas en las comunicaciones.

Las organizaciones también pueden considerar opciones de cifrado al seleccionar los equipos de comunicación. El cifrado se puede utilizar en la mayoría de los equipos de comunicación, incluidos los sistemas de radio, los dispositivos de línea fija y las

comunicaciones por satélite. El cifrado puede mejorar significativamente la seguridad de las comunicaciones, pero requerirá equipo o programas informáticos compatibles. El uso de comunicaciones cifradas podrá estar sujeto a normativas.

Es recomendable que las organizaciones que utilizan protocolos de cifrado los actualicen y auditen periódicamente para abordar nuevas amenazas y vulnerabilidades. La adopción de un enfoque de seguridad en capas, que combina el cifrado con otras medidas como controles de acceso y autenticación segura de usuarios, proporciona una defensa más sólida contra posibles violaciones de la seguridad. Puede ser apropiado utilizar códigos al comunicar información sensible. Esto se analiza brevemente en las secciones siguientes.

Elaboración de un plan de comunicación: introducción de la redundancia necesaria

Los planes de comunicación deben incorporar la redundancia, es decir, deben garantizar que la comunicación siga siendo funcional incluso si falla un componente. Un plan principal, alternativo, de contingencia y de emergencia (PACE) está concebido para maximizar la redundancia de la comunicación y así reducir el riesgo. Un plan PACE describe la secuencia en que se utilizarán los diferentes métodos de comunicación. Por ejemplo, los teléfonos móviles podrían designarse como el método principal de comunicación. Si este método falla, el equipo cambia al método alternativo (p.ej., radio de VHF), seguido por el método de contingencia (p.ej., comunicación satelital) si este también falla.

Un plan PACE contiene dos principios clave. En primer lugar, se refiere a los tipos de comunicación, no a los dispositivos en sí. Por ejemplo, dos dispositivos que dependen de redes móviles no pueden servir como métodos principal y alternativo en un plan PACE porque una interrupción en la red móvil dejaría a ambos inoperables. La única excepción es la comunicación por radio, ya que los sistemas de radio no dependen de un intermediario: dos sistemas de radio de VHF o HF completos pueden servir como métodos de comunicación separados dentro de un plan PACE. Sin embargo, cada sistema debe ser completamente independiente. Si hay un único punto de falla, como una estación de base de radio compartida en una oficina, entonces estos no cuentan como sistemas separados.

El segundo principio es que un plan PACE se aplica secuencialmente: cada paso solo se utiliza si el método anterior falla, lo que garantiza un proceso de comunicación estructurado y confiable. Por ejemplo, si el método principal de comunicación es un teléfono móvil, debería ser la primera opción en cualquier situación. Una emergencia no exige automáticamente cambiar a la opción de “emergencia” del plan PACE. El equipo solo pasa al método alternativo cuando el principal falla y, de manera similar, solo pasa al método de contingencia cuando el alternativo falla y así sucesivamente.

A continuación se muestran algunos ejemplos de planes PACE. Es importante señalar que cada sección del plan PACE tiene un tipo de comunicación diferente, incluso si se utilizan varios dispositivos para comunicarse dentro de ese tipo.

Tabla 16 Ejemplo de plan PACE (oficina principal)

P/A/C/E	Tipo	Dispositivo	Uso(s) principal(es)
P	Línea fija	Internet por cable a través de un proveedor comercial con cobertura wifi para todo el edificio	- Comunicación de datos - Acceso a Internet - Comunicación de voz
A	Móvil	- Respaldo móvil a la conexión a Internet por cable - Teléfono móvil - Punto de acceso móvil	- Comunicación de voz - Comunicación de datos - Acceso a Internet
C	Satélite	Conexión a Internet satelital de respaldo para puntos wifi y personal específicos	- Comunicación de datos - Acceso a Internet
E	Radio de VHF	Estación de base de radio	Comunicación de voz de emergencia

Tabla 17 Ejemplo de plan PACE (lugar remoto pero fijo)

P/A/C/E	Tipo	Dispositivo	Uso(s) principal(es)
P	Satélite	- Conexión a Internet satelital para wifi en todo el edificio - Teléfono satelital	- Comunicación de datos - Acceso a Internet - Comunicación de voz
A	Radio de HF	- Estación de base de radio - Radios para vehículos	Comunicación de voz
C	Radio de VHF	- Estación de base de radio - Radios portátiles	Comunicación de voz
E	Móvil	Teléfono móvil	Comunicación de voz de emergencia que requiere un viaje de 20 minutos a una zona con cobertura móvil

Tabla 18 Ejemplo de plan PACE (equipo móvil)

P/A/ C/E	Tipo	Dispositivo	Uso(s) principal(es)
P	Móvil	• Teléfono móvil • Punto de acceso móvil	• Comunicación de voz • Comunicación de datos • Acceso a Internet
A	Radio de VHF	• Radios para vehículos • Radios portátiles	• Comunicación de voz
C	Satélite	• Teléfono satelital • Localizador de emergencia	• Comunicación de voz • Notificación de emergencia
E	Ninguno	• N/A	• N/A

Un plan PACE reduce el riesgo, pero nunca puede eliminarlo. Hay situaciones y lugares en los que puede resultar poco práctico o imposible tener cuatro tipos de comunicación separados en un plan PACE (véase la Tabla 18 con el último ejemplo de un plan PACE). Cuando esto ocurre, el riesgo se puede reducir aún más aumentando los dispositivos dentro de un tipo de comunicación particular, ya que esto proporciona el mayor respaldo posible ante fallas particulares.

Nota sobre las comunicaciones basadas en aplicaciones

Cada vez es más común utilizar aplicaciones de terceros para enviar mensajes de texto y realizar llamadas de voz o video. Estas herramientas de comunicación basadas en aplicaciones están muy extendidas y son fáciles de usar. Sin embargo, las aplicaciones no pueden asignarse a espacios separados en un plan PACE porque todas dependen del equipo en el que están instaladas. De esta manera, un móvil solo se incluirá en un espacio en el plan PACE aunque tenga instaladas tres aplicaciones de comunicación diferentes. *Para obtener más información sobre la comunicación basada en aplicaciones, véase el capítulo 6.2, “Seguridad en un mundo digital”.*

Capacitación del personal

Una vez elaborado un plan PACE, se puede crear un plan de capacitación para garantizar que todos los miembros del personal comprenden cuándo utilizar qué formas de comunicación y que son competentes en el uso de cada dispositivo. El plan de capacitación suele depender de los tipos de comunicación y los dispositivos utilizados. Si bien es probable que muy pocos miembros del personal necesiten capacitación sobre cómo usar un teléfono móvil, la mayoría necesitará instrucciones sobre cómo utilizar cierto software u otras aplicaciones en el teléfono. Por el contrario, es probable que muy pocos miembros del personal (o ninguno) dominen de inmediato la configuración y el funcionamiento de un sistema de radio de HF. Es una buena práctica garantizar que todo el personal esté capacitado para utilizar y que practique regularmente el uso de todas las formas de comunicación incluidas en el plan PACE.

Al desarrollar la capacitación debe determinarse quién va a realizar la capacitación, qué presupuesto (tiempo y dinero) se requiere para que el personal se vuelva competente en el uso de todo el equipo, y qué nivel de conocimiento tecnológico se requiere para cada usuario. Algunos equipos de comunicación son tan complicados que pueden requerir una o varias personas a tiempo completo para su instalación y mantenimiento.

La capacitación inicial sobre equipos de comunicación puede ser parte del proceso de incorporación del personal, seguida de capacitaciones de actualización periódicas. La capacitación puntual puede ayudar a detectar debilidades y a acostumbrar al personal a implementar el plan PACE. Por ejemplo, un miembro del personal de seguridad de una organización internacional apagaba el wifi cuando visitaba una oficina en un país para comprobar cómo respondía el personal.

También es útil garantizar que el personal esté capacitado en prácticas de comunicación segura, que incluya el reconocimiento de amenazas y el manejo adecuado de la información sensible. Las oportunidades de práctica regulares permiten que el personal repase los conocimientos, entre ellos, la manera de encender el equipo, usarlo, realizar su mantenimiento o solucionar problemas básicos y garantizar que el equipo esté cargado y almacenado correctamente.

Mantenimiento de equipos

Todos los equipos de comunicación están sujetos a fallas con el tiempo y, en algún momento, será necesario reemplazarlos. Esta es una consideración importante al desarrollar un plan de comunicación. Los fabricantes deben proporcionar un plazo estimado de reemplazo (es decir, el periodo de tiempo previsto en el que será necesario sustituir un dispositivo concreto). Las organizaciones deben intentar planificar el reemplazo de todos los dispositivos para estimar las necesidades presupuestarias a largo plazo y prevenir interrupciones en la comunicación.

Además del equipo en sí, deben presupuestarse algunos elementos de mantenimiento comunes, como, baterías de repuesto, cargadores de batería, antenas u otros elementos

periféricos, fundas para teléfonos o protectores de pantalla y cualquier otro accesorio necesario para el funcionamiento seguro del equipo.

Ejemplo: La importancia del mantenimiento

Por razones de costo, una organización decidió no utilizar la comunicación por satélite como método principal y optó por reservarla como medio de respaldo para emergencias. Una auditoría de su infraestructura de telefonía satelital descubrió que aproximadamente el 40 % de las baterías estaban agotadas y el 40 % de los teléfonos necesitaban una actualización de software.

Todos los equipos de comunicación, independientemente del lugar que ocupen en el plan PACE, deben probarse con frecuencia. Las pruebas deben realizarse al menos una vez a la semana en los equipos de comunicación que no se utilizan regularmente y diariamente en los equipos que se utilizan a diario. Además de las pruebas de rutina, lo ideal es probar los dispositivos antes de cualquier viaje planificado y antes de que el personal llegue a un lugar nuevo. Por ejemplo, si un equipo va a visitar una zona determinada, se pueden probar todos los dispositivos del plan PACE para garantizar que funcionan antes de que el equipo se vaya y volver a probarlos al regresar. Esto no tiene por qué ser demasiado complicado; se recomienda enviar un simple mensaje de texto o hacer una llamada de prueba para garantizar la conectividad. Además del equipo en sí, es aconsejable que también se prueben periódicamente las baterías y otros equipos periféricos.

Protección de los equipos de comunicación

Los equipos de comunicación tienen diferentes parámetros de funcionamiento y necesidades de protección. Cualquier equipo electrónico que se enchufe a una toma de corriente necesita tener protección contra cortes de energía y sobrecargas de voltaje o amperaje. En un entorno cálido los equipos generalmente necesitarán un mecanismo de enfriamiento, mientras que en un entorno muy frío puede ser necesario mantenerlos templados. Uno de los mayores desafíos para los equipos de comunicación en los vehículos es mantener los dispositivos limpios y libres de polvo. Los requisitos de protección deben presupuestarse y planificarse.

- *Para obtener más información sobre las precauciones contra los hurtos, véase el capítulo 7.2, “Seguridad del sitio”.*

- Para obtener más información sobre las precauciones contra la interceptación de las comunicaciones o la intrusión digital, véase el capítulo 6.2, “Seguridad en un mundo digital”.

6.1.5 Buenas prácticas relativas a los métodos de comunicación

Comunicación clara y segura

Los principios clave de la disciplina operacional en las comunicaciones son la claridad, la brevedad, la oportunidad y la pertinencia. Es imprescindible que el personal conozca y esté capacitado sobre los riesgos de comunicar ciertos tipos de información, especialmente cuando se utilizan métodos no cifrados.

Procedimientos de operación de radio

La claridad y la brevedad en las comunicaciones por radio se logran mediante el uso de expresiones convencionales y señales de comunicación (como *cambio o repita*). La claridad mejora cuando:

- los mensajes se preparan con antelación;
- los mensajes se presentan punto por punto;
- los usuarios dejan de hablar cuando no tienen nada que añadir;
- los usuarios hablan con frases cortas, utilizando un lenguaje sencillo y de “radiodifusión” estándar, en lugar de dialectos locales, y
- los usuarios no hablan demasiado rápido, especialmente cuando el destinatario necesita escribir el mensaje, y hablan en un tono de voz normal (gritar puede perjudicar la calidad de la recepción).

Existe un protocolo de radio acordado internacionalmente para emergencias (con muchas variaciones locales). La persona que llama solicita autorización para usar el canal repitiendo tres veces MAYDAY o PAN PAN, seguido generalmente de TODAS LAS ESTACIONES. Existe la obligación absoluta de aceptar llamadas de emergencia y de interrumpir conversaciones en curso. Un mensaje de seguridad que no indique una amenaza a la vida o a la propiedad (p.ej., un aviso de disturbios civiles en una localidad que, por lo tanto, debe evitarse) se puede iniciar repitiendo tres veces SECURITÉ.

Procedimientos de comunicación de emergencia

Los procedimientos de comunicación de emergencia deben establecerse con anticipación y deben practicarse habitualmente por todo el personal. El recuadro que figura abajo proporciona orientación sobre la información esencial que debe comunicarse en una emergencia, independientemente del mecanismo de comunicación que se use. Practicar esta secuencia puede ayudar a reducir errores en caso de se produzca una emergencia.

Cómo comunicarse en una emergencia

Indicar la información en el formato y en el orden que se señala a continuación:

1. Quién eres.
2. Su organización.
3. Su ubicación (p.ej., ubicación GPS o rutas o ciudades principales más cercanas).
4. Tipo de emergencia (p.ej., accidente provocado por una mina, bajo ataque o evacuación médica).
5. Número de personas heridas.
6. Actividad negativa actual: ¿es seguro realizar un rescate ahora?
7. Actividad negativa pasada.
8. Próxima hora de comunicación.
9. Cómo contactar a la persona que llama (p.ej., número telefónico o frecuencia de radio).
10. Otra información.

► *Para obtener más orientaciones sobre cómo reportar incidentes, véase el capítulo 4.4.*

También es importante que los miembros del personal revaliden periódicamente todos los contactos y procedimientos de emergencia para que todos puedan comunicarse con el personal apropiado en caso de emergencia. Esto se puede hacer mediante llamadas de verificación mensuales, por ejemplo.

En situaciones de crisis, los responsables de la toma de decisiones pueden verse bombardeados con tanta información que resulta imposible diferenciar los hechos de los rumores. Para ser eficaz, es importante minimizar las comunicaciones únicamente a aquellos asuntos de importancia directa. Nuevamente, esto se puede lograr mediante capacitación y disciplina.

Comunicar información sensible

Al comunicar información sensible, el personal debe considerar los siguientes factores:

- **Evaluar la necesidad de comunicación.** Antes de compartir información sensible, evalúe si es necesario revelarla y con quién debe compartirse. Asegúrese de que compartir la información esté justificado y sea apropiado.

- **Verificar la autorización del destinatario.** Confirme que todos los destinatarios estén autorizados a recibir la información. Esto ayuda a prevenir el acceso no autorizado y garantiza el cumplimiento de las normas de privacidad.
- **Limitar el intercambio de información.** Comparta únicamente la información mínima necesaria para el propósito de la comunicación. Evite proporcionar detalles no pertinentes que puedan aumentar el riesgo de exposición. Todas aquellas personas que tengan acceso a la información deben comprender y respetar la confidencialidad.
- **Elegir canales de comunicación adecuados.** Seleccione el método de comunicación más seguro y apropiado. Si se trata de información sensible, considere reuniones privadas presenciales o plataformas de mensajería segura en lugar de equipos de comunicación no cifrados o foros públicos.
- **Documentar las comunicaciones cuidadosamente.** Mantenga registros precisos de las comunicaciones que involucran información sensible, anotando quién fue informado y qué se discutió. Esto puede contribuir a la rendición de cuentas y la transparencia.
- **Gestionar el consentimiento.** Si la información se relaciona con una persona en particular o sus circunstancias, es una buena práctica obtener su consentimiento para compartir su información personal y ser transparente sobre quién puede tener acceso a la información y con qué fines.

Se debe concientizar al personal de que, incluso en las mejores circunstancias, es posible que se intercepten las comunicaciones, por lo que hay que ser muy cuidadoso respecto a lo que se comunica. En entornos de alto riesgo, es conveniente recomendar al personal que se exprese de manera moderada, objetiva y neutral, y, en los casos en que el personal pueda ser objeto de ataques, que codifique cierta información que pueda revelar su ubicación o movimientos, por ejemplo, utilizando palabras en código para designar oficinas, personas, carreteras y puntos intermedios, vehículos y tipos de carga. Esto es muy común, pero rara vez se gestiona bien y, por lo tanto, no resulta muy eficaz. Requiere información detallada y acuerdos previos. Lo ideal es que las palabras o frases en código se conozcan de memoria (en lugar de estar escritas en un libro de códigos) y se cambien periódicamente. En el caso de acontecimientos políticamente delicados, las expresiones metafóricas pueden permitir una posible negación. Un código descifrado puede constituir una vulnerabilidad importante. Demasiadas palabras en código pueden confundir al personal.

Más información

Orientación y recursos

Davis, J. et al. (2020). Module 9, Communications and information security. En *Security to go: a risk management toolkit for humanitarian aid agencies*. 4.^a edición. Global Interagency Security Forum (<https://gisf.ngo/resource/security-to-go/>).

Foro Europeo Interinstitucional para la Seguridad. (2010). *The information management challenge: a briefing on information security for humanitarian non-governmental organisations in the field* (<https://gisf.ngo/resource/the-information-management-challenge/>).

Global Interagency Security Forum. (s.f.). *Communications technology hub* (<https://gisf.ngo/communications-technology-and-humanitarian-delivery/>).

Grupo temático de telecomunicaciones de emergencia. (s.f.). *Services & activities* (www.etcluster.org/services-activities).

Programa Mundial de Alimentos. (s.f.). Emergency Telecommunications Cluster (www.wfp.org/emergency-telecommunications-cluster).

6.2 La seguridad en un mundo digital

Este capítulo analiza los riesgos digitales y sus consecuencias en la vida real para los trabajadores humanitarios. Proporciona una descripción general de las posibles medidas de mitigación, así como de los desafíos crecientes que presenta la información perjudicial, como la información errónea, la desinformación, la información manipulada y el discurso de odio.

6.2.1 Seguridad digital

Las tecnologías de conectividad global están permitiendo un mayor alcance, entrega de asistencia y estabilidad operacional, además de permitir que las poblaciones afectadas compartan sus experiencias y perspectivas. Los avances en las tecnologías móviles, en particular 4G y 5G, han permitido una transmisión de datos más rápida y han ampliado las capacidades de ancho de banda, mientras que los equipos satelitales de última generación, como Starlink, han extendido enormemente la posibilidad de trabajar en línea en lugares muy apartados, ofreciendo un acceso a Internet fiable, rápido y asequible.

Estos avances tecnológicos también conllevan mayores riesgos para las organizaciones humanitarias, su personal, sus operaciones y las poblaciones a las que prestan asistencia. El creciente volumen y la gravedad de los ciberataques y de otras amenazas digitales (como los hackeos, la vigilancia, los abusos en línea y las filtraciones de datos) obligan a cada usuario a estar preparado para protegerse a sí mismo, sus dispositivos, sus comunicaciones y sus datos contra las amenazas digitales. Establecer prácticas integrales de seguridad digital es cada vez más importante para las organizaciones humanitarias.

Seguridad digital

La seguridad digital, a efectos de este capítulo, se refiere a la protección y salvaguardia de los trabajadores humanitarios que utilizan o se ven afectados por herramientas y tecnologías digitales. Esto incluye el daño informativo, así como la ciberseguridad, es decir, los aspectos técnicos de la seguridad de las computadoras, los dispositivos móviles, las aplicaciones y los servicios de datos y conectividad de los que dependen los trabajadores humanitarios.

Las amenazas digitales a las organizaciones humanitarias están muy extendidas y son multifacéticas. Se debe prestar atención a la seguridad de los dispositivos móviles, el uso de redes y fuentes de Internet no confiables y potencialmente hostiles, la interceptación de datos y comunicaciones digitales y la seguridad física de los dispositivos y los datos. La esfera digital también presenta oportunidades de recopilación de inteligencia para entidades potencialmente hostiles o poco amistosas. Si bien la seguridad digital a menudo forma parte del ámbito de las tecnologías de la información, el personal de seguridad participa cada vez más en los debates sobre seguridad digital, ya que las amenazas digitales pueden tener importantes repercusiones en la seguridad física de los trabajadores humanitarios. Por ejemplo, el hackeo o el acceso no autorizado a datos sensibles, como los itinerarios de viaje o información personal, puede dar lugar a ataques físicos, secuestros y acoso selectivos por parte de agentes hostiles. El ciberespionaje y la vigilancia pueden permitir que agentes estatales y no estatales controlen los movimientos y las comunicaciones de los trabajadores humanitarios, lo que los hace vulnerables a interceptaciones o emboscadas.

La difusión de información errónea o desinformación a través de canales digitales también puede incitar a las comunidades o grupos armados locales a la hostilidad o a la violencia, lo que supone un peligro directo para el personal. El hurto de dispositivos que contienen datos críticos puede provocar violaciones de la seguridad de la información que comprometan la seguridad de las operaciones, poniendo en riesgo a los trabajadores humanitarios y a las comunidades locales. De esta manera, la convergencia de la seguridad digital y física es fundamental, ya que los fallos en la seguridad digital pueden tener graves consecuencias en el mundo real. El personal de seguridad debe comprender los tipos de amenazas digitales a las que pueden enfrentarse los trabajadores humanitarios y cómo pueden colaborar con otros equipos de la organización para mitigar los riesgos digitales y promover prácticas de higiene digital entre el personal.

6.2.2 Amenazas digitales y riesgos de ciberseguridad

La naturaleza de las amenazas digitales puede variar en función del nivel del objetivo, que puede ser una persona, una organización específica o el sector humanitario en general. Aunque muchas veces se producen superposiciones (por ejemplo, las personas pueden convertirse en víctimas cuando sus organizaciones son objeto de ataques), es conveniente que las organizaciones analicen los riesgos específicos y apliquen medidas para mitigar las amenazas en los tres niveles. Esto puede ser especialmente útil en relación con los riesgos de la información perjudicial.

Agentes de amenaza

Las amenazas digitales pueden proceder de una serie de agentes con diferentes motivos (por ejemplo, económicos, ideológicos o estratégicos). A continuación se citan algunos ejemplos:

- **Ciberdelincuentes.** Los ciberdelincuentes (personas, pequeños grupos, bandas o grandes organizaciones y empresas delictivas) se mueven principalmente por el deseo de obtener beneficios económicos y buscan objetivos que les brinden oportunidades. Algunos también tienen motivaciones ideológicas o políticas.

- **Agentes estatales.** Las organizaciones humanitarias que operan en zonas de conflicto o de gran tensión política pueden correr peligro de ser objeto de ataques accidentales o intencionados por parte de Gobiernos y agentes estatales extranjeros. Las entidades gubernamentales que operan en el ámbito digital suelen estar motivadas por cuestiones de seguridad nacional y otras preocupaciones políticas, y pueden ser sumamente capaces de ejecutar ciberataques exitosos, ejercer la vigilancia digital y realizar campañas de influencia perjudiciales en línea.
- **Agentes armados no estatales.** A medida que los recursos digitales son cada vez más accesibles, aumenta su uso potencial por parte de agentes armados no estatales. Estos grupos pueden utilizar las mismas tácticas que los ciberdelincuentes para obtener beneficios económicos, así como para recopilar información y utilizarla como arma por motivos ideológicos y políticos. Es posible que utilicen campañas de influencia en línea, desinformación y otros ataques selectivos para debilitar las operaciones de una organización o las percepciones de las comunidades locales.
- **Otros.** Los empleados descontentos, o las personas que guardan rencor a la organización o a determinados miembros del personal, pueden suponer una amenaza en la esfera digital, al igual que fuera de ella. Las personas influyentes en las redes sociales con agendas políticas pueden utilizar sus plataformas para difundir información perjudicial sobre las organizaciones humanitarias o el sector humanitario en general. Las amenazas también pueden provenir del público influido por dichas personas o por las campañas en línea.

Tipos de amenazas digitales

A continuación se enumeran algunos de los problemas de seguridad digital a los que pueden enfrentarse los trabajadores humanitarios. Todos ellos pueden superponerse u ocurrir simultáneamente, y pueden traducirse en riesgos para la seguridad física.

Tabla 19 Tipos de amenazas digitales

Amenaza	Descripción
Acoso y discurso de odio en línea	El acoso y las amenazas en línea, incluido el discurso de odio, dirigidos muchas veces a los trabajadores humanitarios de grupos marginados o con funciones orientadas al público. Esto puede incluir campañas selectivas que difundan contenidos provocativos o despectivos dirigidos a incitar a la violencia o a debilitar la credibilidad y la seguridad de los trabajadores humanitarios, de una organización concreta o de la comunidad humanitaria en su conjunto.
Robo de identidad	Robo de información personal.
Ingeniería social	Manipulación de personas para que divulguen información confidencial, muchas veces a través de interacciones aparentemente inocuas.

Amenaza	Descripción
Información errónea, desinformación e información manipulada	La difusión de información perjudicial sobre las organizaciones humanitarias, su personal o su trabajo, que debilita la credibilidad, la confianza y la eficacia de las operaciones. Esto puede incluir campañas en línea o filtraciones de datos que dañen la reputación de la organización o de trabajadores humanitarios individuales. Aunque esta información perjudicial puede ser manipulada deliberadamente, también puede difundirse de forma orgánica en las plataformas de las redes sociales.
<i>Phishing</i> (suplantación de identidad) y estafas por correo electrónico	Concebidos para robar credenciales, introducir programas maliciosos u obtener acceso no autorizado a información sensible. Estos riesgos se han extendido a los dispositivos móviles en forma de <i>smishing</i> (suplantación de identidad a través de mensajes de texto SMS). También están aumentando las estafas potenciadas por la inteligencia artificial (IA), como los ataques de <i>vishing</i> (<i>phishing</i> mediante llamadas de voz, en el que se utiliza la IA para clonar la voz de una persona conocida por el objetivo).
Estafas y fraudes en línea	Estafas financieras dirigidas a organizaciones y a trabajadores humanitarios individuales, a menudo mediante prácticas engañosas en línea.
Hackeo y sistemas de intrusión	Su objetivo es acceder o a los sistemas de la organización o dañarlos, a menudo para robar datos confidenciales o para causar daños operativos.
Robo de datos	Robo de datos sensibles de la organización, como, información sobre los beneficiarios de la ayuda, registros financieros y comunicaciones confidenciales, entre otros.
Ataques de programas maliciosos y de secuestro	Introducción de programas maliciosos, incluidos los programas de secuestro, para bloquear sistemas o datos hasta que se pague un rescate o para dañar los sistemas directamente.
Ciberspionaje y vigilancia	El monitoreo y la vigilancia por parte de agentes estatales o no estatales, especialmente en regiones donde las actividades de las organizaciones humanitarias son vistas con desconfianza, pueden incluir: la interceptación de comunicaciones e información sobre los lugares de distribución de la ayuda, el seguimiento de los movimientos o la geolocalización del personal o de los beneficiarios de la ayuda o la identificación del personal, lo que puede causar nuevos ciberataques o incluso daños físicos. Se han documentado incidentes de agentes estatales que utilizaron programas espía contra las organizaciones. <i>Para obtener más información sobre la vigilancia hostil y las medidas de mitigación relacionadas, véase el capítulo 7.5.</i>

6.2.3 Selección en línea de miembros del personal como objetivos de los ataques

Los ataques en línea, especialmente a través de las redes sociales y otras plataformas, pueden dar lugar al acoso, el abuso, la intimidación y el chantaje directos de los trabajadores humanitarios. La selección directa de objetivos es una amenaza creciente y grave, especialmente para quienes desempeñan funciones orientadas al público o pertenecen a grupos infrarrepresentados o marginados (por ejemplo, las mujeres y las personas que se identifican como LGBTQI+).⁸⁶ El acoso puede adoptar diversas formas, como el ciberacoso, el *doxing* (publicación en línea de información privada sin consentimiento) y la suplantación maliciosa de identidad. El ciberacoso puede consistir en mensajes persistentes y amenazadores, mientras que el *doxing* puede hacer pública información personal sensible (como direcciones y datos familiares). La suplantación maliciosa de identidad, en la que los atacantes crean perfiles falsos para engañar o manchar la reputación de la víctima, puede dañar gravemente las relaciones personales y profesionales, y la credibilidad.

Ejemplo: Acoso en línea en Oriente Medio

Un blog de Jordania publicó fotos de perfiles de aplicaciones de citas gay, lo que provocó una fuerte reacción pública y un peligro potencial para las personas cuyas fotos se publicaron, que se enfrentaron a riesgos inmediatos y significativos, entre ellos, el ostracismo social, el acoso y posibles repercusiones legales. Este incidente remarca la importancia de la seguridad digital y las posibles consecuencias de la exposición digital en entornos hostiles. También destaca la necesidad de que las organizaciones humanitarias proporcionen al personal orientaciones claras sobre la protección de su identidad en línea y la importancia de monitorear los espacios en línea locales en busca de posibles amenazas y de tomar medidas proactivas para mitigar los riesgos.

Fuente: Kumar, M. (2017) *Digital security of LGBTQI aid workers: awareness and response*, Global Interagency Security Forum (<https://gisfprod.wpengine.com/resource/digital-security-of-lgbtqi-aid-workers-awareness-and-response/>).

Los ataques en línea pueden tener profundos efectos psicológicos en sus víctimas, generando estrés, ansiedad y una sensación generalizada de vulnerabilidad. El impacto

86 Para obtener ejemplos más detallados de los riesgos digitales a los que se enfrentan los trabajadores humanitarios LGBTQI+, véase Kumar, M. (2017), *Seguridad digital de los trabajadores humanitarios LGBTQI: concientización y respuesta*, Global Interagency Security Forum (<https://gisfprod.wpengine.com/resource/digital-security-of-lgbtqi-aid-workers-awareness-and-response/>).

puede ser aún más grave cuando la información personal se convierte en un arma en entornos hostiles para determinadas identidades o afiliaciones, o cuando los trabajadores humanitarios ya se enfrentan a riesgos significativos debido a la naturaleza de su trabajo.

Estos ataques directos también son más difíciles de detectar para las organizaciones, y los atacantes pueden incluso ser colegas de la víctima. Todo el proceso de una amenaza digital (identificar el objetivo, encontrar vulnerabilidades, contactar con la víctima, llevar a cabo la amenaza, alcanzar una resolución) puede ocurrir totalmente en línea, lo que hace que sea difícil de detectar para cualquiera que no esté directamente afectado.

Para mitigar estos riesgos, las organizaciones pueden impartir una capacitación integral sobre seguridad digital que abarque comportamientos seguros en línea, cómo reconocer y responder a los riesgos en línea (como el acoso y la explotación) y cómo gestionar las identidades y huellas digitales. Se puede alentar a los trabajadores humanitarios a que utilicen cuentas seguras, activen una configuración de privacidad estricta en las redes sociales y consideren el uso de seudónimos para proteger su identidad. También es aconsejable que las organizaciones cuenten con políticas sólidas para abordar la explotación digital, que ofrezcan directrices claras sobre cómo gestionar los incidentes de acoso y espacios seguros para que el personal afectado pueda plantear sus preocupaciones o denunciar incidentes.

Los servicios de apoyo deben estar disponibles para los afectados, incluidos los recursos de salud mental para ayudar a los trabajadores a afrontar el impacto psicológico de ser el objetivo de los ataques, así como asistencia jurídica para abordar cualquier posible violación de la privacidad o la seguridad. Al crear una red de apoyo sólida y fomentar una cultura de concientización sobre la seguridad digital, las organizaciones pueden ayudar a proteger a su personal de la creciente amenaza de ataques en línea y sus consecuencias potencialmente graves.

► Véase el capítulo 5.4 para obtener más información sobre el cuidado del personal, incluida la asistencia de salud mental.

Respuesta a un ataque directo en línea

A continuación se enumeran los pasos que una organización podría considerar después de un ataque en línea contra una persona.

- **Identificar al agresor.** Identificar al atacante y sus acciones, si es posible.
- **Evaluar las plataformas vulneradas.** Identificar las plataformas o dispositivos comprometidos y restablecer las contraseñas. Cambiar los nombres de usuario y las credenciales si es necesario.

- **Contener la difusión información no deseada.** Ponerse en contacto con las redes sociales o los proveedores de telecomunicaciones para contener la difusión de contenidos no deseados. Asegurarse de la seguridad de la comunicación al hacerlo.
- **Alertar a las instituciones financieras.** Notificar, si es conveniente, a los bancos o a las instituciones financieras si hay demandas o amenazas monetarias.
- **Proteger la integridad de la organización.** Minimizar el impacto en la organización para evitar poner en peligro al resto del personal o dañar la reputación de la organización.
- **Notificar a las autoridades pertinentes.** Según la situación, avisar a las autoridades pertinentes, por ejemplo, a la policía local o a la embajada (si la persona afectada es un ciudadano extranjero).
- **Comunicarse con el personal.** Informar al personal para que reporte toda amenaza adicional directamente al personal de seguridad y a otro personal responsable.
- **Considerar la evacuación o la reubicación.** Considerar la posibilidad de evacuar o reubicar a las personas afectadas si la situación se agrava hasta convertirse en una amenaza física.
- **Limitar la divulgación de información.** Compartir solo la información necesaria para contener la amenaza, evitando revelar detalles sensibles.
- **Documentar el incidente.** Llevar un registro detallado de todas las comunicaciones, amenazas y acciones tomadas. Esto puede ser útil para fines legales y protección futura.
- **Proporcionar asistencia psicosocial.** Ofrecer asesoramiento u otro tipo de asistencia psicosocial al personal afectado.
- **Difundir contramensajes.** Si la información errónea o el acoso son públicos, considerar la publicación de una respuesta oficial controlada para contrarrestar las narrativas falsas y mantener la credibilidad.
- **Revisar y reforzar los protocolos de seguridad.** Una vez resuelto el incidente, revisar y actualizar los protocolos de seguridad digital para prevenir futuros incidentes.
- **Monitoreo continuo.** Continuar monitoreando la presencia en línea de la víctima y las plataformas relacionadas para detectar nuevas amenazas o acoso.

6.2.4 Información perjudicial

La información perjudicial (información errónea, desinformación, información manipulada y discurso de odio) se está convirtiendo rápidamente en una amenaza grave para las organizaciones humanitarias. Con el auge de las redes sociales, las imágenes y los videos generados con IA y el creciente número de sitios web alternativos de intercambio de información, este tipo de amenaza solo aumentará en frecuencia, alcance y gravedad.

La información compartida en contextos de crisis humanitarias puede volverse perjudicial a través de varios mecanismos diferentes —descritos con más detalle a continuación— y puede involucrar a una amplia variedad de agentes externos con diferentes intenciones, objetivos y medios de difusión de la información. La confianza y la credibilidad en las instituciones, las autoridades y las fuentes tradicionales de información han disminuido, lo que deja espacio para la aparición de fuentes alternativas de información, incluidas las redes sociales. Aunque las plataformas alternativas pueden amplificar voces que de otro modo no serían escuchadas, también pueden facilitar que la información perjudicial se transmita sin ser verificada y tenga un alcance sin precedentes entre las audiencias, incluidas las partes interesadas en la acción humanitaria.

Es importante tener en cuenta que las fuentes de la información perjudicial pueden ser agentes con los que las organizaciones humanitarias no suelen relacionarse, como empresas tecnológicas, el sector privado, plataformas de redes sociales, personas influyentes y usuarios en general.

Definiciones clave

La información errónea se refiere a la información inexacta o falsa que se comparte sin intención de engañar. Muchas veces se debe a malentendidos, errores o a una falta de verificación adecuada, más que a un intento deliberado de engañar. Esto es distinto de la desinformación, que es información deliberadamente falsa o engañosa. La información manipulada hace referencia a la información veraz que se saca de su contexto original o se manipula para engañar o causar daño. El discurso de odio es contenido dirigido a un grupo o a una persona por sus características inherentes, como el grupo étnico, la religión o el género.⁸⁷

Impacto en la seguridad

Las organizaciones humanitarias a menudo priorizan la aceptación como su enfoque básico de gestión de riesgos de seguridad, fundamentado en una respuesta basada en los principios de neutralidad, independencia, humanidad e imparcialidad. La información perjudicial es especialmente peligrosa, ya que puede socavar la percepción de una respuesta basada en principios entre las partes interesadas, a menudo con independencia de cualquier medida adoptada por la organización o su personal. Esta información también puede utilizarse para manipular la percepción pública, dando forma a las

87 Para consultar un análisis detallado de las definiciones, véase Wardle, C. (2024) *A conceptual analysis of the overlaps and differences between hate speech, misinformation and disinformation*, Departamento de Operaciones de Paz de las Naciones Unidas (<https://peacekeeping.un.org/en/new-report-finds-understanding-differences-harmful-information-is-critical-to-combating-it>).

narrativas y debilitando la credibilidad de las organizaciones humanitarias. A continuación se citan algunos ejemplos:

- **Propagación de narrativas falsas.** Los agentes pueden difundir narrativas falsas para desacreditar a las organizaciones humanitarias, presentándolas como organismos sesgados o motivados políticamente, incluso como pantalla para el espionaje. Esto siembra desconfianza, debilita el apoyo público y justifica las restricciones de acceso a las zonas de crisis. Incluso la información verdadera sobre los esfuerzos de ayuda humanitaria puede ser manipulada. Después de los terremotos de 2023 en Turquía, se difundió, y amplificó en las redes sociales, una noticia en la que se afirmaba que la Media Luna Roja turca vendía tiendas de campaña, lo que intensificó las críticas a la respuesta del gobierno ante la catástrofe. Esta manipulación debilitó la confianza pública tanto en el Gobierno como en la Media Luna Roja turca.⁸⁸
- **Acusaciones de conductas indebidas.** Las campañas de desinformación pueden acusar equivocadamente a los trabajadores humanitarios de delitos o conductas indebidas, como corrupción o colaboración con las fuerzas enemigas, lo que perjudicaría su reputación y podría generar repercusiones jurídicas u operacionales, como la expulsión. Las organizaciones humanitarias pueden ser acusadas de difundir información errónea o desinformación.
- **Difusión de información falsa.** La desinformación, como la información falsa sobre distribuciones u otras intervenciones difundida en línea, puede causar confusión, entorpecer las operaciones y dañar la confianza entre las organizaciones y las comunidades. La información falsa que se aprovecha de las sensibilidades culturales o religiosas, como los rumores sobre las campañas de vacunación, puede incitar a la violencia contra los trabajadores humanitarios y obstaculizar operaciones críticas. La desinformación también puede crear percepciones falsas de sesgo en la distribución de la ayuda.
- **Desacreditación de los informes humanitarios.** Los agentes estatales pueden utilizar la información errónea para debilitar la credibilidad de los informes que documentan los abusos o las crisis de derechos humanos, a menudo calificándolos de “falsos” para desestimar sus conclusiones. Por ejemplo, Myanmar ha negado la existencia de la crisis humanitaria que afecta a los rohinyás.
- **Suplantación de identidad.** Los agentes pueden hackear las comunicaciones de las organizaciones humanitarias para difundir directamente información falsa.
- **Utilización de la información como un arma.** Los agentes hostiles pueden hackear los sistemas de datos para alterar los registros o filtrar información sensible, a efectos de debilitar la credibilidad de la organización o atacar a grupos específicos. En 2022 un hackeo informático expuso los datos de más de 515 000 personas vulnerables, lo que las puso en peligro y dañó la confianza en el CICR.⁸⁹

88 Insecurity Insight. (2023). *The role of social media in the spreading of the Turkish Red Crescent Tent Sale Story in Türkiye*. Social Media Monitoring (<https://insecurityinsight.org/wp-content/uploads/2023/08/The-Spreading-of-the-Turkish-Red-Crescent-Tent-Sale-Story.pdf>).

89 Comité Internacional de la Cruz Roja. (2022). *Ciberataque contra el CICR: qué sabemos* (www.icrc.org/en/document/cyber-attack-icrc-what-we-know).

- **Incitación a la violencia y el discurso de odio.** Las publicaciones en las redes sociales pueden utilizarse para incitar a la violencia u otros comportamientos negativos hacia el personal, los lugares, los bienes y las operaciones humanitarias. El discurso de odio, que se dirige a grupos específicos en función de su identidad, conlleva problemas reales e inmediatos.

Ejemplo: Ejemplos de desinformación en Ucrania

La desinformación afecta todo, desde la seguridad personal y la reputación de las organizaciones humanitarias hasta la percepción general del sector humanitario y su capacidad para alcanzar los objetivos humanitarios y ejecutar los programas.

Durante el conflicto en Ucrania, agentes afiliados a Rusia emplearon la desinformación para obstaculizar y manipular las operaciones humanitarias. Un caso significativo fue la difusión de información falsa sobre las rutas de evacuación. Los canales prorrusos de Telegram afirmaron falsamente que el ejército ucraniano estaba bloqueando determinadas rutas de evacuación o que estas rutas estaban siendo atacadas. Esto causó confusión y miedo entre la población civil, que evitó el uso de rutas de evacuación seguras o retrasó su salida de las zonas peligrosas.

El CICR también se enfrentó a una importante campaña de desinformación dirigida contra sus actividades humanitarias en Ucrania cuando agentes afiliados a Rusia difundieron noticias falsas, en las que se afirmaba que la organización estaba implicada en evacuaciones forzosas de ucranianos a Rusia y en el establecimiento de oficinas en el sur de Rusia para filtrar ucranianos. Las acusaciones infundadas, que se difundieron por las redes sociales y aparecieron ocasionalmente en los principales medios de comunicación, pretendían desacreditar la labor del CICR entre los ucranianos y poner en peligro sus operaciones.

Fuentes: Center for Civilians in Conflict (2023) *When words become weapons: the unprecedented risks to civilians from the spread of disinformation in Ukraine* (<https://civiliansinconflict.org/publications/research/when-words-become-weapons-the-unprecedented-risks-to-civilians-from-the-spread-of-disinformation-in-ukraine>) y Comité Internacional de la Cruz Roja (2022) *Ucrania: desinformación sobre las actividades del CICR* (www.icrc.org/en/document/ukraine-addressing-misinformation-about-icrcs-activities).

Diagnóstico de riesgos de la información perjudicial

Además de garantizar que las amenazas digitales, incluida la información perjudicial, se incorporen a los procesos existentes de diagnóstico de riesgos, las organizaciones deben preparar al personal responsable, como el personal de redes sociales, con las herramientas necesarias para considerar directamente los riesgos de la información perjudicial.

► Para obtener más información sobre el diagnóstico de riesgos, véase el capítulo 4.1.

A continuación se ofrece un ejemplo de un proceso de diagnóstico de riesgos para la información potencialmente perjudicial, adaptado de la herramienta Mis/Disinfo Assessment de Médicos sin Fronteras.⁹⁰

- **Comprender el objetivo.** ¿Cuál es el objetivo (persona, programa, organización, sector) y cómo se está atacando?
- **Comprender el objetivo.** La información perjudicial, ¿se comparte con la intención de causar un daño o se vuelve perjudicial de forma orgánica debido a interpretaciones erróneas y a su difusión generalizada?
- **Comprender la fuente.** ¿Procede la información de una fuente concreta (por ejemplo, un grupo o una persona influyente)? ¿Se trata de información totalmente nueva o ya se compartió antes?
- **Clasificar.** ¿Representa este contenido un riesgo bajo o alto? (Consultar la tabla 20.)
- **Evaluar.** ¿Qué tipo de riesgo supone? (Consultar la tabla 21.)

Tabla 20 Clasificación del riesgo de los contenidos

Bajo	Medio	Alto	Urgente
Malentendido/ información errónea inofensiva	Información errónea que puede causar daños	Información deliberadamente perjudicial que involucra a la organización o a su personal	Propaganda dirigida contra la organización o su personal

90 Véase GISF (2023) *Online risk to real-life harm: disinformation and social listening workshop resources* (www.gisf.ngo/resource/online-risk-to-real-life-harm-disinformation-and-social-listening-workshop-resources/).

Tabla 21 Evaluación del riesgo del contenido

	Bajo	Medio	Alto	Urgente
Gravedad	Sin riesgo de daños o amenazas en la vida real	Riesgo moderado de daño	Riesgo indirecto de daños en la vida real	Amenaza directa de daños en la vida real
Escala	Poca atención	Atención moderada, algunos comentarios	Atención significativa en poco tiempo	Se viraliza
Objetivo	Sin un objetivo específico	Repercute indirectamente en la organización y su personal	Repercute directamente en la organización y su personal	Se dirige directamente a la organización y a su personal
Fuente	Fuente de alcance limitado	Movimiento localizado, <i>ad hoc</i>	Coordinado, intencionado	Redes con alcance significativo

Medidas de mitigación

Una vez evaluados los riesgos de información perjudicial, pueden aplicarse diversas medidas de mitigación, que se enumeran abajo. Deben evaluarse cuidadosamente y adaptarse a los riesgos específicos, ya que lo que funciona bien en un caso puede empeorar la situación en otro.

- **Evaluar el panorama informativo.** Comprenda dónde y cómo obtienen la información las comunidades objetivo identificando las fuentes y los canales de comunicación de confianza. Esto ayuda a identificar y contrarrestar los discursos perjudiciales antes de que se difundan ampliamente.⁹¹ Las organizaciones deben asegurarse de que el mapeo y el análisis de los actores incluyan a personas o grupos que puedan influir en la difusión de información perjudicial.
- **Desarrollar y aplicar estrategias de comunicación.** Elabore estrategias de comunicación sólidas que incluyan el monitoreo de las redes sociales para detectar contenidos positivos y negativos relacionados con la organización, su trabajo y el sector humanitario en su conjunto. Cree una fuerte presencia en las redes sociales en las plataformas relevantes de acuerdo al contexto, y actualícelas regularmente con contenidos positivos, honestos y transparentes que destaquen los mensajes

⁹¹ Para ello, puede ser útil una evaluación del ecosistema de información. Consulte, por ejemplo, Internews (2015) *Mapping information ecosystems to support resilience* (https://internews.org/wp-content/uploads/legacy/resources/Internews_Mapping_Information_Ecosystems_2015.pdf).

centrales y los principios humanitarios. “Verificado”, por ejemplo, es una iniciativa implementada por las Naciones Unidas en colaboración con Purpose para combatir la información errónea relacionada con la COVID-19.

- **Supervisar los contenidos perjudiciales y los cambios en las percepciones.** Invierta en iniciativas de “escucha” de las redes sociales para supervisar las opiniones a lo largo del tiempo y detectar el contenido negativo antes de que se convierta en una amenaza real contra la seguridad.⁹² Las organizaciones también pueden utilizar recursos públicos que supervisan y analizan contenidos para ayudar a detectar posibles amenazas, información perjudicial y percepciones públicas que puedan afectar la seguridad y la eficacia de las actividades humanitarias.⁹³
- **Sensibilizar y capacitar al personal.** Brinde capacitación sobre alfabetización digital al personal, centrándose en cómo manejar los contenidos falsos y gestionar su impacto digital. Incite al personal a actuar como si fueran los ojos y los oídos de la organización en Internet y a reportar los posibles riesgos.
- **Crear redes sólidas.** Desarrolle redes sólidas con los socios dentro y fuera del contexto humanitario para el apoyo mutuo y la verificación de la información. Las relaciones preexistentes pueden mitigar los riesgos reputacionales y permitir el rápido intercambio de contradiscursos. Establecer relaciones con los medios de comunicación y las emisoras de radio locales también puede ser una forma eficaz de compartir información precisa sobre las actividades humanitarias en la zona.
- **Concienciación.** Colabore con otras organizaciones, responsables políticos y medios de comunicación para concienciar sobre los contenidos perjudiciales y para presionar a las empresas de las redes sociales para que actúen de forma responsable.
- **Establecer funciones y responsabilidades claras y la colaboración entre equipos.** Asegúrese de que las funciones y las responsabilidades estén claras respecto al monitoreo y a la documentación de la información perjudicial o que pueda causar daños, que el personal reciba la formación y el apoyo adecuados y que existan protocolos claros sobre cuándo y cómo se compartirá la información pertinente con otras partes de la organización, incluido el personal de seguridad.

En general, es aconsejable que las organizaciones dispongan de una estrategia para responder eficazmente a los incidentes de información perjudicial. Las acciones de respuesta pueden incluir lo siguiente:

- **Reportar los contenidos perjudiciales.** Utilice las herramientas de denuncia de las plataformas de redes sociales para señalar los contenidos perjudiciales y comuníquese directamente con las empresas de redes sociales para agilizar el proceso de revisión y eliminación.

92 Iacucci, A. (2023) *Social Listening*, [diapositivas], Global Interagency Security Forum (<https://gisf.ngo/resource/online-risk-to-real-life-harm-disinformation-and-social-listening-workshop-resources/>).

93 Por ejemplo, Insecurity Insight (s.f.) *Social media monitoring* (<https://insecurityinsight.org/projects/aid-in-danger/social-media-monitoring>).

- **Participar en la verificación de los hechos y en la elaboración de un contradiscurso.** Considere la posibilidad de colaborar con entidades de verificación de los hechos para confirmar la información y elaborar un contradiscurso para corregir las narrativas falsas. Una campaña eficaz de contradiscurso supone comprender los principales nodos y enlaces a través de los cuales se difundió originalmente la información y dirigirse a esas mismas redes. Esto puede ayudar a mantener la confianza y la credibilidad, y evitar al mismo tiempo la difusión de información errónea. Sin embargo, en algunos casos puede ser mejor no llamar más la atención sobre la información falsa.
- **Reconstruir la confianza tras campañas de información perjudicial.** Céntrese en restablecer la confianza de las comunidades afectadas mediante una comunicación y un compromiso transparentes. Esto puede incluir demostrar cómo la organización protege los datos que recopila en relación con las poblaciones objetivo y otros agentes locales, y que ha tenido en cuenta los posibles daños y riesgos si cayeran en manos equivocadas.
- **Colaboración con las autoridades.** Si el contenido supone una amenaza inmediata, considere la posibilidad de notificarlo a las fuerzas del orden o a las autoridades pertinentes.

Respuesta a la incitación a la violencia en las redes sociales

La incitación a la violencia en las redes sociales está prohibida en la mayoría de las plataformas, incluida Meta (Facebook e Instagram), que tiene normas comunitarias contra este tipo de contenidos. Si una organización encuentra publicaciones que incitan a la violencia, puede utilizar las herramientas de denuncia de la plataforma o comunicarse directamente con la empresa para señalar que el contenido infringe las normas de la comunidad o que puede provocar perjuicios potenciales, por lo que debe ser revisado y posiblemente eliminado. Es conveniente proporcionar información detallada a fin de agilizar el proceso de revisión. Si el contenido supone una amenaza inmediata, debe notificarse a las fuerzas del orden o a las autoridades pertinentes, según corresponda, para garantizar una respuesta rápida.

Las actividades de seguimiento pueden incluir:

- Señalar los contenidos que puedan resultar perjudiciales en el futuro para su monitoreo continuo.

- Registrar las medidas adoptadas y los resultados después de un incidente para informar diagnósticos de riesgos y medidas de mitigación de riesgos y respuesta futuros.
- Realizar una revisión posterior a la acción para identificar las lecciones que permitan mejorar los esfuerzos futuros, tal como se haría si se tratara de un incidente de seguridad crítico.

6.2.5 Las tecnologías de la comunicación digital y sus riesgos

Muchos riesgos proceden del uso de redes no confiables, es decir, redes que no están bajo el control de la organización. Cualquier red con un nivel de seguridad desconocido puede considerarse intrínsecamente insegura. La siguiente sección presenta una lista de ejemplos de riesgos asociados a las tecnologías de comunicación digital. No pretende ser exhaustiva, sino más bien proporcionar información sobre los ámbitos de interés común.

Redes móviles

Las redes móviles tienen fallas de seguridad inherentes, como la susceptibilidad al acceso no autorizado y a la interceptación de datos, sobre todo cuando la supervisión regulatoria es poco estricta o está comprometida.

Uno de los principales riesgos del uso de redes móviles es la posibilidad de que partes hostiles intercepten flujos de datos. Estas partes pueden ser Gobiernos locales, bandas, organizaciones delictivas o estados con acceso a las redes. Esta interceptación podría dar lugar a la filtración de comunicaciones sensibles o datos sobre las operaciones, como la ubicación del personal y los movimientos operacionales.

Wifi público

Las fuentes públicas de wifi, como el wifi gratuito o de pago en aeropuertos, cafeterías y hoteles, son un medio común y a menudo necesario de conexión a Internet para el personal que viaja. El principal vector de ataque son los ataques de intermediario, en los que un tercero malintencionado espía en la red, interceptando o interfiriendo las comunicaciones.

No hay forma de saber si el operador de una red wifi la configuró de forma segura, y el riesgo de que un ataque de intermediario tenga éxito aumenta cuando no es así.

También existe el riesgo de que un actor malicioso establezca un “gemelo malvado”, una red wifi falsa que utiliza el mismo nombre que una fuente de wifi legítima, lo que provoca que los usuarios se conecten a la red falsa sin darse cuenta. El atacante podrá entonces interceptar todo el tráfico de Internet en esta red wifi falsa. Por defecto, los teléfonos y los dispositivos pueden conectarse automáticamente a redes wifi “conocidas”, lo que significa que un atacante podría configurar esta misma red en un aeropuerto, y decenas o incluso cientos de dispositivos podrían conectarse automáticamente a ella.

Proveedores locales de servicios de Internet

Los proveedores locales de servicios de Internet pueden ofrecer una conexión más rápida y estable para oficinas permanentes o instaladas por periodos prolongados, así como en lugares donde se ejecutan proyectos de corta duración. Es aconsejable tener cuidado con estas conexiones y tomar medidas para asegurarlas.

Aunque los proveedores de servicios de Internet probablemente no representen una amenaza significativa, cualquier sistema o dispositivo conectado a Internet corre el riesgo de sufrir un ataque. Los ciberdelincuentes o algunos agentes estatales podrían infiltrarse en los proveedores de servicios de Internet, lo que podría dar lugar a la interceptación de comunicaciones y datos confidenciales. Disponer de capas adicionales de cifrado puede aumentar la protección.

Riesgos relacionados con la IA

Las herramientas de IA representan oportunidades y retos para las organizaciones humanitarias. Para los trabajadores humanitarios, los retos incluyen la posibilidad de que se produzcan filtraciones de datos y la propagación de contenidos sesgados o inexactos. Los actores hostiles pueden utilizar la IA para amplificar la información errónea, realizar ataques de suplantación de identidad o incluso ejercer una vigilancia basada en la IA para controlar y atacar a los trabajadores humanitarios. Estos riesgos subrayan la necesidad de actuar con cautela y respetar estrictamente los protocolos de seguridad al interactuar con la IA, tanto en lo que se refiere al uso de herramientas de IA como a la protección frente a las amenazas de agentes hostiles impulsadas por la IA. También existe una creciente preocupación por el uso de sistemas de IA en la selección de objetivos militares, que implica los riesgos de identificación incorrecta y de posibles ataques erróneos. Organizaciones como el CICR están alertando sobre este riesgo.ⁱ

ⁱ Viveros Álvarez, J.S. (2024) “The risks and inefficacies of AI systems in military targeting support” *Derecho y Políticas Humanitarias*, Comité Internacional de la Cruz Roja (<https://blogs.icrc.org/law-and-policy/2024/09/04/the-risks-and-inefficacies-of-ai-systems-in-military-targeting-support/>).

Estaciones públicas de carga

Las estaciones públicas de carga, como las que se encuentran en los aeropuertos, las estaciones de tren y los hoteles, incluyen tomas de corriente estándar y puertos de carga USB. El mayor riesgo está vinculado específicamente a los puertos de carga USB.

El *juice jacking* consiste en colocar un pequeño dispositivo en un puerto de carga USB que puede enviar comandos a un teléfono, una tableta u otro dispositivo conectado para cargarse. Esto podría utilizarse para instalar programas maliciosos o permitir el acceso remoto de un atacante. Cuando no es posible acceder a un tomacorriente de pared para cargar un dispositivo, puede conectarse un bloqueador de datos USB al puerto de carga USB antes de utilizarlo para protegerse de un posible ataque de este tipo.

6.2.6 Controles de seguridad e higiene digital

Medidas de mitigación organizacional

Evaluación de las necesidades tecnológicas

Para comprender las amenazas que una organización y su personal pueden enfrentar, y para implementar las medidas de mitigación de riesgos adecuadas, es importante determinar qué tecnología puede utilizar el personal para realizar su trabajo y los diferentes riesgos de los distintos tipos de proyectos. Esto implica comprender el alcance del programa y las actividades digitales de todas las partes interesadas. Esta evaluación de las necesidades tecnológicas abarcaría equipos y dispositivos de comunicación, así como programas informáticos y aplicaciones.

Por lo general, las organizaciones tendrán menos control y visibilidad sobre los dispositivos de uso personal, aunque estos pueden correr el mismo riesgo. A fin de gestionar los riesgos asociados a los dispositivos personales, las organizaciones pueden impartir una capacitación para el personal sobre buenas prácticas de higiene digital (independientemente del dispositivo que se utilice), establecer protocolos sobre el uso de dispositivos personales para fines laborales y restringir el acceso a información sensible en los dispositivos personales.

Diagnósticos de riesgos

Para evaluar los riesgos de manera eficaz, es conveniente adoptar un enfoque colaborativo entre equipos. Los equipos informáticos pueden centrarse en evaluar las amenazas potenciales a los equipos, los programas y los sistemas informáticos, mientras que los directivos pueden revisar el programa informático que utilizan sus equipos para detectar las vulnerabilidades. El personal de comunicación puede realizar un análisis del contexto digital para entender cómo las distintas partes interesadas podrían utilizar los medios digitales, y el personal de seguridad puede identificar las vulnerabilidades de seguridad y vincularlas con amenazas físicas más amplias derivadas de la exposición digital. El personal de los programas puede evaluar los riesgos de abusos, de selección

de objetivos de actos delictivos o de manipulación relacionados con los aspectos digitales de sus programas, como las transferencias de efectivo, la incidencia o la recopilación de datos. Es fundamental reconocer que, al igual que las amenazas físicas, las amenazas digitales no afectan a todos por igual. Cualquier diagnóstico de riesgos tendrá que ser inclusivo y considerar cómo los diferentes perfiles de identidad pueden afectar los riesgos digitales.

Las organizaciones también deben recordar que la seguridad digital del personal, de la organización y de las comunidades pertinentes se superponen. Una violación de la seguridad en un área repercutirá en las demás, y todos los diagnósticos de riesgos y las medidas de mitigación deben considerar su interdependencia.⁹⁴

Los trabajadores humanitarios también pueden convertirse en víctimas colaterales de un ataque digital dirigido contra un tercero que almacena los datos de su organización o cuyos servicios utiliza la organización; esto también debe tenerse en cuenta en todo diagnóstico de riesgos. Por último, las organizaciones son responsables de cumplir la normativa pertinente en materia de protección de datos (como el Reglamento General de Protección de Datos [RGPD] de la Unión Europea).

► Para obtener más información sobre el diagnóstico de riesgos, véase el capítulo 4.1.

Protocolos de seguridad repetibles

Los protocolos ayudan a los usuarios a saber cómo proceder y a realizar las operaciones de forma sistemáticamente segura. Elaborar protocolos sencillos y repetibles, es decir, estandarizados, bien documentados y fáciles de aplicar siempre de la misma manera, ayuda a garantizar su cumplimiento sistemático. Los protocolos pueden incluir procedimientos para solicitar y adquirir dispositivos, reportar dispositivos perdidos o robados, obtener conexión a Internet y buenas prácticas de comportamiento de los usuarios.

VPN y seguridad web

Las redes privadas virtuales (VPN) y las herramientas de seguridad web protegen los dispositivos, los datos y las comunicaciones de los usuarios finales mientras se desplazan y utilizan redes no fiables. Una VPN cifra los datos cuando salen del dispositivo del usuario para que permanezcan protegidos y ocultos frente a agentes hostiles mientras atraviesan redes wifi, redes móviles e Internet que no son confiables. La seguridad web suele consistir en el filtrado de contenidos web y es una primera línea de defensa fundamental contra programas maliciosos, sitios web maliciosos, ataques de suplantación de identidad y otras amenazas virtuales. En combinación con una herramienta de VPN que cifre el tráfico de Internet, puede proporcionar una protección y un blindaje significativos para los usuarios finales y sus datos.

94 Para obtener más información, véase Davis, J. *et al.* (2020), Module 4, Digital security, en *Security to go: a risk management toolkit for humanitarian aid agencies*, 4ª edición, Global Interagency Security Forum (<https://gisf.ngo/resource/security-to-go/>).

Utilizar sitios web cifrados con SSL que muestren el ícono del candado es una buena idea cuando se usa una conexión wifi no segura. Muchos sitios web gubernamentales, especialmente en los países donde se realiza la mayor parte del trabajo humanitario, se han visto comprometidos en el pasado y no están configurados para cifrar los datos. Es necesario tener precaución.

Las soluciones de seguridad empresarial ofrecen funciones de seguridad avanzadas, integrales y para toda la organización con el fin de proteger los datos de la organización y a los usuarios, incluso en redes remotas o no seguras. Algunas herramientas son Confianza Cero, SSE (Secure Service Edge) y SASE (Secure Access Service Edge). Las soluciones empresariales van más allá del cifrado de sitios web individuales y ofrecen un marco de seguridad más amplio para proteger todo el ecosistema digital de una organización.

Herramientas de comunicación basadas en aplicaciones

A la hora de analizar los riesgos y los beneficios de las distintas aplicaciones y plataformas de comunicación, se deben considerar tres cosas.

- **¿Cuál es la seguridad de la aplicación?** Las aplicaciones de código abierto alojadas en países con leyes sólidas de protección de la privacidad y buenas prácticas de seguridad serán más seguras que las aplicaciones alojadas en países donde el Gobierno controla la red y las leyes de protección de la privacidad se ignoran o no se aplican.
- **¿A quién pertenecen los datos de la aplicación?** ¿Los datos se almacenan solo en el propio dispositivo? ¿Se almacenan los datos en los servidores de una empresa privada, gubernamental o sin fines de lucro? Es importante saber dónde se encuentran los datos y de qué modo se evalúa adecuadamente la seguridad de una aplicación concreta.
- **¿Qué está disponible o en uso actualmente en los países donde se opera?** Una aplicación muy segura puede ser una mala opción si no puede descargarse en un país determinado, si no puede instalarse en los dispositivos utilizados por la mayoría del personal o si es desconocida o difícil de usar.

Gestión de dispositivos móviles

Una plataforma de gestión de dispositivos móviles supervisa y protege los dispositivos móviles. Asimismo, permite la gestión remota centralizada de los dispositivos, que incluye la capacidad de borrar datos confidenciales de los dispositivos perdidos o robados. Si esto no es posible, cifrar los dispositivos y utilizar contraseñas seguras y carpetas de archivos privadas es una buena medida.

Seguridad física de los dispositivos

La seguridad física es un aspecto importante para mantener la seguridad de las personas, los dispositivos y los datos. Si los agentes hostiles pueden tener acceso a un dispositivo, es probable que puedan comprometerlo. El riesgo de filtración de datos se reduce considerablemente si los archivos están cifrados y los dispositivos están protegidos con contraseña, y si nunca se dejan sin vigilancia. Reportar lo antes posible a los equipos informáticos y de seguridad sobre la pérdida o el robo de un dispositivo permite una respuesta rápida para mitigar el posible impacto. Puede haber casos en los que el personal tenga que entregar temporalmente los dispositivos a las autoridades para su inspección. Si hay sospechas de manipulación indebida del aparato, o si el dispositivo desaparece de la vista del miembro del personal durante algún tiempo, el departamento de informática y seguridad querrán saberlo.

Aunque no siempre son prácticas, las bolsas de viaje Faraday pueden proteger los dispositivos móviles de posibles ataques durante los viajes. Las ondas electromagnéticas, como las que se utilizan para las comunicación móviles y wifi, no pueden entrar en la bolsa, por lo que se bloquean los intentos de conexión no deseados o de vigilancia de los dispositivos móviles.

Prácticas de higiene digital

La higiene digital se refiere a las prácticas estándar para mantener la seguridad digital y mitigar los riesgos digitales. La higiene digital puede ayudar a mantener una base de seguridad digital consistente fomentando comportamientos y protocolos buenos y repetibles. A continuación se ofrecen algunas sugerencias de buenas prácticas de higiene de la seguridad, que pueden formar parte de los protocolos y la capacitación sobre seguridad de una organización.⁹⁵

Utilice contraseñas seguras y autenticación multifactor

- **Cree contraseñas seguras.** El personal puede crear contraseñas fuertes y complejas usando una combinación de caracteres, actualizándolas periódicamente y evitando reutilizar las mismas contraseñas en varias cuentas. Una buena práctica es utilizar tres palabras aleatorias para generar contraseñas fáciles de recordar, pero seguras.
- **Utilice la autenticación multifactor.** La autenticación multifactor proporciona una capa adicional de protección contra el robo o descubrimiento de contraseñas.

Instale las actualizaciones de los dispositivos y las aplicaciones

- **Mantenga todo actualizado.** Asegúrese de que todos los sistemas operativos y las aplicaciones instaladas están actualizados antes de viajar. Si está disponible, puede utilizarse un sistema de gestión de dispositivos móviles para mantener actualizados automáticamente los dispositivos y las aplicaciones.

⁹⁵ Para obtener más orientaciones, véase ACT Alliance (2019) *Basic cyber security: A guide for all to manage digital security* (https://gisf.ngo/wp-content/uploads/2021/10/ACT_Digital_Security_Guidelines_2019.pdf).

Refuerce los dispositivos

- **Configuración de seguridad del dispositivo.** Los dispositivos no suelen entregarse con una configuración óptima de seguridad, por lo que las organizaciones deben establecer pautas para el fortalecimiento de la seguridad de los dispositivos como parte de sus políticas de seguridad. En este sentido, el personal puede configurar contraseñas seguras para el dispositivo, desactivar las aplicaciones y los servicios innecesarios, activar el cifrado del dispositivo, activar los modos de bloqueo y desactivar las radios inalámbricas cuando no se necesiten.

Minimice el uso de aplicaciones y redes sociales

- **Limite el uso de las aplicaciones.** Cada aplicación instalada es una posible vulnerabilidad. Es aconsejable reducir al mínimo el uso innecesario de aplicaciones, especialmente durante los viajes, y considerar la eliminación de las que no sean necesarias.
- **Utilice aplicaciones de comunicación seguras.** Las aplicaciones de comunicación cifrada de extremo a extremo son preferibles, pero puede realizarse una evaluación exhaustiva para determinar la aplicación más segura para su uso en diferentes contextos.
- **Precauciones en las redes sociales.** Evite publicar en las redes sociales mientras viaja, ya que puede filtrar información. Desactive los servicios de ubicación y revise la configuración de privacidad y uso compartido de todas las aplicaciones.
- **Metadatos de las fotos.** Desactive los ajustes de ubicación al hacer fotos y elimine los metadatos de las imágenes antes de compartirlas.

Refuerce la seguridad del correo electrónico

- **Sea cauteloso con los correos electrónicos.** Evite hacer clic en enlaces o abrir archivos adjuntos de fuentes desconocidas. Verifique la dirección de correo electrónico del remitente, especialmente cuando se trate de información sensible.

Gestión y cifrado de datos

- **Recuerde cifrar los datos sensibles.** Asegúrese de que todos los archivos confidenciales están cifrados antes de almacenarlos o compartirlos. También se debe anonimizar la información de identificación personal.
- **Intercambio seguro de archivos.** Utilice métodos seguros para compartir archivos, como servicios de correo electrónico cifrado o plataformas seguras para compartir archivos.
- **Haga copias de seguridad.** Realice copias de seguridad periódicas de los datos importantes en un almacenamiento seguro y cifrado para evitar pérdidas.
- **“Limpie mientras trabaja”.** Analice el uso de datos al desplazarse de un lado a otro: datos como las fotos, que son seguros de usar y compartir en un lugar, pueden plantear riesgos de seguridad si se ven en otro. Para mitigar estos riesgos, envíe las fotos necesarias por medios electrónicos seguros y luego elimínelas rápidamente del dispositivo.

- **Borre datos.** Elimine los datos de forma segura cuando ya no los necesite.
- **Revise y controle el acceso.** Valide periódicamente la exactitud de los datos, controle el acceso y mantenga registros de auditoría para garantizar que solo el personal autorizado puede acceder a los datos críticos. El personal debe tener especial cuidado con el tipo de datos que recopila, cómo los almacena y quién tiene acceso a ellos. El personal de seguridad puede recopilar y tener acceso a información personal muy delicada sobre el personal y otros agentes, y debe ser consciente del riesgo de que la información se utilice para perjudicar a la organización, a su personal, a las personas a las que intenta ayudar o a sus operaciones, incluso si se comparte con actores con intereses legítimos, como agentes estatales.⁹⁶

Utilice Internet de forma segura

- **Use VPN en redes wifi públicas.** Utilice siempre una VPN cuando acceda a Internet a través de redes wifi públicas.
- **Evite los sitios web no seguros.** Reconozca y evite los sitios web que no estén protegidos con HTTPS (un protocolo seguro diseñado para enviar datos entre un navegador web y un sitio web).

Reporte los incidentes

- **Respete los protocolos de reporte establecidos.** Notifique los posibles incidentes de seguridad digital, como intentos de suplantación de identidad o posibles violaciones de la seguridad de los datos.

Las organizaciones deben considerar la posibilidad de organizar sesiones y seminarios de formación para el personal con el objetivo de mejorar la alfabetización digital y cubrir las buenas prácticas de higiene digital relativas a la tecnología de la organización y la personal, incluidas las redes sociales. El repaso y la actualización periódicos sobre las nuevas amenazas digitales son cruciales para garantizar que los trabajadores humanitarios estén alerta y bien preparados para protegerse a sí mismos y a sus colegas en el espacio digital.

Más información

Orientación y herramientas de seguridad digital

Access Now. (2020). *Digital security helpline: Self-doxing guide* (<https://gisf.ngo/resource/access-now-digital-security-helpline-self-doxing-guide/>).

ACT Alliance. (2019). *Basic cyber security. A guide for all to manage digital security* (https://gisf.ngo/wp-content/uploads/2021/10/ACT_Digital_Security_Guidelines_2019.pdf).

⁹⁶ Como lo demuestra el intercambio de información personal de refugiados rohinyás por parte de la ACNUR con el Gobierno de Bangladesh, que a su vez compartió la información con las autoridades de Myanmar. Véase Human Rights Watch (2021) *UN shared Rohingya data without informed consent* (www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent).

Davis, J. et al. (2020). Module 4, Digital security” en *Security to go: a risk management toolkit for humanitarian aid agencies*. 4ª edición. Global Interagency Security Forum (<https://gisf.ngo/resource/security-to-go/>).

Front Line Defenders. (s.f.). Security in-a-box (<https://securityinbox.org/en/>).

Global Interagency Security Forum. (2021). Module 2: Information management. En *Keeping up with COVID-19: essential guidance for NGO security risk managers* (<https://gisfprod.wpengine.com/resource/keeping-up-with-covid-19-essential-guidance-for-ngo-security-risk-managers-module-a2-information-management/>).

Global Interagency Security Forum. (s.f.a). Resources & background materials (DCS). *Digital cyber security*. (www.gisf.ngo/themes/digital-cyber-security/resource-background-materials-dcs/).

Global Interagency Security Forum. (s.f.b). 2. *Digital security*. NGO Security Toolbox (www.gisf.ngo/toolbox-pwa/resource/2-digital-security/).

Global Interagency Security Forum. (s.f.c). *Digital security resources. Communications technology and humanitarian delivery* ([/www.gisf.ngo/themes/communications-technology-and-humanitarian-delivery/digital-security-resources/](http://www.gisf.ngo/themes/communications-technology-and-humanitarian-delivery/digital-security-resources/)).

Tactical Tech. (s.f.). *Holistic security manual* (<https://holistic-security.tacticaltech.org/index.html>).

Investigación y análisis sobre seguridad digital

Al Achkar, Z. (2021). Digital risk: How new technologies impact acceptance and raise new challenges for NGOs” en Global Interagency Security Forum (Ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (<https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/>).

Comité Internacional de la Cruz Roja. (24 de junio de 2022). Ciberataque contra el CICR: qué sabemos (www.icrc.org/en/document/cyber-attack-icrc-what-we-know).

Global Interagency Security Forum. (2023a). *The intersection of technology and human security*. [Podcast]. Evolving NGO security risk management (www.gisf.ngo/resource/evolving-ngo-security-risk-management-ep4-the-intersection-of-technology-and-human-security-gisf-podcast/).

Global Interagency Security Forum. (2023b). *Humanitarian security in an age of uncertainty: the intersection of digital and physical risks* (www.gisf.ngo/resource/humanitarian-security-in-an-age-of-uncertainty-the-intersection-of-digital-and-physical-risks/).

Human Rights Watch. (15 de junio de 2021). UN shared Rohingya data without informed consent. (www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent).

Kumar, M. (2017). *Digital security of LGBTQI aid workers: awareness and response*. Foro Europeo Interinstitucional para la Seguridad (<https://gisfprod.wpengine.com/resource/digital-security-of-lgbtqi-aid-workers-awareness-and-response/>).

Rodenhäuser, T., Staehelin, B. y Marelli, M. (2022). Safeguarding humanitarian organizations from digital threat. *Derecho y Políticas Humanitarias*. Comité Internacional de la Cruz Roja (<https://blogs.icrc.org/law-and-policy/2022/10/13/safeguarding-humanitarian-organizations-from-digital-threats/>).

Viveros Álvarez, J. S. (2024). The risks and inefficacies of AI systems in military targeting support. *Derecho y Políticas Humanitarias*. Comité Internacional de la Cruz Roja (<https://blogs.icrc.org/law-and-policy/2024/09/04/the-risks-and-inefficacies-of-ai-systems-in-military-targeting-support/>).

Recursos sobre información perjudicial

Blake, J. (2020). *Disinformation and security risk management for NGOs*. Global Interagency Security Forum (www.gisf.ngo/blogs/disinformation-and-security-risk-management-for-ngos/).

Center for Civilians in Conflict. (2023). *When words become weapons: the unprecedented risks to civilians from the spread of disinformation in Ukraine* (<https://civiliansinconflict.org/publications/research/when-words-become-weapons-the-unprecedented-risks-to-civilians-from-the-spread-of-disinformation-in-ukraine/>).

Comité Internacional de la Cruz Roja. (2021). *Harmful information - misinformation, disinformation and hate speech in armed conflict and other situations of violence: ICRC initial findings and perspectives on adapting protection approaches* (<https://shop.icrc.org/harmful-information-misinformation-disinformation-and-hate-speech-in-armed-conflict-and-other-situations-of-violence-icrc-initial-findings-and-perspectives-on-adapting-protection-approaches-pdf-en.html>).

Comité Internacional de la Cruz Roja. (2022). *Ucrania: desinformación sobre las actividades del CICR* (<https://www.icrc.org/en/document/ukraine-addressing-misinformation-about-icrcs-activities>).

Comité Internacional de la Cruz Roja. (2023). *How misinformation and disinformation harm ICRC's humanitarian work in Burkina Faso* (www.icrc.org/en/document/burkina-faso-how-misinformation-disinformation-harm-humanitarian-action).

Global Interagency Security Forum. (2023c). *Online risk to real-life harm: disinformation and social listening workshop resources* (www.gisf.ngo/resource/online-risk-to-real-life-harm-disinformation-and-social-listening-workshop-resources/).

Insecurity Insight. (2023). The role of social media in the spreading of the Turkish Red Crescent Tent Sale Story in Türkiye. *Social Media Monitoring* (<https://insecurityinsight.org/wp-content/uploads/2023/08/The-Spreading-of-the-Turkish-Red-Crescent-Tent-Sale-Story.pdf>).

Insecurity Insight. (s. f.). Social media monitoring (<https://insecurityinsight.org/projects/aid-in-danger/social-media-monitoring>).

Internews. (2015). *Mapping information ecosystems to support resilience* (https://internews.org/wp-content/uploads/legacy/resources/Internews_Mapping_Information_Ecosystems_2015.pdf).

Tiller, S., Devidal, P. y van Solinge, D. (2023). *The fog of war and information*. MSF Analysis (<https://analysis.ocb.msf.org/the-fog-of-war-and-information/>).

Wardle, C. (2024). *A conceptual analysis of the overlaps and differences between hate speech, misinformation and disinformation*. Departamento de Operaciones de Paz de las Naciones Unidas (<https://peacekeeping.un.org/en/new-report-finds-understanding-differences-harmful-information-is-critical-to-combatting-it>).

7 Gestión de amenazas y situaciones de riesgo específicas

7.1 Seguridad en los viajes

Los trabajadores humanitarios se enfrentan a menudo a mayores riesgos durante sus viajes. Esto hace que la gestión eficaz de los riesgos relacionados con los viajes sea crucial para mantener el acceso a zonas críticas y para garantizar la seguridad y la confianza de quienes viajan. La gestión de estos riesgos es una responsabilidad compartida entre la organización y el personal, y requiere políticas exhaustivas, formación completa y planes de contingencia sólidos. Si prestan especial atención a la seguridad, las organizaciones humanitarias pueden seguir desplazándose incluso a los entornos más difíciles para llevar a cabo su labor. En este capítulo se analizan las consideraciones generales sobre la seguridad en los viajes y se describen buenas prácticas para los distintos modos de desplazamiento.

7.1.1 Consideraciones generales

Política de gestión de riesgos en los viajes

Una política de gestión de riesgos en los viajes bien definida sirve de base para todas las prácticas de seguridad relacionadas con los viajes, transformando el posible caos en una preparación estructurada.

Una política integral de gestión de riesgos en los viajes suele incluir lo siguiente:

- **Normas y procedimientos coherentes.** La política de gestión de riesgos en los viajes establece normas y procedimientos claros y coherentes para la organización y para la persona. Esto puede incluir la identificación de riesgos potenciales, el establecimiento de protocolos para mitigarlos y la definición de procedimientos de respuesta a emergencias. La claridad que aportan estas políticas fomenta un enfoque unificado de la gestión de riesgos en los viajes, lo que les permite a las organizaciones identificar y mitigar los riesgos antes de que se materialicen.
- **Gestión centralizada frente a gestión descentralizada.** Las organizaciones deben considerar cuidadosamente qué aspectos de la gestión de riesgos en los viajes se manejan mejor a nivel central y cuáles a nivel local. Esta decisión puede basarse en los recursos disponibles y en los riesgos específicos asociados a cada escenario de viaje. Por ejemplo, mientras que los datos de seguridad de las aerolíneas podrían gestionarse de forma centralizada, la selección de las aerolíneas y las rutas de viaje adecuadas podría gestionarse mejor en una oficina local por el personal familiarizado con las condiciones locales.
- **Derechos de los viajeros y umbrales de riesgo personal.** Los derechos de los viajeros pueden definirse claramente en la política, en particular en relación con los umbrales de riesgo personales. Una buena práctica es informar al personal sobre su derecho a retirarse de misiones o viajes si considera que los riesgos son demasiado

altos. Esto no solo protege a la persona, sino que también garantiza que quienes viajan están completamente preparados y confían en su capacidad para gestionar los riesgos.

► *Para obtener más información sobre los umbrales de riesgo personales, véase el capítulo 1.1.*

- **Reuniones informativas de seguridad previas al viaje.** Las sesiones informativas sobre seguridad preparan a los viajeros para sus desplazamientos proporcionándoles información esencial, como, información sobre el itinerario y otros detalles del viaje, los riesgos personales y específicos del contexto, las respuestas adecuadas a estos riesgos y recomendaciones sobre la documentación necesaria y los objetos que deben llevar. Estas sesiones también suelen incluir directrices organizativas, políticas internas pertinentes, contactos de emergencia e información sobre seguros de viaje y servicios de asistencia. Las sesiones pueden impartirse mediante diversos métodos, como documentos, videos o conversaciones con los referentes de seguridad, y deben adaptarse al tipo específico de viaje y al perfil de riesgo personal del viajero.
- **Capacitación.** Los requisitos de la organización en materia de viajes, incluida la formación obligatoria, deben estar claramente descritos en las políticas de viajes, los contratos de los empleados y los planes de seguridad. Las organizaciones deben asegurarse de que la formación y las sesiones informativas no se imparten exclusivamente a los viajeros internacionales, sino que también están disponibles para el personal local que pueda viajar a diferentes zonas dentro de un país.

► *Para obtener más información sobre la capacitación, véase el capítulo 5.2.*

El establecimiento de una política integral de gestión de riesgos en los viajes crea un marco de protección que permite al personal viajar con confianza y claridad. Esta política también puede utilizarse para abordar las repercusiones éticas y medioambientales, promover prácticas sostenibles y garantizar actualizaciones periódicas y comentarios de los viajeros. Esto no solo mejora la seguridad y la eficacia de las operaciones humanitarias, sino que también demuestra el compromiso de la organización con la seguridad de su personal, fomentando la confianza y la moral entre el personal.

Sistemas de aprobación de viajes

Un sistema de aprobación de viajes bien estructurado es un componente fundamental de la gestión de riesgos de los viajes. Las organizaciones deben determinar qué tipo de viaje requiere qué nivel de autorización, lo que puede implicar varias consideraciones, incluidos los niveles de riesgo y la distancia del viaje. El sistema ideal es sostenible y pertinente, al tiempo que añade valor y mejora la gestión de riesgos. Un sistema demasiado complejo o que requiera demasiados recursos puede resultar pesado, mientras que uno demasiado simplista puede no ofrecer la protección adecuada.

Un sistema de autorización de viajes abarca varios elementos clave, entre los que pueden figurar los siguientes:

- **Proceso de solicitud formalizado.** El proceso de aprobación de los viajes comienza con una solicitud formal mediante la cual los viajeros presentan itinerarios detallados en los que indican sus destinos, el propósito y la duración del viaje y las actividades previstas. De este modo se garantiza que toda la información pertinente se recoge y revisa antes de conceder la aprobación.
- **Diagnóstico de riesgos.** Cada solicitud de viaje debe someterse a un diagnóstico de riesgos para evaluar los riesgos potenciales asociados al viaje y al destino, incluidos la inestabilidad política, las amenazas para la salud, los peligros medioambientales y los problemas de seguridad locales. Esto también brinda a los viajeros la oportunidad de destacar cualquier consideración personal que deba tenerse en cuenta.
- **Preparación del viajero.** Los viajeros deben estar adecuadamente preparados con las herramientas y los recursos necesarios, como un seguro de viaje, suministros médicos y fondos de emergencia.
- **Informe posterior al viaje.** Un sistema eficaz de aprobación de viajes suele incorporar una sesión informativa posterior al viaje. Puede ser útil que los viajeros informen sobre sus experiencias a su regreso, señalando cualquier incidente u observación que pueda servir de base para futuros diagnósticos de riesgos o modificaciones de la política.

Otras consideraciones

- **Capacidad interna para la gestión de los riesgos de viaje.** Algunas organizaciones han invertido en capacidad interna para gestionar los viajes y mitigar los riesgos que entrañan, por ejemplo, con personal dedicado a la reserva de vuelos. Esto requiere un presupuesto sostenido y recursos especializados, pero puede ser muy eficaz para garantizar que los riesgos de los viajes se gestionan de forma proactiva y exhaustiva.
- **Responsabilidad compartida.** Tanto la organización como el viajero tienen la responsabilidad conjunta de la seguridad del viaje. La organización es responsable de crear y mantener un sistema y un entorno de viajes bien gestionados y seguros, así como de establecer la capacidad de responder y apoyar a los viajeros si surgen problemas. Se espera que el viajero escuche las sesiones informativas y se atenga a las orientaciones y requisitos.
- **Perfiles personales de riesgo.** El perfil de riesgo personal de un miembro del personal puede desempeñar un papel importante en la gestión de los riesgos relacionados con los viajes y debe tenerse en cuenta en la planificación y en la preparación. Por ejemplo, el personal con problemas de salud puede necesitar acceso a los medicamentos necesarios.

7.1.2 Modos de desplazamiento

Las decisiones sobre el modo de desplazamiento deben guiarse por un análisis de riesgos exhaustivo. Por ejemplo, aunque un vuelo corto de una hora en una aerolínea con un historial de mantenimiento cuestionable puede suponer ciertos riesgos, puede seguir siendo una opción más segura que un viaje de 10 horas por carretera a través del país. Las siguientes secciones deben considerarse en este contexto.

Transporte aéreo

Los viajes aéreos conllevan varios riesgos que las organizaciones deben estar preparadas para gestionar. Entre ellos figuran los problemas de salud, como la trombosis venosa profunda, y los riesgos de seguridad, incluidos los secuestros o accidentes aéreos. Los viajeros pueden sufrir estrés por las demoras, la pérdida del equipaje y los complejos procedimientos de control de seguridad.

- **Seguridad y selección de compañías aéreas.** No todas las compañías aéreas son iguales en términos de aeronavegabilidad y calidad de mantenimiento. Varias organizaciones comerciales califican a las aerolíneas en todo el mundo, y esta información puede utilizarse para tomar decisiones informadas. Como mínimo, las organizaciones deben revisar los procedimientos y los registros de seguridad de las aerolíneas antes de utilizarlas.
- **Utilización de líneas aéreas humanitarias.** El Servicio Aéreo Humanitario de las Naciones Unidas y otras líneas aéreas humanitarias prestan servicios esenciales en muchos entornos difíciles. Las organizaciones que deseen utilizar los servicios aéreos de la ONU o de las ONG deben estar familiarizadas con su funcionamiento, incluidas las normas y las reglamentaciones locales, que pueden variar significativamente de las de las compañías aéreas nacionales.
- **Reuniones informativas y apoyo a los viajeros.** Por lo general, los viajeros deben gestionar por sí mismos muchos de los riesgos asociados a los viajes aéreos, pero las organizaciones pueden proporcionarles información y directrices exhaustivas. Los planes de contingencia abordan problemas comunes como las demoras de vuelos, la pérdida del equipaje o los cambios en las condiciones de seguridad. Las agencias comerciales pueden ofrecer servicios que incluyan alertas individuales y seguimiento.

Lista de control de las orientaciones de seguridad aérea y marítima

Garantizar la seguridad y el mantenimiento de aeronaves y embarcaciones marítimas puede ser crucial para el éxito de un viaje. A continuación se presentan algunas consideraciones, en particular para las embarcaciones que la organización contrata:

- **Historial de mantenimiento:** compruebe que la aeronave o embarcación haya recibido un mantenimiento regular y adecuado.

- **Piezas de repuesto para embarcaciones marítimas:** verifique la disponibilidad de repuestos esenciales, incluido un motor secundario y una batería de repuesto, en caso de falla mecánica en el mar.
- **Sistemas de navegación y comunicación:** evalúe los sistemas de navegación y comunicación para garantizar un funcionamiento fiable durante el viaje.
- **Equipo de seguridad:** compruebe el equipo de seguridad, como chalecos salvavidas, dispositivos de señalización de socorro, linternas, extintores de incendios operativos, máscaras de oxígeno de emergencia y remos de repuesto para los botes salvavidas.
- **Combustible:** verifique que el combustible sea suficiente e incluya un margen de reserva adicional a la cantidad necesaria para el viaje, para tener en caso de demoras o desvíos imprevistos.
- **Peso de la carga:** confirme que el peso de la carga está dentro de los límites de seguridad de la embarcación y que está correctamente distribuido para su equilibrio.

Viajes por carretera

Los viajes por carretera siguen siendo la forma más habitual de desplazamiento para las organizaciones humanitarias y también una de las más peligrosas. Los riesgos asociados a los desplazamientos por carretera son numerosos y variados, desde accidentes de tráfico y bloqueos hasta emboscadas por grupos armados e infraestructura vial deficiente. Los viajes por carretera pueden implicar largos trayectos por terrenos difíciles, condiciones meteorológicas impredecibles y regiones con altos niveles de inseguridad. La gestión de estos riesgos requiere una planificación cuidadosa, sistemas sólidos y una gran atención a la seguridad tanto del personal como de los recursos. Las siguientes consideraciones pueden ser fundamentales:

- **Flotas de vehículos y mantenimiento.** Las flotas de vehículos de las organizaciones humanitarias suelen ser variadas y constan de vehículos todocaminos, automóviles de turismo, camiones y motocicletas de distinta antigüedad y kilometraje. El estado y la aptitud técnica para circular de estos vehículos son primordiales. Las revisiones regulares de mantenimiento, incluidas las inspecciones de neumáticos, frenos y equipos de seguridad, deben ser obligatorias. Las organizaciones también querrán asegurarse de que los vehículos están equipados con elementos esenciales como ruedas de repuesto, gatos, botiquines de primeros auxilios y dispositivos de comunicación.
- **Visibilidad.** Puede ser necesario considerar el grado de visibilidad que una organización desea tener durante los desplazamientos, en consonancia con la estrategia de seguridad de la organización en ese contexto. Las organizaciones que deseen ser identificadas visualmente como actores humanitarios tendrán que asegurarse de que todos los vehículos sean claramente identificables mediante colores y logotipos (esto también puede aplicarse a otros tipos de transporte, como las embarcaciones).

- **Competencia y capacitación de los conductores.** La competencia, la moral y la conexión de los conductores con los valores de la organización pueden ser fundamentales para garantizar la seguridad de los viajes. Los conductores deben conocer las normas y las prácticas de conducción locales, que pueden variar significativamente de un país a otro. Es aconsejable capacitar a los conductores y evaluar periódicamente su desempeño. En zonas de conflicto o criminalidad, puede ser necesario capacitar a los conductores en seguridad y conducción defensiva, como conocimiento de la situación, diagnóstico de riesgos y maniobras evasivas.
 - **Sistemas de control de movimientos.** Muchas organizaciones utilizan hojas o fichas de registro para gestionar al personal y los recursos durante los viajes por carretera. Los sistemas de control de movimientos hacen un seguimiento de los viajeros y gestionan los recursos, con alertas y planes de contingencia para el personal que llega tarde o falta. Estos sistemas deben adaptarse al contexto y actualizarse continuamente.
 - **Seguimiento digital y registro de viajes.** Los dispositivos de seguimiento digital y registro de viajes en los vehículos proporcionan funciones de seguridad mejoradas e indicadores detallados de los trayectos, incluido el seguimiento en directo del vehículo. Sin embargo, es esencial que estos sistemas cuenten con la supervisión y los protocolos adecuados. Deben integrarse a la estrategia general de gestión de riesgos en los viajes y contar con el apoyo de una sólida capacidad de respuesta en caso de emergencia.
 - **Protocolos y sesiones informativas sobre viajes por carretera.** Las organizaciones deben establecer protocolos claros para los desplazamientos por carretera, que incluyan directrices sobre los límites de velocidad, las prácticas seguras de conducción y los procedimientos de emergencia. Las sesiones informativas previas a la salida para los viajeros deben cubrir los riesgos específicos asociados al viaje, las condiciones de las carreteras, la situación de la seguridad en la zona y las normas y expectativas culturales locales.
 - **Planes de contingencia para viajes por carretera.** Dada la naturaleza impredecible de los viajes por carretera, es esencial contar con planes de contingencia. Las organizaciones deben tener protocolos claros para responder a incidentes como averías de vehículos, bloqueos de carreteras y emboscadas, rutas alternativas, contactos de emergencia y procedimientos para reubicar/evacuar al personal. En zonas de alto riesgo, las organizaciones también pueden considerar el uso de convoyes o escoltas de seguridad.
- *Para obtener más información sobre las escoltas armadas, véase el capítulo 4.2.*
- **Coordinación con las autoridades y las comunidades locales.** La policía local, las fuerzas armadas y los líderes comunitarios pueden ser una fuente de información oportuna y precisa sobre el estado de las carreteras, las amenazas a la seguridad y otros factores relevantes. Otras organizaciones humanitarias, incluidas los organismos de la ONU, también pueden proporcionar este tipo de información. Las comunidades locales pueden proporcionar un apoyo valioso durante el viaje, como monitorear el estado de las carreteras y prestar asistencia en caso de accidente.

- **Consideraciones medioambientales.** Las organizaciones pueden tener que ser conscientes del impacto medioambiental de sus operaciones. Esto incluye minimizar el uso de vehículos, reducir las emisiones y garantizar una eliminación adecuada de los residuos. Puede ser conveniente realizar una evaluación del impacto ambiental antes de emprender operaciones de transporte por carretera a gran escala o cuando se considere la compra o eliminación de vehículos.

Transporte público

Para el personal que no reside en la zona, la decisión de utilizar el transporte público, como autobuses o taxis, debe basarse en un diagnóstico exhaustivo de los riesgos. En algunas circunstancias, especialmente en contextos de muy alto riesgo o cuando los perfiles personales exponen a determinados miembros del personal a riesgos elevados, esta consideración también puede aplicarse al personal residente. Para los destinos de menor riesgo, puede informarse a los viajeros sobre las opciones de transporte seguro, incluida la forma de identificar a los proveedores de servicios con licencia y buena reputación. En las zonas de mayor riesgo, puede ser aconsejable evitar por completo el transporte público. Las organizaciones deben tener políticas claras en relación con los desplazamientos del personal al trabajo y de vuelta a casa, que incluyan si la organización organizará o pagará el transporte, en lugar de limitarse a desaconsejar el uso del transporte público sin brindar alternativas.

Puestos de control

Las interacciones en los puestos de control pueden ser de apoyo u hostiles. Es posible que los viajeros sean acosados, intimidados o amenazados por las personas que controlan estos puestos, especialmente si son fácilmente irritables o están bajo los efectos del alcohol o las drogas; por el contrario, los puestos de control pueden ser amables y proporcionar información valiosa sobre las condiciones de la carretera. La forma en que el personal interactúa con las personas en los puestos de control puede influir no solo en su propio viaje, sino también en el trato que reciban posteriormente otros trabajadores humanitarios.

Es esencial que el personal evalúe rápidamente el tipo y la ubicación de cada puesto de control, así como el estado de ánimo de quienes los controlan y trabajan en ellos. Los puestos de control suelen encontrarse en los cruces de carreteras, los puentes, los pasos de montaña y las entradas o salidas de las localidades. Los objetivos de los puestos de control varían y pueden incluir el control del tráfico y la seguridad.

En un vehículo individual, el responsable del viaje puede actuar como portavoz si habla el idioma local. En un convoy, puede seleccionarse una persona responsable para cada vehículo, idealmente la persona con más experiencia y conocimientos del idioma local. Los conductores suelen desempeñar un papel clave en las interacciones iniciales, ya que suelen ser los primeros en relacionarse con los guardias de los puestos de control. Todos los miembros del equipo deben saber qué llevan y ser coherentes a la hora de explicar la misión de la organización y el propósito del viaje. Puede ser aconsejable que los pasajeros lleven una identificación en el idioma local; se debe evitar entregar los pasaportes si es posible. Si se les pide que entren en una sala de guardia, los miembros del personal deben intentar permanecer juntos y no dejar el vehículo desatendido.

- *Para obtener más información sobre cómo tratar el acoso contra el personal, véase el capítulo 7.4.*

Seguridad vial

Las organizaciones pueden considerar los siguientes aspectos como parte de sus políticas sobre viajes por carretera.

- Prohibición de llevar armas (en consonancia con la política de la organización y los principios humanitarios)
 - La mayoría de las organizaciones humanitarias no permiten llevar armas en los vehículos ni en ninguna otra forma de transporte, salvo en situaciones de coacción. El personal responsable debe asegurarse de que esta política sea clara y visible (por ejemplo, pegatinas con símbolos de armas tachadas).

- Interacción con agentes armados
 - Se debe evaluar y definir la postura de la organización respecto al uso o relación con escoltas armados y otros agentes armados. Esto puede tener implicaciones para las políticas que prohíben las armas en los vehículos de la organización (especialmente en el caso de las aeronaves y las embarcaciones, puesto la protección armada no puede ubicarse en otro vehículo).
- Transporte de pasajeros o carga no afiliados
 - Elabore una política para el transporte de pasajeros o carga no afiliados.
 - Proporcione material plastificado en las lenguas locales para comunicar esta política.
 - Permita excepciones por cuestiones prácticas (por ejemplo, guías, hospitalidad, emergencias médicas).
 - Anticipe los requisitos culturales (por ejemplo, que las mujeres viajen con familiares varones en determinados contextos).
- Exención de responsabilidad
 - Coloque en los vehículos un documento de exención de responsabilidad que exima a la organización de responsabilidad en caso de incidentes imprevistos.
 - Reconozca la eficacia variable de tales documentos en función de las leyes y circunstancias locales.
 - Considere la viabilidad y los posibles problemas de aceptación de la aplicación de esta política.

Viajes por agua

Aunque a menudo los viajes por agua son necesarios en los contextos humanitarios, como durante las inundaciones o en las temporadas de lluvias, este método de transporte puede estar plagado de riesgos. La gestión de estos riesgos requiere una planificación cuidadosa.

- **Selección de la embarcación.** Las organizaciones deben utilizar embarcaciones adecuadas para las condiciones específicas previstas, ya sean ríos, lagos o aguas costeras. El estado de la embarcación, así como su historial de mantenimiento y el equipo de seguridad, deben inspeccionarse minuciosamente antes de su uso. Antes de cada viaje, compruebe que haya suficiente combustible y una reserva.

- **Competencia y capacitación de la tripulación.** La competencia de la tripulación es tan importante como el estado de la embarcación. Compruebe que los miembros de la tripulación tienen las licencias, certificaciones y experiencia necesarias para operar la embarcación de manera segura. Esto incluye formación en procedimientos, navegación y comunicación de emergencia (véase el recuadro más abajo).
 - **Equipo de seguridad.** Las embarcaciones deben contar con el equipo de seguridad esencial, incluidos chalecos salvavidas, dispositivos de señalización de socorro, extintores de incendios y remos de repuesto.
 - **Riesgo de piratería.** Puede ser necesario tomar precauciones adicionales en regiones conocidas por la piratería. Esto implica seleccionar embarcaciones con elementos de seguridad avanzados, por ejemplo, sistemas de vigilancia y equipos de comunicación seguros. En algunos casos, podría necesitarse protección armada para proteger la embarcación y a sus ocupantes.
- *Para obtener más información sobre el uso de la protección armada, véase el capítulo 4.2.*
- **Planes de contingencia.** Pueden establecerse protocolos claros para responder a emergencias, como averías mecánicas, condiciones meteorológicas adversas y ataques de piratería. Estos protocolos pueden incluir rutas alternativas, contactos de emergencia y procedimientos para la evacuación del personal.
 - **Consideraciones medioambientales.** Los viajes por agua pueden tener lugar en ecosistemas sensibles, y las organizaciones deben ser conscientes de su impacto ambiental. Esto puede incluir minimizar la contaminación, evitar perturbar la vida silvestre local y garantizar que los residuos se eliminan adecuadamente.
 - **Coordinación con las autoridades locales.** Los guardacostas, las autoridades portuarias y los líderes comunitarios pueden facilitar información sobre las condiciones del agua, las amenazas a la seguridad y otros factores relevantes.

Cualificaciones de la tripulación y lista de verificación de competencias

Cuando las organizaciones contratan aeronaves o embarcaciones, es importante tener en cuenta las cualificaciones de la tripulación.

- **Licencias y certificaciones**
 - Asegúrese de que el piloto o capitán y la tripulación tengan las licencias y las certificaciones válidas para sus funciones y el tipo de embarcación que se opera.
- **Competencia mecánica y preparación para emergencias**
 - Evalúe la competencia mecánica de la tripulación y su preparación para abordar situaciones imprevistas.
- **Conocimientos lingüísticos**
 - Asegúrese de que la tripulación domina los idiomas esenciales para la comunicación durante el viaje y en caso de emergencia.

Viajes no convencionales

En terrenos difíciles y regiones apartadas, el transporte convencional puede ser poco práctico o inviable y el personal puede tener que desplazarse a pie o depender de animales. Las siguientes consideraciones son importantes para gestionar eficazmente los riesgos asociados.

- **Trazado de rutas y diagnóstico de riesgos.** Las rutas deben trazarse meticulosamente para evitar las zonas peligrosas. Esto puede implicar la evaluación del terreno, la identificación de posibles amenazas y la planificación de puntos de descanso y fuentes de agua. El personal puede necesitar capacitación especial para abordar posibles amenazas, como en el caso de encontrarse con animales salvajes o grupos hostiles.
- **Preparación del viajero.** Los viajeros deben estar preparados para los retos físicos y mentales que puede suponer este modo de viajar. Esto puede incluir asegurarse de que tienen el equipo y los suministros adecuados para terreno y el clima, y que han recibido capacitación en habilidades de supervivencia, primeros auxilios y comunicación de emergencia.
- **Protocolos de comunicación.** Los viajeros deben disponer de dispositivos de comunicación fiables, como teléfonos por satélite o radios bidireccionales. Deben establecerse controles periódicos con la oficina de la organización pertinente. En zonas con infraestructura de comunicación limitada o inexistente, las organizaciones

quizás tengan que desarrollar métodos alternativos de seguimiento y asistencia a los viajeros, como el uso de guías locales.

► *Para obtener más información sobre las comunicaciones, véase el capítulo 6.1.*

- **Coordinación con las comunidades locales.** Las comunidades locales pueden compartir información y recursos para sortear terrenos difíciles y evitar amenazas a la seguridad, así como proporcionar asistencia en caso de emergencia.
- **Planes de contingencia.** Deben establecerse protocolos claros para responder a emergencias, como lesiones, fallas del equipo y encuentros con grupos hostiles. Los protocolos pueden incluir rutas alternativas, contactos de emergencia y procedimientos para la evacuación del personal.

► *Para obtener más información sobre emergencias médicas, véase el capítulo 5.5.*

Convoyes

Un convoy es un grupo de vehículos que viajan juntos, principalmente por razones de protección, apoyo o eficacia. En contextos humanitarios, los convoyes se utilizan para transportar mercancías, personal o equipos a través de zonas con riesgos de seguridad o dificultades logísticas. Pueden estar formados por vehículos de una sola organización o concertarse con otros agentes.

En zonas de bajo riesgo, el tamaño de un convoy puede ser menos significativo siempre que exista una comunicación fiable entre todos los vehículos (por ejemplo, por medio de radios o *walkie-talkies*). Sin embargo, en entornos de alto riesgo o complejos puede ser necesario considerar cuidadosamente el tamaño y la estructura de un convoy. Aunque viajar en convoy puede reducir los riesgos gracias a la fuerza que da el número, también puede suponer peligros, como ser confundido con una columna militar, y puede atraer una atención no deseada. Normalmente, un convoy tiene un vehículo líder, un cuerpo principal donde se colocan los activos valiosos y un vehículo de retaguardia. En algunas situaciones puede utilizarse un vehículo explorador, que mantiene una distancia segura y contacto por radio con el resto del convoy que va detrás. El responsable del convoy suele ir en el vehículo líder, con otra persona experimentada en el vehículo de retaguardia.

Antes de la salida, el responsable del convoy debe asegurarse de que se compruebe que todos los vehículos son adecuados y tienen combustible, el equipo necesario y la documentación. Es aconsejable que los conductores y los responsables de los vehículos reciban información completa sobre las normas del convoy, incluida la velocidad, el mantenimiento de la distancia, los protocolos de comunicación y los procedimientos para hacer frente a diversas situaciones, como los puestos de control o las averías de los vehículos. Mantener la distancia adecuada entre los vehículos es crucial; normalmente tendrán que estar lo suficientemente cerca como para mantener el contacto visual, pero lo suficientemente separados como para evitar quedar atrapados en el mismo

incidente. La distancia adecuada puede variar en función del terreno, el tiempo y las condiciones de seguridad, y puede ser necesario ajustarla a lo largo del viaje.

7.1.3 Consideraciones de seguridad personal en tránsito

Los aeropuertos, los puertos y las estaciones de autobús y tren pueden suponer importantes riesgos para la seguridad. Estos lugares suelen ser el blanco de actividades delictivas, y los viajeros pueden encontrarse en una situación de vulnerabilidad debido a su desconocimiento del entorno local y las condiciones de seguridad. Las organizaciones pueden tomar medidas proactivas para mitigar estos riesgos.

Las sesiones informativas previas al viaje deben tratar la situación de la seguridad en el lugar de destino, los requisitos legales y administrativos pertinentes (como las vacunas obligatorias), los riesgos potenciales asociados a los aeropuertos, los puertos y las estaciones de autobús y tren, e incluir información de contacto del personal de seguridad local. Además, estas sesiones pueden abarcar lo siguiente:

- **Opciones de transporte seguras.** Se puede brindar orientación sobre las opciones de transporte desde aeropuertos, puertos y estaciones de autobús y tren hasta el destino final. Esto puede incluir proporcionar listas de servicios o lugares de taxi legítimos, aplicaciones de transporte acreditadas y organizar la recogida por una persona designada. Se recomienda utilizar vehículos de la organización, ya que los conductores suelen estar familiarizados con las condiciones locales y pueden proporcionar un medio de transporte seguro y fiable.
- **Medidas de seguridad personal.** Se puede aconsejar a los viajeros sobre medidas de seguridad personal durante el viaje, como mantener los objetos de valor ocultos, permanecer alerta a su entorno y evitar interactuar con desconocidos. Las organizaciones pueden proporcionarles dispositivos de seguridad personal, como silbatos de alarma o dispositivos de seguimiento. Los viajeros quizás necesiten información sobre cómo manejar su equipaje de forma segura, lo que incluye mantenerlo a la vista en todo momento, utilizar candados en las maletas y evitar llevar grandes cantidades de dinero en efectivo u objetos de valor. Es posible que sea necesario considerar la posibilidad de etiquetar el equipaje sin revelar datos personales que puedan ser utilizados por delincuentes.
- **Superar los controles de seguridad.** Los viajeros pueden necesitar orientación sobre cómo desenvolverse en los controles de seguridad en los aeropuertos y en las estaciones. Esto puede implicar conocer las restricciones sobre el equipaje de mano, saber qué documentación se necesita y cuándo, y conocer las medidas de protección específicas. Los viajeros también deben ser conscientes de los posibles riesgos de ciberseguridad durante los procesos de seguridad aeroportuaria y de las precauciones que pueden tomar para proteger la información sensible.

- **Trato con las autoridades.** En algunos casos, los viajeros pueden ser interrogados o tener otro tipo de interacciones difíciles con las autoridades. Las organizaciones pueden ofrecer orientación sobre cómo afrontar estas situaciones, como, por ejemplo, mostrarse cooperativo y paciente, ser sincero y saber cuándo solicitar asistencia jurídica o consular. Los viajeros deben conocer sus derechos y las leyes locales aplicables a su estancia.

Lista de verificación general de seguridad operacional para viajes

Al planificar los viajes del personal, sobre todo en entornos complejos, deben tenerse en cuenta las siguientes consideraciones generales:

- Condiciones meteorológicas
- Condiciones de seguridad en los distintos lugares
- Autorización de las autoridades
- Planes de contingencia
- Identificación (viajeros y vehículos)
- Garantías razonables de que el medio de transporte, como una embarcación, no se utiliza también para actividades ilícitas como el contrabando.

7.1.4 Hoteles y alojamientos temporales

Los viajeros pueden necesitar pernoctar en hoteles o alojamientos temporales. En el caso de que no se haya podido planificar con antelación, el personal debe saber cómo evaluar la seguridad del alojamiento y solicitar los cambios necesarios.

- **Infraestructura de seguridad del hotel.** Los hoteles que aplican las siguientes medidas suelen estar mejor preparados para responder a las emergencias y para proteger la seguridad de sus huéspedes: personal de seguridad, recepción 24 horas, sistemas integrales de control de acceso y sistemas de seguridad contra incendios visibles y operativos.
- **Selección de habitaciones.** Los viajeros deben elegir habitaciones en pasillos muy transitados y con buena visibilidad. Deben evitarse las habitaciones de fácil acceso para los intrusos o ubicadas en zonas aisladas. Es posible que haya que revisar los puntos de acceso, incluidas puertas y ventanas, para asegurarse de que funcionan correctamente y pueden cerrarse con seguridad. Entre las consideraciones a tener en cuenta durante una estancia figuran las

siguientes:

- **Preparación para emergencias.** Los viajeros deben familiarizarse con los procedimientos de emergencia del alojamiento, localizar las salidas más cercanas y asegurarse de que tienen acceso a un botiquín de emergencia básico (que incluya una linterna, material de primeros auxilios y números de contacto de emergencia). Los viajeros también deben conocer la ubicación de los extintores de incendios y otros equipos de seguridad.
- **Interacciones con los visitantes.** Es posible que los viajeros deban actuar con precaución al interactuar con los visitantes en el alojamiento. Esto puede incluir negar la entrada a personas cuya identidad o intención no esté clara, como personas conocidas recientemente, personal de servicio no solicitado y personal que entregue objetos. Si un visitante parece sospechoso, debe avisarse inmediatamente al personal de seguridad (por ejemplo, al personal de seguridad del hotel).
- **Reportar los problemas.** Cualquier preocupación relativa a la seguridad de las habitaciones o al comportamiento del personal del hotel o de otros huéspedes debe comunicarse sin demora a la dirección del hotel. Las organizaciones pueden guiar a los viajeros sobre cómo elevar estas preocupaciones en caso de que sea necesario, lo que incluye ponerse en contacto con las autoridades locales y el personal de seguridad de la organización.
- **Consideraciones culturales.** Los viajeros deben ser conscientes de las normas y expectativas culturales locales cuando se alojen en hoteles y alojamientos temporales. Esto puede incluir respetar las costumbres locales relacionadas con la vestimenta, el comportamiento y las interacciones con el personal del hotel.

► *Para obtener más información sobre la seguridad del sitio, véase el capítulo 7.2.*

7.1.5 Planificación de contingencia y gestión de incidentes

Una planificación de contingencia y una gestión de incidentes eficaces son esenciales. Para ello, es importante elaborar, así como revisar y actualizar periódicamente, planes integrales que puedan aplicarse rápidamente en caso de emergencia. Esto suele implicar la identificación de riesgos potenciales relacionados con los viajes (prestando especial atención a los perfiles de riesgo personales), el desarrollo de estrategias para mitigar estos riesgos y el establecimiento de protocolos de respuesta a incidentes. La formación y los simulacros periódicos pueden contribuir a la preparación.

► *Para obtener más información sobre los planes de contingencia, véase el capítulo 4.3.*

► *Para obtener más información sobre la respuesta a incidentes, véase el capítulo 4.4.*

► *Para obtener más información sobre el cuidado del personal, véase el capítulo 5.4.*

- Para obtener más información sobre las consideraciones médicas, véase el capítulo 5.5.

Más información

Orientación y recursos

Bickley, S. (2017). *Gestión de riesgos de seguridad: una guía básica para las ONG pequeñas*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/security-risk-management-a-basic-guide-for-smaller-ngos/).

Davis, J. et al. (2020). Module 10, Travel safety: airports, vehicles and other means of transport. En *Security to go: a risk management toolkit for humanitarian aid agencies*. 4.ª edición. Global Interagency Security Forum (<https://gisf.ngo/resource/security-to-go/>).

Global Interagency Security Forum. (2024). 4. *Travel and movement*. NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/4-travel-and-movement/>).

Inter-Agency Standing Committee. (2013). *IASC non-binding guidelines on the use of armed escorts for humanitarian convoys* (<https://reliefweb.int/report/world/iasc-non-binding-guidelines-use-armed-escorts-humanitarian-convoys>).

Organización Internacional de Normalización. (2021). *ISO 31030:2021: Travel risk management — Guidance for organizations* (www.iso.org/standard/54204.html).

7.2 Seguridad del sitio

La seguridad del sitio puede disuadir o detener intrusiones, retrasar ataques y mitigar los efectos de un incidente en sus inmediaciones.⁹⁷ Este capítulo se centra principalmente en las oficinas y las residencias para el personal que vive fuera de casa. Sin embargo, también es necesario considerar la seguridad del sitio en los lugares en los que el personal pasa mucho tiempo, como los lugares donde se ejecutan los proyectos, los campamentos de refugiados, los edificios escolares, las instalaciones médicas y los puntos de distribución. A veces también puede ser necesario adoptar medidas de seguridad en los domicilios privados del personal.

7.2.1 Selección del sitio

La protección del sitio empieza por identificar y seleccionar un lugar adecuado, teniendo en cuenta que la elección perfecta rara vez existe. Además del espacio, el precio y otros criterios, pueden evaluarse los puntos fuertes y débiles de un lugar desde el punto de vista de la seguridad: qué es aceptable, qué debe mejorarse y cuánto costaría. Esto le permite a la organización evaluar la idoneidad y detallar y negociar cualquier permiso para realizar modificaciones antes de firmar un contrato de arrendamiento.

Enfoques de seguridad

En cualquier revisión de la seguridad física, tanto si se selecciona un sitio como si se añaden nuevas medidas de seguridad física, es importante tener en cuenta las percepciones y las actitudes de la comunidad local hacia estas medidas. Por ejemplo, construir un muro de 2,5 metros puede ser aconsejable desde el punto de vista de la protección, pero puede levantar sospechas o perturbar el espacio local. Esta *perspectiva de aceptación* puede aplicarse a todos los ejemplos de buenas prácticas mencionados en este capítulo.

Consideraciones sobre el perfil individual

A la hora de elegir oficinas y alojamientos, es importante tener en cuenta los perfiles personales y las necesidades del personal y de los posibles visitantes. Esto puede contribuir a crear un entorno de trabajo seguro, inclusivo y solidario.

En determinados contextos, puede ser culturalmente inapropiado o potencialmente inseguro que las mujeres que forman parte del personal vivan solas. En estos casos, puede ser adecuado optar por modalidades de alojamiento compartido que se ajusten a las normas sociales y satisfagan las necesidades de las compañeras de trabajo. En función del contexto cultural y social, puede ser aconsejable separar el personal masculino del femenino. Los requisitos de accesibilidad para el personal con discapacidad también son una consideración importante. Ofrecer opciones de alojamiento privado o compartido

97 Los riesgos cambian drásticamente en situaciones de insurgencia y guerra, en las que se requieren medidas adicionales. Estas se analizan con más detalle en el capítulo 7.10.

que respeten la identidad de género y la orientación sexual puede ayudar a mitigar los riesgos y garantizar un entorno acogedor.

Consultar con diversos grupos de personal a la hora de elegir los alojamientos puede ayudar a garantizar que se satisfacen adecuadamente sus necesidades.

► Véase el capítulo 1.2 para más obtener información sobre las consideraciones de seguridad inclusiva.

Criterios físicos

Las organizaciones pueden tener en cuenta varios criterios físicos a la hora de seleccionar un sitio. Esto puede incluir lo siguiente:

- **Resistencia estructural.** Es aconsejable que las organizaciones se aseguren de que los edificios son lo suficientemente robustos y resistentes como para soportar los impactos de condiciones meteorológicas extremas y otros riesgos medioambientales, como inundaciones y corrimientos de tierra. Esto puede implicar la necesidad de revisar la integridad estructural del edificio, la calidad de los materiales y la eficacia de los sistemas de drenaje de la zona.
- **Ubicación.** Las organizaciones quizás prefieran evitar zonas que ofrezcan oportunidades de accesos y escapes ocultos, por ejemplo, aquellas con vegetación densa o callejones estrechos y mal iluminados. Las zonas con muchos edificios desocupados, dañados o abandonados también pueden suponer riesgos. En situaciones de conflicto armado activo, los criterios de selección del sitio incluirán a menudo consideraciones sobre la distancia a posibles objetivos militares y el acceso a instalaciones de refugio. Aunque la preocupación por la seguridad puede motivar la elección de barrios acomodados, enclaves diplomáticos o comunidades cerradas, estas opciones podrían transmitir una imagen elitista, lo que podría afectar la percepción que se tiene de la organización.
- **Perímetro de seguridad.** Por lo general, es preferible un doble perímetro, es decir, un edificio o apartamento situado dentro de un recinto o una zona cerrada más grande. Un perímetro gestionado eficazmente puede actuar como elemento disuasorio de accesos no autorizados y proporcionar una alerta temprana en caso de intrusión.
- **Evacuación de emergencia.** ¿Con qué facilidad pueden el personal y los visitantes evacuar el edificio o las inmediaciones en caso de que se produzca una emergencia, como un incendio? Considere las vías de salida, si el diseño del edificio facilita la evacuación segura y rápida de todos los ocupantes y si los bomberos locales pueden acceder al lugar de forma eficiente.
- **Nivel del suelo.** Es conveniente alquilar oficinas o apartamentos por encima de la planta baja para reducir la vulnerabilidad ante los intrusos. Sin embargo, los pisos más altos pueden resultar inaccesibles para los equipos de emergencia y dificultar la

evacuación. Si se puede acceder al tejado, quizás desde un edificio lindero, ocupar el apartamento situado justo debajo podría aumentar los riesgos.

- **Accesibilidad.** Garantizar que las entradas, las salidas y las áreas comunes sean accesibles para las personas con problemas de movilidad y que los procedimientos de emergencia tengan en cuenta sus necesidades. Es aconsejable considerar si el edificio está equipado con rampas, ascensores y aseos accesibles.
- **Aparcamiento seguro.** Puede ser prudente confirmar que el lugar ofrece instalaciones de aparcamiento seguras: la zona de aparcamiento está bien iluminada, monitoreada por cámaras de seguridad y protegida por puntos de acceso controlados, como puertas o barreras. El aparcamiento seguro es un aspecto importante de la seguridad general de las instalaciones, sobre todo en las horas de menor afluencia. Los aparcamientos también pueden presentar riesgos en situaciones de conflicto activo, que se analizan con más detalle a continuación.

► Véase el capítulo 7.10 para consultar consideraciones adicionales sobre la seguridad del sitio en zonas de combate activo.

Propiedad, ocupación y arrendamiento de edificios

- **Propiedad del edificio.** Las organizaciones deben averiguar la propiedad del edificio, por ejemplo, deben saber si es de un particular, un banco, una tienda o una organización religiosa. Comprender la identidad del propietario y su posible papel en la comunidad puede ayudar a entender cómo sus afiliaciones podrían afectar la imagen y el funcionamiento de la organización.
- **Ocupación y arrendamiento.** Al evaluar un edificio, es aconsejable tener en cuenta quién más ocupa o alquila espacios dentro de las mismas instalaciones. La presencia de otros inquilinos podría ofrecer una mayor concienciación y cierto grado de protección colectiva. Sin embargo, otros inquilinos podrían introducir riesgos, sobre todo si son, o pueden llegar a ser, ellos mismos objetivos. Un sitio con un solo inquilino tiene más posibilidades de estar bajo el control total de la organización.
- **Otras organizaciones.** A veces pueden obtenerse ventajas en términos de seguridad y eficiencia si varias organizaciones humanitarias ocupan espacios en el mismo lugar o cerca unas de otras. Los organismos de las Naciones Unidas, por ejemplo, suelen agrupar sus oficinas en una misma zona para mejorar la seguridad y reducir los costes. Algunas ONG también han adoptado este enfoque. Sin embargo, este tipo de lugares pueden convertirse en comunidades cerradas, aislando potencialmente a las organizaciones de la comunidad en general, o crear la impresión de que existe una estrecha asociación entre organizaciones, lo que puede afectar las percepciones y la aceptación locales. La concentración de posibles objetivos en una sola zona significa que un ataque puede tener un impacto mucho mayor si tiene éxito.

El barrio

Es aconsejable examinar los alrededores, idealmente en un radio de al menos 1,5 kilómetros, para tener un conocimiento completo del barrio. Entre las consideraciones clave figuran las siguientes:

- **La estabilidad y la cohesión social de la población local.** Una alta cohesión social podría sugerir la existencia de un sistema fiable e informal de vigilancia vecinal, con residentes atentos y preocupados por la seguridad. Una baja cohesión social podría indicar una falta de interés por la seguridad de los vecinos, lo que podría facilitar el acceso de extraños al lugar.
- **La naturaleza del barrio.** ¿La mayoría de la gente reside en la zona o es frecuente el paso de una gran cantidad de trabajadores o viajeros? Cuanto menos población local haya, más fácil será para los extranjeros entrar en la zona sin llamar la atención.
- **Disponibilidad de las autoridades locales y servicios de rescate.** Determine la ubicación de la estación de bomberos y los puestos de policía más cercanos, así como las residencias de los líderes locales más influyentes. Identifique las zonas más frecuentadas por las patrullas policiales.
- **Medidas de control de acceso.** Considere el tipo de control de acceso utilizado por los residentes locales, incluida la forma en que entran y salen de los locales y si existen sistemas físicos o virtuales/informáticos. ¿Hay guardias apostados fuera de las casas? ¿Están las casas de la zona fuertemente fortificadas?
- **Niveles de criminalidad.** La criminalidad puede ser un factor importante, teniendo en cuenta que los niveles de criminalidad pueden ser altos tanto en las zonas ricas como en las menos ricas. Independientemente de la riqueza de la zona, las organizaciones y su personal deben evitar la apariencia de riqueza. Elegir o no un sitio cerca de una comisaría depende del contexto y de la relación entre la policía y la comunidad local.

En general, cultivar buenas relaciones con los vecinos, sin ser intrusivo, puede ser una medida importante de seguridad del sitio. Establecer incluso una relación básica puede aumentar la probabilidad de que los vecinos actúen si observan algo sospechoso.

7.2.2 Refuerzo del sitio

Por lo que respecta a la seguridad física de los lugares de trabajo y residencia, una pauta útil es “disuadir, detectar, retrasar y responder”.⁹⁸ Esto puede implicar: añadir elementos que dificulten la entrada a un edificio, como muros, rejas y controles de acceso; eliminar elementos que dificulten la visión de posibles intrusos y añadir cámaras, alarmas y guardias; disponer de una habitación segura que retrase el acceso de los intrusos al personal; y establecer procedimientos para responder rápidamente cuando se detecten intrusiones. Las secciones siguientes tratan estas medidas en detalle.

98 Global Interagency Security Forum. (2024). 3. Site security. NGO Security Toolbox(<https://gisf.ngo/toolbox-pwa/resource/3-site-security/>).

El perímetro exterior

A continuación se enumeran los factores que deben cubrirse al considerar la seguridad del perímetro exterior de un recinto.

- **Alrededores.** Si la vegetación que rodea el edificio ofrece posibles accesos o escondites, las organizaciones pueden plantearse podarla, cortarla o sustituirla por arbustos espinosos. La basura o los escombros cerca del perímetro podrían ayudar a un asaltante a vigilar o acceder al edificio, o dificultar la respuesta del personal de seguridad. También es aconsejable retirar rápidamente cualquier escombros que pudiera ocultar artefactos explosivos.
- **Muros y puertas.** La construcción de muros alrededor del recinto puede mejorar la seguridad. Por lo general, las buenas prácticas sugieren que deben tener una altura mínima de 2,5 metros y estar fortificadas con medidas adicionales como alambre de espino o vidrios rotos en la parte superior. También puede ser necesario tomar medidas con respecto a los árboles u otros objetos cercanos que podrían hacer posible escalar las paredes. Las puertas, como puntos potencialmente vulnerables, deben estar debidamente aseguradas, con mirillas para la verificación visual de los visitantes. En algunos contextos puede ser prudente disponer de una salida secundaria, pero seguro.
- **Iluminación y visibilidad.** Una buena iluminación puede servir para disuadir de posibles amenazas, pero hay que procurar encontrar un equilibrio entre aumentar la visibilidad y llamar la atención. La iluminación tampoco debe afectar negativamente a los vecinos. Las luces con sensor que se activan al detectar movimiento pueden ser una buena opción, siempre que dispongan de una fuente de alimentación de energía constante. En zonas propensas a los cortes de electricidad, puede considerarse la posibilidad de recurrir a fuentes de energía alternativas, como generadores o iluminación solar. La decisión de mostrar el logotipo de la organización en el perímetro exterior dependerá de si la organización ha determinado que la visibilidad en el contexto dado aumenta o disminuye su seguridad. En entornos en los que la organización goza de buena reputación, puede ser adecuado mostrar el logotipo, acompañado de traducciones en el idioma local.
- **Sitios desocupados.** En los lugares que permanecen desocupados por algún tiempo, las organizaciones pueden aplicar medidas para crear la ilusión de actividad, como encender y apagar periódicamente las luces y ajustar las persianas para disuadir a posibles intrusos.
- **Coherencia con las prácticas locales de seguridad.** Podría ser aconsejable adoptar niveles de seguridad del sitio similares a los de otros edificios cercanos, incluso si los niveles de riesgo percibidos no parecen justificarlo.

- **Control de acceso a aparcamientos y vehículos.** Los aparcamientos deben diseñarse de forma que impidan el acceso de vehículos no autorizados y reduzcan el riesgo de ataques a los vehículos. Cuando existen riesgos como el vandalismo, el robo de coches, la violencia de las pandillas o los atentados con explosivos, es mejor aparcar los vehículos en lugares seguros, como dentro de un recinto. También es aconsejable asegurarse de que hay suficiente espacio para aparcar cuando se elige un lugar y de que los vehículos están cerrados cuando no se utilizan. Deben establecerse procedimientos operativos para el control de las llaves de los vehículos, la organización del aparcamiento y el uso en caso de emergencia. Las disposiciones relativas al estacionamiento y el combustible deben facilitar la salida del lugar. Esto puede requerir asegurarse de que los vehículos estén completamente llenos de combustible al final de cada día y aparcados de manera que se puedan cargar y salir rápidamente.

Prevención del delito mediante el diseño ambiental

La prevención del delito mediante el diseño ambiental se centra en mejorar la seguridad del sitio mediante la manipulación del entorno físico para influir en los comportamientos y reducir las posibilidades de que se cometan delitos. A menudo esto se pasa por alto durante el diseño o la renovación de las instalaciones, o cuando se desarrollan soluciones de seguridad a lo largo del tiempo. Entre las estrategias prevención del delito mediante el diseño ambiental figuran las siguientes:

- **Vigilancia natural.** Aumentar la visibilidad exterior e interior para exponer a los posibles agresores y mejorar la sensación de seguridad de los usuarios legítimos. Implica una gestión cuidadosa del paisaje, la iluminación y la colocación de ventanas y entradas para tener líneas de visión claras y reducir las oportunidades para esconderse.
- **Control de acceso natural.** Utilizar elementos físicos como estructuras, barreras, paisajismo, iluminación y señalización para dirigir el acceso a puntos específicos y controlables.
- **Refuerzo territorial.** Definir espacios públicos, semipúblicos y privados mediante elementos físicos como edificios, vallas y paisajismo. Esto anima a los ocupantes a desafiar a los intrusos y hace que sea más fácil identificarlos.
- **Mantenimiento.** Evitar signos visibles de desorden, como ventanas rotas, grafitis y equipos abandonados, que pueden crear una impresión de abandono y negligencia que invite a delinquir.

- **Bolardos y barreras antivehículos.** Colocados estratégicamente, los bolardos pueden restringir el acceso de vehículos pero seguir permitiendo el flujo de peatones. Los bolardos pueden ser fijos, desmontables o retráctiles. Las barreras antivehículos pueden proporcionar una mayor protección contra las amenazas procedentes de vehículos y suelen estar diseñadas para resistir impactos a alta velocidad. Las opciones incluyen barreras de hormigón armado, bolardos de acero y sistemas de cables. Los bolardos pueden integrarse en el sistema general de seguridad perimetral, complementando muros y puertas.
- **Integración de las medidas de protección perimetral.** Mediante una combinación de barreras físicas y otras medidas de protección, las organizaciones pueden establecer una defensa en capas. Armonizar estas medidas de protección perimetral con los objetivos de seguridad más amplios de la organización, incluida la promoción de la aceptación y la buena disposición entre la población local, es fundamental para garantizar un enfoque coherente e integral de la salvaguardia del personal y los activos.

El perímetro interior

Es aconsejable que las organizaciones evalúen cada sitio desde la perspectiva de un intruso e identifiquen los posibles puntos débiles, sobre todo alrededor de las puertas y las ventanas, pero también de las puertas del garaje y el sótano.

- **Puertas de entrada.** Las organizaciones debe asegurarse de que las puertas de entrada son resistentes, incluidos los marcos y las bisagras. Si hay cristales en la puerta, considere la posibilidad de reemplazarlos. Instalar un visor óptico (mirilla) junto con una cerradura principal y auxiliar en las puertas exteriores puede mejorar la seguridad. Para mejorar la seguridad interna, las organizaciones pueden considerar la instalación de una cadena de seguridad y un cerrojo corredizo o una barra resistente en la puerta. Colocar candados fuertes en la parte superior e inferior de la puerta con anillos para candados soldados también proporciona mayor protección. Por último, es aconsejable colocar los botones de pánico o teléfonos leños de las puertas de entrada para evitar que un intruso bloquee su acceso.
- **Ventanas.** Las organizaciones pueden querer asegurar las ventanas, sobre todo en la planta baja, con barrotes, rejas o persianas, siempre que sean fáciles de abrir desde dentro en caso de emergencia. Si las ventanas de los pisos superiores son accesibles desde el exterior, puede ser conveniente asegurarlas con barrotes o rejas. Es importante asegurarse de que no puedan desatornillarse o retirarse fácilmente desde el exterior.
- **Rutina nocturna.** Puede ser aconsejable cerrar las cortinas por la noche para evitar que los intrusos observen quién y cuántas personas hay dentro del edificio. El personal puede dejar una luz encendida al salir del lugar para dar la impresión de que todavía hay alguien adentro. Todas las cerraduras y cerrojos deben revisarse para asegurarse de que funcionan correctamente, y deben cerrarse de forma rutinaria al anochecer o antes de acostarse.

- **Salida alternativa de emergencia.** En caso de incendio, intrusión o disturbios, es aconsejable disponer de una salida alternativa del edificio. Esta vía de evacuación, incluidas las protecciones de las ventanas, debe ser de fácil acceso desde el interior, teniendo en cuenta los perfiles personales de todo el personal (como las necesidades de movilidad). Si ya hay rejas en las ventanas, es posible que las organizaciones quieran modificarlas para facilitar la salida desde el interior. Esto podría implicar colocar bisagras en las rejas en un lado y asegurarlas con un candado, asegurando que los ocupantes puedan acceder rápidamente a la llave en caso de emergencia.
- **Alarmas antirrobo y circuito cerrado de televisión (CCTV).** Aunque las alarmas antirrobo y las cámaras de CCTV pueden ser poco comunes en muchos contextos de ayuda, las organizaciones podrían considerar su uso como medida de seguridad adicional. Ambas suelen depender de un suministro eléctrico, aunque algunas alarmas antirrobo funcionan con baterías. Las cámaras de CCTV tienen un efecto disuasorio limitado, a menos que los intrusos sepan que están instaladas y cómo funcionan, y exista una posibilidad razonable de que los descubran. Los dispositivos de seguridad de altos decibelios, que funcionan de forma remota y direccional, generan un sonido insoportable que puede impedir que intrusos o incluso grupos de manifestantes sigan avanzando hacia el interior de las instalaciones. Suelen estar equipados con protección contra sabotajes y funcionan con baterías.

Consideraciones básicas de seguridad contra incendios

Para abordar el riesgo de incendio, deben considerarse los siguientes aspectos:

- Instalar detectores de humo y de monóxido de carbono, y colocar extintores en la cocina y en cada planta: los incendios eléctricos y de aceite requieren un extintor de CO₂ o de polvo; para otros tipos de fuego, debe utilizarse un extintor de espuma o de agua.
- Verificar los extintores y hacerles mantenimiento al menos una vez al año.
- Identificar las vías de evacuación en caso de incendio y asegurarse de que, cuando estén cerradas desde el interior, puedan abrirse rápidamente.
- Organizar simulacros de incendio con regularidad, sobre todo si hay mucha rotación de personal.
- Asegurarse de que los calefactores de gas tienen una ventilación adecuada y termopares (dispositivos que impiden el suministro de gas sin una llama piloto u otra fuente de ignición). Los calefactores sin termopares no deben dejarse desatendidos y no deben utilizarse por la noche.

- Designar formalmente a personas formadas para garantizar que el personal con discapacidad reciba ayuda en caso de emergencia (a veces descrito como un sistema de camaradas de apoyo); estas personas deben ser miembros del personal que pasen la mayor parte del tiempo en las instalaciones.
- Colocar los mapas de evacuación en un lugar notorio, pero no a la vista de los transeúntes, y codificar tal vez la identificación de las habitaciones para ayudar al personal y a los visitantes sin servir también como una guía para posibles intrusos.

Habitaciones seguras

Una habitación segura puede servir como un refugio crítico para los ocupantes durante emergencias, ya que proporciona protección frente a intrusos hasta que llegue la ayuda. La mayoría de estas habitaciones no está diseñada para resistir impactos de bombas o proyectiles.

- **Ubicación y accesibilidad.** Una habitación segura debe ser de fácil acceso, y lo ideal es que se encuentre en el centro del edificio para poder entrar rápidamente. Alternativamente, las plantas superiores pueden convertirse en zonas seguras asegurando las escaleras con rejas con cerradura durante las horas vulnerables, como, por ejemplo, durante la noche.
- **Elementos de seguridad.** Lo ideal es que la habitación segura está equipada con puertas reforzadas y ventanas seguras para disuadir a los intrusos. Debe haber un teléfono o una radio de emergencia para pedir ayuda. Las organizaciones pueden plantearse instalar sistemas de comunicación ininterrumpida para mantener la conectividad durante los cortes de electricidad. En el interior de la habitación segura puede colocarse en un lugar destacado una lista con los números de contacto principales, incluidos los de los servicios de emergencia y los equipos de respuesta internos.
- **Suministros de emergencia.** La habitación segura debe estar equipada con los suministros esenciales para mantener a los ocupantes durante una emergencia. Puede incluir botiquines de primeros auxilios, una pequeña cantidad de agua, alimentos no perecederos y provisiones sanitarias. Se pueden agregar sillas, colchones y ropa de cama en caso de que el personal tenga que refugiarse durante periodos más largos o durante la noche. Los artículos perecederos y los medicamentos deben revisarse y reponerse periódicamente.
- **Capacitación y simulacros.** Las sesiones periódicas de capacitación y los simulacros (incluidos los ejercicios de simulación) familiarizan a los ocupantes del edificio con la ubicación, la disposición y los procedimientos relativos a la habitación segura, e incluyen indicaciones sobre cómo acceder a ella rápidamente y qué hacer mientras se refugian en ella durante una emergencia.

- **Protocolos de comunicación.** Es aconsejable establecer protocolos de comunicación claros dentro de la habitación segura, que describan los procedimientos para contactar con los servicios de emergencia y coordinarse con los equipos de respuesta externos. Es conveniente designar a personas responsables de iniciar la comunicación con las autoridades y proporcionar información actualizada sobre la situación. Un sistema jerárquico de comunicación puede facilitar la difusión de la información y la toma de decisiones.

► *Para obtener más información sobre la seguridad de las comunicaciones, véase el capítulo 6.1.*

7.2.3 Gestión de riesgos de la seguridad del sitio

Conciencia individual

La seguridad del sitio es responsabilidad de todos. Todos, incluidos los recepcionistas, los telefonistas, los limpiadores y los jardineros, deben estar atentos e informar todo evento inusual o sospechoso, así como las violaciones de los procedimientos de seguridad (por ejemplo, si se dejan puertas o ventanas abiertas o llaves tiradas por ahí). En el caso de los inmuebles residenciales, esto incluye a todos los residentes (incluidos los familiares). Se debe comunicar a estas personas que no pueden dejar entrar a desconocidos en la vivienda, dar información a desconocidos que llamen por teléfono, dar detalles sobre la distribución de la oficina o permitir que se dupliquen sus llaves. Los recepcionistas pueden desempeñar un papel clave en el control de los visitantes y las llamadas telefónicas, así como de las cartas y los paquetes que se entregan y pueden recibir formación sobre cómo reportar cualquier cosa o persona que parezca sospechosa.

Guardias

A veces, las organizaciones humanitarias utilizan guardias para sus viviendas, almacenes y oficinas. Los guardias pueden ser contratados directamente o a través de un proveedor local. Pueden ser ineficaces si carecen de formación, están mal instruidos, mal pagados, mal equipados o mal gestionados. Lamentablemente, esto no es inusual en muchos de los contextos en los que se desarrolla la labor humanitaria. Tampoco es raro encontrar una cama en la caseta de vigilancia de los recintos de las organizaciones humanitarias, lo que aumenta la probabilidad de que el guardia se quede dormido durante su turno. Durante el día, los guardias pueden estar ocupados haciendo otras cosas y distraerse. Al contratar guardias, es importante establecer claramente las condiciones del trabajo e incluirlas en el contrato.

Al contratar y gestionar a los guardias, hay que tener en cuenta lo siguiente:

- Obtener referencias confiables y, si es posible, contratar a personas del barrio más cercano. Esto puede garantizar que estén familiarizados con la zona y sus residentes habituales, y puede aumentar su motivación para identificar a posibles infractores.

- Comprobar las capacidades lingüísticas de los posibles empleados. Los principales habitantes de un edificio deben poder comunicarse con el guardia.
- Contratar y desplegar una cantidad suficiente de guardias para detectar intrusiones y apoyarse mutuamente mientras trabajan juntos.
- Asegurarse de que los guardias reciban una presentación completa de la organización.
- Si el guardia tiene que llevar un arma (letal o de otro tipo), las circunstancias en las que se puede utilizar deben registrarse por el contrato firmado con la persona o el proveedor del servicio y reflejar la política de seguridad de la organización. Se recomienda que estas políticas sean revisadas por el asesor jurídico de la organización. Las organizaciones pueden incluir estipulaciones contractuales contra el consumo de sustancias nocivas (por ejemplo, alcohol) durante el servicio y contra trabajos adicionales que puedan afectar al rendimiento del guardia.
- Suministro de equipos esenciales, instrucción y capacitación. El equipo puede incluir ropa de lluvia, linternas, un silbato u otro dispositivo de alarma y una radio portátil o un teléfono en la caseta de vigilancia.
- Proporcionar un libro de guardia con instrucciones sobre cómo llevar el registro y notificar actividades sospechosas, así como una lista de números de contacto clave.
- Proporcionar instrucciones claras y formación sobre cómo tratar a los visitantes y qué hacer si se encuentran con un intruso.
- Proporcionar instrucciones claras sobre el monitoreo de los alrededores, el patrullaje del recinto y las normas relativas a verjas, puertas, ventanas y llaves.
- Normalmente, los guardias solo tienen acceso al perímetro exterior (no al interior), especialmente en las propiedades residenciales. En el edificio de oficinas, normalmente deben tener acceso a los pasillos, las escaleras y el tejado, pero no necesariamente a las oficinas.
- En las zonas donde hay un riesgo alto de intrusión o robo, considere la posibilidad de alternar los horarios de las inspecciones de rutina con rondas en horarios menos predecibles. Puede ser conveniente distribuir a los guardias, con al menos uno en una posición en la que no puedan ser fácilmente observados y dominados (por ejemplo, en una terraza).
- Los perros adiestrados específicamente con fines de vigilancia pueden ser excelentes para alertar rápidamente sobre la presencia de intrusos y para disuadirlos. Sin embargo, un perro es potencialmente peligroso para las personas que no conoce, y puede ser necesario adoptar medidas de control para proteger a los visitantes legítimos y al personal.

Gestión del acceso

El control del acceso comienza con el establecimiento de medidas clave de control de la gestión. Las organizaciones también pueden utilizar tarjetas magnéticas de acceso, cerraduras cifradas (sistemas electrónicos de pulsadores que solo permiten la entrada a las personas que conocen el código), lectores magnéticos, tarjetas inteligentes o dispositivos biométricos. Las oficinas más grandes, ubicadas normalmente en las grandes ciudades, pueden controlar el acceso instalando puertas o torniquetes que funcionan con tarjetas magnéticas. Lo ideal es establecer controles de gestión para todos ellos. Los sistemas pueden ser caros y fallar si se interrumpe el suministro eléctrico o si el mecanismo funciona mal.

Llaves del sitio

Las organizaciones pueden llevar un registro exhaustivo de las llaves y de quién las tiene, y asegurarse de que el número de llaves en circulación está estrictamente controlado. Si hay alguna duda sobre la seguridad de las llaves, es aconsejable cambiar las cerraduras. Las llaves pueden etiquetarse en código para que no puedan identificarse fácilmente. Las llaves de repuesto deben guardarse de forma segura en una caja de seguridad para llaves con un cristal frontal que pueda romperse en caso de emergencia.

Se debe informar a todo el personal con acceso a las llaves, incluido el personal doméstico, de los protocolos de gestión de llaves, por ejemplo, llevar las llaves encima en lugar de dejarlas en escritorios, coches o abrigos y bolsos desatendidos. Por lo general, las llaves no deben duplicarse a menos que el equipo directivo de la organización lo ordene explícitamente, y debe notificarse inmediatamente si se pierde alguna llave.

Ser demasiado estricto con el control de las llaves puede conllevar sus propios peligros. Por ejemplo, el personal puede ser incapaz de escapar de un edificio en llamas si no tiene acceso a la llave de la puerta de salida de emergencia. Del mismo modo, la respuesta a una llamada de emergencia de un compañero puede retrasarse si las llaves del vehículo están guardadas bajo llave.

Con respecto a los visitantes, el control de acceso cumple generalmente dos funciones: establecer el propósito y la legitimidad de un visitante y garantizar que los visitantes no constituyen una amenaza. En algunas circunstancias, el acceso tiene que controlarse de forma muy estricta; se puede disuadir activamente a los visitantes o dirigirlos a

un edificio separado, alejado de las instalaciones principales de la organización. En cualquier caso, es conveniente disponer de un espacio de espera específico para los visitantes. Este espacio debe ser fácilmente visible para el personal de seguridad y la recepcionista. Debe estar conectado a un aseo, pero ningún visitante que esté esperando la autorización debe poder acceder al edificio sin control.

Existen grados de control de seguridad. Por ejemplo, hacer que los visitantes firmen al entrar o salir no es una medida de seguridad en sí misma, ya que cualquiera puede entrar. Los procedimientos estándar más estrictos podrían incluir las siguientes disposiciones:

- todo el personal debe llevar una identificación visible con fotografía cuando se encuentre en las instalaciones;
- todos los visitantes deben mostrar su identificación;
- todos los visitantes reciben una identificación o un pase, que deben devolver al marcharse;
- ningún visitante puede ingresar sin la autorización explícita de la persona que quiere ver o que acepta recibirlo, y
- ningún visitante puede ingresar a menos que lo acompañe un miembro del personal.

Los procedimientos más estrictos incluyen el control de los bolsos de los visitantes y registros corporales manuales o electrónicos (para esto suelen necesitarse guardias mujeres y una capacitación especial).

En entornos de alto riesgo, no se debe dejar entrar a nadie desconocido, sin autorización o que no pueda proporcionar una identificación convincente. Antes de admitir a un visitante en el perímetro interior de un edificio, debe realizarse un primer control superficial en el perímetro exterior para determinar si puede representar una amenaza. Solo se debe dejar entrar a un visitante cuando no parezca representar una amenaza. Establecer el propósito de la visita, ponerse en contacto con el departamento anfitrión, registrar la visita y expedir un pase de visitante puede hacerse luego como un segundo paso dentro de las instalaciones, para de esta manera minimizar la cantidad de personas que esperan en la entrada principal. En caso de duda, debe indicarse a los guardias que se pongan en contacto con un supervisor.

En caso de que se encuentre a una persona sospechosa o no autorizada, se debe alertar inmediatamente al personal o a los referentes de seguridad. Podrían establecerse protocolos para avisar al personal de forma rápida y discreta, por ejemplo, a través de radios o botones de pánico. El personal de seguridad puede plantearse introducir palabras en código para pedir ayuda discretamente. Si la situación se agrava o supone una amenaza importante, puede ser necesario cerrar el edificio para asegurar las instalaciones y proteger al personal. Se recomienda explicar claramente los procedimientos de cierre de emergencia al personal, detallando las medidas que deben tomarse, como asegurar las puertas y bloquear los puntos de entrada.

Política de acceso: cuestiones que se deben considerar

- **¿Debe permitirse la entrada de los vehículos de los visitantes al recinto (si corresponde)?** Quizás sea importante considerar dónde deben aparcar los visitantes. Por ejemplo, en caso de amenaza de bomba, conviene asegurarse de que no haya vehículos ajenos a la organización en el recinto. Las organizaciones también pueden considerar la posibilidad de prohibir el estacionamiento de visitantes alrededor del edificio. A los guardias se les puede ordenar que registren los vehículos, pero se trata de una tarea especializada que requiere una formación adecuada.
- **¿Cuál es la política de la organización con respecto a los visitantes que vienen con guardaespaldas o armas a las instalaciones?** Las organizaciones pueden optar por tener una política relativa a la presencia de armas en las instalaciones de la organización, teniendo en cuenta el contexto y el tipo de visitante (por ejemplo, policías o funcionarios gubernamentales), y si se debe permitir que los visitantes que lleguen con sus propios guardaespaldas ingresen con ellos al recinto. Puede ser necesario considerar la responsabilidad potencial de la organización si se ataca a un visitante cuyos guardaespaldas no fueron autorizados a ingresar. Celebrar las reuniones en un anexo del edificio o en una terraza, donde los guardaespaldas puedan permanecer cerca, puede ser una solución práctica. Los guardias deben recibir formación sobre cómo actuar en este tipo de circunstancias.
- **¿Cómo debe gestionarse el acceso del personal de servicio y las entregas?** El acceso del personal de servicio merece una consideración cuidadosa, incluido el acceso para el personal de mantenimiento, reparación, servicios públicos y entregas. Decidir si debe permitirse la entrada del personal de servicio en los edificios en ausencia del personal pertinente, y si las llegadas pueden planificarse y programarse con antelación. Exigir la identificación del personal de servicio podría mejorar la seguridad y, en el caso de los vendedores ambulantes, el personal podría comprar sus productos fuera de la puerta para limitar el acceso.

► Para obtener más información sobre la protección armada, véase el capítulo 4.2.

Más allá de las medidas tradicionales de control de acceso, como el registro de visitantes, existe una tendencia creciente hacia el uso de métodos de autenticación biométrica, como el escaneado de huellas dactilares o del iris. La incorporación de la

autenticación biométrica a los procedimientos de control de acceso puede reforzar su postura de seguridad al tiempo que mantiene la eficiencia y la comodidad para los visitantes legítimos y los miembros del personal. Algunas organizaciones han optado por la autenticación de doble factor (por ejemplo, identificación biométrica y una tarjeta), o han creado distintos niveles de autorización para diferentes instalaciones o departamentos. Las organizaciones deben tener en cuenta los riesgos de los cortes de electricidad, así como la sensibilidad relativa a la recopilación de datos biométricos y los posibles riesgos de una violación de la seguridad de los datos. Un almacenamiento o cifrado inadecuados de los datos biométricos podría dar lugar al robo de identidad o a otras violaciones de la privacidad en caso de que se acceda ilegalmente a los datos. Estos riesgos pueden gestionarse con medidas adecuadas de almacenamiento de datos, cifrado y seguridad del sistema.

Llamadas telefónicas y cartas amenazadoras

Las llamadas problemáticas pueden ir desde llamadas de broma hasta acoso sexual y amenazas de bomba. Cuando esto suponga un riesgo, el personal debe recibir formación sobre cómo reaccionar. El uso de tecnología de identificación de llamadas o de rastreo de llamadas puede ayudar a identificar el origen de las llamadas problemáticas y contribuir a las investigaciones. Las llamadas de acoso sexual dirigidas a mujeres a veces pueden detenerse haciendo que un compañero de trabajo o de residencia conteste el teléfono. Si la persona que llama insiste, quizá sea mejor cambiar el número de teléfono. Como norma general, el personal no debe compartir su número de teléfono personal y solo debe dar el del trabajo en sus firmas de correo electrónico y tarjetas de visita.

En caso de llamadas amenazadoras, los destinatarios deben tratar de mantener la calma y ser educados; abstenerse de compartir información personal o sensible; dar la menor información posible a la persona que llama; escuchar atentamente para recabar la mayor cantidad de información posible que ayude a identificar a la persona que llama; anotar todos los detalles relevantes, incluidos el nombre y el número de teléfono, si se conocen, y denunciar la amenaza inmediatamente. Si la llamada corresponde a una amenaza de bomba, la pregunta clave será cuándo y dónde explotará la bomba. A menos que se tenga certeza de que la amenaza no es real, el edificio debe ser evacuado inmediatamente. Si la oficina recibe una carta amenazadora, debe tratarse con seriedad y compartirla rápidamente con el equipo directivo, las autoridades y otras organizaciones de la zona, según corresponda.

Cartas o paquetes sospechosos

Aunque no es una amenaza habitual para las organizaciones humanitarias, es posible que se entregue una carta o un paquete contaminado deliberadamente con una sustancia química o biológica tóxica o que contenga explosivos. Los posibles indicadores son restos de pólvora en el sobre, un olor extraño y, en el caso de una bomba, un sonido de tictac o cables visibles. El paquete puede ser inusualmente pesado para su tamaño, la dirección puede estar mal escrita o la carta o el paquete pueden estar dirigidos a alguien que ya no trabaja en la organización. Puede carecer de franqueo postal o tener un franqueo excesivo, lo que indica que no fue despachado en una oficina de correos.

Las cartas o paquetes de este tipo deben dejarse donde están, se debe desalojar la sala y avisar al personal de seguridad. A toda persona que haya manipulado el objeto se le debe solicitar lavarse inmediatamente con jabón, especialmente las manos. Es posible que la carta o el paquete tenga que ser destruido o abierto por personal de seguridad especialmente capacitado y con el equipo adecuado (la contaminación con una sustancia tóxica requiere, como mínimo, que se utilicen guantes de protección y, posiblemente, mascarillas, ya que algunas sustancias pueden entrar en el cuerpo por inhalación).

7.2.4 Centros de distribución

Varias medidas pueden contribuir a aumentar la seguridad del personal y de las poblaciones objetivo en los puntos de distribución.

- **Comprensión de la población objetivo.** Es conveniente conocer bien a la población objetivo, incluida la forma en que esta población, así como otras personas de los alrededores, pueden percibir la distribución, si existen posibles tensiones entre los grupos y la probabilidad de interferencias políticas. El personal debe estar atento a cualquier signo de desesperación por los productos que se distribuyen e identificar a quienes podrían estar interesados en manipular el proceso de distribución.
 - **Gestión del perímetro y del sitio.** Puede ser conveniente definir adecuadamente el perímetro. Para ello, pueden colocarse vallas o muros, o barricadas con supervisión adicional.
 - **Ubicación del centro de distribución.** Puede ser aconsejable elegir un lugar en el que no se obstaculice el tráfico habitual, tanto de vehículos como de peatones, y asegurarse de que el lugar no atrae a transeúntes o molestias no deseadas.
 - **Gestión de los puntos de entrada y salida.** Se debe determinar un punto de entrada y otro de salida. Una gestión eficaz de las aglomeraciones en el punto de entrada puede permitir separar rápidamente a los beneficiarios legítimos de la ayuda de los que no reúnen los requisitos para recibirla. Es necesario asegurarse de que haya personal suficiente para controlar a las personas indisciplinadas. Los puntos de salida deben gestionarse con cuidado, garantizando que los destinatarios puedan abandonar el lugar de forma segura y ordenada.
 - **Control y movimiento de multitudes.** Es importante mantener a la gente en movimiento. El personal o las autoridades pueden supervisar la zona para evitar que se reúnan multitudes, incluidos los familiares que ayudan a los beneficiarios, e impidan la salida de los demás. Se debe considerar la seguridad y la protección de las personas que se marchan del lugar, en particular las mujeres y los niños pequeños. Por ejemplo, transportar bultos grandes puede hacer que los beneficiarios de la ayuda sean más vulnerables a posibles ataques, y el personal podría considerar formas de hacer que los productos distribuidos sean menos llamativos.
- *Para obtener más información sobre los riesgos relativos a la distribución, véase el capítulo 7.6 sobre disturbios civiles.*

Más información

Orientación

Davis, J. et al. (2020). Módulo 8, Comunicaciones y seguridad de la información. En *Seguridad en práctica: herramientas de gestión de riesgos para organizaciones de ayuda humanitaria*. 4ª edición. Global Interagency Security Forum (<https://gisf.ngo/wp-content/uploads/2020/04/2227-EISF-2018-Seguridad-en-pra%CC%81ctica-Spanish.pdf>).

Global Interagency Security Forum. (2024) 3. *Site security*. NGO Security Toolbox (<https://gisf.ngo/toolbox-pwa/resource/3-site-security/>).

International Crime Prevention Through Environmental Design

Association. (s.f.). The International Crime Prevention Through Environmental Design Association (www.cpted.net/).

Safer Edge. (2014). *Office closure*. Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/office-closure/>).

Source8. (2015). *Office opening: a guide for non-governmental organisations*. Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/office-opening/>).

7.3 Seguridad del dinero en efectivo

Aunque la amplia adopción del dinero digital ha reducido en general la cantidad de efectivo que las organizaciones necesitan guardar y manejar, en muchos contextos y circunstancias sigue siendo necesario tener, mover y realizar transacciones en efectivo. En este capítulo se abordan múltiples aspectos de la seguridad del dinero en efectivo, desde el hurto hasta los riesgos asociados a los programas de asistencia en efectivo.

7.3.1 Riesgos

Aunque los riesgos relacionados con el efectivo y su gestión suelen ser responsabilidad del personal de finanzas y del equipo directivo, las actividades que implican el uso de efectivo conllevan importantes riesgos de seguridad. Retirar o transportar grandes cantidades de dinero en efectivo hace que los trabajadores humanitarios sean vulnerables a robos. Viajar con dinero en efectivo, especialmente en zonas apartadas o afectadas por conflictos, aumenta el riesgo de sufrir ataques de delincuentes o grupos armados. También hay que considerar y abordar los riesgos de seguridad de los programas de asistencia en efectivo, incluidos los riesgos relacionados con la transferencia de fondos a los beneficiarios de la ayuda, el fraude y el daño a la reputación.

7.3.2 Medidas de mitigación de riesgos

Un primer paso esencial es llevar a cabo un diagnóstico de riesgos relativo al flujo de efectivo en la organización, seguido del diseño y la aplicación de medidas de mitigación en los puntos de alto riesgo.

En la siguiente sección se destacan las medidas para hacer frente a los riesgos asociados a las actividades relacionadas con el efectivo. Lo ideal sería que el personal de seguridad y de finanzas decidiera y aplicara estas medidas en colaboración.

Reducción del uso de efectivo

Las organizaciones pueden reducir su uso de efectivo mediante el pago con cheques, transferencias bancarias, tarjetas de prepago, tarjetas de crédito u otros métodos de pago electrónicos. Ningún método de pago está exento de riesgos, por lo que es importante establecer directrices sobre el uso de tarjetas de crédito y supervisarlas periódicamente. Las organizaciones que realizan transacciones importantes deben considerar la posibilidad de contratar un seguro específico contra pérdidas o robos.

Riesgos de las transacciones electrónicas

Existen varias formas de transferir dinero sin utilizar efectivo. Los riesgos asociados a estos mecanismos están más relacionados con la seguridad financiera, operativa o digital, aunque pueden tener repercusiones en la seguridad del personal, por ejemplo, si el retraso de una transferencia provoca tensiones con las partes que esperan el pago. Los servicios digitales de transferencia de dinero y las aplicaciones móviles pueden ser vulnerables a los hackeos, los ataques de suplantación de identidad y otras formas de fraude y ciberdelincuencia. Los sistemas informales, denominados hawala, se vieron sometidos a presión tras el 11-S por la preocupación de que algunas transacciones contribuyeran a la transferencia ilegal de fondos a grupos proscritos. La legislación antiterrorista y las prácticas bancarias de reducción de riesgos han impuesto trabas adicionales a las organizaciones que intentan mover grandes sumas de dinero, por lo que, en algunos casos, se ven obligadas a utilizar efectivo de nuevo.

Un riesgo específico relacionado con los pagos financieros electrónicos se deriva de la posibilidad de que las transferencias de donantes a organizaciones o los pagos dentro de las organizaciones sean objeto de ataques. Los delincuentes saben que se envían grandes sumas de dinero de los donantes a las organizaciones operativas y también entre la sede y las oficinas de los programas. Los delincuentes podrían interceptar los correos electrónicos, clonar las cuentas del personal y emitir instrucciones falsas para desviar pagos a cuentas bancarias externas. Los cambios o instrucciones de última minuto en relación con transferencias bancarias importantes también pueden indicar una actividad fraudulenta.

- Véase el capítulo 6.2 para obtener más información sobre las medidas de mitigación relacionadas a los riesgos de seguridad digital.

Discreción

Cuando se maneja dinero en efectivo, la discreción es importante. Cuanta menos gente lo sepa, menor será el riesgo. Las comunicaciones que pueden interceptarse pueden transformarse en algún tipo de código. Si se retira dinero de un banco, la transacción debe organizarse discretamente con antelación; evitar retirar dinero a horas o en días fijos (por ejemplo, antes del pago mensual de los sueldos) puede reducir el riesgo. Para pagar a los proveedores, lo mejor es utilizar alguno de los medios de pagos alternativos al uso de efectivo mencionados anteriormente, sobre todo cuando se trata

de grandes sumas. Si el personal utiliza regularmente el mismo hotel o proveedor, las organizaciones pueden considerar la posibilidad de crear una cuenta.

En algunas economías, y en casos de hiperinflación, la gran cantidad y volumen de efectivo puede suponer un problema. Incluso cantidades relativamente modestas de moneda internacional pueden traducirse en fajos considerables de billetes locales. Al retirar efectivo de un banco, el personal puede intentar que el dinero se entregue en billetes de mayor denominación, y debe tener en cuenta los aspectos prácticos del transporte y el almacenamiento.

Orientaciones para el personal sobre buenas prácticas relativas al manejo seguro del efectivo

- Hacer todo lo posible para limitar el uso de dinero en efectivo.
- Garantizar límites de crédito y de extracción de efectivo razonables.
- Verificar los estados de cuenta bancarios e investigar todo pago desconocido.
- Disponer de una lista con los números de teléfono para llamar en caso de pérdida o robo de tarjetas de crédito.
- Bloquear o cancelar una tarjeta de crédito en caso de pérdida tan pronto como sea posible.
- Mantener los PIN seguros.
- No perder de vista las tarjetas de crédito cuando se entregan para pagar una compra.
- No resistirse al enfrentarse a un ladrón.

Limitar la exposición

Existen varias formas de reducir la exposición a pérdidas o robos. Los pagos puntuales a los proveedores reducen el tiempo que el efectivo se guarda en la oficina. Otra práctica habitual es fijar un límite máximo de efectivo que se puede retirar, transferir o guardar en la caja fuerte de la organización. Sin embargo, reducir el tamaño de las transacciones individuales probablemente aumentará el número de transacciones que hay que hacer, lo que aumenta los costes. Dado que el mayor riesgo se corre al trasladar físicamente el efectivo, las organizaciones deben considerar la posibilidad de trasladar sumas más grandes con menos frecuencia, sobre todo si se dispone periódicamente de formas más seguras de transportarlo, como vuelos en helicóptero o grandes convoyes. Las organizaciones también pueden considerar los riesgos en los distintos puntos de la cadena de transferencia, desde el banco hasta la caja fuerte de la organización y el destinatario final, y representar esta cadena en un diagrama de flujo. Quizás sea posible reducir el número de eslabones de la cadena, por ejemplo, pidiendo a los proveedores que vengan a la oficina a recibir el pago en lugar de llevarles el dinero en efectivo.

Si existen riesgos de allanamiento y robo, es aconsejable no guardar todo el dinero en un mismo lugar y tener a mano una cantidad determinada en un lugar evidente para satisfacer y distraer a los delincuentes. Parte del dinero debe ser fácilmente accesible; el resto debe estar bien escondido. En los viajes, debe animarse al personal a llevar dinero en efectivo en distintos lugares y entre los distintos miembros del personal que viajan. En periodos de mucha tensión, cuando sea necesario retirar, reubicar o evacuar al personal, el dinero en efectivo puede distribuirse entre quienes se marchan, en parte para repartir el riesgo y en parte para garantizar que el personal tenga algo de dinero en efectivo a mano en caso de que se separen. Las organizaciones deben comprobar que el personal se siente cómodo llevando encima grandes cantidades de dinero en efectivo en situaciones de gran tensión o durante los viajes.

En los países en los que la reubicación o la evacuación son muy probables, los movimientos de efectivo deben organizarse y planificarse con antelación. También deben tenerse en cuenta y abordarse las necesidades de efectivo del personal que pueda tener que permanecer en su puesto.

Ejemplo: Sudán

En Sudán una organización necesitaba entregar dinero en efectivo con regularidad como dinero “de emergencia” para los desplazamientos a las oficinas locales. Para reducir la visibilidad y la vulnerabilidad del efectivo, se colocaba una cantidad de billetes entre dos hojas de papel (o una sola hoja doblada), y esto se ponía dentro de una bolsa de plástico especial y se plastificaba. En el papel se imprimían previamente las instrucciones y una línea de puntos. De este modo se formaba un paquete prolijo y protegido de dinero previamente contabilizado. También facilitaba la contabilidad, ya que no era necesario contar el efectivo cuando se entregaba y se devolvía, siempre que la bolsa estuviera intacta.

Reducir la previsibilidad

La rutina aumenta el riesgo, por lo que las organizaciones deben tratar de evitar la previsibilidad en las actividades que impliquen el manejo de efectivo. Los siguientes son algunos de los puntos de riesgo previsible más comunes:

- La nómina mensual.
- Pagos especiales al personal antes de su reubicación o evacuación.
- Llegada de personal a aeropuertos y traslados a hoteles u oficinas (los ladrones pueden vigilar la hora de llegada de determinados vuelos y atacar los vehículos cuando se encuentren en la ruta principal de acceso a la localidad).

- Desplazamientos del personal de la oficina al banco y viceversa, especialmente si utilizan la misma ruta y viajan aproximadamente a la misma hora del día.
- Los traslados al banco en los que participa más de un miembro del personal pueden indicar que se va a depositar o retirar una suma de dinero mayor de lo normal.

Las precauciones de seguridad adicionales pueden reducir la previsibilidad. Por ejemplo:

- Utilizar un vehículo local o alquilado sin distintivos o una ruta menos obvia para llevar al personal del aeropuerto a la oficina o al hotel.
- Cambiar los periodos salariales y los días de pago, aunque es probable que esto no sea bien recibido por el personal.
- Autorizar a diversos miembros del personal a ir al banco, modificando las rutas y los horarios.

Reducir la vulnerabilidad

Las organizaciones pueden aplicar medidas para reducir la vulnerabilidad relacionada con el dinero en efectivo, como orientaciones para viajar con efectivo y medidas de seguridad del sitio.

Para reducir la vulnerabilidad cuando se transporta dinero en efectivo por carretera, se recomienda que participen al menos dos personas y, preferiblemente, más de un vehículo. Lo mejor es evitar la previsibilidad, y esto puede implicar variar el número de pasajeros y coches utilizados. En casos extremos, puede utilizarse una escolta armada o un vehículo blindado, aunque es probable que esto atraiga una atención no deseada. Al retirar dinero de un cajero automático, la opción más segura puede ser ir a un cajero ubicado en una calle concurrida con una cola de personas esperando para hacer lo mismo. Lo ideal es que el personal saque dinero durante el día y en compañía de un colega que vigile los alrededores. Alguien podría ver a los miembros del personal sacando dinero en efectivo y podría seguirlos, por lo que es recomendable evitar las calles menos transitadas o las zonas más conflictivas después de ir a un cajero automático.

En la oficina, las organizaciones pueden instalar cajas fuertes y adoptar medidas rigurosas de seguridad del sitio. A continuación se mencionan algunos aspectos relativos a la seguridad de las cajas fuertes:

- Fijar la caja fuerte al suelo y colocarla en una oficina trasera o detrás de un escritorio para que quede oculta a los visitantes.
- Instalar una cerradura que requiera dos llaves para abrirse y entregar las llaves a dos personas distintas, o utilizar una cerradura de llave y otra con una combinación numérica.
- Estar preparado en caso de que los ladrones amenacen con violencia al personal si no abre la caja fuerte (por ejemplo, aconsejar al personal que entregue las llaves o la combinación si los amenazan).

- Si la persona que posee la llave está a punto de ausentarse o tomarse vacaciones, asegúrese de que se realice un recuento adecuado del efectivo con la nueva persona encargada de la llave, firmado por ambas partes.

► *Para obtener más información sobre la seguridad del sitio, véase el capítulo 7.2.*

Nota sobre el robo de identidad

El robo de identidad y el fraude financiero, incluido el de tarjetas de crédito, son problemas importantes y crecientes. Algunas de las formas más comunes son las siguientes:

- Robo físico de tarjetas y fraude con cheques (impresión de cheques falsos o robo de cheques).
- “Buscar entre la basura” (robar documentos financieros de la basura).
- Redireccionamiento de cuentas (cumplimentación fraudulenta de un formulario de cambio de dirección).
- Arrebatarse una cartera o un bolso.
- Detener a personas, incluso en sus domicilios, mientras sus cómplices llevan sus tarjetas de crédito y sus PIN a un cajero automático cercano.

7.3.3 Programación de asistencia en efectivo

Muchas organizaciones humanitarias han adoptado programas de asistencia en efectivo como una de sus principales modalidades para ayudar a las personas en situaciones de crisis. El mecanismo de transferencia puede tomar diversas formas, como las transferencias digitales o los vales, pero también puede implicar la distribución de dinero en efectivo. El mecanismo de distribución debe ser adecuado al contexto y tener en cuenta las limitaciones prácticas y los riesgos de seguridad. El uso de bancos y otras instituciones financieras reduce potencialmente los riesgos de seguridad asociados a las transferencias en efectivo.

En general, al transportar y guardar efectivo para actividades de programas de asistencia en efectivo, se aplican muchas de las medidas de mitigación enumeradas anteriormente. El análisis de riesgos, las medidas de mitigación y el monitoreo son cruciales. Es aconsejable que el personal lleve a cabo un diagnóstico de riesgos programáticos que tenga en cuenta todos los riesgos de seguridad para las organizaciones, el personal y los beneficiarios de la ayuda antes y durante el programa de asistencia en efectivo. No solo el personal corre riesgos al manejar dinero en efectivo: no es raro que grupos delictivos ataquen y roben a los beneficiarios de los programas de asistencia en efectivo. Los lugares de distribución de efectivo también son lugares de alto riesgo y probablemente se requerirán medidas de seguridad del sitio adecuadas.

También existen riesgos asociados al almacenamiento de los datos financieros y de los beneficiarios. Algunas organizaciones emplean herramientas de gestión de datos de terceros para almacenar y gestionar los datos. Los posibles riesgos para la seguridad de los datos y reputacionales asociados al uso de estas herramientas deben evaluarse antes de su adopción.

Ejemplos de mitigación de riesgos en los programas de asistencia en efectivo

En Afganistán y Somalia, las organizaciones han utilizado con éxito empresas locales de envío de remesas para entregar dinero a personas que viven en zonas remotas e inseguras.

En Etiopía, una organización internacional contrató un seguro contra el riesgo de pérdida al transportar efectivo a proyectos en zonas donde no había bancos.

En Zambia, una organización internacional subcontrató la entrega en zonas rurales alejadas a un grupo bancario y de servicios financieros, que utilizó vehículos de empresas de seguridad para entregar el efectivo, acompañados por la policía local.

La transferencia de efectivo a gran escala crea riesgos institucionales relacionados con el fraude, el desvío y la apropiación indebida. También existen riesgos de cumplimiento en relación con la legislación de antiterrorismo y las sanciones de los donantes en entornos de alto riesgo. Estos riesgos suelen considerarse más graves que si se produjeran con la ayuda en especie, por lo que es preciso analizarlos detenidamente, prepararse, mitigarlos y responder a ellos. El daño reputacional de cualquier actividad fraudulenta relacionada con las operaciones de una organización humanitaria puede tener graves consecuencias (véase el ejemplo más abajo).

Ejemplo: Turquía

En 2015 una investigación de la Agencia de los Estados Unidos para el Desarrollo (USAID, por sus siglas en inglés) reveló un fraude en el que estaban implicadas varias personas, incluidas algunas que trabajaban para ONG, relacionado con la ayuda humanitaria transfronteriza de Turquía a Siria. La investigación descubrió importantes casos de corrupción en el proceso de contratación, como sobornos, manipulación de licitaciones, comisiones ilegales y connivencia entre el personal de logística de las ONG y vendedores comerciales corruptos. Al menos un miembro del personal de una ONG internacional se enfrentó a cargos penales y a la extradición, y las ONG implicadas sufrieron graves daños en su reputación entre sus donantes y el público en general. El enorme volumen y la rapidez con que las ONG internacionales recibieron financiación en Turquía, presionadas para aumentar rápidamente sus operaciones, fue un factor que influyó en la inadecuación de los controles financieros, los procedimientos de adquisición y los requisitos de verificación.

Fuente: Parker, B. (11 de septiembre de 2018) “US bans aid workers in Turkey-Syria scam”, The New Humanitarian (www.thenewhumanitarian.org/news/2018/09/11/us-bans-aid-workers-turkey-syria-scam).

Más información

Orientación, herramientas y análisis

CALP Network. (s.f.). Recursos clave (www.calpnetwork.org/key-resources/).

Comité Internacional de la Cruz Roja. (2021). *SAFE: Security and safety manual for humanitarian personnel* (www.icrc.org/en/publication/4425-safe-manuel-de-securite-pour-les-humanitaires).

Cornish, L. (28 de noviembre de 2017). New security concerns raised for RedRose digital payment systems. Devex (www.devex.com/news/new-security-concerns-raised-for-redrose-digital-payment-systems-91619).

Movimiento Internacional de la Cruz Roja y de la Media Luna Roja. (s.f.). CTP risk matrix template. [Módulo 3, Paso 1, Subpaso 4]. Cash in emergencies toolkit (<https://cash-hub.org/guidance-and-tools/cash-in-emergencies-toolkit/all-toolkits/>).

Parker, B. (11 de septiembre de 2018). US bans aid workers in Turkey-Syria scam. The New Humanitarian (www.thenewhumanitarian.org/news/2018/09/11/us-bans-aid-workers-turkey-syria-scam).

7.4 Criminalidad

En muchos entornos operacionales, la criminalidad es el incidente de seguridad que con más frecuencia afecta al personal humanitario. En este capítulo se analiza el abanico de amenazas que plantean los delincuentes, desde la criminalidad común y el acoso hasta el crimen organizado, la actividad delictiva de bandas y el solapamiento con grupos armados no estatales, y el modo en que las organizaciones humanitarias pueden comprender y gestionar mejor los riesgos de la criminalidad.

7.4.1 Tipos de delitos y entornos criminales

La criminalidad es universal, y las organizaciones que responden a las crisis humanitarias a menudo tendrán que enfrentarse a distintos niveles de criminalidad. Aunque la mayoría de los ataques importantes que afectan a los trabajadores humanitarios han sido perpetrados históricamente por las fuerzas armadas estatales y grupos armados no estatales, en muchos contextos los delincuentes representan la mayor amenaza. Un estudio de 2015 concluyó que las tasas de homicidio intencionado superaban en todo el mundo a las muertes en conflictos.⁹⁹

La actividad delictiva puede verse motivada por una serie de factores, como la elevada desigualdad, la concentración de desventajas y el desempleo generalizado. En muchos contextos humanitarios, la criminalidad aumenta como consecuencia de la inestabilidad política y cuando los Gobiernos carecen de capacidad para hacer cumplir el Estado de derecho y ofrecer oportunidades económicas significativas. En muchos contextos, el fácil suministro de armas puede contribuir al aumento de los delitos violentos. La presencia de operaciones de asistencia puede ser a menudo un imán y un caldo de cultivo para la corrupción y la criminalidad. Además de los delitos de oportunidad, las organizaciones humanitarias pueden ser el objeto del crimen organizado. Los grupos delictivos aprovechan los cambios en el entorno político y económico para ampliar la captación ilegal de rentas.

Las distinciones entre delincuentes, partes en conflicto y otros actores políticos y económicos suelen ser muy difusas. Los grupos armados no estatales y las autoridades gubernamentales colaboran a menudo con grupos delictivos cuando sus intereses coinciden, y los movimientos rebeldes suelen mantenerse gracias a actividades ilícitas como el tráfico de drogas. Sin embargo, a efectos del análisis y la gestión de riesgos, las organizaciones siguen considerando útil distinguir entre la criminalidad por motivos económicos y los riesgos de seguridad derivados de los conflictos armados, los atentados terroristas y los disturbios civiles.

99 Secretariado de la Declaración de Ginebra. (2015) *Global burden of armed violence 2015: every body counts*, Cambridge University Press (<https://doi.org/10.1017/CBO9781107707108>).

Entre los ejemplos de delitos por motivos económicos que las organizaciones humanitarias deben incluir en sus estrategias de evaluación y mitigación de riesgos se incluyen los siguientes:

- hurto menor;
- allanamiento;
- extorsión y soborno;
- robo de carteras y arrebato de bolsos;
- asalto;
- robo a mano armada;
- intimidación y extorsión;
- robo de vehículos, y
- secuestros con pedido de rescate, incluidos los “secuestros exprés”, en los que se retiene a las víctimas el tiempo suficiente para obligarlas a retirar fondos con su tarjeta bancaria.

La mayoría de los delitos enumerados anteriormente implican violencia o de convertirse en violentos. También es importante recordar que trabajar en un contexto de mucha criminalidad, donde predomina la inseguridad, puede tener un impacto grave en el nivel de estrés y en el bienestar general de una persona. Esto se agrava cuando el personal procede de ese país, y los riesgos del entorno afectan también a su familia.

Los delitos de cuello blanco, como la malversación y el fraude, también son comunes, aunque tienen una relevancia directa menor para el deber de cuidado y la gestión de riesgos para la seguridad física (a pesar de que pueden tener efectos secundarios que generen riesgos para la seguridad) y suelen ser competencia de los equipos financieros, jurídicos y de cumplimiento de una organización.

► *Para obtener más información sobre los raptos, véase el capítulo 7.9.*

► *Para obtener más información sobre los riesgos en la esfera digital, véase el capítulo 6.2.*

La presencia de grupos organizados que intentan ejercer el control sobre las zonas y los habitantes locales añade otro nivel de riesgo. El riesgo de acoso y extorsión puede ser especialmente difícil de mitigar, ya que la selección de objetivos es persistente en lugar de oportunista, y las organizaciones pueden verse sometidas a actos repetidos de acoso, intimidación y extorsión. La cultura de las bandas, las normas sociales y el deseo de estatus dentro del grupo suelen crear un entorno en el que se espera y recompensa la violencia. La amenaza para los actores humanitarios que trabajan en estos contextos requiere una atención considerable y medidas sólidas de gestión de riesgos de seguridad.

7.4.2 Consideraciones prácticas

Las buenas prácticas en la gestión de riesgos de seguridad exigen comprender el contexto y los riesgos de la criminalidad, y adoptar medidas para mitigarlos y disuadir a los posibles agresores. Las medidas incluyen el aumento de la protección física de los bienes y de la seguridad general del sitio para evitar robos e irrupciones, así como la orientación del personal sobre cómo reducir la exposición a los riesgos de delitos. Algunas organizaciones han invertido en programas que abordan la criminalidad y la violencia, como forma de reducir los riesgos para la comunidad en su conjunto.

Comprensión del contexto

Al igual que en el caso de la inseguridad relacionada con los conflictos, los análisis del contexto exhaustivos y actualizados, los diagnósticos de riesgos y el mapeo de los actores son herramientas fundamentales para gestionar los riesgos que supone la criminalidad.

Comprender el contexto implica determinar si el riesgo procede del crimen organizado, oportunista o de una combinación de ambos. El crimen organizado es complejo y suele estar vinculado a intereses políticos y económicos más amplios, a diferencia de la criminalidad oportunista, “común” o “callejera”, que es más esporádica y situacional.

Los índices de criminalidad por lo general son más elevados en las zonas urbanas que en las rurales, y los delitos violentos tienden a concentrarse en zonas específicas dentro de las ciudades e incluso barrios.¹⁰⁰ Normalmente, existe un alto grado de agrupación espacial y demográfica para muchos tipos de delitos violentos y no violentos. Dado que la violencia urbana genera cada vez más crisis humanitarias y que la acción humanitaria se desarrolla cada vez más en zonas urbanas, el análisis del contexto, el mapeo de los actores y la evaluación básica de los grupos delictivos —quién, qué, dónde, cuándo y cómo— deben formar parte del diagnóstico de riesgos.

La densidad y la complejidad de los entornos urbanos hacen que las dinámicas de la seguridad puedan diferir entre un gran número de pequeñas zonas muy próximas entre sí, lo que exige diagnósticos de riesgos más puntuales que los que pueden ser necesarios para las zonas rurales. Varias organizaciones humanitarias de América Latina y el Caribe mapean activamente las bandas y los territorios que controlan, y recurren a informantes locales para mantener actualizados los datos. Las líneas pueden cambiar a diario, incluso cambiando según la calle.

Las organizaciones se benefician de la identificación de fuentes fiables de información dentro de la comunidad o entre otros agentes locales. Por ejemplo, los grupos delictivos organizados pueden transportar, entregar y distribuir productos en lugares y horas determinados. Con la ayuda de las comunidades locales, es posible saber cuándo suelen tener lugar las actividades, y así evitar esas horas y lugares.

¹⁰⁰ Véase Muggah, R., Aguirre, K. y Chainey, S. (2017) “Targeting ‘hot spots’ could drastically reduce Latin America’s murder rate”, *Americas Quarterly* (<https://americasquarterly.org/article/targeting-hot-spots-could-drastically-reduce-latin-americas-murder-rate/>).

Las organizaciones también deben evaluar los efectos de su presencia y su programación en las economías delictivas; no basta con suponer que, si no interfieren directamente con sus intereses, los delincuentes responderán del mismo modo. En las zonas con altos niveles de criminalidad violenta, la “sensibilidad a la criminalidad” debe unirse a la sensibilidad a los conflictos entre las competencias y los enfoques de una organización.

► *Para obtener más información sobre los análisis y las evaluaciones, véase el capítulo 4.1.*

Medidas de mitigación de riesgos

Además de realizar un diagnóstico de riesgos y otros esfuerzos para comprender mejor el contexto, las organizaciones podrían considerar algunos de los ejemplos de medidas prácticas de mitigación de riesgos presentados en la tabla 22.

Tabla 22 Medidas prácticas para disuadir, prevenir y mitigar los riesgos de delitos

Medida	Descripción	Notas
Gestión de activos y trabajo a distancia.	• Mantener un inventario actualizado de los bienes e implantar sistemas de seguimiento de los artículos de gran valor. • Realizar auditorías periódicamente. • Tener protocolos para el trabajo a distancia.	Dado que el teletrabajo se ha vuelto más habitual, las organizaciones han tenido que introducir procedimientos relativos al transporte y al almacenamiento de los equipos informáticos y otros materiales de trabajo. Medidas sencillas, como no transportar los ordenadores en bolsos específicos para ellos, pueden reducir significativamente el riesgo.

Medida	Descripción	Notas
Reporte de incidentes	Asegurarse de que se denuncien los incidentes, incluso los de menor importancia.	Incidentes delictivos aparentemente menores pueden tener consecuencias graves. El robo de un teléfono, un ordenador o un bolso que contenga información personal o financiera puede brindar mayores oportunidades para que se cometa un delito. Incidentes delictivos aparentemente menores pueden tener consecuencias graves. El robo de un teléfono, un ordenador o un bolso que contenga información personal o financiera puede brindar mayores oportunidades para que se cometa un delito. Reportar adecuadamente todos los casos y analizarlos correctamente puede favorecer la respuesta y las futuras medidas de prevención. <i>Para obtener más información sobre la denuncia de incidentes, véase el capítulo 4.4.</i>
Medidas de seguridad física, incluido el control del acceso	- Adoptar medidas contra el hurto y el robo en todas las oficinas e instalaciones del proyecto, incluso en aquellas a las que solo puede acceder el personal de la organización. - Instalar medidas de seguridad física como vallas, cerraduras, alarmas y CCTV, según corresponda. Realizar revisiones periódicas de mantenimiento. - Emplear medidas estrictas de control de acceso (por ejemplo, tarjetas de identificación y registros de visitantes) en oficinas, almacenes y centros de distribución.	<i>Para obtener más información, véase el capítulo 7.2 sobre la seguridad del sitio.</i>

Medida	Descripción	Notas
Procedimientos de gestión de dinero en efectivo	• Establecer procedimientos seguros para el manejo de efectivo, incluido el uso de bancos o métodos seguros de transferencia cuando sea posible. – Minimizar las transacciones en efectivo. – Evitar las rutinas relacionadas con los pagos. – Mantener la confidencialidad de la información.	<i>Para obtener más información, véase el capítulo 7.3 sobre seguridad relativa al manejo del dinero en efectivo.</i>
Medidas de seguridad personal	• Promover medidas de seguridad personal para el personal, como mantener una actitud vigilante y estar atento al entorno, evitar zonas y horarios de alto riesgo, evitar rutinas y rutas de desplazamiento predecibles, mantener los objetos seguros y fuera de la vista y del alcance de otras personas, evitar exhibiciones de riqueza y utilizar sistemas de camaradas de apoyo.	Todas las orientaciones deben ser específicas para cada contexto, actualizarse periódicamente y compartirse con el personal. Por ejemplo, en un contexto quizás se recomiende al personal que nunca lleve consigo dinero en efectivo u objetos de valor, mientras que en otro pueden correr un mayor riesgo personal si no tienen algo que entregar a un asaltante.
Enlace con las autoridades	• Mantener un contacto frecuente con las fuerzas del orden locales y otras autoridades.	Compartir información y buscar apoyo cuando sea necesario y si procede. Se debe tener en cuenta, sin embargo, que algunas autoridades pueden no ser fuentes fiables de información y protección en entornos en los que los actores estatales y delictivos están relacionados.
Medidas anticorrupción	• Aplicar y hacer cumplir las políticas anticorrupción, incluida la verificación de antecedentes del personal y los proveedores. • Realizar auditorías periódicas y formación de sensibilización.	–
Gestión de incidentes	• Estar preparado para responder a un incidente y proporcionar apoyo inmediato a las personas afectadas, así como atención a largo plazo.	<i>Para obtener más información sobre cómo responder a incidentes, véase el capítulo 4.4.</i>

Medida	Descripción	Notas
Cuidado del personal	- Considerar y desarrollar estructuras e intervenciones de cuidado del personal. - Proporcionar apoyo psicosocial tras un incidente, así como de manera regular para que el personal gestione el estrés.	Vivir en entornos con niveles altos de criminalidad puede provocar estrés y consecuencias psicológicas negativas en el personal y en sus familias similares a los de trabajar en entornos conflictivos. Ser víctima de un delito violento puede causar traumas físicos y psicológicos duraderos. <i>Véase el capítulo 5.4 sobre el cuidado del personal.</i>
Medidas de seguridad digital	- La criminalidad se perpetra cada vez más en línea, a través de las redes sociales y otros medios de comunicación digitales. - Aplicar medidas de seguridad digital, que incluya orientaciones para el personal sobre cómo mantenerse seguro en línea.	Por ejemplo, según la configuración de privacidad, lo que el personal publica en las redes sociales puede ser utilizado por los delincuentes para identificar y seleccionar a las víctimas. <i>Véase el capítulo 6.2 sobre seguridad digital.</i>

Acoso

El riesgo de acoso por parte de delincuentes y de otras personas es una amenaza importante para los trabajadores humanitarios. El acoso es un comportamiento abusivo que puede ser físico o verbal, y puede tener lugar en persona, por ejemplo, en los puestos de control o durante las distribuciones, o en línea. La mayoría de los casos de acoso son orales: normalmente, el acoso físico se produce tras un incidente previo de acoso oral. Esto puede suceder por diversas razones: puede ser una táctica utilizada por delincuentes para presionar al personal y que cumpla sus exigencias, o los miembros de la comunidad pueden acosar al personal debido a sus percepciones sobre el trabajo que realiza su organización. Los incidentes siempre deben denunciarse, en particular porque pueden dar lugar a amenazas más graves.

Varias medidas pueden ayudar a reducir el riesgo de acoso:

- Monitorear la opinión de la población local sobre la organización y su personal, también en las redes sociales.

- Capacitar al personal sobre cómo comportarse de forma que no llame la atención negativamente, como respetar y adaptarse a las costumbres locales, hablar de las actividades y de la misión de la organización y evitar discusiones sobre la política o la cultura locales.
- Garantizar que el personal cumpla los protocolos de seguridad, como las orientaciones relativas a los viajes, evitar grandes aglomeraciones o entornos cargados, llevar la documentación correcta, mantener una presencia en línea segura y denunciar los incidentes.
- Capacitar al personal sobre el conocimiento de la situación, incluidas las personas sospechosas y las situaciones que podrían agravarse.
- Capacitar al personal sobre cómo responder a distintos tipos de acoso (por ejemplo, retirarse de la situación y dirigirse a un lugar más seguro, pedir ayuda o llamar la atención).

Tras un incidente, las organizaciones pueden analizar con las partes interesadas por qué se produjo el acoso y cómo evitar futuros incidentes. Pueden necesitarse medidas adicionales, como la suspensión de actividades o cambios en los movimientos del personal. El personal afectado también puede necesitar atención tras el incidente.

Más allá de las medidas de protección: la negociación

Al igual que ocurre con otras amenazas a la seguridad, las organizaciones deben ser conscientes de la amenaza delictiva en los entornos en los que trabajan y comprender cómo su propia presencia y programas interactúan potencialmente con la dinámica delictiva e influyen en ella. Si bien las organizaciones humanitarias han desarrollado herramientas de mapeo, divulgación y negociación con los grupos armados y los actores que tienen el poder político, rara vez adoptan un enfoque proactivo similar respecto a los delincuentes.

Las organizaciones humanitarias suelen evitar relacionarse con grupos delictivos debido a los riesgos jurídicos, éticos y reputacionales que dicha relación puede entrañar, sin mencionar los riesgos de seguridad para la organización al convertirse en una entidad conocida para un grupo que puede decidir atentar contra ella o su personal. Entablar negociaciones con estos actores podría considerarse complicidad y dar lugar a problemas judiciales. No existe un marco jurídico similar a los Convenios de Ginebra que proporcione una base y una guía fundadas en principios y una guía para que las organizaciones se relacionen con los actores delictivos como lo harían con las partes en conflicto. También puede ser difícil identificar a quién contactar y quién tiene la autoridad para representar al grupo.

Algunas organizaciones humanitarias tuvieron éxito a la hora de negociar el acceso con actores delictivos adoptando lecciones y prácticas de grupos de desarrollo comunitario que trabajan para disminuir la violencia a nivel de base.

Las negociaciones con los grupos delictivos pueden seguir el modelo de las que se llevan a cabo con grupos armados no estatales, dirigidas a lograr objetivos concretos, como garantizar la seguridad para determinadas actividades del programa o el acceso a lugares controlados por los grupos delictivos. Al igual que en el caso de los actores en conflicto, la mejor manera de lograrlo no es apelando a principios humanitarios abstractos o a la ética, sino identificando un interés del grupo delictivo que esté en consonancia con los objetivos humanitarios. Si los delincuentes son de la zona, es posible que tengan hijos u otros familiares y vínculos sociales con la comunidad que se beneficiarían de los programas de ayuda. También pueden tener interés en ser vistos y tratados como la autoridad de control.

Ejemplo: Operar en Haití en medio del control de las bandas

Una ONG internacional que gestionaba instalaciones sanitarias en Haití se comunicaba y negociaba continuamente con los líderes de las bandas, los miembros de la comunidad, la policía y otras autoridades, haciendo hincapié en la importancia de proteger a los trabajadores y las instalaciones de salud para que estuvieran disponibles para tratar a todo el mundo, incluidos los miembros heridos de las bandas. La organización también mantenía un acuerdo confidencial con la policía que cubría la entrada en las instalaciones de la organización.

Enfoques programáticos de la gestión del riesgo de delitos

Además de la negociación directa, las organizaciones humanitarias han participado en intervenciones programáticas a nivel comunitario dirigidas a reducir la criminalidad y la violencia. Por ejemplo, las organizaciones que trabajan en América Latina y el Caribe han puesto en marcha proyectos centrados en la reducción de la criminalidad y en las alternativas para los jóvenes en situación de riesgo.¹⁰¹ Estos enfoques requieren un análisis muy localizado, incluso calle por calle, y medidas de divulgación.

¹⁰¹ Véase, por ejemplo, Cure Violence Global, que aplica una metodología de salud pública para afrontar la violencia: <https://cvg.org/about/>.

Más información

Investigación y análisis

Comité Internacional de la Cruz Roja. (junio de 2023). Delincuencia organizada. Revista Internacional de la Cruz Roja (923) (<https://international-review.icrc.org/reviews/irrc-no-923-organized-crime>).

Global Interagency Security Forum. (2023). *Good practices, lessons learned, and the unique challenges affecting security risk management in urban humanitarian responses* (<https://gisf.ngo/resource/good-practices-lessons-learned-and-the-unique-challenges-affecting-security-risk-management-in-urban-humanitarian-responses/>).

Humanitarian Outcomes. (2021). *Aid worker security report 2021. Crime risks and responses in humanitarian operations* (<https://humanitarianoutcomes.org/AWSR2021>).

Lucchi, E. (2013). *Humanitarian interventions in situations of urban violence*. ALNAP (<https://alnapp.org/documents/4666/alnap-lessons-paper-urban-violence-1.pdf>).

Mohor, D. (17 de mayo de 2023). Gang violence in Latin America poses a challenge for the aid sector. The New Humanitarian (www.thenewhumanitarian.org/analysis/2023/05/17/gang-violence-latin-america-challenge-aid-sector).

Muggah, R. (2017). A humanitarian response to Central America's fragile cities. The humanitarian consequences of violence in Central America. *Humanitarian Exchange* 69. Humanitarian Practice Network (<https://odihpn.org/publication/humanitarian-response-central-americas-fragile-cities/>).

Muggah, R., Aguirre, K. y Chainey, S. (9 de marzo de 2017). Targeting "hot spots" could drastically reduce Latin America's murder rate. *Americas Quarterly* (<https://americasquarterly.org/article/targeting-hot-spots-could-drastically-reduce-latin-americas-murder-rate/>).

Savage, K. y Muggah, R. (2012). *Urban violence and humanitarian action: Engaging the fragile city*. ALNAP (<https://alnapp.org/help-library/resources/urban-violence-and-humanitarian-action-engaging-the-fragile-city/>).

Secretariado de la Declaración de Ginebra. (2015). *Global burden of armed violence 2015: Every body counts*. Cambridge University Press (<https://doi.org/10.1017/CBO9781107707108>).

Recursos

Cure Violence Global. (s.f.). About Cure Violence Global. (<https://cvg.org/about/>).

Davis, J. et al. (2020). Module 2: Actor mapping and context analysis. En *Security to go: a risk management toolkit for humanitarian aid agencies*. 4ª edición. Global Interagency Security Forum (www.gisf.ngo/resource/security-to-go/).

Instituto Igarapé. (s.f.a). *Humanitarian action in situations other than war* (<https://igarape.org.br/en/hasow/>).

Instituto Igarapé. (s.f.b). Homicide monitor (<https://homicide.igarape.org.br/>).

7.5 Vigilancia hostil

La vigilancia hostil puede representar un riesgo importante para la seguridad de los trabajadores humanitarios y las poblaciones vulnerables. Sin embargo, puede pasarse por alto en la labor estándar de gestión de riesgos de seguridad humanitaria porque a menudo se trata de un riesgo “invisible”. Sobre la base de los conocimientos y las experiencias de los trabajadores de derechos humanos y justicia social, para quienes esta es una preocupación constante, en este capítulo se examinan la vigilancia hostil, sus implicaciones para el trabajo humanitario y las respuestas a ella, incluyendo su detección y las medidas antivigilancia.

7.5.1 Comprender la vigilancia hostil

Mientras que la vigilancia implica un monitoreo sistemático para recabar información o ejercer control, la vigilancia hostil se dirige específicamente a personas, bienes o propiedades e implica la planificación previa a un ataque o intenciones maliciosas. Considere que no toda la vigilancia es encubierta; a veces se pretende que sea visible (por ejemplo, como forma de intimidación).

Tabla 23 Distinción entre vigilancia y vigilancia hostil

Vigilancia	Vigilancia hostil
• La vigilancia puede ser llevada a cabo por diversas entidades, incluidos los Gobiernos y las empresas privadas, con fines de seguridad, recopilación de información o monitoreo. • La vigilancia puede servir a fines legítimos como la seguridad pública o la aplicación de la ley, pero también puede utilizarse de forma perversa, violando la privacidad o reprimiendo la disidencia. • Algunos ejemplos son la vigilancia gubernamental de las comunicaciones, el seguimiento de las redes sociales y la vigilancia empresarial para estudios de mercado.	• La vigilancia hostil se lleva a cabo con intenciones hostiles, amenazando directamente la seguridad de los objetivos. • Su objetivo es recopilar información, identificar vulnerabilidades o planificar y ejecutar acciones hostiles como robos, espionaje o ataques físicos. • El acecho, las actividades de reconocimiento, el uso de tecnologías de programas espía y el monitoreo de las medidas de protección para detectar puntos débiles que puedan explotarse son comportamientos típicos asociados a la vigilancia hostil.

La vigilancia hostil en un contexto humanitario puede ser llevada a cabo por diversos actores, como grupos armados no estatales, fuerzas gubernamentales y delincuentes (véase el recuadro más abajo).

Posibles agentes de vigilancia

- Los grupos armados no estatales pueden llevar a cabo una vigilancia hostil para recopilar información, controlar las actividades humanitarias y atacar a los trabajadores humanitarios.
- En las regiones afectadas por conflictos, las fuerzas gubernamentales o los organismos de seguridad pueden ejercer la vigilancia de las organizaciones humanitarias en un intento de rastrear la posible infiltración de grupos armados no estatales en la población local.
- Los delincuentes pueden llevar a cabo actividades de vigilancia para explotar o perturbar las operaciones humanitarias con fines lucrativos o para favorecer sus intereses.

Las organizaciones deben ser conscientes de que las agencias de inteligencia estatales pueden vigilar a los actores humanitarios y de que esta recopilación de información puede influir en la forma en que otros actores gubernamentales nacionales perciben a estas organizaciones y se relacionan con ellas. Las regiones donde hay conflictos armados o crisis humanitarias son especialmente vulnerables a este tipo de vigilancia.

7.5.2 Tipos de vigilancia hostil

En esta sección se presentan tipos comunes de vigilancia hostil y las tácticas asociadas a cada uno. Estas tácticas pueden utilizarse individualmente o combinadas.

Vigilancia física

- **Tareas de vigilancia:** Las personas pueden de manera individual o en grupos vigilar a sus objetivos desde un lugar oculto para observar y controlar sus movimientos.
- **Observación:** Los agentes hostiles pueden seguir de cerca a sus objetivos, a veces a pie, para recopilar información sobre sus rutinas, actividades o vulnerabilidades.

Vigilancia técnica

- **Escuchas electrónicas:** Los agentes hostiles pueden utilizar dispositivos de escucha, micrófonos ocultos o aparatos para intervenir teléfonos para interceptar y controlar las comunicaciones, incluidas las conversaciones telefónicas, los correos electrónicos y los mensajes electrónicos.

- **Videovigilancia:** Se emplean cámaras y dispositivos de grabación para vigilar las actividades, los movimientos y las interacciones de los objetivos en diversos lugares, como espacios residenciales, lugares de trabajo o espacios públicos.
- **Seguimiento por GPS:** Los dispositivos de seguimiento del sistema de posicionamiento global pueden instalarse de forma encubierta en vehículos o efectos personales para vigilar los movimientos de los objetivos y recopilar datos sobre su ubicación.
- **Vehículos aéreos no tripulados y satélites:** Las tecnologías avanzadas como los vehículos aéreos no tripulados (drones) ofrecen capacidades de vigilancia aérea, lo que permite a los actores hostiles realizar actividades de reconocimiento y vigilancia a distancia. Los satélites proporcionan una amplia cobertura de vigilancia, mediante imágenes de alta resolución y el monitoreo de grandes áreas geográficas en tiempo real.

Cibervigilancia

- **Hackeo y programas maliciosos:** Los agentes hostiles pueden utilizar técnicas de hackeo, suplantación de identidad o programas maliciosos o espía para obtener acceso no autorizado a los dispositivos, redes o cuentas en línea de los objetivos, lo que les permite vigilar las actividades, robar información sensible y datos de contactos, o interrumpir las operaciones.
- **Ingeniería social:** Los agentes hostiles manipulan a personas o empleados mediante engaños o tácticas psicológicas para extraer información o acceder a datos sensibles, contraseñas o sistemas.
- **Exploración de datos e inteligencia de fuentes abiertas:** Los agentes hostiles pueden recopilar información de fuentes públicas, plataformas de redes sociales o bases de datos en línea para reunir datos sobre objetivos, sus afiliaciones o vulnerabilidades.

► Véase el capítulo 6.2 sobre seguridad digital.

Observación encubierta

- **Disfraces e identidades encubiertas:** Los actores hostiles pueden disfrazarse o crearse identidades falsas para mezclarse con el entorno o para “relacionarse” subrepticamente con los objetivos, a fin de llevar a cabo una vigilancia encubierta sin levantar sospechas.
- **Espionaje y operaciones encubiertas:** Consiste en infiltrarse en organizaciones, grupos o comunidades objetivo para recopilar información, establecer relaciones o acceder a zonas o información restringidas.

Ejemplo: Yemen

En Yemen los trabajadores humanitarios sufrieron la vigilancia de agentes gubernamentales locales y de grupos internacionales. Después de las visitas a los proyectos, se contactó a las comunidades destinatarias y se les preguntó por la organización y su personal. Esto afecta la forma en que las comunidades destinatarias ven a la organización y puede socavar las percepciones locales.

7.5.3 Riesgos asociados a la vigilancia hostil

Los riesgos asociados a la vigilancia hostil en la ayuda humanitaria van más allá de las preocupaciones inmediatas en materia de seguridad. En esencia, el riesgo en este contexto se refiere a la incertidumbre en torno a la seguridad y a la eficacia de la labor de asistencia y abarca las amenazas al personal, los recursos y la integridad de las operaciones humanitarias. La vigilancia hostil amplifica estos riesgos al introducir la posibilidad de que se comprometa la confidencialidad, se ataque a objetivos específicos y se interrumpan las operaciones.

Por ejemplo, si se interceptan las comunicaciones o se comprometen los sistemas de datos, la población y las comunidades locales pueden quedar expuestas a represalias por parte de actores hostiles. Del mismo modo, los trabajadores humanitarios que operan en entornos en los que predomina la vigilancia hostil pueden enfrentarse a mayores riesgos de sufrir daños físicos, raptos o acoso.

La percepción de las organizaciones humanitarias como objetivos legítimos de vigilancia o ataques también puede disuadir a las personas de solicitar ayuda o cooperar con las iniciativas humanitarias, lo que aumenta aún más las vulnerabilidades y dificulta el acceso a los servicios esenciales.

7.5.4 Cómo responder a la vigilancia hostil

Los actores humanitarios pueden responder eficazmente a las tácticas de vigilancia hostil si conocen el problema y adoptan medidas preventivas. Esto puede lograrse evaluando los riesgos de vigilancia, capacitando al personal en medidas preventivas y aplicando estrategias de detección y en contra de la vigilancia. La detección de la vigilancia consiste en observar y monitorear atentamente el entorno para identificar posibles amenazas o actividades sospechosas antes de que se conviertan en violaciones

de la seguridad. Las medidas en contra de la vigilancia se centran en contrarrestar y disuadir los esfuerzos de vigilancia hostil.

Antivigilancia y contravigilancia

Existen diferencias entre la antivigilancia y la contravigilancia: esta última excede el alcance de este documento y suele ser utilizada por las fuerzas armadas y las fuerzas del orden con formación y habilidades especializadas. La contravigilancia es reactiva y agresiva, mientras que la antivigilancia es una medida preventiva. La antivigilancia implica tácticas más sencillas, como variar las rutinas y las rutas, aplicar medidas de seguridad física como cámaras y personal de vigilancia, y fomentar las relaciones con la comunidad para obtener apoyo adicional a la hora de detectar y responder a la vigilancia. En lugar de depender de medidas de protección de gran alcance o de la fuerza, la antivigilancia puede integrarse en el enfoque de aceptación de una organización, haciendo hincapié en la interacción y en la comunicación periódicas con las comunidades locales.

Un punto de partida puede ser una conversación con el personal de seguridad o con expertos locales o regionales que conozcan las amenazas y los riesgos de la vigilancia relacionados con el lugar, el perfil del personal o el programa. Esto puede ir seguido de un diagnóstico de riesgos exhaustivo. Una vez detectados los riesgos de vigilancia, las organizaciones pueden formar a su personal e implementar medidas preventivas.

► *Para más información sobre cómo realizar un diagnóstico de riesgos, véase el capítulo 4.1.*

Los defensores y activistas de derechos humanos suelen utilizar una combinación de las siguientes técnicas de antivigilancia según el contexto; algunas de ellas también pueden ser utilizadas por las organizaciones humanitarias para detectar y frustrar la vigilancia hostil.

Tabla 24 Ejemplos de técnicas de mitigación de riesgos

Técnica	Descripción
Reconocimiento de patrones	El establecimiento de patrones de referencia de comportamientos y actividades normales en las instalaciones de la organización o en los lugares donde se ejecutan los programas o proyectos permite detectar anomalías o desviaciones que pueden indicar actividades de vigilancia.
Análisis de rutas	La variación periódica de las rutas y los horarios de las operaciones y el personal humanitarios minimiza la previsibilidad y reduce la probabilidad de ser objeto de vigilancia.
Observación del comportamiento	Formar al personal para que observe y notifique los comportamientos o los individuos sospechosos, como personas que merodean o muestran un interés inusual por las actividades de la organización, puede ayudar a detectar a tiempo las posibles amenazas.
Contramedidas de vigilancia técnica	El uso de equipos de detección electrónica para buscar dispositivos o señales de vigilancia ocultos en las instalaciones de la organización ayuda a identificar los intentos de vigilancia encubierta.
Monitoreo de las comunicaciones	El monitoreo de los canales de comunicación para detectar actividades inusuales o no autorizadas, como intentos de acceso no autorizado o tráfico de red inusual, puede ayudar a detectar intentos de vigilancia electrónica.
Higiene de las comunicaciones digitales y protección de los dispositivos	Evitar las redes wifi abiertas, utilizar VPN y un gestor de contraseñas, abstenerse de compartir información personal sensible por WhatsApp y otras plataformas de comunicación inseguras, verificar la información antes de compartirla y mantenerse alerta ante la información errónea.
Minimización de datos	Adoptar medidas para reducir la cantidad de datos que las personas tienen en sus dispositivos, como los de aplicaciones de citas, los perfiles en redes sociales o en línea y los datos bancarios, que podrían utilizarse en su contra si se viola la seguridad del dispositivo.
Seguridad operacional	Aplicar medidas estrictas de seguridad operacional, como limitar la difusión de información sensible y emplear el principio de la necesidad de saber.
Alianzas de colaboración	Establecer colaboraciones sólidas con expertos en contravigilancia, así como con organizaciones de justicia social y derechos humanos, y valerse de su experiencia para afrontar el riesgo de la vigilancia hostil.

Se pueden incorporar medidas de mitigación en el plan de seguridad para abordar los riesgos de vigilancia identificados, y se puede desarrollar una formación al respecto para que el personal pueda contribuir activamente a los esfuerzos de detección de la vigilancia. El personal pertinente debe conocer y recibir formación periódica sobre las amenazas de la vigilancia, las técnicas de detección y los procedimientos de notificación. Cabe señalar que la concienciación sobre la vigilancia hostil suele estar ausente de los cursos habituales de HEAT; integrar los aspectos fundamentales de la concienciación sobre la vigilancia en estos cursos sería muy conveniente.

La gestión del riesgo de la vigilancia hostil en la asistencia humanitaria exige un enfoque polifacético que abarque la detección de la vigilancia y las estrategias en contra de la vigilancia adaptadas a los retos específicos del sector. Para responder a la vigilancia hostil, los actores humanitarios pueden aplicar una variedad de estrategias, como el reconocimiento de patrones, el análisis de rutas, la observación de comportamientos, las contramedidas de vigilancia técnica, el monitoreo de las comunicaciones y las medidas de seguridad operacional. Fomentar una cultura de concienciación sobre la vigilancia mediante sesiones periódicas de formación y sensibilización ayuda al personal a contribuir activamente a los esfuerzos de detección de la vigilancia. Las alianzas de colaboración con expertos en contravigilancia y con organizaciones de justicia social o derechos humanos pueden aumentar aún más la eficacia de las medidas antivigilancia.

Más información

Recursos sobre la vigilancia

Haggerty, K.D. y Gazso, A. (2005). Seeing beyond the ruins: surveillance as a response to terrorist threats. *The Canadian Journal of Sociology* (<https://doi.org/10.2307/4146129>).

McCue, C. (2007). Surveillance detection - an overview. En *Data mining and predictive analysis* (www.sciencedirect.com/topics/computer-science/surveillance-detection).

7.6 Disturbios civiles

Las protestas, las manifestaciones, los disturbios y otras concentraciones o alteraciones masivas, así como la respuesta de las autoridades y cualquier acto delictivo o extorsión que se derive de ellos, pueden suponer un riesgo para las personas, los bienes y las operaciones humanitarias. En cualquier contexto operacional, pero especialmente en entornos cargados de tensiones y disputas, los disturbios civiles pueden estallar repentinamente e implicar o convertirse en violencia y agresión. La violencia puede surgir espontáneamente o puede ser planificada e instigada. Las reuniones pacíficas planificadas, como los actos políticos o las protestas, pueden desembocar inesperadamente en disturbios civiles. Del mismo modo, las tensiones latentes durante mucho tiempo pueden estallar repentinamente en actos de violencia tras algún acontecimiento desencadenante. Las organizaciones humanitarias también pueden enfrentarse a los riesgos de las multitudes descontroladas, incluso de la violencia de pandillas, donde se ejecutan los programas, como los lugares de distribución y los campamentos de desplazados. Este capítulo abarca algunas de las posibles medidas de mitigación de estos riesgos, incluida la concienciación sobre la situación, la preparación (procedimientos operativos estándar y planes de contingencia) y la formación y concienciación sobre las posibles maneras de proceder.

7.6.1 Monitoreo y análisis de la situación

Aunque es difícil de predecir y controlar, es importante que los disturbios civiles y sus diferentes manifestaciones formen parte del análisis de riesgos y de los esfuerzos regulares de monitoreo.

- **Si bien no siempre se puede predecir, es conveniente identificar los posibles factores desencadenantes.** Algunos ejemplos son: los cambios políticos y económicos, como la decisión de una potencia extranjera de intervenir militarmente; una crisis económica repentina provocada por las condiciones del comercio internacional; la decisión del Gobierno de recortar las subvenciones a productos esenciales como los alimentos o el combustible; la decisión de cerrar un campamento de refugiados antes de que la gente esté dispuesta a volver a casa; la detención o el asesinato de una figura destacada; la distribución de ayuda; y las elecciones nacionales o locales.
- **La tensión y la frustración crecientes pueden detectarse a menudo con antelación.** Es importante monitorear de cerca los medios de comunicación locales y su opinión y, si es posible, esta debe ser una responsabilidad de un miembro del personal o de una unidad. Esto podría incluir el seguimiento de las noticias locales y de las redes sociales, el mantenimiento del contacto con las comunidades y los líderes locales y la comprobación de los niveles de aceptación.
- **El análisis del contexto puede ayudar a predecir las posibles respuestas a los disturbios civiles.** El contexto jurídico y la forma en que se desarrollaron los acontecimientos en el pasado pueden ayudar a predecir cómo pueden responder las autoridades locales y otros actores a las manifestaciones y otras concentraciones. Estos datos pueden incorporarse a la planificación y a las medidas de preparación.

Ejemplo: Las respuestas no violentas a los disturbios civiles pueden suponer un riesgo para las operaciones

La violencia no es el único riesgo al que se enfrenta el personal de las organizaciones humanitarias durante los periodos en los que se producen disturbios civiles. Un ejemplo de esto se produjo durante las elecciones de 2018 en la República Democrática del Congo, donde las autoridades cortaron los servicios de internet y SMS en todo el país durante 20 días, lo que repercutió en las operaciones de asistencia y en la gestión de los riesgos de seguridad.

Las organizaciones podrían considerar las siguientes preguntas como parte de sus tareas de monitoreo y análisis.

- ¿Hubo disturbios civiles en el pasado? Si es así, ¿dónde empezaron y cómo evolucionaron? ¿Hay algún patrón que pueda repetirse? ¿Cuáles fueron las principales causas? ¿Qué nivel de violencia hubo? ¿Quién o qué fue el objetivo de esa violencia?
- ¿Qué factores pueden desencadenar los disturbios civiles? ¿Qué forma puede adoptar la violencia? ¿Cómo respondieron anteriormente las autoridades ante los disturbios civiles?
- ¿Quiénes son los objetivos del resentimiento local y cuál es la causa fundamental de esta tensión?
- ¿Son la organización o su personal vulnerables al riesgo de disturbios civiles? ¿Cómo pueden mitigarse las vulnerabilidades?
- ¿Corren algunos trabajadores más riesgos que otros, teniendo en cuenta su perfil de riesgo personal?
- ¿Existen riesgos para proyectos o tipos de intervención específicos, por ejemplo, proyectos considerados contrarios a la cultura o a la religión locales, o percibidos como un apoyo a una u otra parte beligerante?
- ¿Cómo responden las autoridades ante los disturbios civiles a nivel nacional, local y comunitario? ¿Gas? ¿Cañón de agua? ¿Balas de goma?
- ¿Cómo responden las autoridades religiosas o étnicas ante los disturbios civiles (legislación y prácticas indígenas)?

En relación con las propias actividades y programas de la organización, deben considerarse las siguientes preguntas:

- ¿Qué expectativas tienen los habitantes locales?
- ¿Esperan algo de la organización, por ejemplo, la distribución de asistencia?
- ¿Puede la organización gestionar las expectativas mediante una comunicación clara previa a cualquier actividad programática?

Ejemplo: Personal de las Naciones Unidas asesinado en una protesta inconexa en Afganistán

Una organización que se encuentre cerca de donde se desarrollan los disturbios civiles puede correr el riesgo de sufrir actos de violencia aunque no sea el objetivo directo, como lo demuestra este ejemplo de las Naciones Unidas. En 2011 hubo protestas en el norte de Afganistán en respuesta a la quema de un Corán por un pastor estadounidense en Florida. La protesta fue prevista, pero la violencia se extendió de forma espontánea e inesperada. Cuando los manifestantes irrumpieron en el recinto de las Naciones Unidas, los guardias abrieron fuego. Murieron cuatro guardias, tres miembros del personal de las Naciones Unidas y cinco manifestantes.

7.6.2 Planificación y preparación

Entre las medidas de planificación y preparación podrían figurar las siguientes:

- **Procedimientos operativos estándar y planes de contingencia.** Los planes y los procedimientos deben cubrir todos los acontecimientos posibles que puedan tornarse violentos (protestas planificadas, actos electorales, actos sociales y comunitarios, distribución de asistencia y cualquier otra concentración grande) y sus consecuencias (restricciones gubernamentales, robos, saqueos y otras formas de violencia). Es probable que cada oficina requiera sus propios procedimientos y protocolos de seguridad, que incluyan planes de contingencia (planes de hibernación, evacuación y reubicación); listas de contactos actualizadas (a disposición de todo el personal); listas de contactos actualizadas para emergencias médicas (hospitales y compañías de vuelos chárter, por ejemplo), y protocolos de seguridad de la información (copias de seguridad periódicas de los ordenadores y archivos o documentos marcados para ser destruidos y llevarse en caso de evacuación, por ejemplo). Una vez elaborados los planes, hay que informar y brindar capacitación al personal sobre los procedimientos y las expectativas.

- **Tomar medidas de protección.** Las medidas deben referirse directamente a los riesgos y a las amenazas detectados. Podrían designarse y prepararse habitaciones seguras en cada edificio, con kits de hibernación, equipos de comunicación, botiquines de primeros auxilios y extintores de incendios. En caso de apagones o interrupción de los servicios de comunicación, todos los edificios de la organización deben disponer de sistemas de reserva de energía y comunicaciones.

► Véase el capítulo 7.2 sobre la seguridad del sitio.

- **Gestión de movimientos.** Si los disturbios civiles son inminentes, la organización puede considerar modalidades de trabajo alternativas para su personal, como el trabajo desde el domicilio, la reducción de la cantidad de personal o las restricciones de movimiento. También debe considerarse cuándo y dónde es probable que se reúnan las multitudes y hacia dónde se desplazarán (a través de qué ruta). En el caso de un acto político, las rutas pueden estar claramente definidas. En el caso de una distribución, esto incluiría rutas de entrada y salida bien gestionadas para los destinatarios de la ayuda y el personal, así como el establecimiento de zonas de respuesta de primeros auxilios.

- **Respuesta de gestión de incidentes y crisis.** La organización debe estar preparada para responder rápidamente en caso de que se produzca un incidente crítico o si los disturbios civiles desencadenan una respuesta organizativa de gestión de crisis.

► Para obtener más información sobre la respuesta a incidentes y la gestión de crisis, véase el capítulo 4.4.

- **Capacitación en medidas clave que el personal puede adoptar para mantenerse a salvo a sí mismo y a sus compañeros.** El personal tiene derecho, naturalmente, a participar en reuniones y ejercer sus derechos como ciudadanos, y las organizaciones pueden proporcionar formación para garantizar que, si estos actos se vuelven peligrosos, el personal sepa cómo mantenerse a salvo. Esta formación podría abarcar el conocimiento y la concienciación sobre las normas y procedimientos de seguridad, especialmente en torno a acontecimientos o lugares de alto riesgo, cómo responder a las armas de control de multitudes, como balas de goma, porras y gases lacrimógenos, y orientación sobre cómo buscar seguridad y refugio. El personal debe ser consciente de que su seguridad tiene prioridad sobre el equipo, las instalaciones o los almacenes de la organización. Si es posible, deben retirarse los equipos valiosos, como los ordenadores portátiles, y los equipos que no puedan retirarse podrían deshabilitarse (por ejemplo, los vehículos). Es posible que sea necesario destruir los equipos sensibles que no puedan retirarse o desactivarse.
- **Visibilidad.** El personal debe tener en cuenta su visibilidad en la organización. Si una organización goza de buena aceptación local y no es un objetivo directo, es posible que esté protegida de las multitudes si es claramente visible e identificable. Sin embargo, si una organización es un foco de insatisfacción o no es muy conocida a nivel local, sería mejor retirar la señalización de oficinas y vehículos y que el personal adopte un perfil bajo.

► Para obtener más información sobre las medidas de aceptación, véase el capítulo 4.2.

Orientaciones para periodos electorales

Conocer el contexto

¿Cómo es el sistema político y el proceso electoral? ¿Quiénes son los candidatos y cuál es su programa político? ¿Cuál es el calendario electoral?

Conocer las diferentes etapas del periodo electoral y los riesgos conexos

Las etapas suelen dividirse en preelección o campaña, sondeo o votación, recuento de votos y proclamación de resultados, investidura del ganador y las consiguientes celebraciones o manifestaciones.

Cada una de estas etapas puede durar desde un día hasta meses. Los riesgos conexos incluyen incitaciones en línea a la violencia; actos de violencia o disturbios cerca de los centros de votación o durante concentraciones masivas; escalada y perpetuación de la violencia étnica o sectaria; enfrentamientos entre grupos; robo, vandalismo y ataques físicos contra la propiedad, e intimidación y acoso a individuos, grupos y organizaciones. Las autoridades pueden imponer toques de queda y restricciones de movimiento, restringir los medios de comunicación, cortar servicios (por ejemplo, Internet y electricidad) y detener al personal de la organización. Grupos políticos han confiscado bienes de la organización con fines electorales.

Aplicar medidas de mitigación

Las medidas de mitigación pueden incluir:

- Protocolos de gestión de los desplazamientos, que incluyan las restricciones de movimientos y los toques de queda (especialmente en zonas de alto riesgo y durante determinadas etapas del periodo electoral).
- Orientaciones para el personal sobre cómo permanecer seguro al votar (por ejemplo, no viajar solo y estar atento a la situación).
- Asegurar edificios y vehículos; preparar al personal sobre cómo responder a incidentes de robo, acoso, intimidación y detención, y a un mayor número de puestos de control y controles en las carreteras.

- Adaptación de los métodos de trabajo durante los periodos electorales (por ejemplo, trabajo a distancia).
- Orientaciones para el personal sobre cómo mantenerse a salvo en un clima político caldeado (por ejemplo, evitar discusiones políticas en persona y en línea, no vestir colores que puedan estar asociados a un partido político y mantenerse alerta ante grupos y discusiones que puedan tornarse violentos).

El personal puede recibir formación sobre cómo relacionarse con los partidos políticos y las autoridades en caso de que soliciten apoyo o servicios.

7.6.3 Durante los disturbios civiles

Si los disturbios civiles estallan antes de que la organización haya tenido tiempo de adoptar medidas de mitigación, o si dichas medidas fracasan, es imprescindible que el personal supervise de cerca la situación y esté preparado para tomar medidas inmediatas. Esto podría incluir lo siguiente:

- **Aplicar los planes de contingencia.** Por ejemplo, si entran manifestantes o alborotadores en un edificio, el personal debe refugiarse inmediatamente en una habitación segura.
- **Reconsiderar los modos de transporte y restringir los desplazamientos, sobre todo en zonas de riesgo.** Por ejemplo, puede ser más seguro viajar en vehículos locales discretos o taxis que en vehículos grandes y llamativos.
- **Considerar la posibilidad de solicitar apoyo a las autoridades o a las fuerzas de seguridad.** Es probable que las fuerzas de seguridad vayan armadas, lo que debe sopesarse con la política de la organización y el nivel de riesgo, especialmente si los agentes de seguridad participan en el control o la dispersión de las multitudes.
- **Asegurarse de que se mantiene la comunicación entre el personal.**
- **Posible apertura de los canales de comunicación con los líderes de las protestas.** Lo ideal es que todas las negociaciones sean realizadas por personal que haya recibido formación en este ámbito.

Ejemplo: Organizaciones humanitarias atacadas durante actos de violencia comunitaria

En 2014 pandillas atacaron las oficinas y las viviendas de varias organizaciones humanitarias en Myanmar. Los ataques fueron impulsados por las tensiones entre dos grupos religiosos. Se irrumpió en varias oficinas y edificios, y se destruyeron muebles y equipos. Tras el incidente, el personal humanitario fue trasladado de sus oficinas, lo que interrumpió las operaciones. El incidente muestra cómo las disputas pueden agravarse rápidamente y plantear riesgos para las organizaciones humanitarias en la zona. Un mejor monitoreo del contexto local podría haber detectado los riesgos probables antes del incidente, lo que hubiera dado a las organizaciones más tiempo para preparar al personal y las instalaciones.

7.6.4 Después de los disturbios civiles

Después de un incidente, las organizaciones pueden procurar lo siguiente:

- Considerar las modalidades de trabajo del personal; quizás sea mejor que sigan trabajando desde casa y mantener un perfil bajo mientras la situación se calma.
- Mantener las medidas de protección más estrictas hasta que la situación se haya calmado claramente y no se perciban riesgos de más amenazas o represalias.
- Considerar el impacto del suceso en el personal afectado y proporcionar el apoyo necesario; es necesario estar preparado para asistir al personal que haya sido reubicado o evacuado.
- Considerar la posición de la organización en materia de relaciones públicas y qué mensajes emite, si es que emite alguno; es conveniente revisar constantemente la opinión pública y los esfuerzos de divulgación de la organización.
- Estar preparado para enfrentarse a una vigilancia hostil tras un acontecimiento grave relacionado con la organización.
- Considerar una revisión de las decisiones y las acciones de la organización; aprender de los acontecimientos pasados desempeña un papel fundamental en la mejora del sistema de gestión de riesgos de seguridad de una organización y de su enfoque programático (por ejemplo, cómo se realizan las distribuciones).

Más información

Recursos

Consejo Asesor de Seguridad en el Extranjero. (2019). *Surviving a protest* (www.osac.gov/Content/Report/ob882e6f-co5f-4d1c-9601-15f4ad6883fc).

Consejo Asesor de Seguridad en el Extranjero. (2022). *Preparing for election violence* (www.osac.gov/Content/Report/d7cd68ad-cee9-4386-b647-1e9f5c7745f6).

Consejo Asesor de Seguridad en el Extranjero. (2023). *Coups d'état: thinking through your organization's response* (www.osac.gov/Content/Report/cf6064of-7cob-4410-ae6f-228341955588).

International Foundation for Electoral Systems. (s. f.). *ElectionGuide* (www.electionguide.org/elections).

7.7 Violencia sexual

La violencia sexual es uno de los incidentes más graves a los que pueden enfrentarse los trabajadores humanitarios y puede tener consecuencias de por vida para los supervivientes. Las organizaciones humanitarias tienen el deber de proteger a su personal frente a amenazas de este tipo, ya sean internas o externas a la organización. Aunque el papel que desempeñe el personal de seguridad en la gestión de este tipo de incidentes variará en función de la organización y probablemente tendrá que gestionarse en colaboración con otros colegas (en particular, RR. HH. y otro personal especializado), la gestión de riesgos de seguridad puede ser importante para la prevención, la preparación y la respuesta a estos incidentes. En este capítulo se presentan definiciones y acciones clave que deben tener en cuenta los profesionales de la seguridad, incluida la forma de adoptar un enfoque centrado en el superviviente al responder a este tipo de incidentes.

7.7.1 Definiciones y alcance

La violencia sexual es todo acto de naturaleza sexual, o intento de obtener un acto sexual, no deseado o forzado. Puede ser perpetrada por cualquier individuo contra otro (independientemente de su relación) por medio de la fuerza física, la coacción o las amenazas. Este tipo de violencia incluye situaciones en las que los agresores se aprovechan de un entorno coercitivo o de la incapacidad de una persona para dar un consentimiento auténtico.¹⁰²

La línea que separa el acoso sexual de la coerción o la agresión puede ser a veces difícil de trazar, pero es importante comprender que estos incidentes suelen solaparse y pueden considerarse como parte de un continuo que abarca desde actos menores (por ejemplo, comentarios sexuales) hasta graves (por ejemplo, violación).¹⁰³ Véase la figura 12.

En el contexto del sector humanitario, la violencia sexual puede adoptar muchas formas diferentes, como, por ejemplo:

- selección de objetivos individuales, incluida la administración de fármacos para incapacitar a la persona;
- abuso y explotación sexuales, cuando los trabajadores humanitarios son coaccionados por personas en posiciones de poder (incluidos otros trabajadores humanitarios), y
- como arma de guerra o intimidación, cuando los trabajadores humanitarios son objetivo de los actores armados.

102 Foro Europeo Interinstitucional para la Seguridad. (2019). *Gestión de la violencia sexual contra el personal humanitario: prevención, preparación, respuesta y atención posterior* (<https://gisf.ngo/resource/managing-sexual-violence-against-aid-workers/>), pp. 12-13.

103 Foro Europeo Interinstitucional para la Seguridad (2019) proporciona una lista completa de las formas de la violencia sexual y sus definiciones.

Figura 12 Ejemplos en el continuo



Fuente: Foro Europeo Interinstitucional para la Seguridad (2019) *Gestión de la violencia sexual contra los trabajadores humanitarios: prevención, preparación, respuesta y atención posterior* (<https://gisf.ngo/resource/managing-sexual-violence-against-aid-workers/>).

Nota sobre la violencia de género

La violencia de género es un “término genérico utilizado para hacer referencia a cualquier acto dañino perpetrado contra la voluntad de una persona y que se basa en diferencias (de género) socialmente atribuidas entre hombres y mujeres”. Abarca varias formas de violencia, incluida, entre otras, la violencia sexual. Este capítulo se centra específicamente en los incidentes de índole sexual, desde el acoso hasta la agresión, dada su naturaleza extrema y el papel que desempeñan los profesionales de la seguridad en la mitigación de estos riesgos. Todas las formas de violencia de género deben considerarse y abordarse en una organización, ya que pueden ser precursoras o acompañar a la violencia sexual.

i Comité Permanente entre Organismos. (2015) *Directrices para la integración de las intervenciones contra la violencia de género en la acción humanitaria* (<https://gbvguidelines.org/en/gbv-guidelines/>).

Trabajar en entornos violentos donde el Estado de derecho es débil puede aumentar el riesgo de formas de violencia sexual especialmente traumáticas. El personal también puede sufrir violencia sexual en entornos domésticos, y las organizaciones deben debatir internamente cómo y en qué circunstancias pueden responder a este tipo de acontecimientos para garantizar el bienestar del miembro del personal afectado.

A diferencia de otros incidentes críticos en el sector humanitario, la gestión del riesgo de violencia sexual sigue viéndose obstaculizada por la estigmatización, así como por ideas erróneas sobre lo que es y por qué ocurre (por ejemplo, que solo les ocurre a las mujeres, que la mayoría de los agresores son desconocidos, que hay consentimiento si no hay resistencia física, que siempre es extremadamente violenta y que las víctimas denuncian los incidentes inmediatamente). Es imprescindible que el personal involucrado en la gestión de incidentes de esta naturaleza esté formado y pueda acceder al apoyo de expertos.

Términos conexos y áreas de trabajo

Los siguientes términos y áreas de trabajo presentan similitudes y merece la pena definirlos con mayor claridad.

La protección contra la explotación y los abusos sexuales es un área de trabajo que se centra en la protección de las poblaciones afectadas contra la explotación y los abusos sexuales en el marco de las operaciones de respuesta humanitaria. Para más información, consulte: <https://psea.interagencystandingcommittee.org/>.

La salvaguardia comprende los esfuerzos para proteger a todas las personas (incluidos el personal, los voluntarios y los beneficiarios de la ayuda) de cualquier forma de daño, abuso y explotación. Para más información, consulte: <https://safeguardingsupporthub.org/>.

Desde el punto de vista conceptual, la violencia sexual que afecta a los trabajadores humanitarios y la protección contra la explotación y los abusos sexuales forman parte de la salvaguardia, aunque las definiciones y la forma en que estas líneas de trabajo interactúan en la práctica pueden diferir de una organización a otra. Lo importante es que estas áreas de trabajo colaboren y se apoyen mutuamente cuando corresponda.

7.7.2 Consideraciones sobre los riesgos

Las consideraciones sobre los riesgos relativas a la violencia sexual pueden agruparse en cuatro ámbitos:

- consideraciones sobre riesgos individuales;
- perfiles de los agresores;
- factores de riesgo organizativos, y
- factores de riesgo externos.

Las estrategias de mitigación de riesgos deben tener como objetivo abordar estos cuatro ámbitos. El personal de seguridad puede garantizar que los procedimientos prioricen no solo la gestión del comportamiento del personal, sino también la disuasión de los posibles agresores y el tratamiento de otros factores de riesgo. Por ejemplo, las organizaciones pueden centrarse en formar al personal sobre cómo reducir su exposición al riesgo, y al mismo tiempo implementar medidas para disuadir a los agresores, que aborden las condiciones internas y externas de la organización que contribuyen a la violencia sexual (cuando es posible) y mitiguen los riesgos en estos entornos.

Consideraciones sobre el riesgo individual

Si bien ciertos perfiles corren un riesgo particular de sufrir violencia sexual, esta puede afectar a cualquier persona, y las medidas de preparación y respuesta deben tenerlo en cuenta. La identidad interseccional de una persona puede afectar su vulnerabilidad a la violencia sexual, incluidos el género, la raza, la orientación sexual, la discapacidad y el poder y la elección relativos. Los trabajadores humanitarios nacionales corren un riesgo especialmente elevado, sobre todo en entornos violentos o en sociedades patriarcales. Además, suelen tener menos protección que sus colegas internacionales, por ejemplo, en lo que respecta al apoyo en los desplazamientos de ida y vuelta al trabajo.¹⁰⁴ Una encuesta realizada para las Naciones Unidas ha revelado que los “no funcionarios” (como consultores, becarios y voluntarios) también son especialmente vulnerables y es menos probable que se sientan capaces de denunciar incidentes.¹⁰⁵

En general los incidentes de violencia sexual no se denuncian por varias razones, entre ellas, el estigma social, la falta de canales seguros de denuncia y los entornos jurídicos y culturales restrictivos. Estas barreras afectan tanto a hombres como a mujeres, y en muchos de los contextos en los que trabajan las organizaciones humanitarias pueden ser especialmente difíciles para las personas que se identifican como LGBTQI+.

104 Stoddard, A., Harvey, P., Czwarno, M. y Breckenridge, M. (2019) *Aid Worker Security Report 2019. Speakable: Addressing sexual violence and gender-based risk in humanitarian aid*, Humanitarian Outcomes (<https://humanitarianoutcomes.org/AWSDR2019>).

105 Cronin, E.A. y Afifi, A. (2018) *Examen de las políticas y prácticas de protección de los denunciantes de irregularidades en las organizaciones del sistema de las Naciones Unidas*, Dependencia Común de Inspección de las Naciones Unidas (<https://digitallibrary.un.org/record/1643065?ln=en&v=pdf>).

- *Para obtener más información sobre los riesgos basados en la identidad, véase el capítulo 1.2.*

Perfiles de los agresores

Los agresores pueden ser externos o internos a la organización, por ejemplo, personal, contratistas e individuos pertenecientes a las fuerzas armadas, a grupos armados no estatales y a las comunidades locales. Aunque es más probable que los agresores sean hombres, personas de otros géneros también pueden ser agresores o cómplices.

Los agresores pueden estar motivados por factores que no tienen ninguna relación con los atributos personales o las conductas de la víctima, como las circunstancias personales, incluidos los antecedentes familiares, la personalidad y el comportamiento (por ejemplo, el abuso de sustancias), un entorno organizativo permisivo y compañeros sexualmente agresivos. Los agresores suelen contar con oportunidades y aliados para llevar a cabo su agresión, así como con factores ambientales, culturales y sociales, como los desequilibrios de poder, las justificaciones culturales o sociales, las percepciones de derecho y un clima de impunidad.

En las formas más graves de violencia sexual, los agresores pueden atacar a sus objetivos mediante coacción, incapacitación (por ejemplo, utilizando drogas o alcohol) o fuerza (utilizando armas o fuerza física). Los agresores suelen necesitar:

- medios —el poder, el apoyo y los recursos para delinquir—;
- acceso —acceso psicológico o físico a su objetivo—;
- conocimiento —conocimiento de la vulnerabilidad o susceptibilidad de su objetivo—;
- capacidad —su capacidad de delinquir—;
- motivación —voluntad de delinquir—, y
- oportunidad —circunstancias o momentos permisivos para delinquir—.

Factores de riesgo organizativos

La incomodidad a la hora de hablar de la violencia sexual y las dinámicas de género en las organizaciones hace que las conversaciones sobre este tipo de riesgo en las organizaciones humanitarias sean todavía insuficientes. La falta de atención directa y explícita a esta cuestión puede agravar el riesgo al contribuir a culturas organizativas permisivas. La prevención de incidentes graves puede depender de la rapidez con que se responde a los leves. Permitir casos menores de violencia sexual u otras formas de ataque a personas particulares, como el acoso, la intimidación y las bromas ofensivas, puede fomentar formas más graves de violencia, incluida la violencia sexual (esto se describe a veces como una pirámide de violencia¹⁰⁶). Los agresores se aprovechan de los entornos permisivos y pueden verse influidos por compañeros agresivos. Una organización debe asegurarse de que ningún entorno en el que trabaja su personal

¹⁰⁶ Para consultar un ejemplo de la pirámide de la violencia, véase EISF (2019).

sea un lugar donde predomine la hostilidad de cualquier tipo, ya sea sexual o no. Los incidentes menores deben tomarse con seriedad, ya que pueden ser los precursores de otros más graves.

La cultura organizativa, incluida la inclusividad, desempeña un papel importante a la hora de determinar si se denuncian y abordan los incidentes de violencia sexual. En la comunidad humanitaria, las culturas organizativas pueden valorar a menudo la dureza y las actitudes machistas (especialmente en los contextos patriarcales), lo que puede disuadir aún más la presentación de denuncias. Es aconsejable que las organizaciones dispongan de directrices claras sobre lo que constituye una infracción denunciabile, ya que esto puede ayudar al personal a entender cuándo un comportamiento no es aceptable y a sentirse empoderado para tomar medidas.

Todo el personal debe estar formado y sentirse capaz de abordar las actitudes que pueden hacer más permisiva la violencia sexual, como desalentar el lenguaje ofensivo. Los directores y los puntos focales desempeñan un papel especialmente importante a la hora de garantizar que su personal sienta que puede plantear sus preocupaciones. Mediante la comunicación y la divulgación, el personal de seguridad también puede cambiar la cultura de la organización.

Cuando la cultura en general en un contexto operacional es más permisiva respecto a la violencia sexual, es especialmente importante que los equipos directivos de la organización comuniquen y demuestren con acciones que lo que puede ser aceptado fuera de la oficina no será tolerado por la cultura organizativa dentro de ella.

Encuestas sobre el clima organizacional o consultas específicas

Las consultas a todo el personal pueden ayudar a las organizaciones a comprender mejor la cultura organizativa y si las actitudes y las acciones dentro de la organización son indicativas de un entorno permisivo con la violencia sexual. Pueden adoptar la forma de encuestas sobre el clima organizacional, a veces las realiza una entidad externa, que se centran en las percepciones de los comportamientos aceptables dentro de la organización. En las consultas más específicas se plantean preguntas concretas sobre el acoso, la intimidación y las preocupaciones de determinados grupos de personal, por ejemplo, de las mujeres o las personas que se identifican como LGBTQI+.

Factores de riesgo externos

Los análisis del contexto pueden ayudar a identificar factores externos que afectan al riesgo de violencia sexual, por ejemplo, los siguientes:

- Altos niveles de agresión sexual en el entorno general.
- Un Estado fallido o frágil u otra forma de desmoronamiento del orden público.
- Impunidad generalizada, que incluye un sistema de justicia penal que tolera la violencia sexual o favorece a los agresores.
- Conflicto activo o lugar militarizado.
- Una sociedad conservadora o patriarcal.
- Desequilibrios de poder, por ejemplo, entre hombres y mujeres o entre distintos grupos étnicos.

Estos factores de riesgo ambientales propician la violencia sexual contra la población local y, por extensión, contra quienes trabajan para las organizaciones humanitarias. Los lugares de mayor riesgo pueden incluir zonas donde operan los grupos armados, prisiones y centros de detención, hoteles y alojamientos para el personal y pasos fronterizos y puestos de control. En algunos momentos el riesgo puede aumentar, como al anochecer, durante eventos concurridos y cuando actores armados entran o se retiran de un lugar. Los atacantes pueden agredir sexualmente a los residentes durante los asaltos a las instalaciones. La violencia sexual también puede producirse cuando se detiene o mantiene cautivos a los trabajadores humanitarios.

7.7.3 Mitigación de riesgos: prevención y preparación

Muchas medidas de mitigación del riesgo de violencia sexual se centran en regular la conducta del personal. Aunque la vulnerabilidad de una persona a la violencia sexual depende en parte de la interacción entre su identidad interseccional (quién es la persona), su comportamiento, su ubicación, su función y su organización (su vulnerabilidad interseccional), a veces no hay nada que una persona pueda hacer para mitigar su riesgo inherente de ser objeto de un ataque. Como cualquier otra amenaza, deben tomarse medidas a nivel individual y organizativo para reducir el riesgo.

A continuación se ofrece un resumen básico de las medidas de mitigación de riesgos. Para obtener orientaciones detalladas, consulte la guía del GISF (antes EISF) *Gestión de la violencia sexual contra el personal humanitario*,¹⁰⁷

Gobernanza

Deben existir políticas, sistemas y mecanismos para prevenir, prepararse y responder a los incidentes de violencia sexual que afecten al personal. Esto puede incluir una política de tolerancia cero hacia la violencia sexual y un código de conducta organizativo que mencione explícitamente todas las formas de conducta sexual inapropiada. Estos instrumentos organizativos deben ser transparentes y aplicarse de forma consistente, e incluir directrices para su aplicación práctica.

¹⁰⁷ EISF (2019).

Las buenas prácticas organizativas incluyen la elaboración de declaraciones políticas claras sobre el apoyo que los supervivientes pueden esperar de la organización después de un incidente. Una organización internacional descubrió que garantizar que todos los incidentes de agresión sexual y acoso sexual grave se denunciaran ante el equipo directivo superior contribuía significativamente a la rendición de cuentas.

Funciones y responsabilidades

La forma en que el personal de seguridad participa en la gestión de los riesgos de violencia sexual variará según la organización. Idealmente, el personal de seguridad debería estar preparado para identificar los factores de riesgo, aplicar medidas respetuosas e inclusivas de mitigación de riesgos, comunicar adecuadamente las amenazas, abordar los comportamientos inadecuados, reconocer los signos de un entorno hostil, actuar como testigos empoderados (véase el recuadro más abajo), y elaborar planes de contingencia centrados en los supervivientes que prioricen la seguridad, la confidencialidad, el respeto y la no discriminación.

Testigo empoderado

Mientras que un simple testigo puede presenciar una situación sin actuar, un testigo empoderado reconoce las situaciones perjudiciales o injustas y toma medidas para intervenir, apoyar a los afectados y evitar más daños. Este tipo de testigos disponen de los conocimientos y la confianza necesarios para actuar, ya sea mediante la intervención directa, la búsqueda de ayuda o la asistencia a los afectados, al tiempo que se mantienen a sí mismos y a los demás a salvo.

En las Naciones Unidas, el enfoque del testigo empoderado de un acontecimiento implica los siguientes pasos:

- darse cuenta del acontecimiento;
- interpretar la situación;
- asumir responsabilidades;
- decidir ayudar, e
- intervenir.

El personal de recursos humanos suele ser fundamental en la elaboración de las políticas y las prácticas relacionadas con la violencia sexual, lo que incluye la formulación y difusión del código de conducta, la creación de políticas de deber de cuidado para los supervivientes y el personal, la facilitación de los procesos de respuesta confidenciales y la gestión de las investigaciones internas. También realizan comprobaciones de antecedentes para evitar la selección de agresores sexuales y establecen procedimientos disciplinarios.

Varias funciones pueden estar más directamente implicadas en la gestión de los riesgos de violencia sexual y en el apoyo a los supervivientes.

- **Primer interviniente.** Es el punto de contacto inicial para una persona superviviente de violencia sexual, responsable de garantizar su seguridad inmediata, proporcionar apoyo emocional, ayudar a preservar las pruebas y facilitar la atención médica. Puede ser un miembro del personal formado o un colega de confianza. Dado que todo el personal puede desempeñar esta función, una buena práctica es asegurarse de que tiene acceso a orientaciones sobre primeros auxilios psicológicos.
- **Acompañante de superviviente.** Un acompañante de superviviente actúa como el principal punto de contacto entre el superviviente y la organización. Esta persona debe contar con formación y orientación para ofrecer apoyo emocional, mantener la confidencialidad y ayudar al superviviente a aplicar los protocolos de respuesta de la organización. Es una buena práctica que las organizaciones permitan a los supervivientes elegir a su acompañante.
- **Referente o defensor de salvaguarda.** Algunas organizaciones cuentan con referentes de salvaguarda o defensores que ofrecen al personal un medio confidencial de reportar sus preocupaciones. Es conveniente que haya referentes hombres y mujeres.
- **Investigadores internos.** Las personas que investigan internamente las denuncias de violencia sexual deben ser totalmente independientes del superviviente, del presunto agresor y de sus respectivos supervisores.

Orientación inicial, sesiones informativas y formación

Todo el personal, independientemente de su ubicación, corre el riesgo de sufrir violencia sexual, ya que este riesgo existe en todos los países e incluso puede perpetrarse en línea. Las organizaciones deben garantizar que todo el personal, independientemente de su función o ubicación, esté informado de la naturaleza y de las formas de violencia sexual a las que pueden enfrentarse en su trabajo. Deben ser conscientes de las amenazas en línea, del riesgo de las drogas de violación y de que los agresores pueden ser conocidos suyos e incluso compañeros de trabajo. El personal también debe conocer los factores contextuales y de otro tipo que pueden hacer que determinados perfiles corran más riesgo que otros. Esto permite al personal:

- comprender qué medidas ha adoptado la organización para reducir los riesgos;
- comprender qué procedimientos y normas deben aplicarse;
- utilizar esta información para identificar su propio perfil personal de riesgo (que puede ser único debido a su identidad interseccional), y
- obtener asesoramiento de los referentes y trabajar con su organización para reducir el riesgo.

► Véase el capítulo 1.2 sobre los riesgos basados en la identidad.

Las sesiones de orientación inicial y las sesiones informativas del personal cubren las políticas y los mecanismos de denuncia y rendición de cuentas en relación con la violencia sexual. Para respetar las normas culturales, la organización puede optar por ofrecer sesiones informativas y formación a grupos formados exclusivamente por hombres o por mujeres. La organización puede adaptar su enfoque teniendo en cuenta las actitudes locales para fomentar debates abiertos sobre temas delicados.

La capacitación en seguridad puede proporcionar información importante sobre los riesgos de violencia sexual, por ejemplo, sobre cómo el personal puede reducir su riesgo y responder en caso de que se produzca un incidente. Esto puede incluir orientación sobre las conductas culturalmente apropiadas, cuándo y cómo reportar incidentes o preocupaciones, cómo viajar (por ejemplo, en grupos grandes), cómo establecer límites personales y qué zonas, horas y grupos evitar. Todo el personal se beneficia de la capacitación sobre los riesgos locales y las estrategias de prevención, sus funciones y responsabilidades específicas en la respuesta a la violencia sexual, y la importancia de proteger la confidencialidad cuando se denuncian incidentes. Puede ser aconsejable proporcionar orientación sobre la manera de recopilar y conservar las pruebas en caso de que el superviviente decida emprender una acción judicial.

Las orientaciones iniciales y la formación son una oportunidad para fomentar una cultura organizativa positiva, en la que la organización transmita el mensaje de que la violencia en cualquiera de sus formas es inaceptable y de que no se puede culpar a nadie si es objeto de violencia sexual.

Algunas organizaciones forman a su personal en la intervención en cuanto testigos, que puede ser una estrategia eficaz para prevenir la violencia sexual. La formación puede incluir elementos interactivos como juegos de rol y debates adaptados al contexto específico.¹⁰⁸

Diagnósticos de riesgos y planes de seguridad inclusivos

Un diagnóstico de riesgos inclusivo debe identificar los lugares, los momentos y las situaciones de alto riesgo, además de considerar la manera en que factores como la edad, el sexo, la nacionalidad, la raza, la orientación sexual, la discapacidad, la apariencia

¹⁰⁸ Para obtener más información, consulte EISF (2019), Herramienta 2, Intervención de testigos (pp. 94-95).

y el comportamiento afectan la vulnerabilidad individual. Un diagnóstico de riesgos integral debe abarcar los factores de riesgo individuales, organizativos y externos. Este diagnóstico debe abordar las amenazas tanto externas como internas, puesto que los agresores pueden ser empleados, y comprender los posibles perfiles de los agresores.

El análisis de riesgos puede basarse en diversas fuentes, como los sistemas internos de denuncia, las consultas confidenciales con el personal y la comunidad local, y las aportaciones de los referentes de otras organizaciones de ayuda o de derechos humanos. Al recopilar información, puede ser necesario actuar con discreción, teniendo en cuenta las normas culturales y sociales.

Las directrices y los procedimientos operativos estándar para responder a la violencia sexual deben ser claros y estar a disposición del personal. Deben evitar cuidadosamente una perspectiva que sugiera la “culpabilización anticipada de las víctimas” y prestar la misma atención a comprender y a disuadir a los posibles agresores.

Los planes de contingencia de la organización (como la evacuación o la reubicación del personal afectado) también deben considerar los riesgos de violencia sexual y el apoyo disponible a corto y largo plazo. Puede ser beneficioso debatir con el personal de diversos orígenes culturales qué medidas de prevención, protocolos y apoyo consideran más apropiados. Estas consultas garantizan que la organización responda eficazmente en cada contexto y no cause más daños.

Estrategias de mitigación basadas en la identidad

En algunas circunstancias, los procedimientos de seguridad pueden ser distintos para determinados grupos de personal si el diagnóstico de riesgos indica que su perfil personal los coloca en una situación de mayor riesgo de violencia sexual. Las siguientes preguntas clave pueden tenerse en cuenta para evitar la discriminación indebida.

- ¿Se consideran en el diagnóstico de riesgos los atributos personales y se indica claramente el riesgo diferenciado entre los perfiles del personal (esto implica considerar todas las características identitarias y su interseccionalidad, incluidos el sexo, la orientación sexual, el grupo étnico y las discapacidades visibles e invisibles)?
- ¿Se informó a las personas afectadas de su mayor riesgo (reconociendo que es posible que ya sean conscientes de ello) y tuvieron la oportunidad de analizar las medidas de mitigación de riesgos?

- ¿Podrían aplicarse formas menos extremas de mitigación de riesgos? Una prohibición general o la expulsión de un grupo de miembros del personal es una estrategia común de mitigación de riesgos, pero otras medidas pueden ser más aceptables y adecuadas a las circunstancias. Las consultas con el personal afectado pueden ayudar a identificar opciones alternativas de gestión de riesgos de seguridad.

► Véase el capítulo 1.2, “Enfoque de seguridad centrado en la persona” para un análisis más detallado de los riesgos diferenciados.

Incorporación de los riesgos de violencia sexual a los procedimientos de seguridad

Los procedimientos de seguridad deben tener en cuenta cualquier aumento del riesgo de violencia sexual.

- **Seguridad del sitio.** Los hoteles y los alojamientos utilizados por el personal deben ofrecer la máxima protección contra intrusos. En algunos casos, el diagnóstico de riesgos puede indicar que el personal que corre un riesgo especialmente elevado, como las mujeres, podría alojarse con compañeros o en zonas específicas consideradas más seguras.
- **Seguridad en los viajes.** El personal debe recibir información sobre los procedimientos de viaje adecuados y sobre cómo protegerse a sí mismo y a los demás contra el riesgo de violencia sexual mientras se traslada de un lugar a otro. El personal en situación de alto riesgo (internacional o nacional) puede ir acompañado de casa al trabajo en un vehículo de la organización. Asimismo, puede viajar en grupo o acompañado, dentro y fuera del horario laboral. En un entorno de riesgo particularmente alto, puede ser aconsejable que los miembros del personal en situación de riesgo no se queden solos, ni siquiera durante periodos breves.
- **Seguridad de la información.** Los datos personales de los empleados de la organización no deben exponerse fuera de sus alojamientos ni figurar en la guía telefónica. Deben establecerse medidas de protección para proteger al personal de la divulgación no deseada de su identidad y paradero, tanto en línea como fuera de ella.

- Para obtener más información sobre las medidas de seguridad del sitio, véase el capítulo 7.2.
- Para obtener más información sobre la seguridad en los viajes, véase el capítulo 7.1.
- Para obtener más información sobre la seguridad de la información y la comunicación, véase el capítulo 6.1.

Plan de contingencia

Proveedores de servicios

La creación de una red de proveedores de servicios competentes, que incluya profesionales de la salud y psicológicos, en todos los contextos operacionales puede garantizar un apoyo oportuno a las supervivientes de la violencia sexual (que idealmente debería prestarse en las 24 horas posteriores al incidente). Esta red debe ser evaluada minuciosamente en cuanto a su capacidad de respuesta y sus prestaciones. También pueden evaluarse las actitudes hacia los supervivientes para asegurarse de que no causan más daño culpando a las víctimas o con comentarios inapropiados.

Todo el personal debe tener acceso a un tratamiento médico de emergencia, que incluya anticonceptivos de emergencia, profilaxis postexposición contra el VIH y otros medicamentos para reducir el riesgo de transmisión de enfermedades. En las zonas apartadas, las Naciones Unidas, el CICR o las ONG médicas pueden almacenar los kits de profilaxis postexposición contra el VIH. Si las instituciones sanitarias u otros organismos de la zona no disponen de este tipo de kits y de otros medicamentos específicos, las organizaciones pueden asegurarse de que estén a mano en la oficina y puedan dispensarse bajo supervisión médica (ya que es necesario controlar los efectos secundarios), o de que el superviviente pueda ser transportado inmediatamente a algún lugar donde estén disponibles. Las organizaciones deben identificar previamente lugares seguros para la revisión y la atención médicas, y establecer procedimientos de derivación. Se puede recurrir a clínicas privadas conocidas y de confianza si la persona superviviente decide no denunciar el incidente.

Las organizaciones con restricciones particulares (por ejemplo, contra la anticoncepción) deben informar de ello al personal en general.

- Para obtener más información sobre el cuidado del personal, véase el capítulo 5.4.
- Para obtener más información sobre las consideraciones médicas y de salud, véase el capítulo 5.5.

Logística

Las disposiciones logísticas incluyen un transporte fiable para el superviviente y un acompañante, así como provisiones para la reubicación o repatriación confidencial de los supervivientes, en caso de ser necesario.

Seguro

Con el consentimiento del superviviente y si se ha contratado un seguro, es crucial informar rápidamente a los proveedores de seguros sobre el incidente para garantizar que el superviviente pueda acceder a apoyo médico y psicológico. El plazo para notificar un incidente puede variar en función de los acuerdos vigentes con el proveedor de seguros, y las organizaciones deben saber cuál es la información mínima requerida por las aseguradoras para iniciar el apoyo. Deben establecerse protocolos para mantener la confidencialidad.

También es útil tener acuerdos claros con los proveedores de seguros sobre los tipos específicos de cobertura disponibles para incidentes de violencia sexual. Esto incluye comprender el alcance de la atención médica, el asesoramiento psicológico y otro tipo de apoyo psicosocial, así como cualquier posible apoyo jurídico. Asegurarse de que estas áreas están explícitamente cubiertas en la política puede evitar retrasos y complicaciones si se produce un incidente.

► *Para obtener más información sobre los seguros, véase el capítulo 5.4.*

Consideraciones jurídicas

Las organizaciones deben estar preparadas para asesorar a las personas supervivientes sobre sus opciones, incluidas las implicaciones de denunciar lo ocurrido ante las autoridades locales y las definiciones jurídicas de violencia sexual en ese contexto. Deben establecerse relaciones con profesionales jurídicos locales de confianza que puedan prestar asistencia inmediata si fuera necesario. Para obtener más información sobre las consideraciones jurídicas, consulte el apartado 7.7.4 más abajo.¹⁰⁹

Reportar y denunciar

La existencia de mecanismos sólidos y confidenciales para reportar y denunciar irregularidades no solo ayuda a responder a los incidentes, sino que también puede disuadir a los posibles agresores. El personal responsable debe asegurarse de que estos mecanismos sean confidenciales y accesibles a todo el personal, independientemente de su puesto e idioma. Se debe animar al personal a denunciar incluso los incidentes menores. Los canales para reportar la violencia sexual pueden estar separados de los mecanismos de reporte de otros incidentes de seguridad debido a la necesidad de una mayor confidencialidad. La notificación no oficial de incidentes de violencia sexual (por ejemplo, a través de servicios médicos, asesoramiento y encuestas) puede

¹⁰⁹ Para obtener más información, consulte EISF (2019), “Herramienta 3, Cuestionario sobre el entorno jurídico” (pp. 96-98).

ser considerablemente mayor que los incidentes reportados a través de los canales oficiales.

Una buena práctica es que las organizaciones ofrezcan al personal varios canales de denuncia confidencial, incluidas opciones para plantear preocupaciones de forma anónima, formal e informal. El personal de una oficina puede no denunciar un incidente si todas las denuncias se dirigen a un director superior, que puede ser el agresor o un aliado del agresor. Para hacer frente a este riesgo, una ONG internacional ha introducido un proveedor externo de servicios de ética y cumplimiento para albergar un sitio web de denuncia de irregularidades en línea para reportar las inquietudes éticas o las conductas indebidas que impliquen al personal de la organización.

Los referentes/defensores de salvaguarda pueden ayudar al personal que necesite más información, que tiene dudas sobre si un incidente es lo suficientemente grave como para merecer una denuncia formal o que tiene miedo de las repercusiones que pueda tener la denuncia.

Por último, las organizaciones deben ser transparentes sobre lo que ocurre tras una denuncia, incluidas las investigaciones y las medidas disciplinarias que pueden aplicarse y la forma en que el denunciante puede participar en el proceso. Los denunciantes deben recibir información periódica sobre el curso dado a su denuncia. Pueden seguirse protocolos de intercambio de información basados en la necesidad de saber, de modo de limitar la información a un número mínimo de personas. También puede ser aconsejable mantener un registro seguro de todas las comunicaciones y las decisiones relativas a la respuesta.

Ejemplo: Fallas en la protección de los denunciantes

En 2009 una trabajadora humanitaria voluntaria fue asesinada en Benin tras reportar al director para el país que un contratista de la agencia estaba abusando sexualmente de miembros de la comunidad local. Las investigaciones sobre el incidente indican que errores relacionados con la confidencialidad pueden haber permitido que se revelara la identidad de la denunciante al presunto agresor, que tenía conexiones personales dentro de la organización. El caso pone de manifiesto muchas deficiencias, como la falta de mecanismos de reporte seguros y confidenciales, procesos de investigación sólidos y medidas de seguridad para proteger a los denunciantes.

Fuente: Oficina del Inspector General del Cuerpo de Paz (s.f.) *Resources: Kate Puzey Volunteer Protection Act of 2011* (www.peacecorpoig.gov/resources/resources-kate-puzey-volunteer-protection-act-2011).

Al registrar los informes de incidentes en el sistema de gestión de la información sobre incidentes de la organización, el personal de seguridad querrá considerar cómo garantizar la confidencialidad cuando los nombres y otros detalles puedan ser campos obligatorios. Algunas organizaciones mantienen separados estos tipos de informes de incidentes por razones de confidencialidad. Los informes son necesarios para la gestión de riesgos de seguridad y el análisis de riesgos, pero deben equilibrarse con la seguridad, el bienestar psicológico y el derecho a la privacidad de la persona superviviente.

Selección, investigaciones y medidas disciplinarias

Una selección rigurosa de los posibles empleados, que incluya una verificación exhaustiva de sus antecedentes y de sus referencias en varios países, puede impedir que los agresores conocidos de actos de violencia sexual se desplacen de una organización humanitaria a otra. En los últimos años, varias iniciativas de salvaguardia se han centrado en apoyar a las organizaciones en este sentido.¹¹⁰

Las organizaciones deben contar con un proceso formal para investigar las denuncias de violencia sexual, con medidas específicas si el presunto agresor es empleado de la organización. Las denuncias contra miembros del personal deben ir seguidas de una investigación interna y de medidas disciplinarias cuando corresponda. Si el superviviente desea iniciar acciones legales, se puede recurrir a las autoridades. Los infractores, aliados y facilitadores deben rendir cuentas ante la organización. Para disuadir de nuevas infracciones, el incumplimiento de la política y las investigaciones deben dar lugar a medidas disciplinarias.

7.7.4 Respuesta

Las respuestas oportunas a los incidentes de violencia sexual son fundamentales para garantizar la seguridad y el bienestar de los afectados. La respuesta de una organización dependerá de varias circunstancias, entre ellas, cuándo se produjo el incidente, los deseos del superviviente, la gravedad del incidente y los riesgos que suponga para los demás. A continuación se enumeran algunas cosas generales que considerar al responder:

- Las personas supervivientes de violencia sexual pueden reportar los incidentes de inmediato o días, semanas, meses o años después del incidente. Los factores que influyen en esto son la seguridad, la cultura y el impacto psicológico y emocional del suceso en el superviviente. Las organizaciones deben tratar todos los informes con carácter prioritario, independientemente de cuándo se haya producido el incidente.
- Las organizaciones deben estar preparadas para informar a los supervivientes de cualquier consideración cultural y jurídica pertinente. En algunas regiones, reportar la violencia sexual puede suponer un perjuicio adicional para la persona superviviente debido a las leyes y a las prácticas culturales locales.

¹¹⁰ Por ejemplo, el Plan de Divulgación de Conductas Indebidas (disponible en inglés): <https://misconduct-disclosure-scheme.org/>

- Los riesgos de retraumatización, autolesión y suicidio son muy elevados. Es imprescindible que quienes responden a un incidente de este tipo estén capacitados para proporcionar el apoyo adecuado y mantener la confidencialidad.

Las buenas prácticas ponen de relieve la necesidad de garantizar que las respuestas a los incidentes de violencia sexual se guíen por una atención centrada en el superviviente, que respete en la medida de lo posible sus deseos, siempre que dichos deseos no supongan un riesgo adicional para la persona, sus colegas o la organización. Un enfoque centrado en el superviviente tiene en cuenta sus necesidades y preferencias, y trata de protegerlo de la estigmatización, la discriminación, las represalias u otras consecuencias perjudiciales. El enfoque pretende crear un entorno de apoyo en el que se respeten y prioricen los derechos, la seguridad y la confidencialidad del superviviente, y en el que se lo trate con dignidad y respeto. El enfoque pretende apoyar la recuperación del superviviente permitiéndole elegir la asistencia y la atención que necesita, tomar decisiones sobre la denuncia opcional, y decidir si desean participar en alguna investigación y de qué manera. Esto es distinto de un enfoque dirigido por el superviviente, en el que todo el poder de decisión recae en el superviviente, incluso si estas decisiones pueden poner a la persona o a otros en riesgo de sufrir daños.

► *Para obtener más información sobre el enfoque centrado en el superviviente, véase el capítulo 5.4 sobre el cuidado del personal.*

Comunicación con el superviviente

Como ocurre con todos los sucesos traumáticos, la forma en que las personas y la organización interactúan con el superviviente desempeña un papel importante en la sanación y la recuperación. El apoyo psicológico y emocional puede provenir de colegas y amigos, a través de redes de apoyo entre pares e interacciones compasivas. Toda comunicación con un superviviente debe tener los siguientes objetivos:

- hacerlo sentir seguro;
- hacerlo sentir que tiene el control;
- hacerlo sentir que no se duda de lo que dice y que se lo escucha, y
- hacerlo sentir que la organización se toma en serio el incidente.

La comunicación no debe:

- dar a entender que el superviviente tiene la culpa o juzgarlo de alguna manera;
- minimizar su experiencia;
- imponerle compañía u otro tipo de apoyo;
- decirle cómo debe actuar o sentirse, o normalizar su respuesta, o
- presionarlo para que tome decisiones o actúe de cierta manera.

Respuesta inicial

Cuando una persona sufre violencia sexual, en especial un incidente grave, el momento en que se actúa es clave. A menudo, ayuda priorizar las acciones en un calendario de respuesta que identifique las necesidades inmediatas, a corto plazo y a largo plazo. También es importante reconocer que la experiencia de cada persona es diferente. Algunas pueden necesitar apoyo médico y psicosocial inmediato, mientras que otras pueden solicitarlo más adelante. No existe un camino correcto. Sin embargo, en lo que respecta a algunos aspectos de la respuesta, como la atención médica y la denuncia, los plazos pueden desempeñar un papel más importante.¹¹¹

Según la gravedad, puede ser necesario activar la estructura de gestión de incidentes de la organización, que incluye las funciones de apoyo a la familia y la comunicación. El primero en responder, los referentes responsables o el equipo de gestión de incidentes (para incidentes graves) supervisarán normalmente algunas o todas las actividades de la respuesta inicial que se describen más abajo. Debido a su naturaleza sensible, muchas organizaciones pueden crear un equipo de respuesta a incidentes separado para tratar los casos de violencia sexual.

► *Para obtener más información sobre la gestión de incidentes críticos, véase el capítulo 4.4.*

- **Seguridad.** Garantizar la seguridad inmediata del superviviente y la de otras personas en riesgo es la máxima prioridad, al tiempo que se mantiene la confidencialidad para proteger al superviviente.
- **Atención médica.** La atención médica de urgencia, que incluye el tratamiento de lesiones e infecciones y la prevención de embarazos, debe prestarse con el consentimiento del superviviente lo antes posible. Los supervivientes de agresiones sexuales pueden necesitar anticoncepción de emergencia, tratamiento profiláctico de las infecciones de transmisión sexual, profilaxis postexposición contra el VIH

¹¹¹ EISF (2019) presenta un marco de respuesta detallado de las medidas clave que el personal responsable puede tomar en diferentes momentos.

y medicamentos para otras enfermedades como la hepatitis B. Todo esto debe iniciarse lo antes posible tras el incidente.

- **Atención psicosocial.** Debe ofrecerse acceso inmediato a un apoyo psicosocial adecuado.
- **Identificar a un acompañante de superviviente.** Las organizaciones pueden preguntarle al superviviente quién le gustaría que fuera su acompañante u ofrecerle acceso a un acompañante formado por la organización.
- **Enlace familiar.** Con el consentimiento del superviviente, puede informarse a su familia a través de una persona de contacto designada, siguiendo directrices de absoluta confidencialidad.
- **Ubicación.** Es posible que los supervivientes necesiten ser alojados en un lugar seguro y confidencial, cerca de las personas que les brindan apoyo, y quizás sea necesario reubicarlos o evacuarlos.
- **Denuncia del incidente.** El incidente debe reportarse a través de los canales apropiados, salvaguardando al mismo tiempo la seguridad y la privacidad del superviviente.
- **Asistencia y orientación.** La organización debe dejar claro que cree en el relato del superviviente y proporcionar orientaciones claras sobre los pasos siguientes, garantizando una comunicación y una asistencia constantes durante todo el proceso.¹¹²

A largo plazo, puede necesitarse asistencia administrativa y logística adicional, como organizar la ayuda financiera para el superviviente y el personal de asistencia, organizar el transporte privado para quienes participen en el proceso de respuesta, suspender las obligaciones laborales del personal afectado, acordar cómo comunicar a los colegas la ausencia del superviviente y establecer controles periódicos para abordar las necesidades y las preocupaciones de los supervivientes. Además, puede ser necesario informar a los proveedores de seguros, con el consentimiento del superviviente.

Asimismo, quizás deba ofrecerse asistencia a otros miembros del personal, como los testigos y el equipo en general. Asistir a los supervivientes de violencia sexual es estresante y exigente. A quienes lo hagan se les puede ofrecer asistencia emocional y psicosocial, lo que incluye tomarse descansos o apartarse.

¹¹² Para obtener más consejos para quienes participan en la respuesta inicial, véase EISF (2019) *Herramienta 5, Orientaciones para acompañar a supervivientes* (pp.58-61).

Riesgos de violencia sexual en línea

Las formas de violencia sexual en línea preocupan cada vez más a las organizaciones humanitarias. Aunque cualquiera puede ser objeto de esta violencia, las mujeres y las personas LGBTQI+ se ven afectadas de forma desproporcionada, lo que exige medidas de prevención y respuesta específicas. Entre los riesgos figuran el acoso, el acecho y el ciberacoso, la extorsión sexual y el intercambio no consentido de imágenes íntimas.

- Véase el capítulo 6.2 para obtener más información sobre los riesgos digitales y las medidas de mitigación.

Consideraciones sobre la respuesta

Es posible que los referentes o el equipo de gestión de incidentes deban abordar algunas de las consideraciones de respuesta más complejas que se tratan en la sección siguiente.

Confidencialidad y comunicación

Las organizaciones deben gestionar proactivamente la comunicación en caso de que ocurra un incidente grave de violencia sexual, por lo que deben establecer protocolos internos y externos claros, considerar las implicaciones de compartir información sobre el incidente y el agresor, y garantizar la confidencialidad y la seguridad del superviviente. Al mismo tiempo, las organizaciones deben respetar el derecho de la víctima a hablar, si así lo desea, y deben proporcionar orientación y apoyo, incluido el acceso a referentes formados que puedan ayudar a afrontar los posibles riesgos y consecuencias de la divulgación pública.

Si el incidente es de conocimiento público, puede ser necesaria la gestión de los medios de comunicación.

- Para obtener más información sobre la gestión de los medios de comunicación, véase el capítulo 4.4.

Denuncias a la policía y procedimientos judiciales

Las organizaciones deben asegurarse de que tienen un conocimiento exhaustivo de los entornos jurídicos en los que operan, en particular en lo relativo a los incidentes de violencia sexual, con acceso a abogados locales para proporcionar orientación y apoyo en caso de que se produzca un incidente.¹¹³

113 Para obtener información más detallada, consulte EISF (2019) *Herramienta 3, Cuestionario sobre el entorno jurídico* (pp. 96-98).

La organización puede ayudar al superviviente con cualquier proceso legal o judicial que decida emprender. Esto incluye acompañarlo a denunciar el incidente a la policía, apoyarlo si es necesario un interrogatorio policial y garantizar su seguridad y bienestar durante cualquier proceso de obtención de pruebas. La recopilación de pruebas no compromete al superviviente a tomar medidas legales, pero le permite conservar la opción para el futuro. La denuncia de un incidente a la policía puede ser en sí una experiencia traumática, incluso en las mejores circunstancias.

Es posible que las organizaciones también deban garantizar una representación legal adecuada para la víctima. El asesor jurídico de la organización puede ayudar a aclarar los procedimientos y los plazos de las denuncias, ya que la obtención de documentación oficial puede ser crucial si el superviviente decide presentar cargos más adelante o buscar tratamientos adicionales. La decisión de iniciar acciones legales corresponde al superviviente, que debe sentirse apoyado y empoderado para tomar una decisión informada.

En términos más generales, las organizaciones deben conocer los requisitos legales para denunciar incidentes de violencia sexual a la policía del país, incluida cualquier obligación de denunciar, las implicaciones para el superviviente y el presunto agresor, y si deben permanecer en el país tras la denuncia. Algunos ciudadanos extranjeros pueden optar por no denunciar los incidentes a la policía si ello los obliga a permanecer en el país hasta que concluya el juicio (lo que puede llevar varios años). En algunos países, los supervivientes pueden ser acusados de adulterio o fornicación si no pueden demostrar la agresión. Esto puede dar lugar a que se castigue al superviviente y no al agresor. Las organizaciones también deben considerar el impacto de las acciones legales sobre los presuntos agresores, especialmente si son miembros del personal.

Si se inicia un procedimiento judicial, este suele desarrollarse en el país donde se produjo el incidente y puede requerir la recopilación de pruebas médicas. El riesgo de sufrir más traumas es inmenso en estas circunstancias, y es aconsejable que la organización esté preparada para ayudar a los supervivientes a desenvolverse con seguridad en estos procedimientos, por ejemplo, identificando previamente los centros médicos de confianza y las expectativas acerca de la recopilación de pruebas forenses. Algunos centros médicos que tratan a los supervivientes también pueden presentar automáticamente informes a la policía.

En algunos casos, la atención puede centrarse menos en si el incidente tuvo lugar y más en si fue consensuado, lo que puede plantear diversas dificultades.

Ejemplo: Una segunda experiencia traumática

No es raro que un superviviente sufra un segundo trauma como consecuencia de un trato insensible por parte de la policía. En un caso, una trabajadora humanitaria internacional fue agredida sexualmente mientras trabajaba en el extranjero. Nadie en la organización supo qué hacer inmediatamente después del incidente. Al día siguiente la enviaron, sola, a la embajada de su país para reportar el incidente.

La embajada la envió a la policía local acompañada por el responsable de seguridad de la embajada, un ciudadano del país. Una vez en la comisaría, cuatro policías armados la interrogaron, haciéndole preguntas detalladas sobre el incidente. Cuando dudaba en sus respuestas, la acusaban de mentir. Durante el interrogatorio, otros policías se acercaban para echar un vistazo, pues sentían curiosidad. Los policías encargados del interrogatorio insistieron en que les mostrara sus lesiones antes de permitirle abandonar la comisaría. A continuación, insistieron en que los llevara al lugar del incidente para una recreación que, según ellos, era esencial para la investigación. Nunca se llevó a cabo una verdadera investigación. El agresor nunca fue detenido, y la superviviente se enteró más tarde de que en ese país era muy raro que alguien fuera juzgado o condenado por agresión sexual. Su experiencia en la comisaría fue efectivamente una segunda agresión.

Una persona bien informada y de confianza debe acompañar siempre al superviviente a la comisaría, para garantizar que no sea intimidado ni victimizado aún más, que las entrevistas se realicen en un idioma que el superviviente entiende y que se le proporcione la documentación y la asistencia adecuadas. El acompañante debe estar preparado para intervenir si no se respetan los derechos y la dignidad del superviviente. Es importante que esta persona asuma esta función en cuanto representante de la organización y que no se perciba que actúa a título individual.

Cuando el presunto agresor es un miembro del personal

Cuando el presunto perpetrador de un incidente de violencia sexual es un miembro del personal, las organizaciones pueden tener que tomar una serie de medidas inmediatas y cuidadosamente consideradas, incluida la salvaguardia del superviviente y de otras personas que puedan correr el riesgo de sufrir más daños, así como la protección del presunto agresor. Los presuntos agresores pueden suponer un riesgo continuo para la seguridad del superviviente y de otros miembros del personal, incluido el personal que investiga las denuncias.

Si las acusaciones son graves, la organización puede decidir suspender al presunto agresor o concederle una licencia administrativa (manteniendo la confidencialidad sobre el motivo de su ausencia). Si el presunto agresor supone un riesgo o corre peligro debido a las acusaciones, puede ser necesario trasladarlo a un lugar seguro y acompañarlo durante su estancia. Suele ser aconsejable evitar cualquier contacto entre el superviviente y el presunto agresor, especialmente en los casos graves, aunque deben tenerse en cuenta las preferencias del superviviente respecto al contacto.

Es importante que investigadores formados e independientes lleven a cabo el proceso (con el apoyo de los departamentos pertinentes, como RR.HH. y Seguridad) para evitar que se produzcan nuevos traumas o daños.¹¹⁴ Una investigación deficiente puede ser profundamente perjudicial para el superviviente, el presunto agresor y otras personas afectadas por el incidente. No atender una denuncia puede tener consecuencias igualmente perjudiciales.

7.7.5 Acciones posteriores al incidente

Atención posterior

El personal afectado puede necesitar atención posterior a largo plazo después de un incidente de violencia sexual. Las organizaciones deben establecer un marco de apoyo y evitar al mismo tiempo abrumar a los supervivientes con la toma de decisiones. Es imprescindible que en la política de una organización se describa claramente el alcance, el coste y la duración del apoyo que puede ofrecer de forma realista a los supervivientes, de modo de que no crean equivocadamente que la asistencia es indefinida.

Los supervivientes pueden necesitar un apoyo médico prolongado, que incluya revisiones médicas periódicas y tratamiento para cualquier problema de salud física. También pueden necesitar asistencia psicosocial a largo plazo para afrontar el trauma, la ansiedad, la depresión y otros problemas de salud mental que puedan surgir tras un incidente. Esta asistencia debe adaptarse a las necesidades de cada persona y ser proporcionada por profesionales con experiencia en el tratamiento de traumas.

Se puede desarrollar un plan integral de apoyo a largo plazo a los supervivientes, que tenga en cuenta sus preferencias y necesidades. Esto puede incluir evaluaciones y terapias médicas y psicológicas, apoyo logístico para la atención posterior, una evaluación de las opciones laborales, un plan de reincorporación al trabajo y una transición a los servicios de apoyo a largo plazo (como los servicios nacionales), junto con un cronograma de comunicación y control. La duración del procedimiento judicial debe tenerse en cuenta en el plan de asistencia. Este plan debe ser flexible para adaptarse a los cambios en las necesidades del superviviente a lo largo del tiempo. El trauma puede manifestarse muchos meses o incluso años después de un incidente, y puede ser difícil prever cuándo o cómo surgirán los factores desencadenantes. Lo ideal es que los supervivientes puedan acceder fácil y directamente a los recursos y a la atención psicosociales, incluso si necesitan apoyo meses después del incidente

¹¹⁴ Para obtener información sobre un proceso de investigación interna detallado, incluidos los pasos clave, véase EISF (2019).

o una vez finalizado su empleo. Es importante recordar que los factores culturales pueden influir significativamente en la respuesta de un individuo. Al prestar apoyo, las organizaciones deben permanecer abiertas y sensibles a las distintas vías de recuperación y a las preferencias de los supervivientes

► Véase el capítulo 5.4 para obtener más información sobre el cuidado del personal.

Revisión posterior al incidente

Por último, las organizaciones deben realizar exhaustivas revisiones posteriores a los incidentes, manteniendo una estricta confidencialidad para proteger al personal involucrado, con el fin de evaluar la gestión de los incidentes graves de violencia sexual e identificar las áreas susceptibles de mejora.

► Para obtener más información sobre las revisiones posteriores al incidente, véase el capítulo 4.4 sobre la respuesta a incidentes y la gestión de crisis.

Más información

Orientación

Comité Permanente entre Organismos. (2023). *Definición y principios de un enfoque centrado en las víctimas/los supervivientes* (<https://interagencystandingcommittee.org/iasc-champion-protection-sexual-exploitation-and-abuse-and-sexual-harassment/iasc-definition-principles-victim-survivor-centered-approach>).

Comité Permanente entre Organismos. (s.f.) *Protection from sexual exploitation and abuse* (<https://psea.interagencystandingcommittee.org/>).

Foro Europeo Interinstitucional para la Seguridad. (2018). *Gestión de la seguridad del personal humanitario con perfiles diversos* (<https://gjsf.ngo/resource/managing-the-security-of-aid-workers-with-diverse-profiles/>).

Foro Europeo Interinstitucional para la Seguridad. (2019). *Gestión de la violencia sexual contra los trabajadores humanitarios: prevención, preparación, respuesta y atención posterior* (<https://gjsfprod.wpengine.com/resource/managing-sexual-violence-against-aid-workers/>).

Foro Europeo Interinstitucional para la Seguridad e InterAction. (2014). *NGO Safety and Security Training Project: how to create effective security training for NGOs* (<https://reliefweb.int/report/world/ngo-safety-and-security-training-project-how-create-effective-security-training-ngos>).

Global Interagency Security Forum. (2022). *Gestión de la violencia sexual contra el personal humanitario [Formación]*. DisasterReady (<https://ready.csod.com/ui/lms-learning-details/app/course/581feec5-4ce2-493a-9266-90ed6099bc48>).

Karaman, S. (s.f.) *Online harassment of politically-active women: an overview*. XYZ, Tactical Technology Collective Project (<https://xyz.informationactivism.org/en/online-harassment-of-politically-active-women-overview/>).

PEN America. (s.f.). *Best practices for employers. Online harassment field manual* (<https://onlineharassmentfieldmanual.pen.org/best-practices-for-employers/>).

Persaud, C. (2012). *Género y seguridad: Directrices para la transversalización del género en la gestión de riesgos de seguridad*. Foro Europeo Interinstitucional para la Seguridad (<https://gisf.ngo/resource/gender-and-security/>).

Safeguarding Resource & Support Hub. (s.f.). *Together, we can build a safer sector* (<https://safeguardingsupporthub.org/>).

Steering Committee for Humanitarian Response. (s.f.). *Misconduct disclosure scheme* (<https://misconduct-disclosure-scheme.org/>).

Investigación y análisis

Cronin, E.A. y Afifi, A. (2018). *Examen de las políticas y prácticas de protección de los denunciantes de irregularidades en las organizaciones del sistema de las Naciones Unidas*. Dependencia Común de Inspección de las Naciones Unidas (<https://digitallibrary.un.org/record/1643065?ln=en&v=pdf>).

Deloitte. (2019). *Safe space survey report* (https://viraltopiczone.wordpress.com/wp-content/uploads/2019/01/d3bcc-un_safe_space_survey_report_15_january_2019_final.pdf).

Humanitarian Women's Network. (2016). *Full survey results* (https://interagencystandingcommittee.org/sites/default/files/migrated/2016-11/hwn_full_survey_results_may_2016.pdf).

Mazurana, D. y Donnelly, P. (2017). *STOP the sexual assault against humanitarian and development aid workers*. Centro Internacional Feinstein, Universidad de Tufts (<https://fic.tufts.edu/publication-item/stop-sexual-assault-against-aid-workers/>).

Nobert, M. (2017). *Humanitarian experiences with sexual violence: compilation of two years of Report the Abuse data collection*. Report the Abuse (<https://reliefweb.int/report/world/humanitarian-experiences-sexual-violence-compilation-two-years-report-abuse-data>).

Oficina del Inspector General del Cuerpo de Paz. (s. f). *Resources: Kate Puzey Volunteer Protection Act of 2011* (www.peacecorps.org/resources/resources-kate-puzey-volunteer-protection-act-2011).

Stoddard, A., Harvey, P., Czwarno, M. y Breckenridge, M. (2019). *Aid Worker Security Report 2019. Speakable: addressing sexual violence and gender-based risk in humanitarian aid*. Humanitarian Outcomes (<https://humanitarianoutcomes.org/AWSDR2019>).

7.8 Detención y arresto

La gestión eficaz de los incidentes de detención y arresto requiere planificación e inversión en capacidades locales y protocolos de respuesta bien establecidos. Las situaciones de detención y arresto normalmente requerirán la aplicación de un plan de respuesta a incidentes (descrito en el capítulo 4.4). En cualquiera de las situaciones analizadas aquí, la prioridad es la liberación segura y rápida de los miembros del personal. Para lograrlo, la organización necesita un enfoque de respuesta informado, que probablemente incluya la movilización del apoyo de las partes interesadas locales.

7.8.1 Definiciones

Es importante diferenciar entre detención y arresto, tanto para reportar estas situaciones como para dar una respuesta eficaz.

La detención se refiere a la retención de una persona contra su voluntad por un individuo o un grupo (por ejemplo, grupos comunitarios, autoridades locales, milicias o grupos militares). Aunque no hay intención de perjudicar al detenido, tampoco hay una condición clara para su liberación. Las detenciones pueden ser frecuentes en el trabajo humanitario; tanto las detenciones cortas como las largas son habituales. Los supuestos motivos de las detenciones pueden incluir credenciales o documentos administrativos incorrectos, mientras que las causas subyacentes pueden ir desde el descontento con la calidad o la ubicación del programa, la identidad equivocada del trabajador humanitario o la organización, las sospechas y la información errónea, hasta la simple búsqueda de sobornos. También puede existir frustración por el hecho de que las autoridades no interactúen con un grupo concreto, o no lo hagan de forma satisfactoria; a menudo los trabajadores humanitarios pueden considerarse una fuente de influencia.

El arresto se refiere a la detención formal por una autoridad oficial (normalmente la policía, pero también las fuerzas armadas) o por las autoridades presuntas. El arresto difiere del tipo más general de detención mencionado anteriormente en la implicación de autoridades oficiales que invocan sus poderes legales. La situación puede ser más difícil y peligrosa cuando las autoridades gubernamentales arrestan a alguien de manera extralegal (es decir, sin la debida orden de detención), o cuando la persona arrestada “desaparece”. Las autoridades pueden entonces negar el arresto y oponerse a revelar el paradero de la persona.

7.8.2 Riesgos

Los riesgos de detención y de arresto aumentan en contextos en los que se depende considerablemente de la ayuda humanitaria, en los que existe una opinión negativa de una organización humanitaria o de la labor humanitaria en general y en los que hay intereses políticos o financieros en juego. Este tipo de incidentes conlleva riesgos secundarios que también deben tenerse en cuenta:

- Riesgos para la salud, la seguridad y el bienestar del personal detenido o arrestado, especialmente si sufren violencia, padecen enfermedades o han sufrido traumas en el pasado. Retener a una persona en contra de su voluntad puede agravar sus problemas de salud mental existentes. Posiblemente tampoco tenga acceso a atención médica, libertades básicas, privacidad, intérpretes, asesoramiento jurídico u otro tipo de apoyo.
- Perturbaciones en las operaciones, especialmente si se retiene a personal clave durante periodos prolongados. Una estrategia habitual es retirarse y suspender la programación mientras se arregla la liberación.
- Riesgos para la reputación de la organización y las relaciones con las comunidades locales, los donantes y los socios. Esto podría poner en peligro la capacidad de funcionamiento de la organización.
- Riesgos de que el personal sea retenido en instalaciones inadecuadas, especialmente si presentan vulnerabilidades particulares.
- Riesgos para los colegas encargados de apoyar o visitar al personal detenido o arrestado. Estas personas corren el riesgo de sufrir intimidaciones y represalias, además del estrés propio de su función.

Las organizaciones humanitarias pueden planificar y prepararse para este tipo de incidentes, especialmente en contextos de alto riesgo, y disponer de mecanismos de respuesta bien establecidos.

7.8.3 Planificación, preparación y mitigación de riesgos

Una planificación y preparación eficaces son cruciales para mitigar los riesgos asociados al arresto y a la detención de trabajadores humanitarios. Nótese que, obviamente, no suele ser posible impedir un arresto que se realiza siguiendo un procedimiento legal. Aunque un arresto que no se ajuste a un procedimiento legal adecuado puede impugnarse, es poco probable que pueda evitarse.

Como parte de su planificación y preparación, lo ideal sería que las organizaciones diseñaran planes de contingencia detallados y de varios niveles para proteger a su personal y garantizar la continuidad de las operaciones con respecto a los riesgos de detención y arresto.

Contexto, análisis de riesgos y planes de contingencia

- **Los riesgos de detención y de arresto se incorporan a la gestión de riesgos de seguridad.** Los diagnósticos de riesgos y los planes de contingencia incluyen los riesgos de detención y de arresto. Los planes de contingencia incluyen procedimientos de evacuación y extracción. Los análisis del contexto incluyen una descripción general del entorno político, jurídico y de seguridad en las zonas de las operaciones.
- **El mapeo de los actores** puede apoyar el acceso, la negociación y los esfuerzos para entablar relaciones con las comunidades locales, las autoridades y otras partes interesadas, lo que puede facilitar una respuesta rápida ante un arresto o una detención.

Preparación jurídica

- **Comprensión del contexto jurídico y político del entorno operacional.** El personal debe conocer la jerarquía de las fuerzas de seguridad nacionales u otras autoridades *de facto* en la zona de operaciones de la organización. Esto puede incluir las estructuras de clanes y comunidades, y tener claros los procedimientos jurídicos relacionados con las detenciones en el país.
- **Información jurídica.** El personal debe estar informado sobre la legislación local, sus derechos y los procedimientos que deben seguirse si alguien es detenido o arrestado. Las organizaciones deben ser claras respecto al tipo de apoyo que pueden prestar al personal detenido y arrestado, incluido el apoyo tras la liberación y a los familiares.
- **Apoyo jurídico.** Es aconsejable establecer contactos con profesionales jurídicos locales y organizaciones humanitarias jurídicas internacionales que puedan prestar asistencia inmediata.
- **Monitoreo periódico.** El personal responsable puede examinar y reportar las tendencias relacionadas con las detenciones y los arrestos en el contexto operacional, así como los agentes involucrados.

Formación y sensibilización

- **Mantener actualizados los planes locales de respuesta.** Deben mantenerse protocolos claros y el personal debe conocer los procedimientos para reportar y responder a incidentes de detención y arresto, a qué partes interesadas notificar, y las funciones y las responsabilidades dentro de la organización. Los planes deben incluir protocolos de comunicación y procedimientos de notificación progresiva, así como medidas para garantizar la continuidad de las operaciones si se detiene o arresta a personal clave.
- **Capacitación en seguridad.** El personal debe recibir orientación y capacitación sobre las medidas de seguridad personal, la concienciación acerca de la situación, la prevención de riesgos y los protocolos durante las interacciones con las autoridades.

- **Simulacros.** Los simulacros y los ejercicios de simulación periódicos permiten al personal practicar los procedimientos de respuesta en caso de detención.
- **Documentación.** El personal debe conocer la documentación que debe llevar consigo y otras medidas que debe seguir para acceder a las zonas de operaciones y desplazarse con seguridad por ellas.

Incidencia y creación de redes

- **Funciones y responsabilidades en materia de comunicación.** Los trabajadores humanitarios deben ser capaces de explicar sus funciones y la misión de la organización en términos sencillos y atractivos. Esto puede requerir una práctica regular.
- **Interacción con las partes interesadas.** El personal debe colaborar con las autoridades locales, los líderes comunitarios y otras partes interesadas para establecer relaciones y reducir la probabilidad de que se produzca un incidente.
- **Incidencia internacional.** Las organizaciones pueden colaborar entre sí y a través de canales diplomáticos para abogar por la protección de los trabajadores humanitarios.

Cuidado del personal

- **Protocolos de cuidado del personal** (incluidos el apoyo y el asesoramiento en salud mental) pueden establecerse para la atención del personal antes, durante y después de un incidente.

► Véase el capítulo 5.4 sobre el cuidado del personal.

Enlace familiar

- **Trabajar con las familias** es fundamental para responder eficazmente a situaciones a medio y largo plazo. Los familiares pueden ser los responsables de la alimentación y el cuidado de la salud de su familiar detenido o arrestado. También es probable que tengan que gestionar la fianza y el pago de multas. Considere la posibilidad de establecer protocolos de apoyo y comunicación con las familias la persona detenida o arrestada, incluido el apoyo financiero o jurídico que puede proporcionarse y en qué condiciones.

Monitoreo y evaluación

- **Revisiones e informes periódicos.** Las organizaciones pueden revisar y actualizar periódicamente los diagnósticos de riesgos, los planes de contingencia y los programas de capacitación. Esto ayuda a identificar los avances y sirve de alerta temprana para futuros riesgos.
- **Análisis de incidentes.** Las entrevistas y las revisiones de los arrestos o las detenciones pueden ayudar a identificar aprendizajes y a mejorar las respuestas futuras.

Algunos miembros del personal pueden ser detenidos o arrestados por motivos ajenos a su trabajo o al de la organización humanitaria. Entre los factores que pueden influir en ello figuran las afiliaciones sociales o culturales, las dinámicas de poder y la actividad política o delictiva. Las organizaciones humanitarias deben tener una política clara sobre el apoyo que prestarán en caso de arrestos o detenciones no relacionados con el trabajo. Si la detención o el arresto se deben a circunstancias políticas, las organizaciones humanitarias deben tener cuidado de no dar la impresión de que se están entrometiendo en la política local. Sin embargo, esto no debe ser un obstáculo automático para asumir la responsabilidad del personal en esta situación y hacer todo lo posible para garantizar su regreso seguro.

7.8.4 Respuesta a un incidente

Cuando desaparecen miembros del personal, el primer reto es averiguar y comunicar la naturaleza exacta de la situación. Esto puede llevar horas, días o incluso semanas. La información básica debe establecerse y comunicarse en un informe de incidentes que luego se comparte con el personal apropiado.

Las buenas prácticas implican tener claro quién ha sido o debe ser notificado y quién sabe ya del incidente fuera de la organización, incluyendo si la policía, las fuerzas de seguridad o las autoridades han sido o serán informadas; si la prensa o terceras partes están enteradas del incidente, y si se ha notificado a los familiares más próximos. La gestión de la información puede ser difícil, pero debe ser cuidadosamente considerada y abordada por el personal encargado de la respuesta. También debe tenerse en cuenta el monitoreo de la prensa, las redes sociales y otros medios de comunicación, ya sean locales, nacionales, regionales o internacionales.

Las organizaciones deben considerar la privacidad y la confidencialidad a la hora de reportar o compartir información. En situaciones prolongadas, una organización puede decidir intensificar su respuesta e iniciar una campaña pública para conseguir la liberación de un miembro del personal o poner de relieve su estado. Lo ideal es hacerlo con el permiso de la persona afectada.

Los procedimientos de respuesta a incidentes se tratan con más detalle en el capítulo 4.4. A continuación figuran algunas consideraciones más detalladas.

En caso de detención o arresto

En caso de detención, es probable que un enfoque de mano dura sea contraproducente y aumente el antagonismo hacia el miembro del personal y la organización. La detención puede tener por objeto obligar a la organización o a otra entidad a prestar atención y entablar un diálogo serio, en cuyo caso responder a esta expectativa puede bastar para poner fin al incidente.

En algunos casos, el detenido puede ser capaz de negociar su propia liberación, y las organizaciones deben formar al personal en consecuencia. Hacer hincapié en su labor humanitaria y en el carácter neutral, imparcial e independiente de su organización y sus actividades suele ser un primer paso importante, y el personal de algunas organizaciones lleva consigo documentos oficiosos o de otro tipo para aclarar el papel de la organización. Llevar información de contacto de emergencia también es útil en caso de detención.

Si se arresta a un miembro del personal y se desconoce su paradero, la prioridad es determinar dónde se encuentra y bajo la autoridad de quién. Esto puede implicar visitar a las autoridades locales pertinentes, informar a la embajada (si se trata de un ciudadano extranjero) y utilizar las redes locales para recopilar información. Es importante recordar que un miembro del personal puede ser arrestado por motivos legítimos y tener que rendir cuentas de sus actos. En cualquier caso, las organizaciones pueden plantearse contratar a un buen abogado local que conozca las lenguas y el sistema locales, tenga experiencia en este tipo de situaciones y disponga de contactos útiles.

Cuando esté claro quién ha detenido o arrestado al miembro del personal y dónde se encuentra, las organizaciones deben tratar de garantizar la protección de sus derechos. Las organizaciones deben considerar la posibilidad de abogar ante las autoridades locales por un trato justo y humano del personal afectado, incluido el acceso a atención médica, asesoramiento jurídico y garantías procesales. Esto puede hacerse tras una evaluación y conversaciones con las partes interesadas, ya que la atención de una organización internacional puede agravar la situación. En caso de que no se atiendan estas peticiones, podrán analizarse medidas adicionales. Cualquier maltrato o violación de los derechos debe documentarse y, si procede, exigir la rendición de cuentas (teniendo en cuenta que esto puede causar más daños que beneficios).

Los arrestos pueden realizarse sin que se presenten cargos formales; en estos casos la organización puede abogar por que se presente una acusación en un plazo determinado. La acusación puede referirse al individuo (por ejemplo, estar implicado en un delito) o a la organización (por ejemplo, realizar tareas de espionaje encubierto a través de las actividades humanitarias). En cualquier caso, la prioridad principal es trabajar por la liberación segura y rápida de la persona. En la mayoría de los casos, solo una vez que el miembro del personal haya sido absuelto de cargos injustos deben hacerse esfuerzos para limpiar el nombre de la persona o de la organización.

Como parte de un plan de contingencia más amplio, la organización puede tener que analizar qué apoyo administrativo y financiero se proporcionará al miembro del personal afectado y a su familia. ¿En qué circunstancias se organizaría la asistencia jurídica o se pagaría una fianza? ¿Con qué medios y quién sería responsable? Muchas organizaciones tienen seguros que cubren algunas de estas contingencias. Puede ser necesario considerar si la cobertura es aplicable y se extiende a todo el personal o solo a las personas clave. Esto puede considerarse a nivel político como parte de una posición más amplia de gestión de riesgos.

► *Para obtener más información sobre los seguros, véase el capítulo 5.4.*

Es posible que las organizaciones deseen proporcionar apoyo adicional a las personas cuya función es visitar al personal detenido o arrestado y servir de enlace con las autoridades, ya que puede ser una tarea difícil con muchas repercusiones potenciales en dichas personas (por ejemplo, en su salud mental, así como en sus relaciones con las autoridades o con los grupos locales). Esta función no debe recaer aleatoriamente en una persona en función de su proximidad al contexto. También es fundamental mantener y gestionar el contacto con la familia del miembro del personal arrestado o detenido. Lo ideal es informarlos de las medidas que se están tomando; las organizaciones deben tratar de mantener una línea de comunicación directa y regular, estar al tanto de las medidas que la familia tiene intención de tomar o ha tomado, y advertirles si lo que planean hacer puede perturbar, complicar o ser contraproducente para la respuesta prevista por la organización.

► *Para obtener más información, véase el capítulo 4.4 sobre enlace familiar.*

Es probable que el apoyo de la comunidad y de las partes interesadas locales influya en la posibilidad de lograr la liberación de un miembro del personal detenido. Se podría mapear la dinámica social y de los clanes e identificar a los interlocutores para apoyar las consultas y las peticiones. Las organizaciones que no son de la zona pueden encontrar útil la información de los agentes locales para mantener un control sobre el estado del personal afectado y transmitir mensajes informales.

Consideraciones posteriores al incidente

Los miembros del personal liberados y las personas implicadas en el incidente, como los familiares o el equipo de gestión de incidentes, pueden necesitar apoyo adicional tras un incidente. Esto puede incluir una licencia laboral, apoyo médico y asesoramiento.

► *Véase el capítulo 5.4 para obtener más información sobre el cuidado del personal tras un incidente.*

Puede ser conveniente hablar con las autoridades pertinentes, las partes interesadas y los líderes de la comunidad para saber por qué se produjo la detención o el arresto y qué se puede hacer para evitar un incidente similar en el futuro.

Muchas organizaciones celebrarán una sesión formal de información sobre los hechos o un examen posterior a la acción.

► Para obtener más información sobre el examen posterior a la acción, véase el capítulo 4.4.

Más información

Orientación y recursos

Buth, P. (2010). *Crisis management of critical incidents*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/crisis-management-of-critical-incidents).

Davidson, S. (2013a). *Family first: liaison and support during a crisis*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/family-first/).

Davidson, S. (2013b). *Managing the message: communication and media management in a security crisis*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/managing-the-message).

Hostage International. (s. f.). *Best practice in family support* (<https://hostageinternational.org/resource/best-practice-in-family-support/>).

Hostage US. (s. f.). *Hostage US guides* (<https://hostageus.org/resources/hostage-us-guides>).

7.9 Rapto, secuestro y situaciones de rehenes

Los incidentes de rapto, incluidos los secuestros y las situaciones de rehenes, pueden tener consecuencias físicas y emocionales duraderas. Prevenir, prepararse y responder a un rapto requiere inversión y planificación organizativa. Este capítulo aborda las buenas prácticas en la gestión de los riesgos de rapto. Incluye orientaciones sobre los secuestros virtuales y exprés, que se han hecho más frecuentes en los últimos años, y aborda las repercusiones a largo plazo y otras cuestiones de carácter duradero asociadas a los secuestros.

7.9.1 Definiciones

El rapto se refiere a cualquier captura ilegal y forzosa de una persona. El secuestro se refiere a un rapto con el propósito explícito de obtener algo a cambio de la liberación del secuestrado. Normalmente se trata del pago de un rescate, aunque los agresores pueden exigir concesiones políticas. En algunos casos, lo que aparentemente puede ser una causa política puede ser, de hecho, una extorsión.

El término “toma de rehenes” se utiliza para describir una situación en la que se conoce el paradero de la persona raptada y su liberación depende del cumplimiento de exigencias específicas. En un operativo de asedio, los agresores y sus rehenes han sido localizados y rodeados por las fuerzas de seguridad, y los agresores amenazan con matar a los rehenes a menos que se les facilite una vía de escape.

Tipos de secuestros

- **Secuestro extorsivo:** el motivo principal es el beneficio económico o político. Los secuestradores exigen un rescate a la familia o colegas del secuestrado a cambio de su liberación. También pueden exigir la liberación de prisioneros, cambios políticos o publicidad para su causa.
- **Secuestro exprés:** la víctima es retenida durante un periodo breve, normalmente inferior a 24 horas, y obligada a pagar un rescate rápido (por ejemplo, sacando dinero de un cajero automático). Estos secuestros suelen ser oportunistas y no se planifican demasiado.

- **Secuestro virtual:** los delincuentes intentan coaccionar a las víctimas para que paguen un rescate alegando falsamente que han secuestrado a alguien conocido. Las tácticas incluyen mantener a la víctima al teléfono para impedir que verifiquen la seguridad de la persona o la autenticidad de cualquier grabación de audio o video de la supuesta víctima. Este tipo de secuestro se ha visto favorecido en los últimos años por las nuevas tecnologías, especialmente la IA.
- **Secuestro del tigre:** se secuestran personas conocidas de un objetivo que es obligado a participar en un delito, como acceder a un lugar seguro para robar dinero en efectivo, a fin de garantizar la liberación segura de las personas secuestradas.

7.9.2 Planificación, preparación y capacitación

Para hacer frente a la amenaza de rapto, las organizaciones deben evaluar quién corre más riesgo y adaptar sus medidas de mitigación de riesgos y de preparación al contexto. La formación periódica, los ejercicios de simulación, la asignación adecuada de recursos, el aprendizaje continuo y la adaptabilidad son esenciales tanto para la prevención como para la respuesta. A continuación se exponen ejemplos de acciones.

En la sede

- Establecer y mantener actualizadas las políticas y los protocolos de seguridad que abordan específicamente los riesgos de rapto, y garantizar que todos los miembros del personal las conocen y reciben orientación al respecto.
- Crear una estructura organizativa de gestión de crisis con la selección y formación del personal pertinente.
- *Para obtener más información sobre la estructura de gestión de crisis, véase el capítulo 4.4.*
- Establecer vínculos a nivel local e internacional para garantizar la experiencia necesaria para prestar un apoyo eficaz en la gestión de incidentes cuando sea necesario. Por ejemplo, analizar qué ayuda gubernamental puede esperarse si un miembro del personal es secuestrado o identificar expertos externos cualificados para la gestión de crisis y el apoyo posterior a los secuestrados y sus familias.¹¹⁵
- Mantener actualizados los registros del personal, incluidos los datos de contacto de los familiares cercanos y cualquier afección médica. Considerar la posibilidad de que todo el personal documente las preguntas de “prueba de vida” (más adelante se brinda más información al respecto).

¹¹⁵ Existen varias organizaciones de respuesta especializadas que apoyarán a las organizaciones y a las familias durante los raptos, y muchas de ellas están asociadas a pólizas de seguros especiales. Algunos Gobiernos mantienen equipos especializados de las fuerzas del orden para intervenir si uno de sus ciudadanos es raptado.

- Ser claro acerca de las responsabilidades y obligaciones para con el personal y sus familias en caso de secuestro, incluso cuando el personal está en comisión de servicio.
- Informar plenamente al personal del riesgo de rapto antes de asignarlo a zonas de alto riesgo.
- Preparar plantillas o directrices para las declaraciones a los medios de comunicación y los comunicados de prensa en caso de rapto.
- Impartir formación al personal sobre las estrategias de mitigación del riesgo de rapto y cómo sobrevivir a un incidente de este tipo.
- Asegurarse de que se dispone de pólizas de seguro, que incluyan el seguro médico y el seguro de riesgos especiales o de secuestro y rescate.

En las oficinas operacionales

- Garantizar la existencia de una estructura organizativa de gestión de crisis con personal capacitado.
- Garantizar el conocimiento de la política de secuestros y rescates de la organización y que el personal está preparado para responder a los raptos (incluidas las llamadas de los secuestradores).
- Desarrollar planes de contingencia específicos para los raptos y revisarlos y actualizarlos periódicamente, así como los procedimientos operativos estándar.
- Establecer y mantener canales de comunicación eficaces y fiables para reportar incidentes y compartir notificaciones durante la gestión de un incidente crítico.
- Establecer y mantener contacto con las embajadas pertinentes (si los secuestrados son ciudadanos extranjeros) y otros agentes diplomáticos, como las Naciones Unidas, en coordinación con el equipo de gestión de crisis del país.
- Saber a quién dirigirse en el Gobierno en caso de secuestro y, si existen equipos especializados, invertir tiempo en comprender cómo funcionan y responden.
- Estar informado sobre la estructura de mando de las fuerzas de seguridad nacionales y otros agentes armados relevantes en la zona de operaciones de la organización.
- Comprender la política gubernamental sobre el contacto con los agresores: negociar directamente con los agresores podría tener consecuencias graves.
- Garantizar que se llevan registros claros y mantener la confidencialidad. Estos registros deben marcarse como “confidencial”, y el personal debe esperar que los registros puedan ser solicitados en algún momento como parte de una investigación.
- Estar preparados para prestar apoyo psicosocial al personal afectado y a sus familias y abordar los problemas relacionados con el trauma y el estrés.

- Véase el capítulo 5.4 para obtener más información sobre el cuidado del personal tras un incidente crítico.

Seguro de secuestro, rescate y extorsión

El seguro de secuestro, rescate y extorsión está diseñado específicamente para proteger a personas y organizaciones contra las pérdidas financieras y las responsabilidades conexas.

Aunque los términos y la cobertura varían según la póliza y la aseguradora, el seguro de secuestro y rescate puede proporcionar lo siguiente:

- Servicios preventivos, como información y directrices específicas para cada país.
- La disposición de asesores de respuesta a crisis que puedan ofrecer apoyo en las negociaciones y asesoramiento estratégico.
- Cobertura para demandas judiciales, relaciones públicas, gastos de descanso y rehabilitación, asistencia médica y psiquiátrica, indemnización por accidente personal, pérdida de ingresos y cualquier otra responsabilidad legal relacionada. También podría cubrir el reembolso de los rescates si no es ilegal en la jurisdicción correspondiente (por ejemplo, si los agresores son grupos o individuos penalizados).

Los seguros de secuestro, rescate y extorsión suelen incluir una cláusula de confidencialidad, por la que solo se informa de los detalles de la póliza al equipo directivo. Es importante que las organizaciones puedan analizar el plan de seguros con el personal sin incumplir esta cláusula. Las organizaciones pueden elaborar una declaración y nombrar a un portavoz en caso de consulta.

Algunos planes de seguros permiten deducir el 10 % de la prima anual para preparación y formación.

- Para obtener más información sobre los seguros, véase el capítulo 5.4.

7.9.3 Medidas de reducción de riesgos

A continuación se ofrecen ejemplos de medidas para reducir los riesgos de rapto.

- **Conocimiento del contexto.** Recopilar información sobre el contexto de seguridad y los riesgos de rapto mediante, por ejemplo, el monitoreo de la información de seguridad, la asistencia a reuniones informativas sobre seguridad específicas del contexto y la comprensión de las medidas adoptadas por otras organizaciones que operan en la misma zona.
 - **Comunicación y aceptación.** Discutir el papel y el trabajo de la organización con los agentes pertinentes, garantizando al mismo tiempo la calidad y la aceptación del programa.
 - **Evitar la previsibilidad.** Variar las rutinas y el horario de los desplazamientos, tanto en los trayectos al trabajo como fuera de él.
 - **Reducir la visibilidad.** Minimizar la visibilidad evaluando las marcas, como los logotipos en los vehículos, siendo conscientes de los comportamientos que pueden llamar la atención, utilizando transportes de confianza en lugar de vehículos identificables para algunos desplazamientos, operando en equipos más pequeños y limitando la presencia en las redes sociales.
 - **Aplicar los procedimientos operativos.** Utilizar canales de comunicación seguros para la información sensible, garantizar que se aplican y respetan las medidas de gestión de riesgos en los viajes y mantener actualizados los planes de contingencia para situaciones imprevistas.
 - **Eliminación de posibles vulnerabilidades.** Restringir temporalmente el acceso a las zonas de alto riesgo, pedir al personal que trabaje a distancia y considerar la suspensión de los programas son estrategias a tener en cuenta cuando hay indicios que sugieren un aumento del riesgo. Algunas organizaciones consideran útil que el personal viaje con dispositivos relacionados con el trabajo temporales y “limpios”, como teléfonos y ordenadores portátiles, para evitar el uso indebido de los datos almacenados. Una medida más extrema es retirar al personal de mayor riesgo.
 - **Seguridad del sitio.** Aplicar controles de acceso y procedimientos de identificación estrictos en alojamientos, oficinas y lugares donde se ejecutan los proyectos. Aunque los secuestros suelen producirse durante los traslados, sigue siendo fundamental mantener la seguridad de los sitios.
- Véase el capítulo 7.2 sobre la seguridad del sitio.
- **Mayor concienciación y antivigilancia.** Estar atentos (colectiva e individualmente) a cualquier indicio de vigilancia y comportamiento inusual. Un rapto normalmente implica planificación, y los agresores posiblemente vigilen la residencia, la oficina y los movimientos de su objetivo durante algún tiempo antes de hacer su movimiento. Se recomienda una formación periódica sobre los protocolos de reporte y las prácticas antivigilancia.

► *Para obtener más información sobre la vigilancia hostil, véase el capítulo 7.5.*

- **Uso de la tecnología.** Los equipos digitales de rastreo pueden llevarse personalmente o instalarse en los vehículos, lo que permite emitir alertas digitales y seguir las rutas. Estos equipos deben utilizarse con precaución y evaluarse en función de los riesgos de seguridad.
 - **Apoyo y protección locales.** Establecer y mantener buenas relaciones con los líderes de la comunidad y las autoridades locales puede facilitar el acceso a asesoramiento sobre medidas de protección y los posibles riesgos de raptó. En algunos contextos también puede ofrecer cierta protección. Sin embargo, las dinámicas de poder pueden cambiar rápidamente, por lo que es necesario considerar cuidadosamente este aspecto antes o en el momento de solicitar dicho apoyo.
 - **Protección armada.** Utilizar guardias o guardaespaldas armados puede ser un elemento disuasorio para los posibles agresores en residencias, oficinas y durante los viajes. Sin embargo, el uso de protección armada también puede aumentar la visibilidad e incrementar el riesgo tanto para el personal armado como para el resto de los empleados. Esto debe evaluarse cuidadosamente a la luz de las políticas, los principios, la imagen y las medidas de aceptación de la organización. También es fundamental tener en cuenta las sanciones y la legislación antiterrorismo a la hora de recurrir a la protección armada.
- *Para obtener un análisis más detallado sobre la protección armada, véase el capítulo 4.2.*
- **Política pública de “no rescate” u otras concesiones sustanciales.** Adoptar una postura sobre los rescates en los documentos políticos y en las comunicaciones públicas puede hacer que el personal sea un objetivo menos atractivo. En realidad, a veces las familias, las empresas privadas, los Gobiernos y las organizaciones humanitarias pagan algo de dinero. Una estrategia de “no pago” es difícil de mantener sin una preparación sostenida en todos los niveles de una organización y un alto nivel de contacto con la comunidad y conexiones con una amplia variedad de partes interesadas.

Mitigar los riesgos de secuestros exprés y en línea

Los secuestros exprés suelen tener una motivación económica, y los secuestradores no pretenden dañar físicamente a la persona secuestrada. Algunas de las siguientes medidas pueden ayudar a mitigar los riesgos:

- Realizar un diagnóstico de riesgos (zonas de alto riesgo, objetivos probables, impacto).

- Brindar formación al personal sobre el conocimiento de la situación, la manera de evitar convertirse en un objetivo (recomendaciones sobre el uso de cajeros automáticos) y el modo de responder adecuadamente para una liberación segura (cumplimiento de las exigencias).
- Llevar objetos de valor limitados (mínimos) y tarjetas bancarias con saldos bajos o límites de extracción diarios.

Los secuestros en línea están concebidos para conseguir dinero rápidamente. Las medidas de mitigación incluyen:

- Formar al personal sobre la existencia de falsificaciones generadas por IA y sobre cómo identificar los indicios de que se trata de un secuestro en línea (como, por ejemplo, que los agresores intenten mantener al objetivo en la llamada, bloqueen sus esfuerzos por contactar o hablar con la supuesta víctima y rebajen rápidamente las exigencias de rescate).
- Formar al personal para que responda con calma: colgar, ponerse en contacto con la supuesta víctima o pedir detalles que solo ellos conozcan.
- Asegurarse de que el personal es consciente de que no debe acceder a pagar un rescate, especialmente en persona, ya que esto podría ponerlo en mayor riesgo.

7.9.4 Respuesta a un incidente

Consideraciones generales sobre la respuesta

Cuando se produce un rapto, la organización suele activar su estructura de gestión de crisis. Las organizaciones más grandes pueden tener un equipo de gestión de crisis en la oficina central, apoyado por un equipo de gestión de incidentes en la oficina operacional o en el lugar del incidente. Las organizaciones internacionales también pueden contar con un equipo regional de gestión de crisis. Estos equipos suelen contar con el apoyo de colegas con una amplia variedad de conocimientos especializados, generalmente en materia de seguridad, salud, informática y comunicaciones. Normalmente, la organización designará a un comunicador para que transmita los mensajes a y de los agresores. (Esta función no es la misma que la de un negociador, y esta persona no actuará como responsable de la toma de decisiones ni como miembro formal de un equipo de respuesta). Los equipos de respuesta suelen trabajar con otras

organizaciones, como las fuerzas del orden, organismos gubernamentales, medios de comunicación y compañías de seguros.

Una responsabilidad clave del equipo de gestión de crisis es desarrollar y aplicar una estrategia de respuesta a incidentes específica, que se adapte en función de la evolución de las circunstancias. Esta estrategia, elaborada por expertos como asesores jurídicos, ayuda a garantizar el cumplimiento de los marcos jurídicos pertinentes y guía el enfoque de la respuesta de la organización, incluidas las negociaciones con los agresores, la gestión de las partes interesadas y las comunicaciones. El equipo de gestión de crisis deberá revisar periódicamente las estrategias relativas a los agresores, los familiares, las autoridades, los medios de comunicación y otras organizaciones.

► Véase el capítulo 4.4 para consultar más buenas prácticas sobre la manera de responder a incidentes críticos y establecer una estructura de gestión de crisis.

Las acciones durante las fases iniciales de una sospecha de rapto pueden incluir las siguientes:

- Determinar los hechos y elaborar un informe del incidente.
- Garantizar la seguridad del resto del personal, tal vez restringiendo sus movimientos o trasladándolos a un lugar más seguro.
- Evaluar si deben suspenderse los programas.
- Informar a otras oficinas y al equipo directivo.
- Informar a los familiares y prepararlos para posibles contactos de los agresores.
- Alertar a las compañías de seguros.
- Consultar a expertos externos pertinentes, de acuerdo con el plan de gestión de crisis.
- Gestionar las comunicaciones y la información, incluida la creación de un libro de registro para dejar constancia de los acontecimientos, los debates, las decisiones, las responsabilidades y las medidas adoptadas en todas las oficinas pertinentes.
- Identificar a un comunicador.
- Monitorear los medios de comunicación en busca de información relativa al incidente.
- Garantizar la disponibilidad financiera para cubrir los costes iniciales, lo que puede requerir obtener fondos de la sede.

Durante las fases iniciales de un rapto, el personal de respuesta a menudo necesitará ser relevado de otras tareas y disponer de un espacio de trabajo e instalaciones específicas. Los miembros del equipo necesitarán descanso y apoyo regulares y, si la crisis se prolonga durante mucho tiempo, un traspaso fluido a los suplentes.

Expertos externos

En algunos casos, un especialista en situaciones de rapto puede unirse al equipo de gestión de crisis desde fuera de la organización, como, por ejemplo, desde el Gobierno local o el país anfitrión, la compañía de seguros o una empresa de seguridad privada. Su función es asesorar y apoyar, no tomar decisiones. Los expertos en la gestión de raptos pueden presentarse voluntariamente o ser recomendados. Su conocimiento del contexto local y regional y su comprensión de los aspectos jurídicos, así como sus capacidades, redes y experiencia, pueden ser de un valor incalculable.

Aunque los asesores externos no suelen gestionar un incidente ni entablar negociaciones directas con los agresores, pueden aportar un valor añadido importante al actuar como asesores y entrenadores del personal, como los equipos de respuesta y de medios de comunicación. Pueden ofrecer una perspectiva objetiva, ayudar a anticipar posibles escenarios, contribuir a garantizar la disponibilidad de la respuesta y evaluar su eficacia. Es necesario cerciorarse de que no surja ningún conflicto de intereses; por ejemplo, en el caso de un experto recomendado o designado por el Gobierno, puede haber discrepancias en términos de políticas, objetivos y enfoques.

Cuando se rapta a un conjunto de miembros del personal de varias organizaciones, la colaboración entre las distintas partes implicadas es esencial para garantizar un enfoque unificado. Es aconsejable formar equipos conjuntos de gestión de crisis a nivel operacional y de la sede. Aunque cada organización querrá participar, los miembros del equipo deben ser elegidos por su habilidad y competencia en la gestión de incidentes, más que como representantes de sus respectivas organizaciones. Se puede recurrir a expertos externos para mantener la objetividad y el enfoque.

Incluso cuando un incidente afecta solo a una organización, puede tener implicaciones para la seguridad de otras en la misma zona. Existe, por tanto, una responsabilidad colectiva en materia de seguridad. El pago de un rescate o la forma en que una organización interactúa con las autoridades también tienen implicaciones de seguridad más amplias. La organización a la que pertenece la persona raptada es la responsable de elegir el enfoque de la respuesta, sin embargo, puede ser prudente escuchar los consejos de otras personas con experiencia en la materia, especialmente si han vivido situaciones similares.

Cuando se desconoce el paradero de la persona raptada

Un rapto será especialmente difícil cuando se desconozca el paradero y la situación de la víctima y sea imposible ponerse en contacto con los agresores. La organización objetivo puede tratar de generar publicidad sobre el incidente, pero como ocurre con cualquier interacción con los medios de comunicación, esto puede ser contraproducente si eleva innecesariamente el perfil de la persona raptada y aumenta su valor para los agresores. Alternativamente, puede ser un buen enfoque si indica a las autoridades que existe un amplio conocimiento de la suerte de la persona en cuestión y que la prolongación de su rapto dañaría gravemente la imagen de las autoridades y su capacidad para establecer o mantener el Estado de derecho. Las organizaciones de derechos humanos y otras organizaciones de incidencia política suelen ser más eficaces que las organizaciones humanitarias a la hora de generar este tipo de publicidad, por lo que podría ser posible cooperar con ellas. En otros casos, posiblemente no haya mucho que hacer más allá de difundir información y fotografías de la víctima e intentar encontrar a alguien que pueda proporcionar una pista o un contacto.

Gestionar las relaciones con la familia

- **Contacto inmediato y enlace familiar.** Es crucial informar rápidamente a la familia de la persona raptada, preferiblemente en persona y, si es posible, antes de que se enteren del incidente a través de los medios de comunicación o de terceros. Se recomienda una visita en persona. Se aconseja activar funciones específicas de enlace familiar. Las personas que desempeñan las funciones de enlace familiar, ya sean especialistas internos o subcontratados,¹¹⁶ pueden ayudar a generar y mantener la confianza y deben tener muy buenas habilidades interpersonales y ser capaces de comunicarse en el idioma de la familia. Algunos Gobiernos también cuentan con oficiales de enlace familiar, que deben complementar, pero no sustituir, la participación de las organizaciones.

En algunos casos, las familias, sobre todo si son de la zona, pueden preferir gestionar ellas mismas los raptos, aprovechando los conocimientos y las redes locales, especialmente si las rivalidades sociales o políticas locales son las que impulsan los raptos. Sin embargo, en los casos delictivos o motivados por razones políticas pueden no estar mejor preparadas que la organización. A veces, el personal puede ser raptado por motivos no relacionados con su trabajo, y algunas organizaciones

¹¹⁶ Si una organización no cuenta con un oficial de enlace familiar específico o personal capacitado en esta materia, se puede acordar previamente el apoyo de organizaciones especializadas como Hostage International: www.hostageinternational.org.

pueden optar por no intervenir a menos que estén directamente implicadas. En estas circunstancias, es importante que la familia y la organización comprendan y acuerden la estrategia de respuesta y en qué casos es posible el apoyo mutuo.

- **Desarrollar un enfoque claro.** Mantener una comunicación transparente con la familia es esencial para fomentar la confianza. La falta de confianza puede llevar a la familia a actuar de forma independiente, por ejemplo, acudiendo a los medios de comunicación, visitando el lugar donde se produjo el rapto o negociando por su cuenta. La familia también estará más preparada que la organización para pagar un rescate y puede empezar a vender activos para reunir el dinero. Aunque las familias tienen su propio derecho de iniciativa, las organizaciones deben orientarlas sobre las posibles consecuencias y riesgos de tales acciones. El pago de un rescate no garantiza la liberación y puede dar lugar a nuevas demandas.
- **Gestión de la divulgación de información.** Compartir información con familiares y otras personas debe equilibrarse cuidadosamente con la necesidad de gestionar eficazmente el incidente.

► *Para obtener más información, véase el capítulo 4.4 sobre enlace familiar.*

Enlace con las autoridades

Es aconsejable informar inmediatamente a las autoridades —departamentos e instituciones gubernamentales pertinentes— sobre un secuestro. Esto incluye a las autoridades del país donde tuvo lugar el rapto, así como al Gobierno del país de la víctima (esto puede implicar a varias autoridades si tiene más de una nacionalidad). Aunque el rapto se produzca en una zona no controlada por el Gobierno, este debe ser notificado.

El equipo de gestión de crisis tendrá que decidir una política y cómo aprovechar las relaciones con todas las autoridades pertinentes. Las autoridades tendrán acceso a información y datos de inteligencia, a redes y a servicios que posiblemente no estén disponibles para la organización y, por lo tanto, pueden estar en una mejor posición para conseguir la liberación. Este es especialmente el caso de las autoridades del país donde se produjo el rapto. Al mismo tiempo, las autoridades pueden tener una agenda que no redunde en el interés directo y el bienestar de la persona raptada. También pueden desconfiar de la capacidad de una organización humanitaria para gestionar adecuadamente el rapto o pueden querer evitar que la organización entable un diálogo con los agresores, a los que pueden considerar “terroristas” o rebeldes (en algunos países, este contacto puede ser ilegal). Si las autoridades desean resolver el incidente rápidamente, pueden estar predispuestas a utilizar la fuerza en lugar de, o junto con, cualquier negociación.

A continuación se enumeran algunos aspectos prácticos y principios que deben acordarse y confirmarse con las autoridades pertinentes:

- La seguridad y el bienestar de la víctima deben ser la principal preocupación.
- La estrategia global de respuesta.
- La estrategia de medios de comunicación (incluida la confidencialidad).
- Un enfoque conjunto sobre la relación con la familia; es conveniente colaborar con los oficiales de enlace familiar del Gobierno.
- La elección de un comunicador (ver más abajo).

Algunas organizaciones han conseguido que se incluya a un miembro de su personal en un equipo de gestión de respuesta del Gobierno. En un acuerdo de este tipo, es importante que el representante de la organización comprenda la posición de esta y los límites de la relación.

Orientaciones para el primer contacto con las autoridades locales

- Discutir y acordar dentro de los diferentes equipos de respuesta la línea a seguir.
- Preparar un guión para informar a las autoridades sobre los hechos.
- Comunicarse con una persona de contacto formal, que la organización ya debería conocer.
- Aprovechar todos los medios para garantizar que la seguridad de la persona raptada sea la máxima prioridad.
- Anticipar que, una vez informadas, las autoridades podrán ponerse en contacto con los medios de comunicación.
- Establecer un procedimiento de contacto para futuras sesiones informativas.

► *Para obtener más información sobre el enlace con las autoridades durante las crisis, véase el capítulo 4.4.*

Gestión de la comunicación

La gestión eficaz de la comunicación durante un rapto implica una planificación estratégica, el mantenimiento de la confidencialidad y la coordinación con las partes interesadas internas y externas, para garantizar la seguridad y el bienestar de la persona raptada y su familia.

Compartir detalles fuera de la organización debe evaluarse cuidadosamente, y solo debe ocurrir como parte de un plan deliberado dirigido a conseguir la liberación de la víctima. Adoptar el principio de la “necesidad de saber” para compartir información se considera una buena práctica.

Es aconsejable que el equipo de gestión de crisis tome las decisiones relacionadas con la comunicación con las partes interesadas internas y externas, con el apoyo de un equipo de comunicación de crisis. El equipo de comunicación de crisis se encargaría de gestionar las relaciones con los medios de comunicación, lo que incluye la elaboración y aplicación de estrategias de comunicación, el monitoreo de los medios de comunicación y la designación de un portavoz. También pueden ayudar a proteger la privacidad de la víctima y su familia mediante la gestión de las redes sociales. Puede ser aconsejable cerrar las cuentas de las redes sociales para impedir que los agresores accedan a ellas.

Los mensajes claros y concisos ayudan a gestionar la cobertura mediática. Un mensaje central puede destacar que la organización responsabiliza a los agresores de la seguridad y el bienestar del miembro del personal afectado y que se está haciendo todo lo posible para que sea liberado. Dado que los distintos medios de comunicación (internacionales y nacionales) pueden presentar la noticia de manera diferente, es esencial que el personal de comunicación de las distintas oficinas se consulte entre sí antes de emitir cualquier declaración de la organización.

Para gestionar las preguntas de los medios de comunicación y el interés público, la organización puede publicar actualizaciones en su sitio web. Esto ayuda a reducir las consultas telefónicas y garantiza la coherencia de los mensajes. Las organizaciones deben asumir que los agresores están monitoreando las noticias, por lo que no es prudente intentar comunicarse o negociar a través de los canales públicos de los medios de comunicación. Los mensajes de los medios de comunicación pueden distorsionarse fácilmente, y ello socava los auténticos esfuerzos de comunicación y negociación. Es importante relacionarse con los editores y los periodistas para fomentar la colaboración.

Si la familia desea hacer un llamamiento público, debe hacerse de forma constructiva y gestionarse con cuidado. Los destinatarios no suelen ser los agresores, sino las autoridades responsables de la seguridad, con mensajes dirigidos a garantizar la continuidad de los esfuerzos por resolver la situación.

Ejemplo: Controlar los rumores

Durante la fase final de las negociaciones para la liberación de los trabajadores humanitarios raptados en Somalia, el control de los rumores se convirtió en un verdadero reto. Mientras la situación seguía siendo tensa, otra organización humanitaria anunció inesperadamente que las personas raptadas habían sido liberadas y se habían marchado en un avión el día anterior. Este rumor circuló inmediatamente entre la comunidad humanitaria y fue recogido por los medios de comunicación locales. La organización implicada en las negociaciones tardó dos horas frenéticas en averiguar de dónde había salido el anuncio y emitir una rectificación.

La publicidad puede ser beneficiosa si a los agresores les preocupa su reputación, sin embargo, este no suele ser el caso de los grupos que utilizan los raptos para llamar la atención. En tales casos, los agresores pueden involucrar ellos mismos a los medios de comunicación y transformar la situación en un peligroso espectáculo en el que la muerte de la víctima puede utilizarse para crear un clímax dramático. Para contrarrestarlo, hay que convencer a los medios de comunicación de que no participen en la difusión sensacionalista de la situación.

Cuando existe la posibilidad de que las personas raptadas tengan acceso a los medios de comunicación, el envío de mensajes de apoyo a través de estos canales puede ayudar a levantar su ánimo.

Una comunicación interna eficaz, por ejemplo, mediante sesiones informativas o mensajes en la intranet, puede ayudar al personal a sentirse incluido e informado de una manera que apoye y refuerce el esfuerzo de respuesta formal. A veces, el personal hace un llamamiento voluntario para recaudar fondos a fin de apoyar a la familia de la víctima.

► *Para obtener más información sobre comunicación y gestión de crisis, véase el capítulo 4.4.*

Rescate

En principio, nunca debe pagarse ningún rescate, ya que esto aumenta el riesgo general de que se repitan o imiten los incidentes contra la misma organización u otras en la misma zona. La realidad es que, en muchos casos, se paga algún rescate o concesión, aunque las organizaciones puedan negarlo.

Cuando el pago de un rescate sea una estrategia viable, debe realizarse previamente un análisis jurídico y político exhaustivo que ayude a identificar cualquier posible

implicación o riesgo jurídico o financiero (en todas las jurisdicciones pertinentes: el país donde se produjo el incidente, el país de origen de la organización y el país de origen de la persona raptada). Dicho esto, las consideraciones políticas pueden influir en la decisión del Gobierno de aplicar esta legislación. Las organizaciones también deben ser conscientes de que, incluso si tienen un seguro que cubra los pagos de rescates, estos se reembolsan más tarde, por lo que la organización tendrá que asegurarse de que dispone de los fondos necesarios para realizar el pago en primera instancia.

7.9.5 Negociaciones y comunicación

Comunicación y negociación con los agresores

Un elemento crítico en las negociaciones serán las exigencias planteadas por los agresores y la cuestión de quién, en la práctica, puede o debe satisfacerlas. Los objetivos y exigencias de los agresores pueden cambiar. Hay muchos ejemplos de situaciones en las que las demandas políticas se marchitaron, y dejaron solo una demanda de dinero. Lo contrario también puede ser cierto: una banda delictiva puede “vender” a una persona raptada a un grupo con motivaciones políticas si no hay rescate. Si los agresores piden concesiones políticas de las autoridades, esto escapará al control de la organización.

Orientaciones para el contacto inicial con los agresores

- Asegurarse de que se informa a un comunicador y de que dispone de un guión para el contacto, que deberá estar en los idiomas pertinentes.
- Grabar siempre la conversación. Esto puede requerir un equipo aparte (por ejemplo, un teléfono inteligente).
- Adoptar una actitud cooperativa.
- Pedir hablar con la víctima.
- Exigir pruebas de que la persona raptada está viva.
- Explicar las responsabilidades limitadas del comunicador (véase más abajo).
- Establecer un plazo de respuesta.
- Establecer un procedimiento para devolver las llamadas (por ejemplo, número de teléfono, palabra clave).
- Una vez establecido el contacto, preparar un guión revisado para las interacciones posteriores.

Entre las buenas prácticas para comunicarse con los agresores figuran las siguientes.

- Grabar y registrar todos los detalles y guiones relativos a las llamadas con los agresores. Estos deben ser confidenciales.
- Evaluar las motivaciones de los agresores y determinar si su comportamiento sigue un patrón coherente a lo largo del tiempo. ¿Son agresivos y amenazadores, racionales y objetivos, o muy emocionales? ¿Qué tono y estilo de comunicación serían más eficaces para distender la situación y establecer una buena relación?
- Solicitar pruebas de identidad y posesión para confirmar que la persona raptada sigue viva y que no ha sido transferida a otro grupo. Aunque una grabación en cinta o video puede ser útil, no es una prueba definitiva de vida, sobre todo teniendo en cuenta el aumento del uso de la IA (que puede duplicar voces y videos). La organización debe pedir un detalle concreto e íntimo a la familia o a un amigo cercano, algo que sea poco probable que los agresores sepan. Las preguntas de prueba de vida también pueden utilizarse si constan en los registros. Si no se aportan pruebas creíbles de identidad y vida, las organizaciones deben plantearse interrumpir las negociaciones.

Prueba de vida

Es fundamental demostrar que una persona raptada sigue viva, por lo que las organizaciones deben considerar la posibilidad de exigir preguntas de prueba de vida como parte de la información a los familiares más cercanos. Se debe tener cuidado con la forma en que se almacena y transmite esta información. Tan pronto como sea posible, deben obtenerse de la familia preguntas adicionales de prueba de vida para que la organización pueda seguir comprobando esto a medida que avanza el incidente. Estas preguntas deben ser únicas y fáciles de responder para la víctima.

- Referirse a la persona raptada por su nombre siempre que sea posible para humanizarla a los ojos del agresor y fomentar un buen trato, incluyendo la indicación de cualquier necesidad especial que pueda tener, por ejemplo, llevar gafas o tomar cierta medicación. Señalar otras preocupaciones, como el estado emocional de la familia y los hijos, y explorar si se puede encontrar la manera de organizar un intercambio de mensajes, puede ser beneficioso.

- Hacer hincapié en que el comunicador no tiene autoridad decisoria y necesita consultar con otras personas. Esto da tiempo para pensar y deja a la organización cierto margen de maniobra. Al mismo tiempo, no debe darse ninguna indicación de que un tercero (las autoridades o un experto en respuesta a crisis, por ejemplo) está asesorando a la organización. Es necesario estar preparado en caso de que los agresores exijan hablar con el responsable de la toma de decisiones en lugar de con el comunicador.
- Reiterar la política de no pagar rescate para demostrar que la organización sigue siendo coherente y que el paso del tiempo no debilita su determinación.
- Acordar horarios y métodos de comunicación, previendo imprevistos para problemas como la mala cobertura de telefonía móvil y las interrupciones de la red. Esto incluye establecer una palabra clave con los agresores para confirmar su identidad, con el objetivo de garantizar que la organización no se está comunicando con impostores.
- Mantener la comunicación. Las organizaciones no deben romper el contacto con los agresores a menos que exista la certeza de que la persona con la que están hablando no es el verdadero agresor o de que la víctima ya no está viva. Los agresores deben saber que la organización desea mantener la comunicación.
- No aceptar ir a un lugar determinado para un encuentro. Si la presión es muy fuerte, la organización debe insistir en garantías detalladas de seguridad. Existe el riesgo de nuevos raptos.

En algún momento, el comunicador de la organización puede hablar directamente con el miembro del personal raptado, y es importante tener claro qué tipo de información y mensajes deben transmitirse. El comunicador debe tratar de evitar proporcionar a la persona raptada cualquier información que los agresores no deban conocer, pero tranquilizarla asegurándole que se está haciendo todo lo posible para conseguir su liberación. A menudo, las víctimas se preocupan por cómo su familia está afrontando la situación, y el comunicador puede intentar aliviar esta preocupación.

El papel del comunicador

La designación de “comunicador” es deliberadamente distinta de la de “negociador”, ya que el equipo de gestión de crisis debe conservar el control de cualquier negociación. Designar a un comunicador en las fases iniciales también puede servir para crear un desfase temporal que permita la consulta y el análisis internos y externos antes de responder a las demandas de los agresores, y refuerza la idea de que el comunicador no está capacitado para tomar decisiones. Estas personas deben estar bien preparadas y recibir apoyo cuando se comuniquen directamente con los agresores. Suelen depender directamente de la autoridad decisoria superior del equipo de gestión de crisis. Dado que los raptos pueden durar mucho tiempo, puede ser necesario más de un comunicador.

El comunicador debe ser capaz de gestionar eficazmente altos niveles de estrés y, al mismo tiempo, ceñirse a una estrategia de negociación. Esta función puede ser desempeñada por alguien de la organización o por un experto externo. Lo ideal es que el comunicador sea un ciudadano nacional que domina la lengua y el dialecto de los agresores, comprende la cultura y tiene un sólido conocimiento de las dinámicas locales y las interacciones sociales. Deben ser fiables y capaces de trabajar bajo presión extrema, estar disponibles 24 horas al día, 7 días a la semana, y dispuestos a seguir las instrucciones del equipo de gestión de crisis. El comunicador debe estar bien formado, idealmente mediante ejercicios de simulación, ya que es probable que se enfrente a exigencias y presiones inesperadas por parte de los agresores.

Los comunicadores no son miembros del equipo de gestión de crisis ni participan en sus reuniones periódicas. De esta manera se evita que sepan demasiado y revelen accidentalmente información importante a los agresores. Si los agresores exigen hablar con alguien que no sea el comunicador designado, la organización debe asegurarse de que el comunicador preferido escuche discretamente la conversación.

Los comunicadores también pueden ser ajenos a la organización. Un intermediario puede surgir de la propia comunidad o puede ser buscado por la organización, propuesto o contactado por las autoridades o incluso propuesto por los agresores. No es raro que personas respetadas e influyentes a nivel local se involucren en la resolución de los raptos: los ancianos han desempeñado un papel decisivo en Somalia y Afganistán, por ejemplo.

En una situación de gran aceptación, en la que la comunidad conserva cierta influencia sobre los agresores, una persona de confianza de la comunidad local puede conseguir la liberación del secuestrado. No obstante, debe quedar claro que no pueden asumir compromisos en nombre de la organización sin su consentimiento previo. Frente a delincuentes bien organizados y más autónomos respecto a la comunidad, los líderes tradicionales pueden resultar ineficaces. La cuestión de la confianza es crucial. ¿En nombre de quién actúa el intermediario? ¿Tiene conexiones con los agresores? ¿Quién controla las negociaciones? También habrá que considerar la cuestión del pago. Es posible que las organizaciones tengan que plantearse el reembolso de algunos gastos de funcionamiento de los intermediarios locales, por ejemplo, para cubrir los viajes, el alojamiento, la comida y la comunicación. Sin embargo, este tipo de pagos puede no ser apropiado si la organización está tratando con una persona que, en términos locales, se sabe que ya es relativamente rica.

Las autoridades también pueden proponer un negociador oficial. El primer paso del negociador será probablemente establecer un clima de diálogo. Al principio, la atención se centrará probablemente en cuestiones menores sobre las que se pueda llegar a un acuerdo. Esto sentará las bases para debatir cuestiones más difíciles. Si las autoridades

proporcionan el negociador, existe el riesgo de que entren en juego consideraciones distintas de la preocupación por la seguridad y la liberación de la persona raptada. Otra posibilidad es que una entidad no gubernamental de prestigio proponga un enviado para intentar mediar en la liberación.

Liberación por la fuerza

No es raro que las fuerzas de seguridad traten de localizar a la víctima e intenten rescatarla o generen una situación de asedio para obligar a los agresores a rendirse. Se trata de una estrategia de alto riesgo para la víctima. Hay varias formas en que los escenarios de liberación forzada pueden salir mal, con resultados potencialmente fatales.

Desde el punto de vista de la organización, hay dos elementos especialmente importantes.

- ¿Quiénes llevan a cabo la acción están bajo un mando general claro? Si no es así, las acciones descoordinadas podrían poner en peligro la vida de la víctima.
- ¿Disponen las tropas de una descripción clara de la víctima para poder diferenciarla de los agresores, y han recibido instrucciones claras de disparar únicamente contra quienes les disparan? La víctima puede llevar el mismo tipo de ropa que los agresores y puede resultar herida en medio de la confusión de un asedio.

En realidad, la capacidad de la familia o de la organización para influir en los planes y en las acciones de las fuerzas de seguridad puede ser limitada. Las autoridades responderán como consideren apropiado, y es probable que la acción directa de cualquier autoridad se mantenga en secreto por razones de seguridad operacional.

Respuesta a situaciones de asedio repentino

Algunas situaciones de asedio pueden producirse repentinamente y escapar en gran medida al control de la organización. Un ejemplo es el asedio en 2015 al hotel Radisson Blu en Mali, donde había trabajadores humanitarios entre los rehenes. Mientras que las fuerzas armadas liderarán la respuesta a estas situaciones, las organizaciones pueden aspirar a realizar lo siguiente:

- Averiguar rápidamente si algún miembro del personal se ha visto afectado por el incidente.
- Aplicar medidas para proteger al personal restante, como su reubicación fuera de la zona.

- Movilizar a los equipos de gestión de crisis para que se ocupen del enlace familiar, gestionen las relaciones con los medios de comunicación y se coordinen con las autoridades.
- Estar preparado para prestar apoyo al personal afectado, incluida atención médica y psicológica, pago de seguros y repatriación.
- Realizar una revisión posterior a la acción para evaluar la eficacia de las medidas de protección previas al incidente y la respuesta de la organización, y compartir las conclusiones con el personal pertinente.

7.9.6 Gestión de las secuelas

Un rapto puede concluir con la liberación o la muerte de la víctima o, en algunos casos, quedar indefinidamente sin resolver. Las organizaciones humanitarias deben estar preparadas para gestionar una serie de resultados posibles.

Liberación

El retorno de las personas liberadas debe organizarse y gestionarse adecuadamente. Durante la liberación inicial, los supervivientes deben ser recibidos por alguien conocido, tal vez un colega cercano. Una compañera sería lo mejor cuando la víctima también es mujer. De manera prioritaria, se deberán atender sus necesidades físicas inmediatas y su comodidad.

Si fueron raptados miembros del personal de distintas organizaciones, es posible que la situación no se resuelva al mismo tiempo para todas las partes interesadas. En este caso, hay que tener mucho cuidado con las declaraciones públicas hasta que el incidente se resuelva para todas las partes.

Entre las consideraciones de buenas prácticas figuran las siguientes:

- Atender las necesidades del superviviente y sus familiares, tanto de forma inmediata como a largo plazo.
- Informar y comunicarse con las partes interesadas pertinentes, como los medios de comunicación, otras organizaciones y las autoridades, y gestionar sus interacciones y el acceso al superviviente.
- Informar al superviviente cuando esté preparado.
- Hacer un seguimiento de las personas y los grupos que apoyaron la respuesta.

- Proporcionar apoyo, como tiempo libre, a los miembros del equipo de respuesta.
- Desactivar la estructura de gestión de crisis, lo que incluye archivar registros y documentos, y elaborar un informe final del incidente que pueda compartirse con las partes interesadas internas y externas.

Los raptos pueden ser experiencias traumáticas. Los supervivientes pueden necesitar ayuda a largo plazo y acceso a apoyo profesional, especialmente durante las fases iniciales. La organización debe tomar todas las medidas posibles para reducir la carga sobre los supervivientes y permitir que se recuperen.

Es una buena práctica involucrar a los supervivientes en la toma de decisiones que los afectan directamente, siguiendo un enfoque centrado en el superviviente, pero hacerlo de forma progresiva y en consonancia con el asesoramiento médico y los propios deseos de la persona.

► *Para obtener más información, véase el capítulo 5.4 sobre cuidado del personal.*

Resolución infructuosa

Una resolución infructuosa puede implicar la confirmación de la muerte con la recuperación del cuerpo, la notificación de muerte sin la recuperación del cuerpo, o que el caso no se resuelva (por ejemplo, si no se obtiene una prueba de vida o no hay contacto por parte de los agresores).

Es aconsejable que las organizaciones estén preparadas para proporcionar apoyo a largo plazo a la familia y al resto del personal afectado por el incidente.

► *Para obtener más información sobre lo que puede incluir este tipo de apoyo, véase el capítulo 5.4 sobre el cuidado del personal.*

En caso de que se recupere el cuerpo de la víctima, es probable que sea necesario realizar una autopsia y una investigación, ya sea en el país donde se produjo el incidente o en otro lugar. También puede haber una investigación forense formal (o indagatoria) en el país de origen de la persona raptada. Las organizaciones deben estar dispuestas a cooperar con las autoridades y a compartir pruebas.

La familia también puede cuestionar la manera en que la organización gestionó el incidente, iniciar una investigación y emprender acciones legales contra ella. En este caso, los registros que la organización mantuvo mientras se desarrollaba el incidente serán una importante fuente de pruebas.

Si las cosas van mal en un rapto gestionado por las autoridades, la organización puede solicitar una investigación sobre cómo se llevó a cabo la operación y si lo que salió mal podría haberse evitado.

Revisiones posteriores a la acción

Las revisiones posteriores a la acción se centran en lo que ocurrió y por qué: las decisiones tomadas, por qué se tomaron y cuáles fueron los resultados. Una revisión posterior a la acción puede incluir elementos de rendición de cuentas, pero no debe ser un ejercicio de asignación de culpas. El objetivo de la revisión debe ser determinar qué medidas pueden adoptarse para evitar incidentes similares en el futuro y cómo gestionarlos en caso de que se produzcan.

Es importante que una organización sea transparente sobre sus conclusiones, especialmente con el personal afectado por el incidente. La revisión puede difundirse a través de una sesión en la que se invite a las principales partes interesadas, incluido el superviviente, a compartir las lecciones aprendidas. El hecho de que el Consejo Noruego para los Refugiados no compartiera abiertamente la información con el personal afectado fue considerado como una deficiencia durante el proceso judicial que siguió al rapto de miembros del personal en Dadaab (Kenia) en 2012.

► Para obtener más información sobre las revisiones posteriores a la acción, véase el capítulo 4.4.

Más información

Orientación y recursos

Buth, P. (2010). *Crisis management of critical incidents*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/crisis-management-of-critical-incidents).

Clamp, D. (2022). *Ten years on: learning from the Steve Dennis case*. Global Interagency Security Forum (www.gisf.ngo/blogs/ten-years-on-learning-from-the-steve-dennis-case/).

Davidson, S. (2013). *Managing the message. Communication and media management in a security crisis*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/managing-the-message).

Foro Europeo Interinstitucional para la Seguridad. (2017). *Abduction and kidnap risk management guide* (www.gisf.ngo/resource/abduction-and-kidnap-risk-management-guide/).

Hostage International. (s.f.a). *How we can help* (www.hostageinternational.org/how-we-can-help/).

Hostage US. (2022). *A life after captivity. Reintegration guide* (www.gisf.ngo/resource/a-life-after-captivity/).

Hostage US. (s.f.). *Hostage US guides* (<https://hostageus.org/resources/hostage-us-guides>).

Merkelbach, M. y Kemp, E. (2016). *Duty of care: a review of the Dennis v Norwegian Refugee Council ruling and its implications*. Foro Europeo Interinstitucional para la Seguridad (www.gisf.ngo/resource/review-of-the-dennis-v-norwegian-refugee-council-ruling/).

7.10 Amenazas relacionadas con el combate y los restos de material de guerra

En este capítulo se examinan las amenazas derivadas de los grandes conflictos armados o ataques terroristas, incluidos los bombardeos, los ataques con misiles y artillería, el fuego cruzado y de francotiradores, los artefactos explosivos improvisados (AEI) y las armas químicas, biológicas, radiológicas y nucleares (QBRN). También incluye un análisis de las tácticas de asedio y los peligros de los restos de material de guerra, como las minas terrestres y las municiones sin detonar. En este capítulo se presentan medidas de mitigación que las organizaciones deben tener en cuenta; sin embargo, en entornos extremos que impliquen combates importantes, las buenas prácticas recogidas en este volumen no serán suficientes y no pueden sustituir la consulta directa con expertos.

7.10.1 Cuestiones y consideraciones básicas

Las primeras cuestiones que hay que considerar en las zonas de combate activo son si la organización está dispuesta y tiene la capacidad necesaria para operar en estas condiciones y si los beneficios de hacerlo (es decir, la criticidad del programa) compensan los riesgos residuales. ¿Existen necesidades significativas de asistencia y/o protección, y posibilidades de satisfacerlas, que justifiquen la presencia de la organización? ¿Cuántos empleados y de qué tipo serán necesarios para desempeñar eficazmente esta función? ¿Qué recursos adicionales (formación, equipamiento, conocimientos especializados, seguros, etc.) serán necesarios para cumplir con el deber de cuidado?

La realidad es que, en la mayoría de las zonas de combate activo, la presencia humanitaria, en especial de las organizaciones internacionales, será mucho menor que en entornos de conflicto bajo o sin conflicto. Junto con otros civiles, los trabajadores humanitarios corren el riesgo de sufrir violencia colateral (y de ser el blanco directo de los agentes armados), y las medidas de gestión de riesgos de seguridad poco pueden hacer al respecto, salvo evitar los lugares de mayor riesgo y adoptar protocolos de refugio. Para la mayoría de las organizaciones, los costes y las capacidades necesarias para mitigar los riesgos para el personal en los conflictos armados activos más importantes son prohibitivos, y las que deciden operar suelen ejecutar sus programas en zonas más seguras y centrarse en las poblaciones desplazadas y en las necesidades conexas.

El riesgo para las organizaciones en contextos de combate no siempre se limita a la violencia colateral. En numerosas ocasiones se han registrado ataques directos contra agentes y operaciones humanitarias por parte de fuerzas militares nacionales y grupos armados no estatales. Las organizaciones que se sienten cómodas mitigando

los riesgos de violencia colateral normalmente no operan en lugares donde existe un alto riesgo de ataque directo y donde los esfuerzos de aceptación y acceso negociado son insuficientes para mitigar estos riesgos. En estas circunstancias, los principales proveedores de ayuda suelen ser personas y grupos de voluntarios locales e informales, que tienen aún menos capacidad para protegerse.¹¹⁷ Esto nos lleva a otra pregunta básica: si una organización apoya estos esfuerzos *ad hoc* mediante subvenciones u otros medios, ¿en qué medida está ayudando a mitigar los riesgos de sus socios?

Por último, aunque solo un pequeño grupo de organizaciones humanitarias deciden trabajar en las zonas de alto riesgo más extremas, la coordinación y la comunicación en estos contextos son más vitales que nunca. En estos contextos, las organizaciones deben esforzarse por buscar, apoyar y participar en los esfuerzos de acción colectiva dirigidos a solucionar el conflicto, conseguir el acceso humanitario y abogar por la protección y el paso seguro de la ayuda.

7.10.2 Medidas generales de mitigación para las zonas de combate

Las organizaciones que pretendan operar en zonas de combate activo, donde pueden enfrentarse a la violencia directa o colateral de ataques aéreos o munición pesada (bombardeos, artillería, minas terrestres o granadas, por ejemplo), deben incluir las siguientes consideraciones generales en su planificación de gestión de riesgos de seguridad.

Diagnóstico de riesgos y medidas de mitigación

Las amenazas relacionadas con el combate deben analizarse cuidadosamente en los diagnósticos de riesgos. Puede ser necesaria la colaboración de especialistas para determinar y aplicar medidas de mitigación (más abajo se ofrecen algunos ejemplos). Las estructuras de gestión de crisis y los planes de contingencia actualizados son especialmente importantes en zonas de conflicto activo. Es conveniente que las organizaciones dispongan de un sistema para controlar los niveles de seguridad y adaptar las medidas de gestión de riesgos de seguridad cuando se produce una transición de no conflicto a conflicto (o viceversa), que puede ocurrir lenta o repentinamente.¹¹⁸ Cuanto mayor es el riesgo, mayor es el deber de cuidado de la organización. Esto significa que se debe identificar al personal de mayor riesgo y proporcionarle el máximo nivel de apoyo de la gestión de riesgos de seguridad. Las organizaciones también deben considerar cómo apoyar a los socios que ejecutan programas en su nombre en estos contextos.

► Véase el capítulo 3.5 sobre alianzas.

117 Véase GISF y Humanitarian Outcomes (2024) *State of practice: the evolution of security risk management in the humanitarian space*(https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

118 Para consultar un análisis más completo, véase GISF y Humanitarian Outcomes (2024).

Selección del lugar

La ubicación del personal y de los bienes suele ser la primera consideración, y debe basarse en el diagnóstico de riesgos y el análisis del contexto. Las oficinas, los almacenes y las residencias deben situarse lejos de objetivos militares obvios o probables, como aeródromos, cuarteles, depósitos de combustible, edificios oficiales o puntos estratégicos como cruces de carreteras, terminales ferroviarias, centrales eléctricas y edificios de radio y televisión. Si la organización está trabajando en una zona susceptible de ser atacada, sus instalaciones deben trasladarse tan lejos como lo permitan las necesidades operacionales. Se pueden determinar con anticipación lugares de repliegue inicial y secundario en caso de que la violencia se intensifique en la zona o se extienda fuera de ella.

Selección y personal

Lo ideal es que el personal humanitario que trabaja en zonas afectadas por combates, en especial el que tenga responsabilidades en materia de seguridad, tenga experiencia previa en entornos comparables, así como formación especializada en los ámbitos pertinentes de gestión de riesgos de seguridad. Además, deben demostrar buen criterio, capacidad para trabajar bajo presión y resistencia mental. La selección, siempre un reto en la ayuda humanitaria, lo es aún más en las operaciones en medio de conflictos armados. Estos entornos requieren una mayor inversión tanto en la gestión de riesgos de seguridad como en el cuidado del personal en general, que incluye subsidios de descanso y recuperación y apoyo para la salud mental. Los servicios de salud mental pueden ofrecerse a todo el personal con carácter optativo, en lugar de bajo petición, con el objetivo de reducir el estigma y animar a más personal a recurrir a ellos.

► Véase el capítulo 5.4 para obtener más información sobre el cuidado del personal.

Formación

Es una buena práctica garantizar que el personal reciba formación en los procedimientos operativos estándar y sobre qué hacer en caso de que se produzca un incidente grave o aumente la violencia. La formación del personal dirigida a prepararlo para trabajar en zonas de combate activo debe incluir el conocimiento de la situación, los primeros auxilios, el uso de equipos de protección personal y otros equipos pertinentes, los procedimientos de evacuación y refugio, qué hacer en caso de fuego y estrés y primeros auxilios psicológicos.

► Para obtener más información sobre la formación, véase el capítulo 5.2.

► Para obtener más información sobre los primeros auxilios, véase el capítulo 5.5.

Desconflicción

Las iniciativas de desconflicción, como el Sistema de Notificación Humanitaria para la Solución de Conflictos (HNS4D, por sus siglas en inglés), proporcionan información sobre los movimientos y la ubicación de una organización a los agentes militares, con el objetivo de evitar ataques involuntarios y daños colaterales.

En algunos casos, es posible que uno o varios agentes armados no participen en la desconflicción o utilicen la información con fines malignos. Si la organización sabe que los combatientes están actuando de mala fe y pueden tener como objetivo a trabajadores humanitarios, puede ser aconsejable un enfoque de bajo perfil respecto a las ubicaciones y movimientos (incluida una sólida seguridad de la información).

En los casos en que la organización considere más seguro tener un perfil visible e informar a los agentes militares de su presencia, podrían adoptarse medidas adicionales como pintar el logotipo con colores brillantes en los techos y en las paredes de los edificios de la organización, marcar los vehículos, utilizar matrículas especiales o utilizar material término reflectante visible para drones, armas antitanque y otros sistemas de armamento que utilicen cámaras de imagen térmica. La bandera de una organización puede no ser visible desde lejos o en un día sin viento. No hay que suponer que todos los posibles actores que representan una amenaza conocen el nombre y el logotipo de la organización humanitaria, ni siquiera el propósito de dicha organización.

► *Para obtener más información sobre la desconflicción, véase el capítulo 2.1.*

Protección física del sitio

Mitigar los riesgos de un combate activo en las instalaciones de una organización (oficinas, residencias y lugares de trabajo) puede resultar costoso y requerir asesoramiento y apoyo especializados. Las amenazas pueden incluir ataques directos o daños colaterales de bombardeos, misiles o proyectiles, ataques con granadas desde fuera del perímetro, incursiones armadas y explosivos transportados en vehículos. En las zonas de combate, las instalaciones requerirán normalmente protección física o fortificación, y puede ser necesario situarlas cerca de refugios apropiados.

Medidas de fortificación

En una explosión pueden producirse lesiones por fragmentación primaria (trozos del cuerpo o de la carcasa del explosivo) o por fragmentación secundaria (restos del entorno propulsados por la onda expansiva, como cristales de ventanas). A pesar de su nombre, las barreras protectoras contra explosivos están diseñadas para detener la metralla y las balas, pero no necesariamente la onda expansiva de una bomba. Pueden ser de hormigón, acero, sacos de arena, bidones de aceite o cajas rellenas de tierra, y se utilizan para proteger las puertas y las ventanas de un edificio y la ruta de entrada a un refugio.

Las salas de amortiguación a lo largo de los muros de un edificio pueden proporcionar protección contra las explosiones. Las lesiones causadas por cristales pueden reducirse aplicando una película de seguridad o protectora contra explosiones, en el interior de la ventana. Tenga en cuenta que si esta película protectora se aplica a una ventana con doble acristalamiento resulta bastante ineficaz, al igual que si se aplica en la parte exterior de la ventana. Tampoco detiene la metralla ni las balas. Aunque la película protectora está diseñada para mantener el cristal unido, no está pensada para mantenerlo en su marco. En una explosión grande, todo el cristal de la ventana podría salir despedido hacia la habitación. Mantenerse alejado de las ventanas y tenerlas abiertas para evitar la presión hacia el interior son dos medidas sencillas de mitigación. Asegurar o retirar objetos que puedan convertirse en proyectiles peligrosos, como cubos de basura y macetas, también puede ayudar a mitigar los riesgos. Aunque reacondicionar los edificios para que resistan las ondas expansivas puede ser costoso y llevar mucho tiempo, reforzar zonas clave como los vestíbulos, donde es más probable que se produzca una explosión, puede ser una medida práctica.

Ciertas características de los edificios pueden proporcionar una protección adicional, aunque es probable que ningún edificio cumpla todos los requisitos. Lo ideal es que los edificios no se conecten directamente con zonas fuera del control de la organización, como las vías públicas. Las entradas principales no deben estar en línea directa de fuego desde un espacio fuera del control de la organización, y las oficinas deben estar separadas de almacenes o garajes con acceso para vehículos, y tener su propio perímetro de seguridad. Un perímetro exterior claramente definido con pocos puntos de acceso puede asegurar aún más la zona interior del recinto. Es preferible evitar los garajes subterráneos, porque presentan grandes riesgos en caso de coche bomba, pero, si se utilizan de todas maneras, el acceso debe limitarse al personal. Las barreras de acceso de vehículos pueden proporcionar una protección adicional. Los aparcamientos y las zonas de descenso de visitantes deben situarse fuera del perímetro exterior.

Medidas de control perimetral

Las medidas de control de velocidad en las carreteras de acceso a los puntos de entrada pueden ayudar a evitar que los vehículos aceleren y embistan contra el edificio. Las medidas pueden incluir equipos especializados o, alternativamente, barriles llenos de grava o grandes macetas de hormigón con flores o arbustos, ligadas entre sí de forma segura. Si el perímetro exterior está cerca del edificio, se pueden instalar bloques o macetas de hormigón como medidas adicionales de separación para minimizar el impacto de una explosión.

Cuanto más lejos del edificio se produzca una explosión, menor será su impacto. Aunque lo mejor sería que entre el edificio y la explosión hubiera una distancia de 30 metros, esto no suele ser factible. Es aconsejable que las entradas de personal y visitantes, así como las zonas de aparcamiento, estén separadas. Los vehículos del personal, incluso dentro de perímetros seguros, deben ser revisados para detectar si han sido cargados secretamente con explosivos que puedan detonarse por control remoto o

si un terrorista suicida se ha apropiado de un vehículo. Los vehículos y los visitantes autorizados a entrar en el edificio deben ser registrados en el perímetro exterior.

Se recomienda dejar un espacio sin obstáculos de al menos 10 metros entre el perímetro exterior y el interior. Los corredores de circulación dentro de este espacio pueden emplearse para controlar el tráfico, de modo que cualquier movimiento no autorizado fuera de estos corredores provoque una respuesta inmediata por parte del personal de seguridad. Dentro del edificio, lo ideal es que los espacios accesibles a los visitantes estén separados de las zonas reservadas al personal. Se recomienda aplicar medidas de control de los visitantes (y posiblemente también del personal) en la entrada, incluido el registro de bolsos. Lo ideal es que la entrada o el vestíbulo sean lo suficientemente espaciosos para realizar estos controles y que no se conecten directamente con otras partes del edificio, en caso de que se produzca una explosión en esta zona. Los activos importantes, como los sistemas informáticos centrales, deben ubicarse en un lugar más oculto dentro de las zonas restringidas del edificio y no deben ser fácilmente identificables.

Medidas de refugio

Aunque la fortificación física puede reducir los daños de los cuasiaccidentes, como los efectos de las explosiones y la metralla, es menos eficaz contra los impactos directos: ningún refugio, ni siquiera un búnker de hormigón, puede ofrecer una protección completa contra todas las armas. La mejor protección suele consistir en una acción inmediata, como refugiarse o, si no hay aviso previo, tirarse al suelo para reducir la exposición al impacto de fragmentos. Los refugios subterráneos, como sótanos o aparcamientos, suelen ser las opciones más seguras, siendo las habitaciones reforzadas en la planta baja la siguiente mejor alternativa. Los refugios deben ser lo suficientemente grandes como para que quepan todas las personas del edificio, junto con el equipo esencial, y estar lo suficientemente cerca como para que se pueda llegar a ellos rápidamente. Las organizaciones deben fijar un plazo para llegar al refugio, alrededor de uno o dos minutos. El personal que no pueda llegar a un refugio en ese tiempo desde su lugar habitual de trabajo necesitará su propio refugio en un lugar más cerca. Si las autoridades han identificado o construido refugios públicos, el personal debe saber dónde están.

Las trincheras de refugio y los hoyos de protección pueden servir para protegerse de los proyectiles de mortero y los bombardeos de aviones o helicópteros que vuelan bajo. Deben ser profundos (2 metros), estrechos y lo suficientemente grandes como para cuatro personas. Una buena construcción es una zanja pequeña en forma de L, con dos puntos de entrada y salida. La parte superior puede protegerse con troncos y dos capas de sacos de arena. También necesitan mantenimiento: la lluvia puede hacer que las entradas se desmoronen y que se inunde la zanja. El personal debe tener cuidado con las serpientes u otros animales peligrosos, que pueden hacer nidos en las trincheras u hoyos de protección.

- *Para más información sobre las buenas prácticas en materia de seguridad del sitio, véase el capítulo 7.2.*

Equipos de protección personal

En las zonas de combate activo suele ser necesario contar con equipos de protección personal, sin embargo, hay que tener en cuenta que estos equipos no son una solución en sí misma, sino más bien un elemento del plan seguridad.

La elección del equipo de protección personal depende de las amenazas específicas de la zona, dado que debe equilibrarse la protección con la movilidad y la comodidad. Aunque los niveles más altos ofrecen más protección, también suelen ser más pesados y restrictivos, y los usuarios necesitarán cierta instrucción inicial. Hay que procurar que el equipo de protección personal proporcionado se ajuste bien y lo pueda usar todo el personal que lo necesite; en ocasiones, el equipo no está diseñado para mujeres y la talla puede ser limitada. Los chalecos y los cascos deben identificar a la organización humanitaria para distinguir al usuario de los combatientes. En la mayoría de las circunstancias, no se debe usar el equipo de protección personal sin estos elementos visibles de identificación (a menos que la organización sea un objetivo particular), para evitar que quien lo usa sea confundido con un actor militar.

Existen varios tipos de chalecos antibalas con distintos niveles de seguridad. Los niveles de seguridad se clasifican generalmente según las normas del Instituto Nacional de Justicia de Estados Unidos (NIJ, por sus siglas en inglés).¹¹⁹ En la norma NIJ 0101.06 hay cinco niveles de seguridad, del IIA (el más bajo) al IV (el más alto). Los chalecos más utilizados por los trabajadores humanitarios que operan en condiciones de combate son los chalecos antibalas flexibles de nivel IIIA, que protegen contra la mayoría de los proyectiles de armas cortas, o los chalecos portaplacas de nivel III con inserciones de blindaje duro (placas frontales y laterales), que protegen de los proyectiles de fusil. Los cascos balísticos (nivel III) protegen de las lesiones en la cabeza provocadas por las balas y los fragmentos.

Los vehículos blindados pueden proporcionar una buena protección contra algunas amenazas relacionadas con el combate. Los vehículos blindados civiles se construyen con materiales reforzados como acero endurecido, fibras sintéticas y gruesos cristales antibalas. Los componentes específicos utilizados dependen del nivel de protección deseado. Pueden ofrecer protección frente a agresiones y ataques, balas y disparos. A menos que se diseñen específicamente como vehículos a prueba de minas, no proporcionan una protección adecuada contra la explosión y la metralla de una mina antitanque o una bomba bien fabricada al borde de la carretera. Los vehículos blindados son mucho más pesados que los vehículos normales y muy caros. Dado el peso adicional y, en consecuencia, la mayor distancia de frenado que requieren, se necesita un conductor especialmente entrenado. Puede resultar difícil para los no expertos distinguir un vehículo blindado de uno estándar. Sin embargo, cuando se sabe que una organización utiliza vehículos blindados, esto puede afectar la forma en que la población

119 Véase <https://nij.ojp.gov/library/publications/understanding-nij-010106-armor-protection-levels>.

local y los agentes armados perciben la organización; el uso debe estar en consonancia con los enfoques de seguridad de la organización en el contexto en cuestión.

► *Para obtener más información sobre los enfoques de seguridad, véase el capítulo 4.2.*

Formación en conducción defensiva para acciones evasivas

Existen cursos para formar a los conductores sobre cómo reaccionar si un vehículo se ve sometido a un fuego cercano. La decisión de alejarse a toda velocidad o detenerse dependerá de la procedencia del fuego y del objetivo. Por lo general, hay más protección dentro del vehículo que fuera, y alejarse de la zona mientras se permanece lo más agachado posible suele ser la mejor opción, pero cada situación será diferente.

Si se ve atrapado en un fuego cruzado mientras se encuentra fuera a pie, el personal debe buscar inmediatamente refugio detrás de un objeto sólido, manteniéndose agachado y desplazándose a un lugar seguro en cuclillas en caso de fuego con armas de bajo calibre. Si se ve atrapado en un bombardeo de artillería, debe tirarse al suelo y permanecer boca abajo.

7.10.3 Armas y tácticas de combate

Las armas utilizadas en los grandes conflictos varían ampliamente en cuanto a su escala, gravedad y letalidad, y la posibilidad de exposición a una o más de ellas en una zona de operaciones puede estar más allá del umbral de riesgo de muchas organizaciones humanitarias. Las siguientes secciones de este capítulo describen cada una de ellas con más detalle, junto con posibles medidas de mitigación. En general, para las organizaciones que trabajan en zonas de conflicto activo, algunas áreas importantes que considerar y en las que invertir son las siguientes:

- concientización y capacidad de alerta temprana;
- acceso inmediato a un refugio o cobertura adecuados;
- planes de evacuación y protocolos de refugio;
- disponibilidad de equipo de protección personal, y
- formación y simulacros para amenazas específicos, incluida la formación en primeros auxilios en caso de traumas.

En la tabla 25 se describen las categorías y las características de las armas de combate típicas utilizadas en los grandes conflictos.

Tabla 25 Descripción de las armas de combate

Arma	Descripción
Bombardeo aéreo	Bombas lanzadas desde aviones en vuelo (ataques aéreos). Incluye las tradicionales bombas lanzadas desde el aire y las modernas bombas planeadoras, que pueden recorrer una distancia máxima de 60 kilómetros hasta el objetivo.
Misiles o cohetes	Arma explosiva autopropulsada que puede ser guiada hacia un objetivo preciso (misil guiado) o simplemente orientada en una trayectoria (cohete).
Drones (vehículos aéreos no tripulados)	Vehículos aéreos no tripulados que pueden transportar cargas explosivas. También se utilizan para la vigilancia y la selección de objetivos.
Proyectiles o morteros (artillería)	Disparo de proyectiles de artillería con una trayectoria en arco elevado para alcanzar objetivos a distancia. A veces se denominan <i>proyectiles de artillería</i> o <i>morteros</i> .
Lanzacohetes portátil	Granadas antitanque disparadas desde el hombro capaces de destruir vehículos blindados y posiciones fortificadas a corta distancia.
Artefactos explosivos improvisados (AEI)	Arma explosiva que puede colocarse en un lugar, llevarse encima o transportarse en un vehículo. Puede activarse a distancia o por contacto.
Armas de bajo calibre	Armas de fuego portátiles, como, rifles y pistolas.
Minas	Artefactos explosivos ocultos diseñados para ser detonados por la presencia, la proximidad o el contacto de una persona o un vehículo.
Municiones sin explotar (MUSE)	Bombas, proyectiles de artillería, granadas u otras municiones que se han disparado, soltado o lanzado pero no han detonado.
Fósforo blanco	Sustancia tóxica utilizada como cortina de humo que puede ser lanzada por proyectiles de artillería, cohetes y granadas.
Armas químicas, biológicas, radiológicas y nucleares (QBRN)	Bombas y otras armas o tácticas que utilizan sustancias biológicas o químicas, radiación o explosiones nucleares para causar la muerte y/o peligros tóxicos.

Bombardeo desde plataformas aéreas

Al tratar la amenaza de violencia colateral de los ataques aéreos, es importante recordar que los lugares de alto riesgo son aquellos situados en las proximidades de los objetivos

de alto valor, donde la destrucción sería militarmente ventajosa. Los objetivos habituales de los ataques aéreos son las instalaciones militares, los aeródromos, las centrales eléctricas, las torres de comunicación, los puentes, los cruces de carreteras clave, los sistemas de transporte e incluso, cada vez más, los hospitales. Las armas utilizadas para los bombardeos aéreos incluyen misiles y drones.

Los misiles varían en alcance, precisión y velocidad, lo que puede repercutir en la eficacia de los sistemas de alerta y en el tiempo disponible para refugiarse. Los misiles disponen de sistemas internos de guiado que les permiten dirigirse hacia un objetivo específico tras su lanzamiento.

- Los misiles balísticos viajan a velocidades hipersónicas durante la mayor parte de su vuelo, y los misiles balísticos intercontinentales alcanzan sus objetivos en unos 30 minutos. Su precisión ha mejorado notablemente, y algunos sistemas modernos alcanzan una precisión de decenas de metros. Pueden transportar cargas explosivas muy grandes, a menudo medidas en miles de kilogramos, lo que les confiere una inmensa capacidad destructiva.
- Los misiles de crucero suelen volar más bajo y más despacio, con tiempos de aproximación medidos en horas para misiones de largo alcance. Aunque sus ojivas suelen ser más pequeñas que las de los misiles balísticos, los misiles de crucero modernos pueden transportar cargas explosivas de varios cientos de kilogramos.
- Los misiles balísticos lanzados desde el aire, como el Kinzhal ruso, pueden alcanzar velocidades hipersónicas como los misiles balísticos, lo que se traduce en tiempos de aproximación cortos, pero pueden maniobrar durante el vuelo. Suelen transportar cargas mayores que los misiles de crucero, pero menores que los misiles balísticos tradicionales.

Los drones, o vehículos aéreos no tripulados, son una alternativa de bajo coste a los misiles y a las bombas lanzadas desde el aire. El dron Shahed 136, de tipo kamikaze, lleva una carga explosiva de 40 kilogramos y puede volar hasta 2400 kilómetros a unos 100 kilómetros por hora. Está diseñado para una misión unidireccional, ya que se estrella contra su objetivo, y funciona efectivamente como un misil barato. Los drones de inteligencia o de recopilación de información (o drones de vigilancia) son relativamente pequeños, navegados, que pueden llevar o no cargas explosivas. Algunos drones de vigilancia pueden utilizarse para coordinar ataques con misiles balísticos. La presencia de estos drones puede servir como una indicación de alerta.

Los ataques directos contra los agentes humanitarios, aunque posibles, son menos probables que el riesgo de daños colaterales. Las armas utilizadas tendrán diferentes tiempos de aproximación y algunas pueden ser más fáciles de interceptar que otras. Ucrania desarrolló en 2022 un sistema de notificación nacional basado en una aplicación, que proporciona alertas de ataques aéreos con información sobre el tipo de arma que

se utilizará. Pueden establecerse protocolos organizativos que indiquen al personal que se refugie bajo tierra o en una habitación interior, en función del tipo de ataque.

Bombardeo de artillería desde plataformas terrestres

El bombardeo de artillería desde plataformas terrestres suele dirigirse contra las posiciones (como búnkeres y trincheras) y los movimientos de las fuerzas adversarias. A menudo se utiliza para destruir las líneas de suministro, los depósitos y los centros logísticos. Se pueden hacer distinciones básicas entre disparos aleatorios o de saturación, disparos de predicción y disparos de observación.

- Los disparos aleatorios o de saturación son muy imprecisos. Pueden ser el resultado del tipo de arma utilizada, como lanzacohetes múltiples, que saturan una zona con proyectiles, o de una táctica deliberada, como una descarga de artillería o un bombardeo de saturación.
- Los disparos de predicción son menos aleatorios. La puntería se basa en cálculos cartográficos, sin capacidad para ajustarse a un objetivo concreto.
- Los disparos de artillería o los ataques aéreos de observación implican que drones o personas en tierra vigilan dónde caen los proyectiles, cohetes o bombas, y transmiten instrucciones para guiar la puntería de los equipos de disparo. Este tipo de disparos puede ser muy preciso y permite seguir o cambiar de objetivo.

Las armas antitanque y los lanzacohetes portátiles son armas disparadas desde el hombro que lanzan cohetes con ojivas explosivas. Se suelen utilizar contra vehículos blindados, fortificaciones y personal enemigo en línea de visión directa. Son portátiles, versátiles y fáciles de usar. Evitarlos, es decir, permanecer fuera de su radio de alcance de entre 200 y 500 metros, es la mejor medida de mitigación. Si se encuentra dentro de la zona de alcance, minimizar el tiempo que pasa en zonas abiertas y evitar patrones de movimiento predecibles puede reducir el riesgo de ser blanco de un ataque, y los vehículos blindados y los refugios fortificados pueden ser medidas de mitigación fundamentales.

Fuego cruzado y francotiradores

El fuego cruzado es un riesgo en la proximidad de cualquier fuego de armas de bajo calibre o de artillería. Aunque la mayoría de los disparos de armas de bajo calibre suelen tener un alcance efectivo de solo 300 metros, algunas ametralladoras superan los 1800 metros y las balas pueden viajar hasta 6 kilómetros. Los disparos de francotiradores son selectivos, y algunos de los rifles que utilizan pueden alcanzar un objetivo a larga distancia (más de 1 kilómetro).

La mejor defensa contra el fuego cruzado y los francotiradores es reducir la exposición manteniendo al personal fuera de alcance (lo que puede ser posible solo cuando las líneas de batalla son relativamente estables) y alejado de las zonas donde se producen ataques con armas de bajo calibre o actúan francotiradores. En caso de fuego cruzado

repentino, cuando el personal no es el objetivo, debe echarse al suelo inmediatamente e intentar trasladarse a un lugar más seguro. Cuando estén en el interior de un edificio, deben mantenerse alejados de las ventanas y las puertas e intentar que haya al menos dos paredes entre ellos y las balas. Esto también aumentará la protección contra el rebote de las balas.

Estas precauciones también se aplican en el caso de fuego de celebración, como puede ocurrir en fiestas o manifestaciones, en las que las lesiones y las muertes por caída de proyectiles constituyen un riesgo grave.

Prevención y respuesta ante tiradores activos

Los incidentes con tiradores activos son una amenaza crítica en determinados contextos, con el potencial de causar numerosas víctimas y un impacto psicológico significativo en los supervivientes. Las organizaciones humanitarias no son inmunes a este tipo de amenazas, que pueden producirse con poca o ninguna advertencia previa. La mitigación de riesgos suele requerir múltiples niveles de seguridad, cada uno de ellos concebido para ralentizar o bloquear el acceso del tirador a los edificios o recintos. La capa más interna suele ser una sala reforzada.

Comprender los indicadores de violencia potencial, aplicar medidas de mitigación y disponer de un plan de respuesta bien preparado puede reducir significativamente los riesgos asociados a este tipo de incidentes. La formación puede incluir orientaciones sobre la estrategia *correr*, *esconderse*, *contar*.

- **Correr.** Si hay un camino seguro, intente evacuar la zona. Animar a los demás a que se vayan con usted, pero no deje que su indecisión lo detenga. Deje sus pertenencias y mantenga las manos visibles para los actores armados de respuesta inicial.
- **Esconderse.** Si la evacuación no es posible, busque un lugar donde esconderse. Debe ser un lugar fuera de la vista del tirador, que brinde protección si se producen disparos en su dirección y, si es posible, que no restrinja las vías de salida. Se deben cerrar las puertas con llave o bloquearlas, apagar las luces y silenciar los teléfonos. Si es probable que se produzca un incidente con un tirador activo, debe considerarse la construcción de una habitación segura.
- **Contar.** Una vez que sea seguro hacerlo, se debe llamar a los servicios de emergencia (u otros contactos de emergencia según el protocolo de la organización) y proporcionarles toda la información posible. Esto incluye la ubicación del tirador, una descripción del tirador y sus armas, y el número de personas en el lugar.

Minas, artefactos explosivos improvisados y municiones sin detonar

Minas

Los grupos armados colocan minas para defender sus posiciones, obstaculizar los movimientos del enemigo, impedirle el acceso a determinadas rutas y/o canalizarlo hacia una ruta determinada. También pueden colocarse alrededor de posibles objetivos, como torres de tendido eléctrico (torres de transmisión), centrales de agua y electricidad y empalmes ferroviarios, para protegerlos de sabotajes y ataques. Se han utilizado minas en zonas civiles y agrícolas para causar temor y desplazamientos generalizados. Una vez colocadas, las minas pueden moverse por grandes distancias como consecuencia de las inundaciones o los corrimientos de tierra.

En general, existen dos categorías: las minas antitanque y las minas antipersonales.

- **Las minas antitanque** son grandes y tienen una potencia explosiva considerable. Normalmente requieren un gran peso o movimiento para activarse, pero esto puede no ser así si son viejas e inestables, y pueden causar la destrucción casi total de un vehículo no blindado (incluidos la mayoría de los vehículos blindados civiles, que solo están protegidos contra las armas de bajo calibre).
- **Las minas antipersonales** son más pequeñas. Algunas están diseñadas para causar lesiones al arrancar una mano o un pie. Otras pueden causar daños mucho más graves, incluso mortales. Los dispositivos de fragmentación directa están diseñados para dispersar fragmentos de proyectiles que matan o hieren hasta una distancia de 500 metros en una dirección determinada.

Ejemplo: minas múltiples

En 1995 un vehículo de una ONG chocó contra una mina antitanque en una carretera de África Central. La explosión mató a dos pasajeros e hirió a otros tres. Durante la noche, se colocaron nuevas minas antipersonales alrededor de los restos. Al día siguiente, una lugareña que había venido a mirar pisó una de esas minas y perdió la pierna.

Los cursos de concienciación sobre minas para el personal son un elemento esencial de la gestión de riesgos de seguridad en las zonas en las que las minas se utilizan activamente o quedan restos de conflictos anteriores. Esto incluye:

- Mantenerse alerta y saber a qué prestar atención.
- Identificar, marcar y reportar minas y municiones sin detonar.
- Técnicas de evasión.
- Qué hacer en una zona minada en vehículo o a pie.
- Respuesta de emergencia (en caso de detonación y lesiones).

Organizaciones internacionales especializadas en desminado humanitario, como HALO Trust y Mines Advisory Group, proporcionan formación e información. En el propio país, las principales fuentes de información general y específica de la localidad incluyen:

- La organización nacional de lucha contra las minas o las autoridades y fuerzas de seguridad locales.
- Organizaciones de desminado y un centro de acción contra las minas de la ONU.
- Observadores militares o fuerzas de mantenimiento de la paz de la ONU.
- Hospitales y puestos de salud que se ocupan de las víctimas de las minas.
- Población local.

Los conocimientos locales son especialmente importantes. Al trasladarse a una zona nueva en la que hay combates activos o hubo en el pasado, las organizaciones pueden informarse sobre el historial de los combates en la zona; los accidentes (¿han sido alcanzados vehículos, personas o animales por minas y, en caso afirmativo, cuándo y dónde?); a dónde va la población local y qué zonas evita; qué carreteras o tramos de carretera se han utilizado y en qué medida; y cómo se utilizan las carreteras (¿la población local camina, utiliza bicicletas o vehículos?). Las minas antitanque pueden no haber sido detonadas y seguirán siendo un peligro.

La población local suele crear sus propias señales de advertencia para marcar los campos de minas, pero pueden ser difíciles de identificar para los extranjeros y pueden ser ambiguas o poco claras. Las señales pueden no ser más que un pequeño montón de guijarros o dos ramas cruzadas al comienzo de un sendero. Se puede preguntar a la población local qué señales utilizan y si tienen un sistema común: si cada uno lo hace a su manera, no hay una señal común. Las operaciones de desminado marcan los campos identificados de diferentes maneras en los distintos países, pero normalmente las señales son suficientemente claras. El color rojo se utiliza normalmente en dichas marcas. Es importante recordar que las señales pueden haberse caído u oscurecido.

Artefactos explosivos improvisados

Los artefactos explosivos improvisados pueden utilizarse contra vehículos, instalaciones o personal militar, así como contra civiles. También se usan con frecuencia para denegar el acceso a zonas o a rutas. Pueden detonarse por control remoto o por la víctima o pueden tener un temporizador. Los dispositivos que son activados por la víctima, como cuando pisa una placa de presión o tira de un cable, requieren restricciones de movimiento cautelosas. Los dispositivos con temporizador suelen tener como objetivo un patrón de actividad, o su detonación se retrasa para permitir que el agresor huya. Los dispositivos de detonación por control remoto o por mando pueden ser más exactos. A menudo, los artefactos explosivos improvisados son colocados por una fuerza en retirada para complicar la reocupación de una zona. Cuando se utilizan como bombas trampa, se ocultan o camuflan: una puerta o una ventana de una casa pueden ser bombas trampa, al igual que un pozo, un cadáver o un objeto doméstico de aspecto inocente, como un juguete. Una táctica habitual consiste en atacar un objetivo y, poco después, atacar el mismo lugar para herir a los socorristas y a las personas que llegan para ayudar a los heridos. Es importante comprender cómo se utilizan los artefactos explosivos improvisados para que la organización pueda ajustar sus procedimientos operativos estándar en consecuencia.

Municiones sin detonar

Las municiones sin detonar son materiales que debían explotar al impactar pero no lo hicieron. Los proyectiles de artillería y mortero, e incluso la munición de armas de bajo calibre, pueden seguir siendo explosivos y volverse cada vez más inestables con el tiempo. Las bombas y los proyectiles pueden haberse enterrado profundamente en el suelo, lo que representa un peligro continuo, por ejemplo, para agricultores y constructores. Los vehículos militares o militarizados destruidos o abandonados y los edificios utilizados por grupos armados pueden contener municiones sin detonar, así como combustibles volátiles y residuos químicos. Las municiones sin detonar pueden suponer una amenaza mucho mayor que las minas terrestres porque su dispersión puede ser más aleatoria e impredecible y porque es probable que las propias municiones sean inestables. Un riesgo particular son las municiones en racimo lanzadas con artillería o desde un avión. En el aire, los contenedores se rompen y luego distribuyen una multitud de pequeñas bombas que pueden saturar toda una zona.

Guía esencial para el personal: minas y municiones sin detonar

Al enfrentarse a minas y municiones sin detonar, el consejo para el personal debe ser: no tocar, no acercarse, marcar si es posible, reportar.

Las municiones sin detonar suelen ser visibles, aunque pueden estar enterradas parcial o incluso totalmente. Hay que suponer que son inestables y no tocarlas. El personal debe marcar su posición e informar a las autoridades.

Cualquier objeto lo suficientemente grande puede convertirse en una trampa para transportar explosivos. Por lo general, el objeto trampa es visible, pero no el explosivo vinculado a él. Todo lo que se encuentre en una zona sin neutralizar puede ser una bomba trampa, por lo que el personal en la zona no debe entrar en edificios vacíos o ruinas, y no debe recoger nada ni abrir persianas o puertas.

Por lo general, las minas no son visibles. En una zona en la que se hayan utilizado minas, el personal no debe viajar por ninguna carretera que no haya sido confirmada como despejada. Si se ve una mina, hay que marcar el lugar e informar a las autoridades.

Las personas sin formación nunca deben manipular minas o municiones sin detonar. Un curso estándar de HEAT no cuenta como formación en este sentido.

Amenazas químicas, biológicas, radiológicas y nucleares

Hasta la fecha, las organizaciones humanitarias han tenido poca experiencia directa con las amenazas químicas, biológicas, radiológicas y nucleares (QBRN). En realidad, ninguna organización humanitaria está actualmente equipada para proteger a su personal, y mucho menos a la población civil local, en caso de que se produzca un incidente catastrófico con armas QBRN. La mayoría de las organizaciones que han tomado la decisión de operar en zonas de conflicto grave han decidido que la probabilidad de que ocurra es lo suficientemente baja como para aceptar el riesgo. Sin embargo, el riesgo nunca está ausente en ningún escenario de conflicto importante, por lo que es importante evaluar y analizar el riesgo, y considerar las medidas de mitigación.

Las armas químicas se desplegaron varias veces en la guerra civil siria (a partir de 2012) y en Ucrania (a partir de 2022), donde el riesgo adicional de incidentes nucleares deliberados o accidentales se debatió con frecuencia entre las organizaciones humanitarias que operaban allí. Los riesgos pueden ser los siguientes:

- Accidentes industriales, como un incendio o una explosión en una planta química o de almacenamiento, un accidente en una central nuclear o una fuga de una instalación de contención biológica. Estos incidentes pueden liberar sustancias tóxicas en el medioambiente, lo que supone riesgos inmediatos y a largo plazo para la salud de la población y de los equipos de respuesta.
- Accidentes durante el transporte de agentes QBRN con fines industriales o militares.
- Peligros como terremotos o tsunamis pueden dañar plantas industriales o instalaciones militares de almacenamiento, lo que puede provocar la liberación de materiales QBRN.

- Daños colaterales en plantas industriales, hospitales (departamentos de radiología) o instalaciones de investigación, fabricación y militares como consecuencia de un conflicto.
- Ataques directos de fuerzas armadas que liberan agentes químicos o biológicos para causar un gran número de víctimas masivas u otros grupos que utilizan materiales QBRN para crear armas como las *bombas sucias* (dispositivos de dispersión radiactiva).

Las personas pueden estar expuestas a peligros QBRN de diversas maneras, como la inhalación, el contacto físico (entre personas o con objetos) y el consumo de alimentos o agua contaminados.

A efectos de la mitigación de riesgos, las cuestiones clave que considerar incluyen determinar quién es el personal de mayor riesgo (como el personal médico), si existen procedimientos operativos estándar respaldados por expertos que puedan adoptarse (como el uso y el tipo de equipos de protección personal), los planes de contingencia que pueden ponerse en marcha (como la retirada, la evacuación y el apoyo médico de emergencia) y si es aconsejable una formación especializada para el personal de mayor riesgo (como capacitación sobre la manera de reducir la exposición en caso de sospecha de contaminación). Cualquier medida de gestión de riesgos de seguridad debe estar respaldada por especialistas.

Fósforo blanco

El fósforo blanco se utiliza en una zona de combate para crear una cortina de humo. Se forma una nube muy rápidamente que no solo obstaculiza el contacto visual, sino que también altera la radiación infrarroja, por lo que interfiere con los sistemas de óptica infrarroja y de rastreo de armas, como los que utilizan las armas guiadas, entre ellas, los misiles antitanque. Puede ser lanzado por pequeñas granadas de humo, cañones de tanques y morteros u otro tipo de artillería. En el momento de la explosión, las partículas ardientes se proyectan hacia el exterior, seguidas de chorros de humo blanco, que luego se fusionan en una nube muy blanca.

Aunque su uso declarado no sea el de arma química, el fósforo blanco es, no obstante, un producto químico tóxico que, cuando se utiliza en zonas pobladas, tiene efectos nocivos sobre las personas. Las partículas ardientes se adhieren a la piel y pueden producir quemaduras graves. Las partículas siguen ardiendo hasta que se consumen por completo o hasta que se quedan sin oxígeno. Además, el fósforo puede ser absorbido por el organismo a través de las zonas quemadas y causar daños en el hígado, los riñones y el corazón o incluso disfunción orgánica. Las partículas de fósforo también pueden penetrar en el organismo por vía oral. La inhalación del humo es peligrosa e irritará los ojos, la nariz y las vías respiratorias, pero no supone la misma amenaza letal que las quemaduras y la ingestión.

Más información

Investigación general

Global Interagency Security Forum y Humanitarian Outcomes. (2024). *State of practice: the evolution of security risk management in the humanitarian space* (https://humanitarianoutcomes.org/security_risk_mgmt_humanitarian_space_2024).

Mitigación de riesgos en conflictos armados

Comité Internacional de la Cruz Roja. (2006). *Staying alive: safety and security guidelines for humanitarian volunteers in conflict areas* (<https://reliefweb.int/report/world/staying-alive-safety-and-security-guidelines-humanitarian-volunteers-conflict-areas>).

Comité Internacional de la Cruz Roja. (2021). *SAFE: security and safety manual for humanitarian personnel* (www.icrc.org/en/publication/4425-safe-manuel-de-securite-pour-les-humanitaires).

Torelli, C. (2024). *Explosive violence monitor 2023*. Action on Armed Violence (<https://aoav.org.uk/2024/explosive-violence-monitor-2023/>).

Wilson, O. (2017). *Counter-terrorism: IED, bomb, and active shooter procedures*. Risks Incorporated (<https://gisf.ngo/resource/risks-counter-terrorism-procedures/>).

Amenazas químicas, biológicas, radiológicas y nucleares

Comité Internacional de la Cruz Roja. (2014). *Chemical, biological, radiological and nuclear response: introductory guidance. For training purposes only* (www.icrc.org/en/doc/assets/files/publications/icrc-002-4175.pdf).

Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja. (2023). *Riesgos químicos, biológicos, radiológicos y nucleares (QBRN)* (<https://epidemics.ifrc.org/manager/disaster/chemical-biological-radiological-and-nuclear-cbrn-hazards>).

Iniciativa de Centros de Excelencia Químicos, Biológicos, Radiológicos y Nucleares. (s. f.). *Chemical, biological, radiological and nuclear risk mitigation* (https://cbrn-risk-mitigation.network.europa.eu/index_en).

Naciones Unidas. (2019). Policy on chemical, biological, radioactive and nuclear threats and attacks. *Security management*, sección Q, capítulo 4 (<https://policy.un.org/en/security/specific-security-considerations/chemical-biological-radiological-and-nuclear-threats-and>).

Roper, R. y Goodzey, C. (2005). Extreme emergencies: humanitarian assistance to civilian populations following chemical, biological, radiological, nuclear and explosive incidents - a sourcebook. *Journal of Homeland Security and Emergency Management* 2(2) (<https://doi.org/10.2202/1547-7355.1146>).

Minas y municiones sin detonar

Servicio de las Naciones Unidas de Actividades relativas a las Minas. (2015). *Landmines, explosive remnants of war and IED safety handbook* (www.unmas.org/en/landmines-erw-and-ied-safety-handbook).

Servicio de las Naciones Unidas de Actividades relativas a las Minas. (2023). *Marking explosive ordnance hazards*. International Mine Action Standards 08.40, tercera edición (www.mineactionstandards.org/standards/08-40/#:::text=The%20marking%20of%20explosive%20ordnance,unintentional%20entry%20into%20hazardous%20areas).

Equipos de protección personal

Instituto Nacional de Justicia. (2024). *Understanding NIJ 0101.06 Armor Protection Levels* (<https://nij.ojp.gov/library/publications/understanding-nij-010106-armor-protection-levels>).

Epílogo

La gestión de riesgos de seguridad humanitaria ha progresado notablemente en las dos últimas décadas, pasando de una postura principalmente reactiva a un enfoque proactivo más alineado con los objetivos estratégicos y operacionales de las organizaciones humanitarias. Estos avances han permitido la continuidad de la acción humanitaria en entornos cada vez más peligrosos, con el apoyo de un personal mejor formado, sistemas de seguridad más sofisticados, una mejor coordinación interinstitucional y una creciente atención a los perfiles de riesgo personales y al bienestar del personal. A pesar de ello, siguen existiendo importantes deficiencias.

Todavía existe una gran disparidad entre las organizaciones en términos de recursos: las organizaciones locales suelen carecer de la financiación, las herramientas y la formación necesarias para gestionar los riesgos en el mismo grado que sus homólogas internacionales. El acceso seguro a las zonas de conflicto, especialmente en los conflictos en los que intervienen grandes agentes estatales, sigue siendo restringido. Además, los riesgos de la seguridad digital, los entornos de conflicto cada vez más fragmentados y los retos del cambio climático han añadido nuevas capas de complejidad a las operaciones humanitarias, que la mayoría de los sistemas de gestión de riesgos de seguridad existentes aún no están equipados para abordar con eficacia.

Con vistas al futuro, el sector debe asegurarse de que los trabajadores humanitarios y las organizaciones locales no se rezaguen en el desarrollo de las prácticas de seguridad. Las alianzas equitativas, la transferencia bidireccional de conocimientos y el aumento de la financiación directa pueden contribuir en este sentido. La IA y las herramientas digitales están mejorando la detección de las amenazas, el diagnóstico de riesgos y la coordinación, pero también introducen retos, riesgos y amenazas nuevos. Los futuros sistemas de gestión de riesgos de seguridad tendrán que incorporar estas tecnologías de forma eficaz, sin descuidar los riesgos.

Es necesario adoptar más ampliamente un enfoque de seguridad centrado en la persona, que reconozca los diversos perfiles de riesgo de los trabajadores humanitarios, sus fortalezas y sus vulnerabilidades, y que se adapte a las prácticas de gestión de riesgos de seguridad para satisfacer las necesidades individuales. La gestión de riesgos de seguridad también debe ser más previsor, adaptable y ágil para adecuarse al ritmo de los cambios de las amenazas mundiales y responder eficazmente a los nuevos riesgos que vayan surgiendo. Aunque este documento presenta un amplio y detallado conjunto de prácticas y herramientas para la gestión de riesgos de seguridad, estas deben adaptarse a las necesidades y a las capacidades de las organizaciones y su personal. El sistema debe estar al servicio de las personas, no al revés.

Por último, el aumento de la violencia contra los trabajadores humanitarios, en especial por parte de agentes estatales, subraya la necesidad de reforzar la rendición de cuentas. Las resoluciones del Consejo de Seguridad de las Naciones Unidas destacan este aspecto, y una mayor colaboración entre los equipos de seguridad y de incidencia dentro de las organizaciones puede apoyar el fortalecimiento de las medidas de rendición de cuentas con el fin de proteger mejor a los actores humanitarios.

Adelicia Fairbanks

Editora principal

