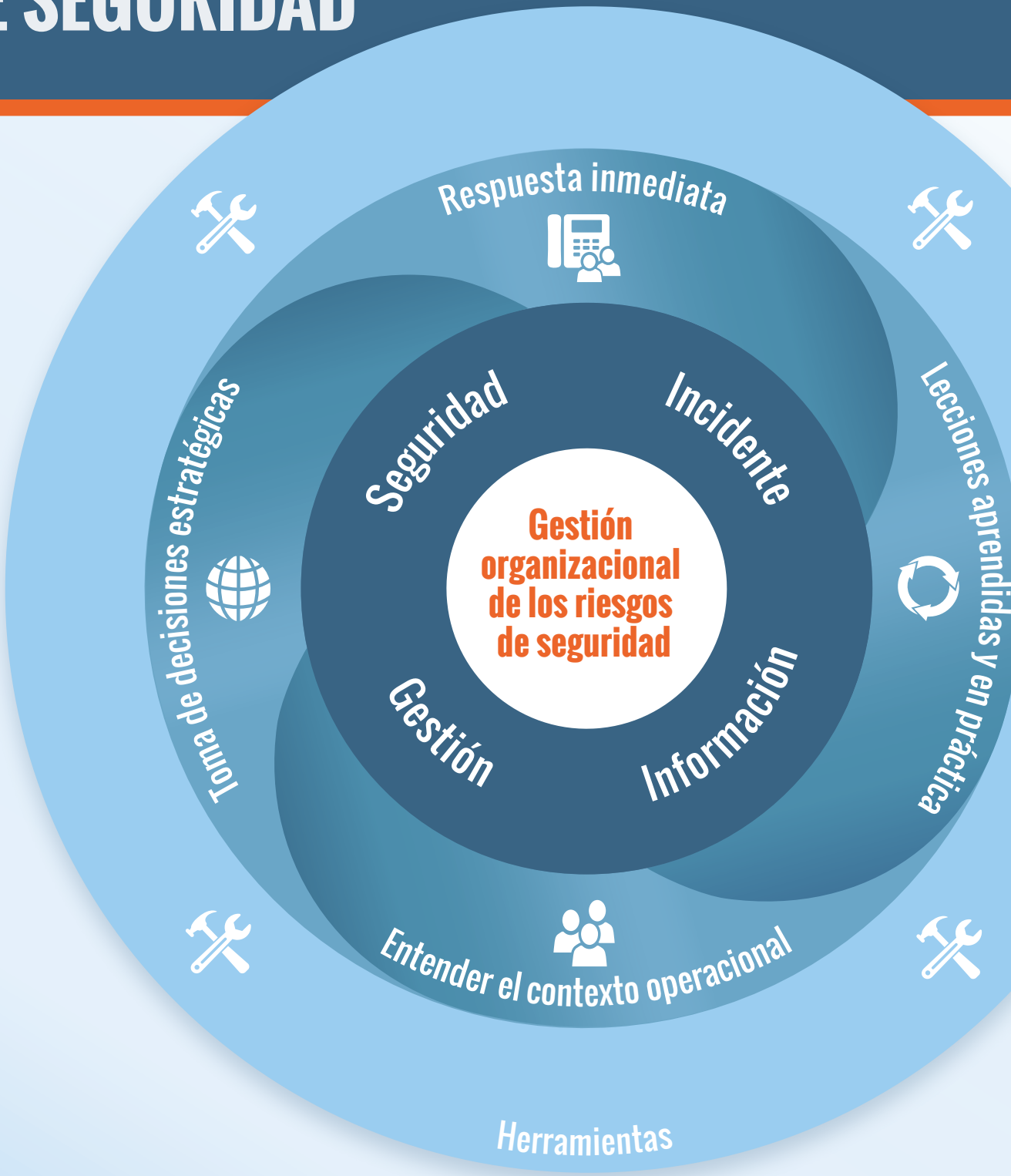
MANUAL DE GESTIÓN DE LA INFORMACIÓN SOBRE INCIDENTES DE SEGURIDAD



Funded by European Union Humanitarian Aid

eisf

redr uk
people and skills for disaster relief

Aid in Danger

Insecurity Insight
Data on People in Danger

Fecha de publicación: septiembre de 2017

"La gestión de información sobre incidentes implica recopilar, registrar, analizar y utilizar información a fin de mantener la seguridad del personal y el acceso a los beneficiarios. Una buena gestión de la información sobre seguridad encuentra el equilibrio adecuado entre dichas ventajas y los costes administrativos del sistema."

AGRADECIMIENTOS

El presente manual ha sido elaborado en colaboración entre RedR UK, Insecurity Insight y el EISF, dentro del proyecto Gestión de la Información sobre Incidentes de Seguridad (GIIS), financiado por la Oficina de Ayuda Humanitaria de la UE. Para obtener más información, se puede consultar la página del proyecto de RedR.

El proyecto ha sido coordinado por Marine Menier (RedR UK). El manual ha recibido las valiosas aportaciones de Christina Wille (Insecurity Insight) y Lisa Reilly (EISF). La editora fue Adelicia Fairbanks (EISF). El equipo del proyecto quiere agradecer a las personas que integran el Grupo Asesor y a otras que han contribuido —demasiadas como para citarlas una por una— por compartir con nosotros su experiencia, sus herramientas y sus comentarios, que tan útiles han sido. El proyecto GIIS reconoce el gran número de contribuciones recibidas y la voluntad de participar de organizaciones y personas.

DESCARGO DE RESPONSABILIDADES

Este manual se enmarca dentro de un proyecto más amplio dirigido a capacitar al sector humanitario y al de desarrollo; otras actividades de capacitación complementan la presente herramienta. Este documento plasma las prácticas actuales en el sector, ofrece recomendaciones y observaciones, incluso la visión y las recomendaciones de terceros. No es de obligado cumplimiento y es un trabajo que continúa.

A pesar de que el Proyecto GIIS se ha esforzado para garantizar la precisión y la calidad de la información que se aporta en el Manual de gestión de la información sobre incidentes de seguridad, RedR UK, Insecurity Insight y el EISF no se responsabilizarán, en la medida que la ley así lo permita, por ninguna pérdida, daño o inconveniente que surja a consecuencia del uso, o de la incapacidad de usar, o de la interpretación que se haga de la información incluida en el presente manual. RedR UK, Insecurity Insight y el EISF no asumirán responsabilidades ni serán responsables ante nadie por los posibles daños causados por decisiones o acciones que se emprendan confiando en la información presente en este Manual de gestión de la información sobre incidentes de seguridad.

La información en este documento se presenta "como es", sin condiciones, garantías ni otros términos de ningún tipo, y la confianza en el material o en otra información incluida en el presente documento será absolutamente por su cuenta y riesgo.

Diseñado por Tutaev Design.
Traducido al español por María José Castro Lage y revisado por Gonzalo de Palacios.

ABREVIATURAS

AiD	Aid in Danger
AWSD	Aid Worker Security Database
CICR	Comité Internacional de la Cruz Roja
DIH	Derecho Internacional Humanitario
EAS	Explotación y abuso sexual
EISF	European Interagency Security Forum
FAQ	Preguntas habituales
GIIS	Gestión de Información sobre Incidentes de Seguridad
GPR8	Good Practice Review 8 [Informe de Buena Práctica 8]
IASC	Inter-Agency Standing Committee [Comité Permanente entre Organismos]
ISO	Organización Internacional de Normalización
ODI	Overseas Development Institute
OIG	Organización Internacional Gubernamental
OMS	Organización Mundial de la Salud
ONG	Organización No Gubernamental
ONGI	Organización No Gubernamental Internacional
ONGL	Organización No Gubernamental Local
PAP	Primeros auxilios psicológicos
PEP	Post Exposure Prophylaxis [Profilaxis post expoxición]
RS	Referente de Seguridad
SLT	Saving Lives Together [Salvar Vidas entre Todos]
SOP	Procedimientos Operacionales Estándar [Standard Operating Procedures]
UNDSS	Departamento de Seguridad de Naciones Unidas

Nota aclaratoria de género
En todo el documento, cuando resulta obligatorio indicar un género gramatical, se utiliza el masculino como genérico (es decir, englobando además el femenino y los no binarios).

ÍNDICE

INTRODUCCIÓN

Acerca de este manual

La gestión de información sobre incidentes de seguridad (GIIS) es la recopilación, el reporte, el registro, el análisis, el intercambio y uso de información (datos incluidos) vinculada con un incidente de seguridad. La gestión de información sobre incidentes de seguridad es un elemento crucial de una gestión de riesgos de seguridad más amplia en una organización, dirigida a respaldar la seguridad organizativa para así mejorar en última instancia el acceso a poblaciones necesitadas.

El *Manual de GIIS* pretende realizar una importante contribución al fomento de prácticas relacionadas con la gestión de información sobre incidentes de seguridad en organizaciones no gubernamentales (ONG).

El manual está pensado para ayudar a quien lo utilice a establecer y desarrollar una gestión de información eficaz para sistemas de reporte y monitoreo de eventos de seguridad, tanto internos como externos, en toda la organización y en el sector.

El presente documento forma parte de un proyecto sobre GIIS más amplio, dirigido a reforzar las respuestas humanitarias a crisis mediante la capacitación de las ONG para que mejoren la gestión de información relativa a incidentes de seguridad y realcen su capacidad de compartir información sobre incidentes de una manera segura y adecuada para respaldar una buena toma de decisiones en distintas esferas de la organización.

El *Manual de GIIS* presenta un amplio abanico de herramientas y pautas, desde consejos sobre cómo diseñar un informe de incidentes de seguridad eficaz hasta el intercambio eficiente de información sobre incidentes de seguridad con una gran diversidad de partes interesadas pertinentes. El enfoque de gestión de riesgos de seguridad y el vocabulario que se presenta en estas pautas sigue la norma mundial que emitió la Organización Internacional de Normalización (ISO), "Gestión de riesgos – principios y directrices" (en lo sucesivo, ISO 31000:2009).

Este manual aborda la gestión de información sobre incidentes de seguridad, no la gestión de incidentes de seguridad en sí.

La mayor parte de este manual se puede aplicar a todo tipo de incidentes, incluso incidentes críticos, es decir, eventos que perturban las operaciones normales y rutinarias y exigen una respuesta de gestión de crisis por parte de la organización. Durante todo el documento, el término "incidente" se utilizará para referirse a todo tipo de incidentes. Al hablar de un incidente crítico, se especificará. Puede hablarse en ocasiones de "incidentes no críticos", en referencia a todos los incidentes que no se considerarían críticos y que, por lo tanto, no precisan de una respuesta de gestión de crisis. No obstante, es importante subrayar que algunos accidentes pueden ser considerados críticos por una organización, pero no por otra que tenga la capacidad de abordar el incidente mediante procedimientos rutinarios de gestión.

Aunque a menudo se minusvalora, la recopilación y gestión de información relativa a incidentes que no se consideren críticos, incluso "conatos", puede ser tan importante como la información sobre acontecimientos críticos para analizar y decidir respecto a la seguridad de una manera fundamentada. Por lo tanto, este manual dispone de herramientas para ayudar a desarrollar normas con el fin de reportar y gestionar la información de todos los incidentes, incluso aquellos que suceden más a menudo y que, por lo general, no se considerarían críticos.

El presente manual plasma prácticas actuales en el sector y ofrece recomendaciones y comentarios para ONG. Hace uso de recursos de un amplio elenco de expertos, entre ellos el European Interagency Security Forum (EISF), Insecurity Insight, RedR UK y varias de sus organizaciones miembro y redes más amplias. Como utiliza herramientas y pautas existentes, pretende evitar la duplicación al subrayar y extraer los elementos de gestión de información sobre incidentes de seguridad. El presente manual no es preceptivo, sino que presenta un vasto menú de opciones para que las organizaciones refuercen su gestión de información sobre incidentes de seguridad.

A pesar de que este manual se ha escrito centrándose en organizaciones y operaciones humanitarias, la información se puede aplicar sin problemas también a otras ONG, sobre todo a organizaciones que trabajan en desarrollo.

Esta versión del manual (publicada en septiembre de 2017) incorpora los comentarios y las contribuciones que se han recibido de las partes interesadas dentro del sector humanitario y de desarrollo.

Este documento es de acceso abierto y estará disponible en inglés, francés y árabe.

¿A Quién va dirigido este manual?

El *Manual de GIIS* va dirigido a toda persona con algún grado de responsabilidad en la gestión de información sobre incidentes de seguridad dentro de una organización no gubernamental, más allá de su cargo o ubicación. Se ha diseñado como herramienta para asesores de seguridad, responsables, referentes y analistas, así como para cargos superiores y responsables generales de proyecto / programa con responsabilidades en seguridad en las ONG; y sobre todo va dirigido a profesionales.

¿Cómo utilizar este manual?

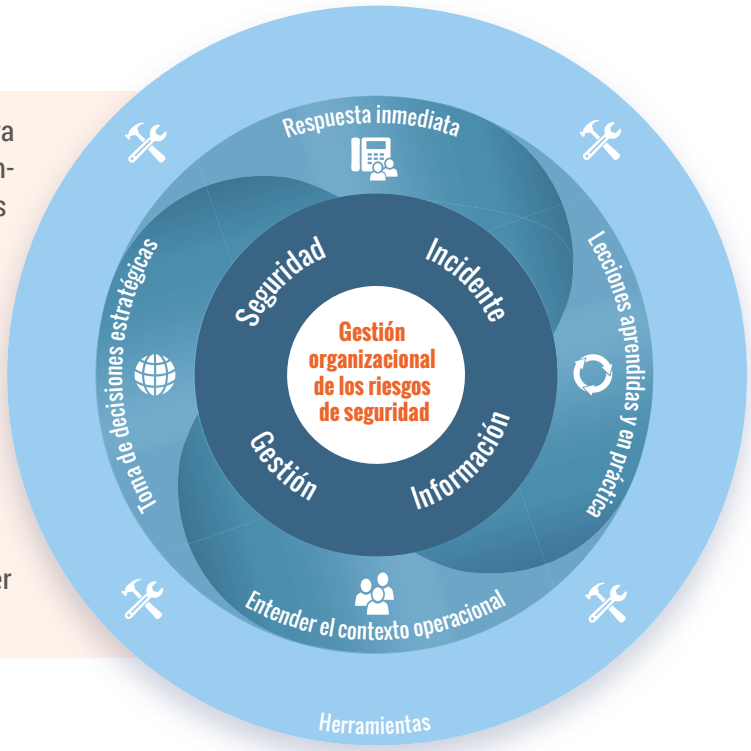
El *Manual de GIIS* se divide en capítulos y ofrece una panorámica de la gestión de información sobre incidentes de seguridad:

- al principio, el manual presenta el concepto de GIIS y cómo este encaja dentro de la gestión de riesgos de seguridad más amplia en una organización.
- sigue con la introducción de los cuatro objetivos clave de GIIS y destaca los pasos cruciales en una gestión eficaz de información sobre incidentes de seguridad para lograr cada uno de los objetivos;
- en todo el texto se hace referencia a las herramientas y se pueden encontrar al final del manual.

El diagrama siguiente ilustra los distintos elementos de la gestión de información sobre incidentes de seguridad. La estructura del presente manual sigue el diagrama y cada apartado del manual señalará de qué parte del ciclo se está hablando.

El ciclo de GIIS: seguridad organizacional con el fin de lograr acceso sin trabas para prestar ayuda

El diagrama es cíclico para mostrar que la gestión de información sobre incidentes de seguridad es un proceso continuo en el que todos los elementos se nutren unos de otros para cumplir cuatro metas principales. En el centro de la información sobre incidentes de seguridad está la seguridad organizacional con el objetivo de acceder sin trabas a prestar ayuda.



En este manual encontrará temas de debate, consejos, sugerencias y plantillas sobre cuatro objetivos principales de la gestión de información sobre incidentes de seguridad que hacen referencia a cuatro marcos temporales distintos y diferentes grados de prioridad en la organización:

Objetivo uno: dar información para una reacción y una respuesta inmediatas ante un incidente de seguridad. La finalidad es asegurar que se procura y se utiliza información para fundamentar la respuesta inmediata ante el incidente. Eso suele producirse en los ámbitos de terreno o país al poco tiempo de que se haya producido el incidente.

Objetivo dos: poner en práctica lecciones aprendidas tras un incidente de seguridad para seguimiento y prevención. La finalidad es entender qué ha sucedido con vistas a planificar y a aplicar cualquier cambio y procedimiento necesarios para ayudar a tratar el riesgo de eventos parecidos en un futuro, con especial hincapié en la prevención. Eso suele producirse en el ámbito de país / sede poco después del evento de seguridad.

Objetivo tres: entender el contexto de seguridad de la ONG. La finalidad es mejorar el conocimiento sobre el contexto a través de datos, tanto internos como externos, sobre incidentes. Eso ayudará a fundamentar decisiones estratégicas, a una comunicación general y a una autorreflexión entre organismos de ayuda. Eso suele producirse en el ámbito de país y en los puestos directivos en sede, y es mejor revisarlo de forma habitual.

Objetivo cuatro: fundamentar las decisiones estratégicas en una organización. La finalidad es hacer balance de la naturaleza cambiante de los incidentes, entender los entornos de trabajo que más desafíos suponen, la exposición general de la organización al riesgo e identificar las mejores respuestas estratégicas. Eso se produce en los ámbitos de país, región y sede dentro de un marco temporal razonable tras un evento de seguridad y durante las fases de planificación y programación.

Es importante considerar los cuatro objetivos como parte de un todo, todos ellos alimentando el objetivo general de reducir los riesgos de seguridad para la organización y, de esa forma, mejorar el acceso de la ayuda a las poblaciones necesitadas.

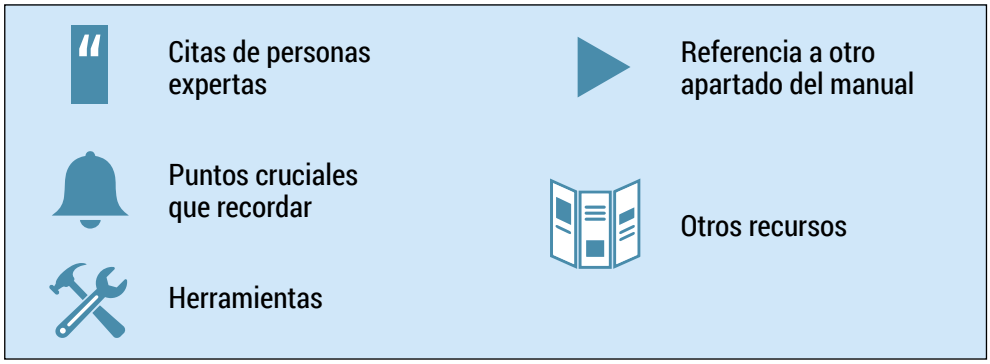
Cada apartado ofrece pautas sobre pasos cruciales y sobre cómo crear normas y categorías bien definidas que permitan a las organizaciones analizar los datos con más facilidad. Cuando las agencias comparten datos resulta fundamental tener unas definiciones y unos procedimientos éticos estándar.

Se invita a las organizaciones y a sus plantillas a:

- Utilizar el manual para lograr comprender mejor la gestión de información sobre incidentes de seguridad y qué pasos cruciales se pueden tomar para mejorar la gestión general de riesgos de su organización.
- Utilizar las herramientas que se ofrecen al final de este manual para mejorar el sistema de gestión de información sobre incidentes de seguridad de la organización. Aquí puede encontrar una lista de las herramientas.
- Utilizar la "Herramienta I: Matriz de autodiagnóstico en GIIS" para diagnosticar las necesidades de gestión de información sobre incidentes de seguridad de la organización. Esto se debería revisar de manera constante. Tras un periodo de tiempo definido, las organizaciones deberían reflexionar sobre su progreso desde su autodiagnóstico inicial.

Se puede consultar todo el manual o se pueden entregar capítulos o herramientas concretas a personal específico. Los cuatro objetivos principales que se describen en este manual son distintos, pero están relacionados entre sí: mejorar las prácticas para cumplir un objetivo ayudará a la organización a cumplir los demás objetivos y, en su conjunto, contribuirán a la preparación operacional y a la seguridad organizacional.

Para que sea más fácil, se utilizan los iconos siguientes en todo el documento para orientar a quien lo utilice en la identificación del tipo de recursos que se ofrecen:



Para facilitar la exploración, se introducen hipervínculos en las herramientas y en las referencias a recursos externos, así como en las referencias cruzadas a otros apartados del manual.

Los rectángulos en el margen derecho de cada página tienen hipervínculos al inicio del capítulo que corresponda.

Las referencias en las notas al pie tienen hipervínculos a "Referencias y bibliografía" al final del manual.

Definiciones Clave

Análisis: el proceso de transformar hechos, cifras, objetos, etc., desorganizados en información significativa que se puede utilizar a distintos efectos, como la toma de decisiones informadas.

Crisis: un acontecimiento que precisa de una respuesta más amplia que la posible a través de gestiones o procedimientos rutinarios. La respuesta puede precisar de la contribución de expertos o de una gestión de alto nivel (posiblemente desde sede). Muchas organizaciones considerarán "crítico" un incidente que se deba gestionar como una situación de crisis.

Datos: hechos y estadísticas que se han recopilado para referencia o análisis; información en bruto o desorganizada que se refiere a condiciones, ideas u objetos, o que está representada por los mismos.

Deber de cuidado: "la responsabilidad o la obligación legal de una persona u organización de evitar actos u omisiones que se pueda pronosticar, dentro de lo razonable, que tienen probabilidades de causar daño a otros".[1] Las organizaciones también deberían considerar su deber moral de cuidado.[2]

Diagnóstico de riesgos: proceso para identificar amenazas a la seguridad que podrían afectar al personal, a los bienes y a los programas, y analizar su probabilidad e impacto a fin de determinar el grado de riesgo que implican.

Evento: un acontecimiento o cambio en un conjunto concreto de circunstancias. Dentro de este manual, "evento" se utiliza como equivalente de "incidente".

Flujo horizontal de información: compartir información lateralmente entre organizaciones y entre organizaciones y partes interesadas.

Flujo vertical de información: información que sube y baja dentro de la estructura de una organización. Cuando una parte interesada en una región recopila informes sobre incidentes y los envía a sede para un análisis más minucioso, es un flujo de información ascendente. Según se analiza la información y se esbozan conclusiones, se pueden difundir de manera descendente al personal en el terreno.

Gestión de información: el término paraguas que se utiliza para describir políticas y directrices diseñadas para:

- regular los tipos de información que las organizaciones recopilan, almacenan y transmiten;
- reducir los riesgos inherentes en estos procesos para el personal y las organizaciones; y
- asegurar que las personas adecuadas pueden acceder a la información en el momento oportuno.[3]

1 E. Kemp y M. Merkelbach, "Can you get sued? Legal liability of international humanitarian aid organisations towards their staff", *Security Management Initiative*, 2011.

2 E. Kemp, y M. Merkelbach, *Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications*. European Interagency Security Forum (EISF), 2016.

3 R. Ayre, *The Information Management Challenge: A Briefing on Information Security for Humanitarian Non-Governmental Organisations in the Field*. EISF, 2010.

Gestión de información sobre incidentes de seguridad: recopilación, informes, registro, análisis, divulgación y uso de información (datos incluidos) vinculada a un incidente de seguridad con el objetivo general de lograr acceso sin trabas para prestar ayuda mejorando la gestión organizacional de riesgos de seguridad.

Habilidades analíticas: la capacidad de visualizar, articular, conceptualizar o resolver tanto problemas complejos como sencillos, incluso la capacidad de aplicar un pensamiento lógico para descomponer problemas complejos en elementos más pequeños.

Incidente: cualquier acontecimiento donde se comprometa la seguridad del personal; donde personas dependientes o terceras partes resulten heridas o dañadas durante las actividades de la organización; donde se roben, dañen o se pongan en riesgo bienes o pertenencias de la organización; donde se interfiera con la prestación de ayuda o se comprometa el trabajo independiente de la agencia de ayuda, incluso daños a la reputación.

> **NOTA:** Los incidentes pueden ser organizativos (que afectan directamente a la organización y a su capacidad para prestar ayuda), así como externos (que afectan a otros ajenos a la organización). Informar de ambos puede ser beneficioso para la gestión de información sobre incidentes de seguridad.

Más allá, los incidentes se pueden clasificar como:

Accidentes: acontecimientos fortuitos que provocan perjuicios, daños o pérdidas a una organización, su personal o sus programas. En comparación, los "incidentes" provienen de la voluntad de una o varias personas de causar daños a personas oentidades, confiscar bienes o perturbar la prestación de ayuda, ya sea directamente contra esa organización y su personal o de otra forma. Independientemente de si un acontecimiento es un incidente de seguridad o un accidente, se debería informar de ambos. No obstante, cuando el presente manual se refiere a "incidentes" o a "incidentes de seguridad", se refiere ante todo a eventos relativos a la seguridad. Sin embargo, se pide a los lectores que no se olviden de que los modelos, las herramientas y las pautas que se incluyen aquí también sirven como orientación para gestionar información relativa a accidentes, tales como accidentes de tráfico.

Conatos: eventos que casi provocan perjuicios, daños y pérdidas a la organización, su personal o sus programas, o que tenían el potencial de conllevar heridas graves, muerte o secuestro y que solo han provocado lesiones menores, daños o pérdidas. También se pueden denominar "cuasi accidentes" o "intentonas".

> **NOTA:** Se pueden considerar los impedimentos administrativos (p. ej.: obstáculos aduaneros y fiscales demasiado burocráticos, otorgar visados o permisos de viaje para zonas afectadas por catástrofes, etc.) como incidentes e informar de ellos como tales, ya que también pueden ofrecer información sobre el contexto.

Incidente crítico: un incidente que perturba las operaciones normales y rutinarias. Un incidente crítico puede provocar la muerte, lesiones o una enfermedad mortal y activa la respuesta de gestión de crisis de una organización. Estos incidentes suelen precisar de una respuesta urgente.

Información: lo que se transmite o lo que representa una disposición o una secuencia concreta de datos. Es la comunicación o la recepción de conocimiento o inteligencia. Los datos en bruto se transforman en información a través del análisis.

Información sobre incidentes de seguridad: datos e información vinculados a un evento de seguridad concreto o a una secuencia de acontecimientos.

Marco de gestión de riesgos de seguridad: un conjunto de medidas, protocolos, planes, mecanismos y responsabilidades que respalda la reducción de riesgos de seguridad para la plantilla, los programas y una organización.

Personal: plantilla, voluntarios y otras personas que entren dentro del paraguas de la organización, incluso consultores, socios, visitantes, etc.

Propietario de la información: la persona (o el grupo de personas) que tienen la capacidad de crear, editar, modificar, compartir y limitar el acceso a los datos.

Riesgo: "el efecto de la incertidumbre sobre los objetivos".[4] El riesgo también puede ser la probabilidad de que una amenaza afecte a la organización y el impacto que tendrá si lo hace.

Seguridad (*safety*): estar libre de riesgos o daños derivados de actos y eventos no intencionados, accidentales o fortuitos.

Seguridad (*security*): estar libre de riesgos y daños derivados de actos de violencia, agresión o delitos intencionados contra el personal, los bienes o las propiedades de la organización.

Seguridad de la información: la "conservación de confidencialidad, integridad y disponibilidad de información… Puede implicar otras características, como son la autenticidad, la asunción de responsabilidades, el no repudio y la fiabilidad".[5]

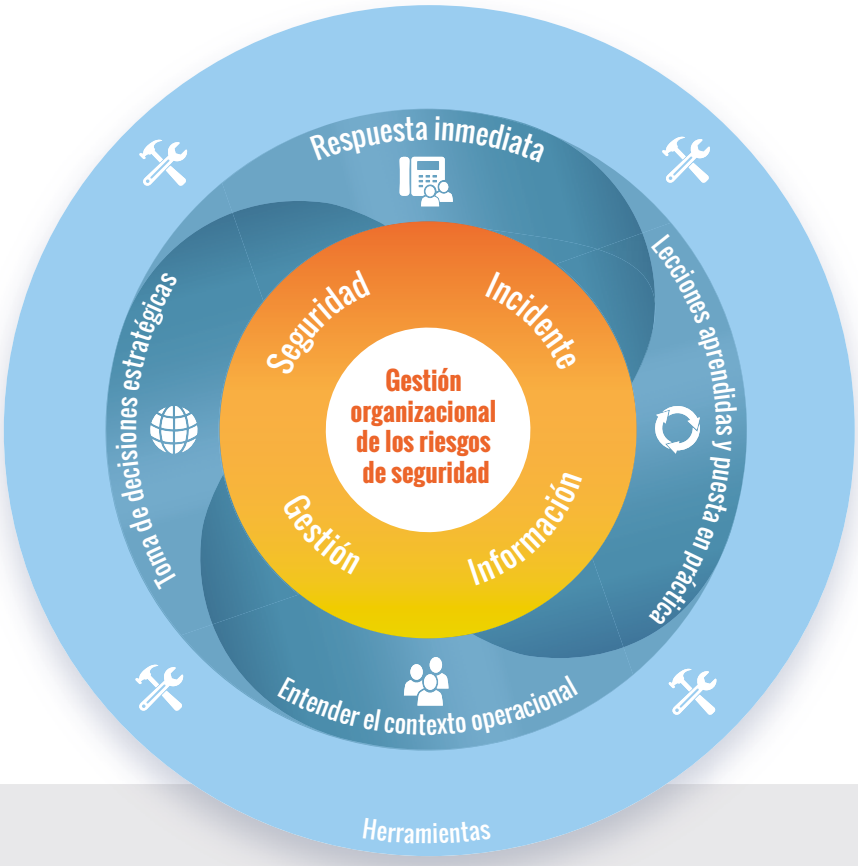
Tipología de incidentes: la clasificación de incidentes según unos tipos generales.

Herramienta II: Tipología de incidentes propone una tipología usada por Insecurity Insight en sus análisis y está basada en tipologías de varias organizaciones.

Violencia sexual: "todo acto sexual, la tentativa de consumar un acto sexual, los comentarios o insinuaciones sexuales no deseados, o las acciones para comercializar con la sexualidad de una persona mediante coacción, amenazas de daño o uso de la fuerza física por otra persona, independientemente de la relación de esta con la víctima, en cualquier ámbito, incluidos el hogar y el lugar de trabajo. La violencia sexual adopta muchas formas, tales como la violación, la esclavitud sexual y la trata de personas, el embarazo forzado, el acoso sexual, el abuso y la explotación sexual, y el aborto forzado".[6]

4 ISO/IEC 27000:2014
5 ISO 31000:2009
6 Comité Permanente entre Organismos (IASC). *Directrices para la integración de las intervenciones contra la violencia de género en la acción humanitaria. Reducir el riesgo, promover la resiliencia e impulsar la recuperación*. 2015.

CAPÍTULO I: PRESENTACIÓN DE LA GESTIÓN DE INFORMACIÓN SOBRE INCIDENTES DE SEGURIDAD



Este apartado presenta la gestión de información sobre incidentes de seguridad y habla de cómo encaja esta dentro de un enfoque de gestión de riesgos de seguridad más amplio para así reforzar la prevención de incidentes de seguridad y la preparación para los mismos.

- ¿Qué es la gestión de información sobre incidentes de seguridad?
- Retos clave en la gestión de información sobre incidentes de seguridad
- Gestión de riesgos de seguridad y GIIS
- Atribuciones de seguridad del personal y GIIS
- Seguridad de la información
- Gestión de incidentes y GIIS: los beneficios de que la organización esté preparada
- Deber de cuidado

Herramientas pertinentes:

- Herramienta I: Matriz de autodiagnóstico en GIIS

¿Qué es la gestión de información sobre incidentes de seguridad?

La gestión de información sobre incidentes de seguridad es recopilar, reportar, registrar, analizar, compartir y utilizar información (datos incluidos) vinculada a un evento de seguridad o a una secuencia de eventos.

Una gestión eficaz de información sobre incidentes de seguridad aumenta la capacidad de una ONG de compartir y utilizar información sobre incidentes tanto dentro como fuera de la organización de una manera segura y adecuada para respaldar una buena toma de decisiones en los distintos ámbitos de una organización.

La gestión de información sobre incidentes de seguridad no debería limitarse a eventos graves de fallecimiento, lesiones o secuestro ni a los países más afectados. Es ventajoso que las organizaciones reporten y analicen todos los incidentes que repercutan en la prestación de ayuda. Eso permite a las organizaciones, entre otras cosas:

- adoptar de inmediato las medidas de reducción de riesgos adecuadas y eficaces, lo que permite que se informe con rapidez a los responsables para que estos puedan ofrecer el apoyo preciso al personal afectado o involucrado en un incidente;
- mejorar el análisis de contexto al establecer tendencias y patrones emergentes para fundamentar las decisiones operativas que tome el personal directivo;
- informar a las partes interesadas externas de amenazas y riesgos potenciales, de forma que ellas también puedan aplicar medidas de tratamiento del riesgo;
- mantener un registro institucional completo de incidentes de seguridad.

Los pasos cruciales en la gestión de información sobre incidentes de seguridad son:

- reportar;
- registrar;
- analizar datos recopilados por medio de un incidente;
- compartir información (en términos internos y externos);
- tomar decisiones en el ámbito de terreno, normalmente como respuesta inmediata a un incidente;
- tomar decisiones a nivel de país o región, usando la información sobre incidentes que se han reportado para aplicar las lecciones aprendidas y así mejorar los procedimientos de seguridad;
- analizar los datos sobre incidentes para identificar tendencias y patrones;
- usar el análisis de tendencias para fundamentar análisis de contexto, diagnósticos de riesgos y para tomar decisiones informadas sobre las mejores medidas de tratamiento del riesgo que deberían aplicarse para mejorar la seguridad de la organización;
- decisiones estratégicas en sede, que implican utilizar análisis de tendencias elaborados a partir de incidentes sobre los que se ha reportado para tomar decisiones informadas que afecten a toda la organización.

Estos pasos cruciales se tratarán en mayor profundidad en el "Capítulo II: Los cuatro objetivos de gestión de información sobre incidentes de seguridad".

Retos clave en la gestión de información sobre incidentes de seguridad

Los retos en la gestión de información sobre incidentes de seguridad pueden estar vinculados tanto a factores personales como de la organización.

Incidentes que no se reportan
Muchos de los incidentes nunca se han reportado ni registrado. Se reportan más los no críticos que los conatos, aunque en ambos casos quedan incidentes sin reportar. Eso no significa que no se produzcan los conatos, sino que se les da menos atención en comparación con otros incidentes que implican un riesgo mayor en entornos más hostiles.

Los incidentes no críticos en entornos hostiles pueden indicar que la situación se ha deteriorado y que han empeorado las tensiones; se debería informar de ello al puesto directamente superior que corresponda o al referente de seguridad (RS) y puede proponerse una necesidad de revisar el análisis de contexto y de riesgos de la organización.

Diferencias en definiciones
La percepción de qué constituye un incidente o no puede variar mucho entre una organización y otra, al igual que entre una persona y otra dentro de la misma organización. Una ONG puede pensar que merece la pena reportar sobre una breve ráfaga de disparos durante la noche, mientras que otra puede pensar lo contrario si el entorno operativo es tal que los disparos sean algo habitual. De manera parecida, el personal internacional y el nacional pueden tener distintas perspectivas sobre qué representa un incidente del que haya que reportar.

Los responsables tienen que ofrecer pautas claras sobre qué constituye un incidente del que haya que reportar en determinados lugares para garantizar un enfoque coherente en toda la organización.

Todo el personal debería entender lo mismo por los términos relativos a la gestión de información sobre incidentes de seguridad para poder comunicarse con eficacia —tanto en términos internos como externos—. Una falta de coherencia en el uso de estos términos provoca problemas en el análisis. Por ejemplo, en los documentos de seguridad se pueden mencionar incidentes relacionados o parecidos, como “robo” y “hurto”, sin definir la distinción. Para recabar y comparar datos de distintas agencias, así como de distintos países dentro de una organización, es preciso tener definiciones comunes.

Preocupación por la reputación
Un incidente de seguridad indica que algo ha fallado en algún lado. A pesar de que las organizaciones de ayuda pocas veces son responsables de que se produzca un incidente de seguridad, a menudo pueden identificar elementos relacionados con sus procedimientos o con el comportamiento de su personal que de alguna manera pueden haber contribuido a que se haya producido el evento o haber influido en las consecuencias del incidente. Debido al impacto potencial que la información relativa a incidentes puede tener en la reputación de una organización, muchas ONG pueden preferir no compartir detalles sobre qué ha fallado, sobre todo con actores externos.

"En otros sectores es una práctica habitual aprender de conatos y de otros errores. En el sector de la aviación, por ejemplo, todas las empresas están obligadas a informar de cualquier error –ya sea técnico o humano– y eso ha servido para desarrollar directrices que han hecho que volar sea uno de los medios de transporte más seguros a día de hoy[7]. Por lo tanto, compartir el aprendizaje que se extrae de lo que no ha funcionado en una ONG podría ayudar a toda la comunidad humanitaria y de desarrollo en su conjunto".

Las organizaciones salen beneficiadas si establecen con claridad en sus políticas cuándo compartir información que se haya reportado sobre incidentes dentro y fuera de la organización, cómo asegurar la confidencialidad cuando sea preciso y qué pasos seguir para gestionar con sensatez la información.

Carga administrativa
Documentar los incidentes lleva mucho tiempo y absorbe bastantes recursos humanos. No obstante, si las organizaciones consiguen establecer un sistema eficaz, se puede reducir la carga administrativa y así evitar que el personal tenga que perder el tiempo buscando las instrucciones para registrar incidentes y reportar sobre los mismos. Ofrecer herramientas y plantillas sirve para que el registro y los informes sean no solo más coherentes en toda la agencia, sino también menos laboriosos y, por lo tanto, que sea más probable que se hagan.

Las políticas y los procedimientos para gestionar la información sobre incidentes deberían explicarse al personal y mantenerse de la manera más sencilla posible.

Cultura organizacional
El personal responsable, en cualquier ámbito, es el encargado de compartir información en vertical dentro de la organización, es decir, a su superior inmediato o a sede, pero la información adecuada a menudo no se comparte por diversos motivos. Los responsables (nacionales e internacionales) pueden evitar compartir la información en vertical por miedo a reacciones negativas de cuadros superiores, a admitir que se ha infringido alguna política o para "guardar las apariencias". El personal nacional que está en primera línea es el más afectado por muertes y lesiones en las ONG, pero pueden considerar que su reputación se verá afectada si reportan un incidente. Muchas personas temen que se les penalice con menos oportunidades de ascenso o, en el peor de los casos, perder su trabajo.

Al analizar los incidentes, se puede desvelar cualquier conducta inadecuada o un incumplimiento de los procedimientos de seguridad (o del código de conducta). La organización puede decidir si es preciso tomar medidas disciplinarias. Este asunto suele despertar debate dentro de las organizaciones, que consideran que las sanciones son un factor adicional para no reportar. Sería ventajoso para las organizaciones tener una postura clara al respecto y conciliar dichas preocupaciones.

La respuesta ante incumplimientos de los procedimientos de seguridad debe ser contundente. Las políticas sobre seguridad son ineficaces si los cuadros superiores o el personal de seguridad las incumplen sin consecuencias.

Comunicación entre agencias
Puede resultar difícil intercambiar información entre organizaciones, incluso informes sobre incidentes y sobre la situación. En "Objetivo tres: Entender el contexto operacional" se aborda en más profundidad cómo superar los principales desafíos de la colaboración, como son la confidencialidad, la confianza y la gestión de información.

[7] C. Wille, "Lessons from the Aviation Industry: What Can We Learn for Humanitarian Security Risk Management?", *EISF*, 2016.

Gestión de riesgos de seguridad y GIIS

La gestión de riesgos de seguridad implica que una organización establezca políticas, protocolos, planes, mecanismos, y que delimite las responsabilidades del personal para respaldar un mejor acceso a través de una mejor seguridad organizacional. El diagrama que aparece a continuación, que ilustra un marco de gestión de riesgos de seguridad que abarca toda la organización, presenta los distintos pilares que permiten una gestión eficaz de los riesgos de seguridad.[8]

Aunque se destaca el monitoreo de incidentes como un pilar fundamental del marco de gestión de riesgos de seguridad, la información sobre incidentes de seguridad bien gestionada puede alimentar y reforzar todos los elementos clave de la gestión de riesgos de seguridad.

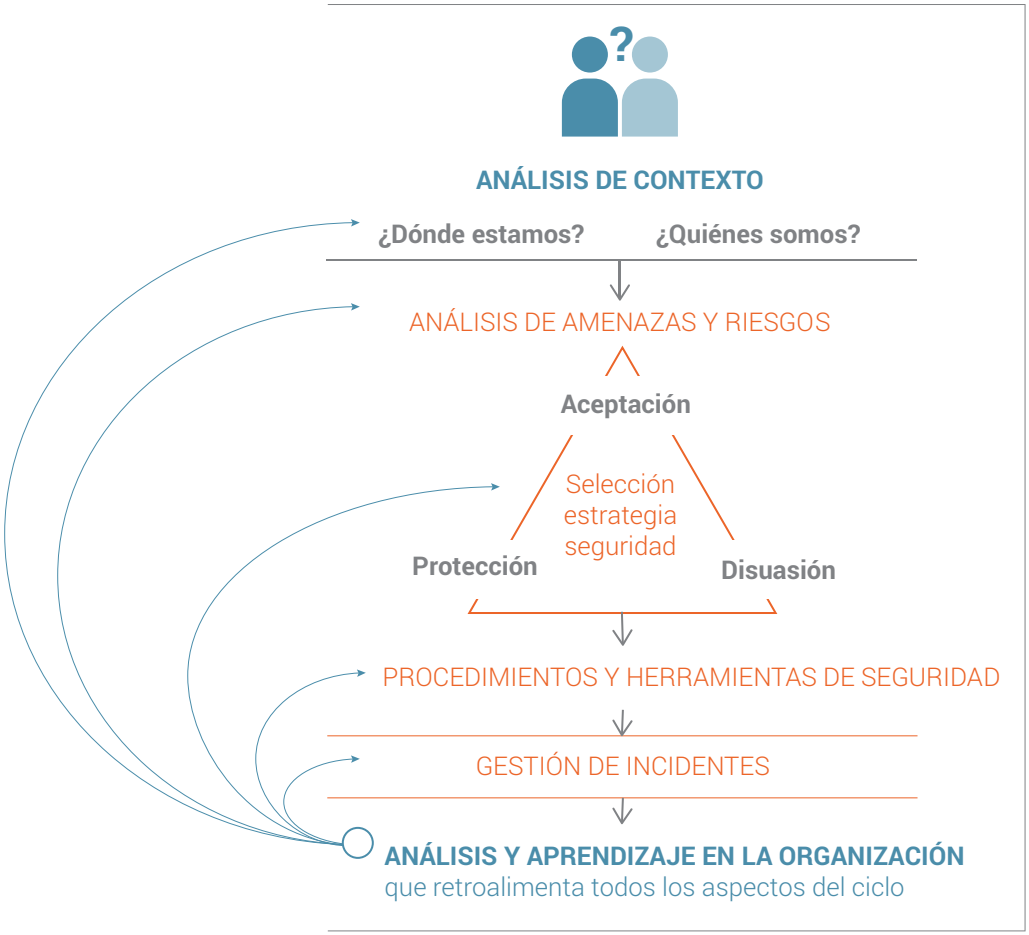
La gestión de información sobre incidentes de seguridad, desde asegurar que se establecen estructuras de gestión de crisis a tiempo tras un incidente crítico hasta el uso de información sobre incidentes no críticos para informar al personal de los riesgos del viaje, es un elemento esencial de una buena gestión de riesgos de seguridad.

> *"Un incidente es la ocasión y la oportunidad perfecta para aprender y mejorar. Su análisis debería nutrir todo el marco de gestión de seguridad".*

Los referentes de seguridad y los analistas de seguridad pueden utilizar la información de incidentes internos y otras fuentes para entender el contexto en distintos lugares. La información que se extrae y se analiza tras un incidente debería fundamentar el análisis de riesgos de la organización al subrayar las amenazas y las vulnerabilidades en el contexto en cuestión. Puede fundamentar la revisión de los procedimientos operacionales estándar (SOP) y los planes de contingencia, y también se puede utilizar como prueba sólida que sostenga la modificación de las políticas.

[8] S. Bickley, *Security Risk Management: a basic guide for smaller NGOs.* EISF, 2017.

El diagrama[9] siguiente refleja los pasos cruciales en la gestión de riesgos de seguridad. Una buena gestión de información sobre incidentes permitirá que las organizaciones utilicen esta información para fundamentar cada uno de los pasos en este proceso.



Competencias de seguridad del personal y GIIS

El órgano para profesionales de seguridad de las ONG, la Asociación de Seguridad en ONG Internacionales (INSSA, por sus siglas en inglés), incluye la gestión de información como una de sus áreas clave de competencia para el personal responsable en los ámbitos país, región, global y de seguridad estratégica.

El personal en cada uno de los ámbitos respaldará los sistemas y los procesos generales de la organización en gestión de riesgos de seguridad y es de gran importancia:

- distinguir con claridad las responsabilidades del personal en cada uno de los ámbitos; y
- asegurar que el personal tiene el apoyo y la formación necesarios para cumplir sus responsabilidades en función del ámbito en el que se encuentren.

Véase el "Módulo sobre gestión de personas" dentro de la guía del EISF "Seguridad en práctica" para más información sobre la interconexión entre gestión de personas y seguridad organizacional.

[9] Este diagrama proviene de los cursos de introducción a la seguridad de RedR UK.

Seguridad de información

En el contexto de gestión de la información sobre incidentes de seguridad, es importante para una organización velar por que sean seguros los medios de comunicación que se utilizan para reportar, recopilar, analizar, compartir, almacenar y usar la información.

Las organizaciones a menudo tienen que compaginar la necesidad de gestionar la información sobre incidentes de seguridad de una forma segura y los corsés presupuestarios. No obstante, es fundamental abordar la seguridad de los datos, más allá de los recursos financieros de los que se disponga. Para un análisis de las radios, los teléfonos móviles, satélites, correos electrónicos y otros aspectos técnicos de la gestión de información, consulte la guía de revisión de buenas prácticas número 8 (GPR8) del Overseas Development Institute (ODI) en su capítulo de telecomunicaciones y la guía "Seguridad en práctica" del EISF.

Es primordial la obligación jurídica y ética de las ONG de asegurar la confidencialidad de la información, sobre todo si se trata de "datos personales" —es decir, toda información referente a una persona identificada o identificable—. Los fallos al crear o al aplicar políticas de gestión de la información pueden tener repercusiones negativas para el personal y para las organizaciones, y podrían derivar en acciones y reparaciones legales.

> *"Una buena gestión de la información sobre incidentes de seguridad consiste, en parte, en lograr el equilibrio adecuado en ese contexto entre las ventajas que aporta recopilar, registrar y comunicar determinados conjuntos de información y los riesgos que conllevan esas acciones".*

Las ONG deberían reforzar su cultura de gestión de la información al asegurarse de que la seguridad de la información esté integrada en políticas y procedimientos de gestión de riesgos más amplios e incorporada a la perfección en el pensamiento organizacional y programático. La mayoría de los riesgos pueden mitigarse mediante la concienciación ante riesgos, sentido común y una buena disciplina, lo que aquí se denomina "mantener la casa en orden". Mantener la casa en orden va desde el papeleo y las copias físicas hasta la seguridad digital —la mejor seguridad digital del mundo no protegerá ante personal que deja documentos sobre su mesa por la noche o que tira a la papelera documentos sensibles sin triturarlos—.

La seguridad de la información no es un reto que tengan que abordar solo los departamentos de informática. "Mantener la casa en orden" y las soluciones técnicas se sostienen en una formación eficaz del personal y recursos suficientes, de forma que se cree una cultura de gestión de la información sólida en la que el personal ponga en práctica casi automáticamente las políticas de seguridad.

Para asegurar una buena seguridad de la información en la gestión de información sobre incidentes de seguridad, las organizaciones deberían afrontar las siguientes cuestiones clave en todas las esferas y etapas de recopilación, reporte, registro, análisis, uso e intercambio de información:

- **Seguridad física:** la protección de hardware informático, instalaciones de oficinas y bienes de la organización ante circunstancias físicas y eventos que pueden provocar daños graves y pérdidas, incluso robo, incendio y catástrofes naturales.
- **Seguridad digital:** la protección de archivos electrónicos almacenados en dispositivos informáticos —desde móviles y PDA hasta USB y ordenadores— frente a un acceso no autorizado, corrupción, pérdida, mal uso o destrucción. Siempre deben seguirse unas medidas de seguridad digital básicas, como la protección con contraseña de cuentas de usuario, redes inalámbricas de internet y documentos sensibles .

- **Accesibilidad:** la clasificación de información y personal de forma que solo el personal con funciones pertinentes o suficientes responsabilidades pueda acceder a la información (véase "Categorías de información" en Objetivo tres).
- **Copias de seguridad:** pautas sobre cómo y con qué regularidad hacer copias de seguridad de los archivos, de forma que se asegure la mínima perturbación de la programación, ya que el riesgo de daños o pérdidas en el hardware nunca se puede eliminar por completo.
- **Destrucción de información:** directrices claras sobre cómo y cuándo debe destruirsela información (tanto en soportes físicos como digitales), siendo conscientes que puede ser preciso hacerlo con rapidez. En entornos de riesgo elevado, sobre todo en los que existen sospechas de vigilancia avanzada, tal vez no deban recopilarse ni registrarse determinados tipos de información. Además, la gestión de información delicada debe separarse con claridad de la gestión de información rutinaria. Así, si un contexto en deterioro exige que se destruya con rapidez información delicada, será posible identificar con rapidez lo que ha de destruirse.
- **Seguridad en las comunicaciones:** una política de gestión de la información debería identificar cómo y qué comunicar a entornos determinados. Quizás el momento de mayor vulnerabilidad de la información es su comunicación: la radio no es segura, las llamadas telefónicas se pueden intervenir y se pueden interceptar los correos electrónicos, etc.

Véase en la guía GPR8 de ODI el capítulo sobre seguridad de las comunicaciones.

Seguridad en pocas palabras
Un elemento esencial en la seguridad de la información son unas herramientas y tácticas sólidas de seguridad digital.

"Security-in-a-box" es una iniciativa desarrollada en colaboración entre Front Line Defenders y Tactical Technology Collective, gracias a la cual se han elaborado guías para la comunidad que ofrecen consejos a medida sobre herramientas y tácticas que son pertinentes para las necesidades de grupos de personas concretos. Estos consejos cubren los principios básicos de las plataformas de redes sociales y teléfonos móviles, incluso consejos sobre cómo utilizar estos de una manera más segura. Las herramientas y las guías tácticas de Security-in-a-box ofrecen instrucciones paso a paso sobre cómo instalar y utilizar el software y los servicios de seguridad digital más básicos (estos recursos se pueden descargar desde su página web).

Gestión de incidentes y GIIS: las ventajas de la preparación organizacional

Aunque este manual no se centre en la gestión de incidentes, planteamos que la gestión de información sobre incidentes de seguridad es un elemento esencial de la gestión de incidentes y la preparación organizacional.

La preparación organizacional significa tener instaurados procedimientos claros y formación sobre la gestión de incidentes y la gestión de información sobre incidentes, lo que asegurará las mejores reacciones y respuestas posibles ante los eventos.

Los incidentes, sobre todo los que son críticos, suelen tener las siguientes características:
- un componente de sorpresa;
- insuficiente información;
- un ritmo de eventos superior al de respuesta;

- cuestiones importantes que conllevan un escrutinio externo;
- pérdida de control (real o percibida);
- alteración de procesos normales de decisión; y
- que a quien afectan directamente tiende a tomar un enfoque cortoplacista.

Salvo si los incidentes son críticos, normalmente se los aborda dentro del marco de procedimientos preestablecidos. No obstante, incluso los incidentes no críticos pueden crear confusión y pánico en quienes no están preparados para darles respuesta.

La finalidad de la preparación y de la gestión de incidentes de seguridad es reducir el impacto de los incidentes y mejorar la capacidad de una organización de tratar los actuales y aprender para un futuro.

Tras un incidente, una organización intentará:

- prevenir daños adicionales y garantizar la salud o la seguridad de víctima(s) y personal;
- asegurar al personal y a las familias de las víctimas que una respuesta responsable y eficaz está en camino;
- garantizar una gestión organizacional continua durante todo el incidente, sobre todo si es un evento de larga duración, como un secuestro;
- garantizar la continuidad de los programas;
- reducir la pérdida de activos (como teléfonos, ordenadores, vehículos, etc.);
- reemplazar los activos perdidos por el robo, etc.;
- cumplir las responsabilidades organizacionales y reducir el riesgo de litigio / demandas de responsabilidad;
- presentar reclamaciones (por ejemplo, notificar a las autoridades locales de cualquier amenaza contra el personal);
- salvaguardar la imagen y la reputación de la organización;
- compartir información crítica con otras ONG y socios que también puedan estar en riesgo durante o después de un incidente;
- elaborar comunicados de prensa o aportar a los medios y agencias de noticias humanitarias / de desarrollo información seleccionada que informe al público al tiempo que proteja a las personas involucradas.

La sensibilización en materia de seguridad, el análisis de amenazas, vulnerabilidad y riesgos, procedimientos eficaces, realizar simulacros de seguridad, un contacto fluido y amplio con socios y agencias externas y una buena planificación de las contingencias, son todas ellas maneras proactivas de abordar los incidentes y, así, crisis potenciales.

La preparación organizacional es esencial para una gestión de incidentes y una gestión de información sobre incidentes de seguridad eficaces.

Aunque las políticas no pueden cubrir todos los supuestos, será un gran avance tener planes de contingencia y planes de gestión de incidentes, actualizarlos con regularidad planteando escenarios con la pregunta "¿qué sucedería si...?", así como tener instaurados procedimientos de gestión de crisis eficaces para mantener la situación bajo control y que las operaciones sigan siendo seguras.

"En el caso de eventos delicados, por ejemplo una agresión sexual a alguien de la plantilla, responder de antemano a la pregunta "¿qué sucedería si quien comete un incidente de violencia sexual es parte de la plantilla?" ayudará a la organización y a la plantilla a prepararse adecuadamente para ello".2

Resulta muy valioso reflexionar sobre preguntas como las siguientes al encarar incidentes que se producen más habitualmente:

- ¿Respondimos adecuadamente y lo mejor que pudimos ante los eventos más recientes?
- ¿Qué hemos aprendido de los conatos? ¿Hemos modificado nuestra manera de trabajar en función de lo que hemos aprendido?

Antes de que se produzca un incidente, y como buenas prácticas de gestión, se aconseja a la organización asegurarse de que una gestión de información sobre incidentes sólida forma parte de las políticas y los procedimientos de gestión de incidentes generales de la organización. Una organización puede hacerlo al:

- Desarrollar, aplicar y revisar con regularidad las políticas y los procedimientos organizacionales. Por ejemplo, sobre gestión e informes de incidentes, incluso conatos, sobre cómo tratar casos de violencia sexual u otros eventos especialmente delicados, sobre seguridad de datos, recursos humanos, etc.
- Elegir un sistema para registrar y reportar incidentes que permita una gestión segura de información sobre incidentes de seguridad dentro y fuera de la organización (para saber más sobre sistemas de registro, véase "Objetivo cuatro: registro sistemático de incidentes").
- Definir una estructura e identificar funciones y responsabilidades en la gestión de incidentes y en la gestión de información sobre incidentes para todo el personal y las personas a las que se han otorgado responsabilidades y a referentes, en todos los ámbitos de la organización, desde terreno hasta sede.
- Diagnosticar e identificar recursos (tanto internos como externos) que permitan a la organización responder de manera eficaz y eficiente ante cualquier incidente.
- Dar orientación y formación a personal clave en gestión de incidentes y gestión de información sobre incidentes.

Resulta beneficioso para las organizaciones incluir procedimientos claros y formación en gestión de información sobre incidentes dentro de una respuesta de gestión de incidentes más amplia. Eso asegurará que se recopilan datos y que estos se analizan y reportan de forma adecuada, lo que respalda la respuesta inmediata ante el incidente y a su vez beneficia a la organización a largo plazo.

Véase Herramienta I: Matriz de autodiagnóstico en GIIS, donde se ofrece un formulario de autodiagnóstico que ayuda a las organizaciones a evaluar sus fortalezas y sus debilidades en gestión de información sobre incidentes de seguridad.

Deber de cuidado

¿Por qué deberían preocuparse las organizaciones sobre la gestión de información sobre incidentes de seguridad?

La GIIS tiene cuatro objetivos principales, que se describen con más precisión en el "Capítulo II: Los cuatro objetivos de gestión de información sobre incidentes de seguridad", pero el razonamiento que rige la gestión eficaz de información sobre incidentes de seguridad es mantener a salvo y seguros al personal, los programas y la organización. Una gestión organizacional sólida de riesgos de seguridad respalda un mayor acceso a población necesitada, pero también permite que las organizaciones como empleadoras cumplan sus responsabilidades de deber de cuidado para con el personal.

Las ONG tienen un deber legal (y se podría incluso decir moral) de cuidado: "El deber de cuidado es una obligación legal que se impone a una persona o a una organización por

el que se exige que respeten un cuidado normal y razonable al realizar actos (u omisiones) que presenten un riesgo razonablemente previsible de dañar a otros".[10]

El deber de cuidado hacia personal y personas no contratadas sobre las que la organización muestre determinado grado de control[11] exige que las ONG tengan sistemas y procesos de gestión de riesgos de seguridad sólidos.[12] Dicha obligación incluye aplicar una gestión de información sobre incidentes de seguridad sólida.

Un sistema de gestión de información sobre incidentes de seguridad bueno y eficaz favorecerá:

- una mejor comprensión del entorno con sus amenazas y desarrollar las medidas pertinentes, preventivas o protectoras para tratar los riesgos;
- documentar el conocimiento organizacional; y
- un mejor conocimiento y la comprensión de las tendencias en el sector y las prácticas de la comunidad, sobre todo en relación con la seguridad.

Si se produce un deterioro notable en la situación de seguridad, sobre todo en entornos de conflicto y postconflicto, es imperativo que las organizaciones tengan instaurados procedimientos que les permitan demostrar el deber de cuidado sobre todo el personal y aquellas personas de las que sean responsables.

"Si la gestión de incidentes puede verse como una herramienta de aprendizaje esencial en lo relativo a gestión de riesgos de seguridad, la gestión de información sobre incidentes se convierte en la mejor manera de demostrar la madurez de la organización al analizar eventos y tomar decisiones. Una recopilación concienzuda de datos, el análisis, los informes y los registros de incidentes que experimenta una organización, y cómo los aborda, podría ser de vital importancia dentro de la defensa de una organización en caso de que se produzca un incidente y se inicie un proceso legal contra ella".

Caso Práctico: Dennis contra el Consejo Noruego de Refugiados (Norwegian Refugee Council – NRC), 2015

El caso de Dennis contra el Consejo Noruego de Refugiados, considerado el primer caso de prueba sobre deber de cuidado dentro del sector de la ayuda, desprende algunas lecciones importantes para la gestión de información sobre incidentes de seguridad.

Resumen de los hechos:

El 29 de junio de 2012, Steven Dennis, empleado de NRC, fue herido y secuestrado, junto con otros tres compañeros, tras un ataque durante una visita VIP a uno de los campos de refugiados en Dadaab (Kenia). Cuatro días después, se liberó a los rehenes durante una operación armada de rescate que llevaron a cabo las autoridades keniatas y milicias locales. Tres años después, Dennis presentó una demanda en el Tribunal de Primera Instancia de Oslo contra su antiguo empleador, NRC, solicitando indemnización por las pérdidas económicas y no económicas tras el secuestro. Después de una revisión minuciosa de los hechos que rodearon el caso, el tribunal sentenció que NRC había cometido una negligencia grave y ordenó que la organización indemnizara a Dennis.[13]

[10] E. Kemp y M. Merkelbach, "Can you get sued? Legal liability of international humanitarian aid organisations towards their staff", *Security Management Initiative,* 2011.
[11] Incluso consultores, visitas, voluntarios, etc.
[12] E. Kemp y M. Merkelbach, "Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications", *EISF,* 2016.
[13] E. Kemp y M. Merkelbach, "Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications", *EISF,* 2016.

Lecciones extraídas:

El plan de seguridad de NRC, que se basaba en información de fuentes tanto internas como externas e incidentes, señalaba que el riesgo de secuestro era elevado. Su análisis también indicaba que el personal internacional corría más riesgo de secuestro que el personal nacional. Dicha información se utilizó para establecer medidas eficaces para tratar los riesgos, entre ellas el uso de escolta armada y la restricción de las visitas VIP a la zona. No obstante, NRC cambió los procedimientos de seguridad antes de la visita VIP conforme a un nuevo diagnóstico de los riesgos. Según las pruebas que se aportaron, el tribunal decidió que ese nuevo diagnóstico no era claro ni tenía garantías. Básicamente, se consideró que la información en la que se basó la decisión de seguridad era frágil y contradictoria respecto a la información sobre seguridad sólida que se había registrado previamente.

NRC defendía que el riesgo de secuestro se había mitigado porque no se habían producido incidentes de secuestro en la zona en los nueve meses precedentes. Sin embargo, el tribunal argumentó que la ausencia de incidentes no implica necesariamente que el riesgo haya desaparecido, sino que también se puede atribuir a fuertes medidas de tratamiento de riesgos, entre las que estaban la ausencia de visitas VIP y que casi todas las ONG que operaban en Dadaab en aquel momento utilizaban escoltas armadas. Un mejor análisis de la ausencia de incidentes podría haber ayudado a NRC a identificar el grado de riesgo real, en lugar del que se percibía.

Cuando se produjo el incidente, NRC limitó la información que compartió sobre el incidente con el personal involucrado y afectado. Se ha dicho que esa falta de transparencia por parte de la organización tuvo una gran influencia en que Dennis decidiera llevar a juicio a NRC.

Una gestión sólida de información sobre seguridad en este caso podría haber llevado a NRC a tomar decisiones de seguridad distintas sobre las visitas VIP, que hubieran evitado que se produjese el incidente.

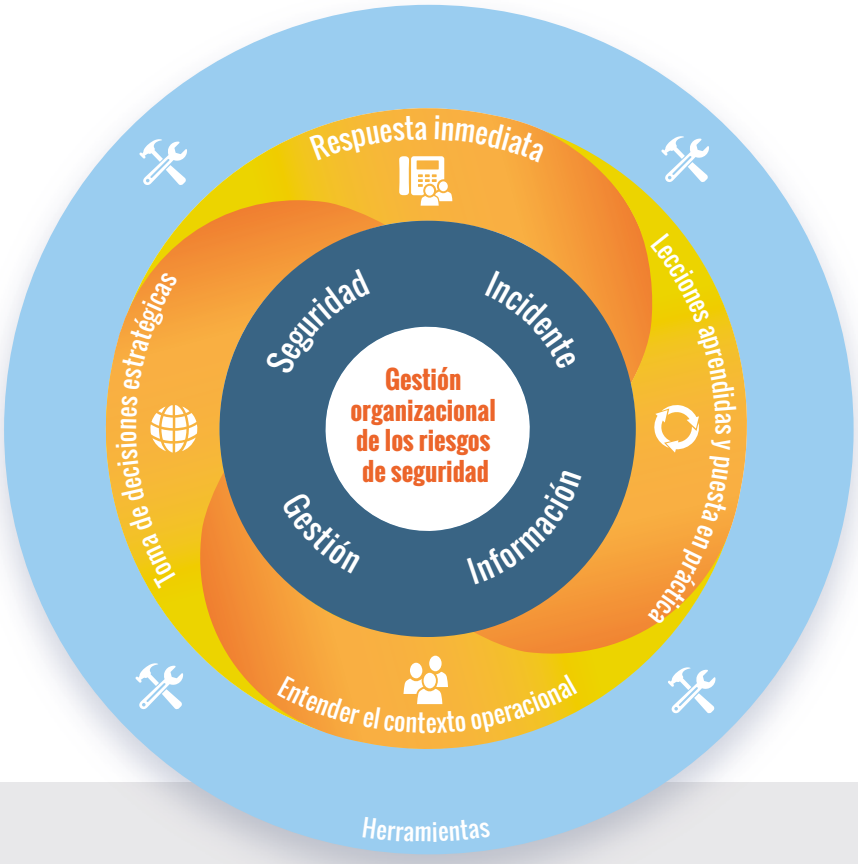
Y, si de todas maneras se hubiese producido el incidente, la documentación de información robusta sobre seguridad que se habría usado para tomar las decisiones de seguridad podría haber ayudado a NRC a defender dichas decisiones.

Un distinto enfoque sobre el intercambio de información tras el incidente también podría haber conllevado un debate menos litigioso y más abierto sobre los errores y las lecciones aprendidas entre la organización y el personal afectado.

Irish Aid ha desarrollado unas directrices para ayudar a que las organizaciones demuestren mejor su compromiso de cumplir sus obligaciones legales sobre el deber de cuidado. Dichas directrices van encaminadas a orientar a las organizaciones sobre cómo alcanzar un grado elevado de profesionalidad en el cumplimiento de los objetivos de su misión. Cada tema va con acciones clave, indicadores y notas orientativas. Adherirse a estas directrices debería ayudar a asegurar que una organización cumple sus responsabilidades de deber de cuidado y de demostrar que los procedimientos para reportar incidentes de seguridad incluyen a las personas del rango correcto, de la manera correcta y en el momento correcto. El Ministerio de Asuntos Exteriores, la Unidad de Estabilización y el Centro de Operaciones de Paz Internacionales (ZIF) de Suiza también han publicado recientemente directrices sobre el deber de cuidado. Se pueden encontrar aquí.[14]

[14] Irish Aid, *Irish Aid Guidelines for NGO Professional Safety & Security Risk Management.* ALNAP, 2013.

CAPÍTULO II: LOS CUATRO OBJETIVOS DE LA GESTIÓN DE INFORMACIÓN SOBRE INCIDENTES DE SEGURIDAD



El presente capítulo ofrece una visión general de los cuatro principales objetivos de la gestión de información sobre incidentes de seguridad y los pasos clave para cumplirlos. Este capítulo abarca:

- Objetivo uno: respuesta inmediata
- Objetivo dos: lecciones aprendidas y en práctica
- Objetivo tres: entender el contexto operacional
- Objetivo cuatro: toma de decisiones estratégicas

- Todas las herramientas son pertinentes para este capítulo.

I. OBJETIVO UNO: RESPUESTA INMEDIATA

El presente apartado aborda la gestión de información sobre incidentes de seguridad con la finalidad de fundamentar la reacción y la respuesta inmediatas a un incidente de seguridad. Este apartado abarca:

- 1.1 Pautas sobre cómo reportar un incidente: qué, cuándo, cómo y a quién
- 1.2 Manejar el estrés
- 1.3 Proceso de seguimiento de incidentes de seguridad
- 1.4 Comunicación
- 1.5 Manejar casos delicados: violencia sexual contra el personal

Herramientas pertinentes:

- Herramienta II: Tipología de incidentes
- Herramienta III: Incidentes organizacionales o externos
- Herramienta IV: Plantilla para reportar incidentes
- Herramienta V: Matriz para analizar incidentes
- Herramienta VI: Cómo llevar a cabo una reunión informativa sobre los hechos
- Herramienta VII: Buenas prácticas para informar sobre incidentes de género y mecanismos de denuncia para informar de explotación y abusos sexuales (EAS)

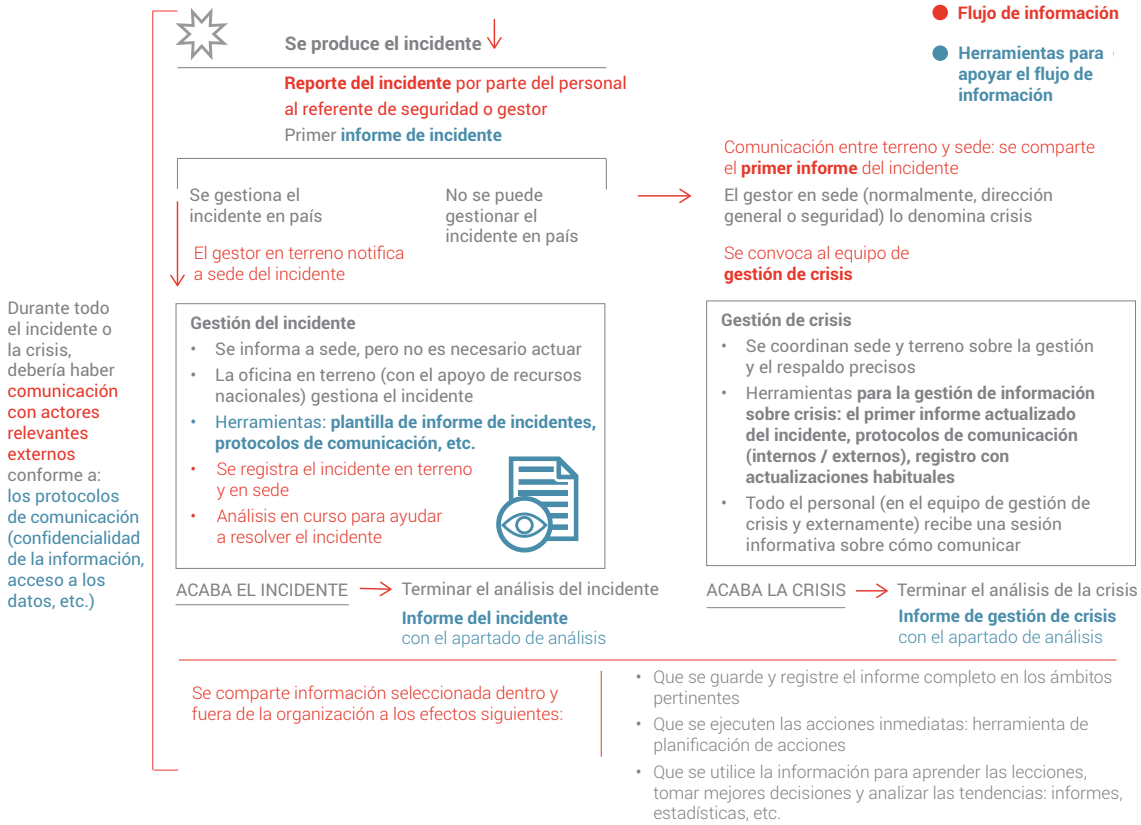
"Normalmente, el personal involucrado en un incidente hace una primera llamada de emergencia al referente de seguridad. En función de la información que se transmita de forma oral, el referente de seguridad aconseja y procura información básica, del tipo quién hizo qué y a quién, dónde y cuándo. Luego, cuando el personal está seguro, el referente de seguridad cumplimenta el informe de incidentes con más minuciosidad, utilizando la información reunida a partir de una reunión informativa adecuada con el personal involucrado en el incidente".

Uno de los principales objetivos de la gestión de información sobre un incidente de seguridad es fundamentar la reacción y la respuesta inmediatas a un evento. La finalidad es asegurar que quienes toman las decisiones y el personal afectado o involucrado buscan y utilizan dicha información para fundamentar la respuesta inmediata al incidente. Eso suele producirse en el ámbito de terreno o país, durante el evento o poco tiempo después del mismo.

La información que se registra y se reporta debería ayudar a identificar el apoyo que precisa el personal afectado y si la organización necesita aplicar algún cambio inmediato en sus operaciones, como restringir los movimientos o suspender temporalmente sus operaciones. Existe un vínculo directo entre la información requerida y las opciones de respuesta que deberían considerarse.

Cuando se produce un incidente, el personal debería dar prioridad a reportar, responder y registrar.

Las organizaciones precisan de un flujo de información eficaz que asegure que todo el personal pertinente en sede, oficinas regionales, oficinas nacionales y en terreno recibe la información necesaria y que la información desencadena los mecanismos de respuesta adecuados. El diagrama siguiente[15] muestra el posible flujo de información dentro de una organización tras un incidente de seguridad.



15 Este diagrama proviene de los cursos de introducción a la seguridad de RedR UK.

Se puede compartir la información que sea necesaria y adecuada sobre el incidente con otras organizaciones que trabajan en la misma zona o país para permitir que puedan tomar medidas de precaución para prevenir que se vuelva a producir el incidente.

En la gestión de información sobre incidentes de seguridad, resulta esencial un buen reporte y registro de un incidente justo después de que se produzca.

Recuerde que la finalidad del informe inmediato es ofrecer enseguida respaldo al personal.

1.1 Pautas sobre cómo reportar un incidente: qué, cuándo, cómo y a quién

Las organizaciones deberían dar instrucciones al personal sobre la gestión de información sobre incidentes de seguridad y deberían empezar por orientar con claridad sobre el reporte de incidentes.

> *"Los procedimientos para reportar incidentes se suelen abordar dentro del apartado de los SOP en un plan de seguridad. Algunas organizaciones han decidido elaborar un documento independiente para abarcar la política sobre reporte de incidentes de la organización y dar pautas al personal en todos los ámbitos de la organización (desde sede hasta terreno) que enlazan con otros documentos sobre políticas (recursos humanos, código de conducta, política de seguridad, etc.)".*

Establecer un protocolo de reporte de incidentes eficaz permite al equipo gerente:

- apoyar a las personas afectadas;
- percibir patrones y tendencias en los incidentes;
- mejorar la formación, los procedimientos y las estructuras físicas; y
- asignar recursos de forma adecuada.

Es importante que el personal sepa a quién debería reportar y que los procedimientos para reportar incidentes se corresponden con la estructura para reportar, así como qué sucede luego. La tabla siguiente muestra los pasos clave en el reporte y el análisis de información sobre incidentes de seguridad y unos marcos temporales aproximados a modo de orientación:

Cuándo	Paso	Acciones
Justo después de que se produzca el incidente	Descripción breve y cronológica de los hechos	Se realiza el informe sobre el incidente, se ejecutan las acciones de respuesta inmediata.
	Análisis preliminar de los riesgos	
Tras la respuesta inmediata al evento	Reunión informativa sobre los hechos tras el incidente: ¿cuáles son los hechos / análisis que han de revisarse / añadirse al informe del incidente de seguridad realizado tras introducir nuevos elementos / información?	Se realizan modificaciones en el informe (o los informes) de incidentes de seguridad ya presentado para incorporar información nueva. Se diseña un plan de acción. Se vuelven a evaluar los SOP. Se informa sobre las acciones emprendidas a la persona que reporta el incidente y a otras afectadas del personal.
	Nuevo análisis de los riesgos, por ejemplo, capital humano, financiero y material, operacionales, legales, de imagen / reputación, etc., y acciones que se han emprendido o se han de emprender para mitigar dichos riesgos.	
En las semanas posteriores al incidente	El referente de seguridad o el responsable designado se aseguran de que se emprenden las acciones y determinan si el análisis anterior era preciso.	Si fuera necesario, se actualizan los informes de incidentes. Se revisa el plan de acción y, bien se considera logrado, bien se elabora uno nuevo. Todo SOP actualizado se mantiene o se vuelve a las condiciones anteriores. Se informa al personal afectado.
	Se decide si el incidente está "cerrado" a efectos de la gestión de incidentes. Si no, se debería elaborar otro plan de acción.	

Qué reportar

La mayoría de las organizaciones utilizan una definición amplia de incidentes de seguridad a efectos de reporte. Es importante que esta definición esté unificada en toda la organización para ofrecer coherencia y es importante incluir todos los incidentes: críticos, no críticos y conatos. Véase Introducción– Definiciones clave para consultar las definiciones relativas a la gestión de información sobre incidentes de seguridad.

Una organización puede verse afectada por distintos tipos de incidentes que no estén directamente vinculados a cuestiones de seguridad (por ejemplo, de salud y fortuitos). Será la organización quien decida si se deben reportar y registrar dichos casos a través de los mismos mecanismos. De lo contrario, se debería dejar claro al personal cuál es el proceso alternativo para incidentes de salud y fortuitos. Si se combinan dentro del mismo sistema de registro, se debería incluir una indicación clara, en forma de etiquetado de datos, para permitir que los análisis se centren en todas las categorías o solo en las seleccionadas de seguridad o las de salud y fortuitos.

"Si existen dudas, se debería reportar el incidente al responsable de seguridad, al referente de seguridad o la oficina central. Ese personal decidirá cómo hacer seguimiento del incidente".

No se puede definir todo el abanico de situaciones que pueden constituir un incidente de seguridad. Por lo tanto, se define el término con amplitud e incluye, sin ser exhaustivo:

- todos los delitos contra la plantilla y los bienes de una organización (por ejemplo, robo, allanamiento, hurto, asalto de vehículos, secuestro, etc.);
- todos los casos en los que se amenace a la plantilla de la organización a mano armada o con actos de violencia;
- todos los casos de acoso o de conducta amenazante, del tipo que sean;
- actos de guerra y conflicto armado, como bombardeos, minas, disparos o agresión militar;
- saqueo, ataques contra la propiedad y vandalismo;
- todos los casos en los que la plantilla de la organización pueda estar involucrada en actividades ilegales;
- toda violación de la normativa sobre seguridad de la organización;
- todos los casos de intento de soborno hacia las organizaciones para acceder a localidades, caminos o población afectada, lleguen a consumarse o no;
- amenazas internas y casos de fraude dentro de la organización.

Además, se debería aclarar cuándo deben reportarse incidentes que se producen fuera de las horas de trabajo del personal nacional o durante el tiempo personal del equipo internacional. Unas buenas prácticas incluirían el reporte de todos los incidentes, incluso fuera de las horas laborales habituales, ya que mejora el análisis de contexto. No obstante, en esas circunstancias los procedimientos de reporte pueden ser distintos.

"Dar ejemplos de incidentes de seguridad que se deberían reportar serviría para que el personal pueda identificar qué constituye un incidente. La categorización no es necesaria al principio del proceso, pero ayudaría al personal a entender si debería reportar. Las personas precisan de ejemplos que sean pertinentes en su área de operaciones. También se puede decidir tratar cada cierto tiempo una categoría de incidentes que el equipo no conozca muy bien. Los casos prácticos son abundantes".

Para acceder a una lista completa de los tipos de incidentes, véase "Herramienta II: Tipología de incidentes".

Las organizaciones necesitan dejar claro al personal si el reporte de incidentes debería abarcar también aquellos que son ajenos a la ONG, es decir, que afecten a otras organizaciones. A menudo, las organizaciones se centrarán en el reporte y el registro de incidentes organizacionales (es decir, incidentes que afecten directamente a la organización, su personal, sus bienes y su reputación) y no incluyen incidentes externos en su sistema de reporte y registro. Los eventos externos se suelen monitorear en terreno para no perder información importante sobre el contexto, pero la organización debe definir qué constituye un incidente que afecta a la organización y el procedimiento que se seguirá para informar de manera formal sobre eventos externos. Debido al tiempo que lleva esto, las organizaciones pueden confiar en organismos externos que trabajan para la comunidad de ONG para el registro y el reporte de eventos externos.

"A menudo es labor de la misión en terreno supervisar y registrar este tipo de incidentes, dentro de sus indicadores de diagnóstico de riesgos, y no quedan registrados en las estadísticas globales de la organización".

Véase "Herramienta III: Incidentes organizacionales o externos".

Para reportar un incidente, una plantilla favorece que se mantenga una coherencia en los informes. Dicha plantilla puede ser un documento de Word, una hoja de cálculo, una plataforma en línea etc., y debería incluir:

- persona(s) que escribe(n) el informe (incluyendo sus datos de contacto, cargo(s) y fecha);
- qué ha sucedido (descripción y tipología del incidente);
- víctima(s) (nacionales, internacionales, sexo, edad, etc.);
- tipo de trabajo que se desarrollaba;
- cuándo se produjo el incidente;
- dónde se produjo el incidente;
- si el incidente fue accidental o deliberado, y detalles sobre ello, sobre todo en el último caso;
- decisiones adoptadas, acciones de seguimiento (aplicadas o recomendadas) y análisis.

Si un incidente precisa de respuesta urgente, se puede orientar al personal para asegurar que da prioridad a las seis preguntas clave:

- quién está involucrado;
- qué ha sucedido;
- dónde se produjo el incidente;
- cuándo se produjo el incidente;
- qué ha hecho usted al respecto;
- qué ayuda se necesita.

Véase: "Herramienta IV: Plantilla para reportar incidentes", que contempla la información inmediata más solicitada para la gestión de información sobre incidentes de seguridad y el análisis preliminar.

Véase: "Herramienta V: Matriz para analizar incidentes" para consultar otras preguntas y elementos que se pueden añadir más adelante para ayudar a un análisis en profundidad.

La coherencia al escribir informes sobre incidentes de seguridad puede mejorarse mediante la formación del personal. Las pautas siguientes sobre cómo describir un incidente pueden ponerse a disposición del personal junto con una plantilla de informe sobre incidentes.

Idioma	Hay que usar términos que sean concretos y describan con claridad la conducta que se produjo. Se deben especificar los detalles y no suponer que otras personas van a entender generalidades. Por ejemplo, se debe evitar utilizar palabras tales como "agresiva", "disgustada" o "alterada". En su lugar, es mejor relatar qué conducta se observó que llevó a considerar que la persona estaba siendo agresiva, que estaba disgustada o alterada. Hay que recordar que la descripción del incidente es en lo que se apoyarán otras personas para conseguir información sobre las personas involucradas y sobre el incidente. Es importante asegurarse de que el informe no traslada imágenes negativas sobre las personas involucradas. El informe tiene la capacidad de influir en otras personas, así que debe prestarse atención para que esté bien elaborado y ofrezca una narración objetiva del incidente. Revise su informe antes de entregarlo para asegurarse de que no ha utilizado terminología parcial ni deja preguntas sin respuesta.
Fiabilidad de la observación	¿Otras personas que escucharan o vieran el incidente estarían de acuerdo con su narración por escrito? Si alguna otra persona ha estado involucrada en el incidente o lo ha presenciado, es aconsejable consultar a esa persona para asegurarse de que el informe coincide con lo que ella ha observado. Personas distintas tendrán diferentes percepciones de un incidente y si se ignora su visión, puede ser negativo. Además, es importante percatarse de que los recuerdos de las personas cambian con el tiempo.
Objetividad	Al escribir un informe sobre incidentes de seguridad respecto a un evento actual, debe hacerse hincapié en mantener toda la objetividad posible y en evitar que una situación precedente influya en él. La persona que escribe el informe sobre el incidente, lo hace en posición de registradora, no de juez. Por lo tanto, hay que asegurarse de que el informe no contiene declaraciones moralistas, sarcasmo ni comentarios condescendientes.
Causa del incidente	Si no se cree tener información objetiva, puede manifestarse la opinión propia, siempre que se haga una clara distinción entre lo que es opinión y lo que son hechos. Aun si se desconoce la causa real de un incidente después de que se haya intentado averiguar, se debería aportar toda la información que se tenga sobre lo que sucedió antes o durante el evento, ya que esto puede ofrecer pistas a quien lo lea. Si quien reporta en realidad no fue testigo del incidente, hay que asegurarse, no obstante, de manifestar que la información proviene de lo que se ha reportado y quién lo ha reportado.

Cuándo reportar
El momento preciso y el grado de minuciosidad del informe dependen de la categoría del incidente:

- **Los incidentes que requieren acción inmediata**: deberían reportarse enseguida a efectos de pedir apoyo e instrucciones adicionales. Los incidentes críticos que suponen una amenaza considerable o vigente para el personal, los bienes o los programas de la organización se suelen considerar urgentes a efectos de informar y responder de inmediato.
- **Incidentes que no precisan de una acción inmediata:** los incidentes o conatos que reflejen inseguridad o un cambio en el entorno de amenazas, pero que no suponen un riesgo inmediato para el personal, los bienes o los programas de la organización, suelen no ser urgentes a efectos de reportar y, por lo tanto, pueden incluirse en un informe diario o semanal planificado a un superior inmediato o al referente de seguridad.

Los informes sobre incidentes pueden irse completando en varias etapas según se vaya disponiendo de más información.

De inmediato: los informes inmediatos sobre incidentes se realizan en cuanto es seguro hacerlo, a menudo por radio o por teléfono. Una situación puede ser confusa en un principio, así que debería darse un tiempo para diagnosticar qué acaba de suceder, las condiciones de seguridad del personal y de otras personas involucradas, y de qué ayuda se precisa. Al reportar sobre un incidente por teléfono o por radio, el personal debería hablar con claridad, precisión y concisión. Si no se pueden dar todos los detalles (a causa de una falta de tiempo o porque no sea seguro hacerlo durante un incidente en curso), aporte la información que le sea posible para provocar la respuesta adecuada. Incluso el intercambio de información más breve puede salvar vidas.

El personal que tenga más probabilidades de recibir informes inmediatos sobre incidentes (como son los operadores de radio, superiores inmediatos y coordinación) debería recibir formación sobre cómo responder. Conocer qué preguntas hacer y tener empatía con quien reporta puede tener un gran impacto en la eficacia de las respuestas y en la recuperación de las personas afectadas.

En las horas y los días siguientes: algunos incidentes pueden requerir un informe de seguimiento del incidente, o varios. Eso se puede hacer tantas veces como sea preciso, con la frecuencia y la minuciosidad que se determine en la fase inicial y se puede revisar con regularidad. En una situación de seguridad en curso, la coordinación o la autoridad designada deberían mantener un documento en el que se registren diariamente las actividades. Eso no solo serviría para mantener un registro de decisiones y actividades para ir mejorando la gestión de la situación, sino que también aportaría la información necesaria para actualizaciones y, en última instancia, respaldaría el aprendizaje organizacional. La información debería compartirse por escrito cuando sea posible, para reducir los riesgos de errores de comunicación y malentendidos. Eso también ayuda a las personas bajo estrés a organizar mejor sus pensamientos. Véase más adelante el apartado "Manejar el estrés".

Una vez se ha estabilizado o se ha "cerrado" el incidente: algunos incidentes pueden precisar de un informe completo / definitivo sobre el incidente de seguridad, normalmente por escrito. En cuanto sea adecuado hacerlo, se pedirá a las personas involucradas que relaten por escrito el evento y las acciones que se realizaron. Si la oficina en terreno necesita tomar medidas concretas para tratar el riesgo, incluso corregir procedimientos existentes, formación, asignación de recursos, etc., deben manifestarse con claridad estas disposiciones de seguimiento, identificarse la(s) persona(s) responsa-

ble(s) de su puesta en práctica y especificarse el marco temporal. Los informes de seguimiento posteriores deberían registrar el progreso de las acciones recomendadas hasta su finalización. El informe completo sobre el incidente debería ser la base para un nuevo diagnóstico o para la actualización de los SOP pertinentes de la organización. Esto se tratará en más profundidad en el "Objetivo dos".

Debería transmitirse al personal qué esperar y qué preguntar al reportar un incidente. Se deberían identificar con claridad los desencadenantes y explicar de antemano y con claridad las respuestas. Para minimizar que se dejen incidentes sin reportar, el procedimiento debería ser claro pero flexible: el reportar puede ser sencillo o puede ser más exhaustivo cuando así se precise.

Cuando sea posible, es mejor elaborar el informe del incidente justo después del incidente, cuando los hechos todavía están frescos. Sin embargo, y en función de la gravedad del incidente, el personal puede estar todavía emocionalmente implicado en ese momento, así que puede ser de ayuda que otra persona revise el informe antes de presentarlo.

Cómo reportar

El procedimiento para reportar incidentes debería identificar el canal de comunicación más seguro, sin perder de vista los tres momentos distintos para reportar.

El procedimiento para reportar incidentes debería aclarar si se deben usar radios, teléfonos satelitales o correos electrónicos y asegurarse de que el personal tiene formación sobre el uso seguro de dispositivos (uso de encriptado, si fuera necesario). Se debería informar al personal sobre la necesidad de asegurar la confidencialidad en el reporte de incidentes.

El procedimiento de reporte también debería aclarar las diferencias en los canales para reportar distintos tipos de incidentes. Por ejemplo, un robo y un incidente de violencia sexual requerirán de distintos mecanismos de reporte. Los incidentes que precisen de una respuesta administrativa, por ejemplo, reclamaciones al seguro, reposición de activos, etc., también pueden precisar de un procedimiento específico. Véase más adelante en este apartado "Manejar casos delicados: violencia sexual contra el personal" para saber más sobre el reporte de casos delicados.

Se pueden desarrollar distintos procesos para reportar incidentes, en función de la naturaleza del incidente, es decir, de la confidencialidad y de la sensibilidad que demande. Aun así, es importante destacar que el canal no debería ser la principal cuestión (salvo que haya una seria preocupación sobre interceptación o privacidad). En particular, si se trata de incidentes que precisan de una respuesta urgente, lo que prima es que la información se traslade a los destinatarios previstos lo más rápido posible para que las personas afectadas reciban la ayuda que necesitan.

También resulta fundamental que el personal respete la confidencialidad de la información internamente, para asegurar que no haya interferencias en la gestión del evento. Los referentes pueden usar la tabla "Categorías de información" en el "Objetivo tres".

A quién reportar

Todo el personal debería ser capaz de reportar un incidente y el procedimiento para reportar incidentes de la organización debería indicar con claridad a quién podría reportar incidentes el equipo. Por ejemplo, puede ser a través de correo electrónico a una persona concreta o mediante un sistema automático de reporte en línea que envíe informes de manera automática al personal pertinente dentro de la organización.

La tabla siguiente da ejemplos de personas y sus tareas y responsabilidades correspondientes en caso de incidente:

Quién	Tareas o responsabilidades
Todo el personal	Debería reportar el incidente a su superior o al referente de seguridad designado.
Referente de seguridad (en terreno o país) Responsable (en terreno o en oficina de país)	Al recibir el informe inicial de incidentes, debería asegurarse de que se da apoyo al personal afectado, informar a la oficina de país / región si se necesita apoyo, hacer seguimiento del incidente y organizar una reunión informativa sobre el incidente y su análisis. Debería proponer medidas operativas inmediatas a la gestión regional. Asegurar la comunicación con el personal de terreno, si fuera preciso.
Referente de seguridad de país o región Responsable (en país o región)	Al recibir la información de terreno o de la oficina del país, debería velarse por apoyar a las personas afectadas, transmitir información a sede si fuera preciso respaldo, asegurar el seguimiento y las reuniones informativas potenciales si debe retirarse al personal de la ubicación en terreno. Hablar y acordar medidas operacionales inmediatas potenciales con la dirección de país o de terreno.
Responsable o asesor de seguridad (en sede)	Tras recibir información de la oficina regional o de país, debería asegurar apoyo de sede si así se solicita. Hará de enlace con quienes deciden en sede para validar el grado de gestión adecuado.
Gerencia y dirección ejecutiva / dirección general (en sede)	Recibirá la información sobre incidentes del responsable / asesor de seguridad en sede o de responsables regionales o país. Debería asegurar el seguimiento de acciones concretas en sede, si fueran precisas. Garantizar la comunicación sobre el incidente al personal de sede, si eso fuera preciso.

Cada organización debe adaptar el flujo de información relativo a un incidente para que refleje los cargos del personal, la jerarquía y la presencia operacional.

Las responsabilidades del personal en el reporte y la gestión de información sobre incidentes de seguridad deberían quedar claras en las políticas (por ejemplo, en las políticas de gestión de riesgos de seguridad, en las políticas sobre reporte de incidentes, el código de conducta, etc.) y en los documentos sobre procedimientos. Estas funciones deberían subrayarse durante el proceso de bienvenida y revisarse con regularidad durante todo el ciclo laboral.

1.2 Manejar el estrés

El personal que reporta un evento mientras se está produciendo o justo después tiene muchas probabilidades de sufrir un estrés considerable. Se recomienda que el personal que reciba el primer informe verbal procure:

- mantener la calma;
- identificar a la persona que está haciendo el informe;
- velar por la seguridad de las personas involucradas en el incidente;
- dar prioridad a la información necesaria, por ejemplo: estado, qué se ha hecho, qué hay que hacer de inmediato;
- recabar información conforme a la plantilla para reportar incidentes;

- tranquilizar a la persona que está reportando el incidente y acordar los siguientes contactos.

La finalidad de este primer informe es conseguir los hechos necesarios para fundamentar una respuesta inmediata. No se trata de afrontar emociones (a menudo denominada "ventilación emocional"). La ayuda psicológica y la posibilidad de afrontar emociones para las personas tras un evento traumático deberían llevarla a cabo profesionales cuando se demande. Este momento de afrontar emociones (o ventilación) es de gran pertinencia en incidentes críticos, pero algunos incidentes no críticos también tendrán efectos traumáticos en las personas involucradas. La organización debería asegurarse de que se da apoyo al personal en ambas situaciones.

1.3 Proceso de seguimiento de incidentes de seguridad

Todos los incidentes de seguridad deberían tener un seguimiento para asegurar que se capta toda la información relativa al incidente para así fundamentar lecciones aprendidas, actualizaciones de contexto y decisiones.

El proceso de seguimiento de incidentes proporciona actualizaciones del informe del incidente a raíz de nuevos hechos u otros que puedan surgir. Es también muy útil seguir este proceso cuando se dan cambios de personal en puestos clave y relevantes, por ejemplo, la coordinación de seguridad. En algunos casos, esto puede requerir que se elabore una nueva versión del informe del incidente.

Este proceso debería captar cada nuevo evento o cada nueva acción que se produzca durante la gestión del incidente, hasta que finalice el incidente y se cierre.

Los incidentes críticos, como el secuestro de personal, pueden prolongarse bastante tiempo y se dispone de nueva información de manera esporádica. Es importante que la organización capte esta nueva información de una manera significativa para poder analizarla y explicarla en el proceso de decisión. Eso debería formar parte del plan de gestión de crisis.

Se deberían definir procesos de seguimiento para todos los incidentes, de forma que se asegure que la información y las lecciones aprendidas no se pierden ni dejan de tener prioridad en entornos cambiantes.

Reunión informativa sobre los hechos

Debería celebrarse una reunión informativa sobre los hechos tras el incidente, después de que el personal involucrado haya recibido el apoyo adecuado. Se recomienda que esta reunión se realice en las 48 horas posteriores a un evento de seguridad. La extensión de la reunión variará en función de la naturaleza y de la complejidad del incidente.

Al organizar una reunión informativa sobre hechos a efectos de recopilar información, es importante tener presentes los principios básicos de los Primeros Auxilios Psicológicos (PAP).[16]

- llevar a cabo la reunión solo después de que se haya salvaguardado la seguridad física y psicológica básica de la persona;
- la reunión debería tener lugar en un sitio seguro;
- el empoderamiento de la persona afectada debe ser el fin;
- ser claro sobre el proceso, las expectativas y las acciones de seguimiento.

[16] Para obtener más información sobre los PAP, véanse las pautas de la Organización Mundial de la Salud (OMS) aquí.

Es importante recordar que el impacto de conatos y pequeños incidentes en personal concreto puede ser mucho más grave que el impacto en la organización. Por ejemplo, sufrir acoso por parte de miembros de la comunidad o un atraco fallido puede afectar profundamente a una persona.

Véase "Herramienta VI: Cómo llevar a cabo una reunión informativa sobre los hechos" para más pautas sobre cómo organizar una reunión informativa a efectos de recopilar y analizar información. Cabe percatarse de que esto no es un intento de formar a quien lea este documento sobre los PAP ni sobre cómo convertirse en investigadores profesionales, sino una lista de consejos para llevar a cabo entrevistas seguras y útiles para averiguar los hechos a efectos de reportar incidentes.

Fuentes de información

Se debería verificar la precisión de la información recabada hablando con partes interesadas internas y externas para recabar distintas perspectivas, es decir, triangular la información obtenida.

Un elemento crítico al analizar la información de seguridad es la credibilidad de la información y la validez de la fuente.

La siguiente matriz de fiabilidad y validez es una herramienta sencilla que puede ser de ayuda en ese proceso de verificación.[17]

Fiabilidad de la fuente

	Calificación	Descripción
A	Absolutamente fiable	No cabe duda sobre la veracidad, la credibilidad y la competencia de la fuente. Historial de fiabilidad absoluta.
B	Normalmente fiable	Dudas menores. Historial de información sobre todo válida.
C	Bastante fiable	Dudas. Ha aportado información válida en el pasado.
D	A menudo no fiable	Dudas considerables. Ha aportado información válida en el pasado.
E	No fiable	Le falta veracidad, credibilidad y competencia. Historial de información no válida.
F	No se puede juzgar su fiabilidad	Información insuficiente para valorar su fiabilidad. Puede ser fiable o no serlo.

Validez de la información

	Calificación	Descripción
1	Confirmada	Lógica, coherente con otra información pertinente, confirmada por fuentes independientes.
2	Probablemente cierta	Lógica, coherente con otra información pertinente, no confirmada.
3	Posiblemente cierta	Razonablemente lógica, coincide con otra información pertinente, no confirmada.
4	Dudosamente cierta	No es lógica, pero es posible, no hay más información al respecto, no confirmada.
5	Improbable	No es lógica, contradice otra información pertinente.
6	No se puede juzgar su veracidad	No se puede determinar la validez de la información.

[17] Ejército de Estados Unidos. *Field Manual No. 2-22.3. Human Intelligence Collector Operations,* 2006.

Ejemplo: una calificación A3 es de una fuente muy fiable, pero la información solo es posiblemente cierta; mientras que una calificación D1 es que una fuente de información normalmente no fiable ha aportado información confirmada (verificada por otras fuentes).

Esta matriz es más fácil de usar si una organización cuenta con un mapa actualizado de actores. La fiabilidad de las fuentes es algo que debe observarse durante un largo periodo de tiempo; el referente de seguridad debería contrastar regularmente cualquier información sobre las operaciones obtenida para evaluar la fiabilidad de las fuentes y la validez de la información recibida.

Puede que las organizaciones reciban información de seguridad de otras ONG o de personas de una forma indirecta, a través de terceros o eludiendo a las partes interesadas habituales. Esto alguna vez se cita como flujo de información diagonal. Por ejemplo, testigos del asalto a un vehículo de una ONG, sin forma de contactar directamente con la organización, llaman en su lugar al consorcio. El consorcio transmite el mensaje a la dirección de seguridad de la ONG, que a su vez transmite el mensaje a la oficina de país en el terreno.

1.4 Comunicación

Se debería elaborar una política organizacional que señale qué información sobre seguridad debería compartirse y con quién, tanto externa como internamente y, en concreto, justo después de un incidente; y que identifique a la persona responsable de compartir la información en los distintos ámbitos de una organización (desde terreno hasta sede) y fuera de la misma. Esa política debería abarcar asuntos de confidencialidad para proteger la identidad de las personas afectadas y a otras partes interesadas importantes, según proceda.

Se recomienda que se identifique a una persona de referencia de cada ámbito necesario de la organización (desde terreno hasta sede) como responsable de las comunicaciones externas para asegurar que se realizan bien y a tiempo.

"Se debe abordar la ética de utilizar información privilegiada en zonas de conflicto durante la gestión de incidentes de seguridad. Un referente de seguridad debería ser capaz de filtrar información específica a efectos de adherirse a la ética al tiempo que se difunde la información pertinente de manera eficaz para asegurar lo mejor posible la seguridad del personal y de la misión de la organización".

Las organizaciones pueden utilizar mecanismos de coordinación para recabar información e introducirla en sus análisis de contexto y su gestión de incidentes, tanto a través de procedimientos formales como mejorando las relaciones informales profesionales con partes interesadas clave.

La jefatura de un equipo o referente de seguridad debería determinar el grado de información que se ha de compartir tanto dentro como fuera de la organización, conforme a las políticas de la misma.

Comunicación con las autoridades

Respecto a muchos incidentes, puede ser adecuado compartir lo que se sabe con la policía o con otros cuerpos de seguridad, sobre todo durante un incidente crítico como un bombardeo, un atentado, un secuestro o un ataque, para ayudar a resolver el incidente, reducir su impacto o mitigar la probabilidad de que un evento parecido afecte a otros.

El acuerdo y la colaboración con el Gobierno del lugar suele ser un elemento clave para la eficacia de las operaciones de una ONG. Por lo tanto, en algunos contextos, se recomienda encarecidamente a las organizaciones que informen de los incidentes a las autoridades locales y a la policía. Sin embargo, dicha información se debería basar en el contexto, teniendo en cuenta diversos factores, y se debería sopesar antes de que se produzca un incidente para incluirse en los SOP de la organización o en sus planes de contingencia.

Comunicación con los medios

Los incidentes de seguridad críticos o de perfil elevado pueden atraer mucho la atención y la presión de fuentes externas, en particular de los medios. Otros incidentes también pueden interesar a los medios de comunicación, en función de la agenda que tengan (por ejemplo, sus tendencias al publicar, etc.).

La preocupación primordial siempre debería ser la seguridad de las personas directamente afectadas por el incidente y el bienestar de sus compañeros y familiares. Se puede poner en peligro la vida de otras personas al compartir información. Sin embargo, la velocidad a la que viaje la información correcta puede salvar vidas. La forma en la que responde una organización, no solo ante el incidente, sino también ante la información y las opiniones sobre el mismo, es importante en la protección del personal y de la organización.

Recuerde: una vez que la información es de dominio público, no se puede retractar, mientras que siempre se pueden publicar detalles adicionales más tarde.

Las tareas organizacionales clave se deberían adaptar a la escala del incidente con el que se está tratando y la responsabilidad de las mismas también se debería asignar durante la fase de planificación. Véase la tabla siguiente para orientar al personal responsable en la preparación de la estrategia de comunicaciones externas sobre seguridad de una organización, en concreto al tratar con los medios:

	Asegurarse el control de la información.
	Seguir monitoreando información disponible sobre el evento de todas las fuentes.
	Dar prioridad al monitoreo de redes sociales para mantenerse al tanto de la información disponible sobre el incidente que sea de dominio público. Monitorear las fuentes en idiomas de la zona, así como en el idioma de la sede y otros, según convenga.
	Identificar (o hacerlo previamente) a una persona portavoz.
	Intentar evitar que se publique. Si eso no fuera posible, corregir o eliminar historas, mensajes, imágenes y vídeos problemáticos de cualquier fuente. Explicar que esto se debe a que la atención de los medios puede poner en peligro al personal.
	Asegurarse de que las llamadas de teléfono entrantes por parte de los medios se registran con fecha y hora y que se derivan a la portavoz principal.
	Preparar mensajes clave y respuestas a las preguntas más habituales para la portavocía principal o para portavoces adicionales.
	Informar y practicar con las portavocías principales / adicionales.
	Elaborar un borrador por escrito de una declaración para que la portavocía la pueda leer si fuera necesario; eso sirve para que las personas no se desvíen del mensaje.
	Atenerse a los hechos y no dar información “que no puede constar en ningún lado”.
	Coordinar la comunicación interna y la externa para que coincidan.
	Registrar las decisiones que se han tomado y los factores que han influido en dichas decisiones.

	Asegurarse de que se ve la ONG como una fuente de información creíble, autorizada y fiable.
	Decir la verdad, evitar utilizar la fórmula "sin comentarios". No hacer especulaciones. Si se precisa de una respuesta, pero la información es limitada, mejor emitir una declaración.
	Respetar a los periodistas y sus plazos de entrega y devolver las llamadas de los medios.
	Invitar a los medios que llamen a consultar la página web o las redes sociales de la ONG para ver actualizaciones, Twitter, por ejemplo.
	Ofrecer a los medios que llamen incluirlos en el listado de correos de la agencia y asegurarse de que reciben todas las noticias y los comunicados que se suban a internet.
	Utilizar herramientas como Twitter para publicar información breve, con enlaces a la página web, donde se podrán encontrar las declaraciones y los comunicados de prensa.
	Asegurarse de que todo el personal que desempeña funciones en contacto con el exterior (como guardias de seguridad y conductores) conoce la respuesta adecuada a cualquier pregunta y a quién derivar las consultas.
	Siempre hay que tener en cuenta que el principal objetivo es la seguridad y la protección del personal afectado de forma directa..
	No revelar datos personales de aquellas personas afectadas o involucradas en el incidente.

Véase la guía del EISF "Gestionar el mensaje" para más herramientas y orientación, incluida la plantilla de una declaración.

Colaborar con otras agencias

Una parte importante de la postura general sobre seguridad para cualquier organización de ayuda debería ser la estrecha colaboración y un intercambio de información con otras agencias y ONG que operen en la misma zona o en áreas que se consideren pertinentes en términos operacionales.

En comunicación, la coordinación tiene especial relevancia cuando un incidente de seguridad involucra a un grupo de personas de distintas organizaciones. Para la respuesta inmediata resultará clave una coordinación previa, y se debería hablar y convenir con antelación en una gestión de incidentes y un reporte de incidentes coherentes y coordinados. Esto se puede abordar en SOP específicos.

Cuando la información sobre un incidente de seguridad no se recopila, gestiona y difunde de una forma horizontal, es difícil esbozar las amenazas de una región. Los mecanismos de colaboración en seguridad prosperan cuando tanto la comunicación vertical como la horizontal "cierran el círculo" (es decir, se retroalimentan) constantemente y cuando las partes interesadas trabajan de una manera coordinada.

Tras incidentes de seguridad, debería celebrarse con celeridad una reunión informativa sobre el incidente de seguridad con otras organizaciones pertinentes, si se considera adecuado compartir información.

El formulario en el que se reporta el incidente se podría utilizar como documento de pauta para la reunión informativa. El referente de seguridad o los responsables pertinentes deberían identificar de antemano los datos / la información más oportunos que se pueden compartir con las organizaciones. Sin embargo, en estas decisiones se

debería considerar la categoría de información en la que encajan las distintas partes del incidente (véase "Objetivo tres").

Los elementos cruciales en la reunión informativa sobre el incidente deberían centrarse en aclarar quién hizo qué, dónde y cuándo. En aras de proteger a las personas afectadas, las organizaciones no deberían revelar quién estuvo involucrado. Sin embargo, si se consideran fundamentales el grupo étnico, la nacionalidad u otros factores personales, hay que sopesar cómo puede compartirse dicha información al tiempo que se mantiene la confidencialidad. La construcción de vínculos de confianza antes de que se produzca un incidente es esencial para compartir información con matices.

Una reunión informativa posterior también se puede contemplar como una oportunidad de procurar el apoyo de otras organizaciones, ya sea apoyo logístico, asistencia, una mejor coordinación y mejorar el intercambio de información o, en circunstancias más extremas, adoptar una postura política conjunta como comunidad de ONG en un asunto específico (véase "Objetivo cuatro").

Como siempre, la decisión de compartir información debería contemplar toda repercusión posible en la seguridad del personal de la organización y de otras personas afectadas.

Cuando una organización recibe información sobre un incidente de seguridad de otra organización, en concreto sobre incidentes críticos, se aconseja:

- evitar contactar con la ONG que encabeza la gestión del incidente (si el incidente está en curso), salvo que exista información importante que compartir porque puede ayudarle a responder ante el incidente;
- evitar interferir de ninguna manera, salvo que así se solicite;
- no compartir la información con otras (la ONG afectada decide quién debería conocer la situación);
- evaluar la necesidad de poner en práctica medidas específicas para mitigar la exposición de la organización a un evento parecido, comunicar dicha necesidad a las partes interesadas internas más importantes y poner en marcha las medidas para tratar el riesgo que se hayan identificado;
- definir qué información es necesaria para explicar las medidas que se mencionan anteriormente (si fuera preciso) sin revelar información confidencial;
- intentar reducir los rumores posibles dentro de la organización al abordar las preguntas y al solicitar al personal que mantenga la confidencialidad;
- evaluar la necesidad de revisar y actualizar las medidas de seguridad para la organización.

Las organizaciones que operan en una zona parecida deberían utilizar mecanismos colaborativos para compartir información que podría ser de utilidad a otras organizaciones en el diagnóstico de un contexto de seguridad. Este tipo de intercambio estructurado de información entre distintas organizaciones se ve en más profundidad en el "Objetivo tres".

1.5 Manejar casos delicados: violencia sexual contra el personal

Algunos incidentes tienen que enfocarse con delicadeza y un cuidado particular, sobre todo en lo referente a la gestión de información sobre un incidente de seguridad. El impacto de dichos incidentes puede tener efectos multiplicadores particulares para quienes estén involucradas, la organización, y la comunidad humanitaria y de desarrollo general.

En este apartado, nos referimos a incidentes de seguridad que se suelen considerar particularmente traumáticos para la(s) persona(s) involucrada(s). A efectos de claridad,

utilizaremos el ejemplo concreto de violencia sexual contra personal de ayuda, aunque los principios y el enfoque de gestión que se trazan en este apartado se podrían aplicar a otros tipos de situaciones, incluso a secuestros o al asesinato de personal. Las directrices en este apartado se deberían utilizar en conjunción con el resto del manual y quienes las utilicen deberían reflexionar sobre el enfoque que se centra en la superviviente.

Las pruebas que reunió *Report the Abuse*[18] sugieren que en los lugares de trabajo de las ONG se produce violencia sexual, donde entra desde el acoso sexual hasta la violación, y que la mayoría de los que la cometen son compañeros de la superviviente. Las cooperantes corren especial riesgo, aunque los hombres también pueden sufrir violencia sexual.

Un informe publicado en 2016 sobre este tema descubrió que solo el 16% de las ONG humanitarias evaluadas mencionaban al menos una vez la violencia sexual como riesgo para el personal dentro de sus políticas y sus procedimientos, sin entrar en mecanismos de respuesta coherentes, delicados y centrados en la superviviente.[19]

Un gran paso para desarrollar mejores estrategias de prevención y respuesta es elaborar un sistema de gestión de la información sobre incidentes de seguridad adecuado que incorpore información sobre violencia sexual contra el personal.

La violencia sexual contra cooperantes es una amenaza grave que no solo merma la seguridad del personal de los programas, sino que también menoscaba considerablemente la eficacia y la eficiencia de las operaciones de la ONG. Es importante considerar la violencia sexual como una violación de derechos, lo que significa que se puede aplicar directamente una dimensión de protección a la gestión de tales casos.

Incidentes que quedan sin reportar: motivos y obstáculos

En todo contexto, país y cultura quedan incidentes de violencia sexual sin reportar. Existen varios motivos por los que los incidentes de violencia sexual en el contexto humanitario se quedan sin reportar:

- falta de conocimiento o ausencia de canales o procedimientos para reportarlos;
- carencia de inversión organizacional en la formación y el conocimiento necesarios para recibir informes de violencia sexual;
- pruebas o recursos legales limitados, o preocupación porque reportar el incidente no conllevará ni justicia ni condena;
- preocupación por etiquetas discriminatorias, que se culpe a la víctima o respuestas con el mito de la violación por parte de la organización y los compañeros;
- la vergüenza, la culpa o la humillación arraigadas socialmente sobre haber vivido violencia sexual;
- temor a represalias, consecuencias profesionales o personales;
- falta de confianza en el sistema.

Todos estos son motivos de peso por los que una persona puede no reportar, y la estructura y la cultura organizacionales sustentan la mayoría de ellos. Cada ONG debería reflexionar sobre la cultura que está creando y si es accesible, comunicativa, abierta a reacciones constructivas, de confianza, delicada y centrada en los supervivientes. Si se involucra al personal de todos los ámbitos en unas conversaciones productivas y seguras sobre este tema, pueden disiparse en gran medida algunas de las preocupaciones que llevan a que no se reporten los incidentes.

[18] Véase la página web de Reporte the Abuse para obtener más información: http://reporttheabuse.org/about/

[19] M. Nobert, *Prevention, Policy and Procedure Checklist: Responding to Sexual Violence in Humanitarian and Development Settings*. Report the Abuse, 2016.

"En la actualidad, no existen unas buenas prácticas que puedan seguir las ONG para prevenir la violencia sexual en sus lugares de trabajo y para garantizar que cumplen el deber de cuidado que tienen para con su personal. Tampoco se dispone de unas directrices minuciosas sobre cómo responder cuando se produce un incidente. Sin embargo, Report the Abuse está en proceso de desarrollar dichas buenas prácticas y se prevé la publicación de la primera herramienta en la primavera / verano de 2017".[20]

Consideraciones importantes sobre la violencia sexual y la GIIS:

- Consentimiento informado: en todas las etapas de recopilación y uso de la información que aporte una superviviente sobre un incidente, debe contarse con su consentimiento informado.
- Formación sobre el reporte y la gestión de incidentes de violencia sexual: conocer cómo recibir información sobre un incidente de violencia sexual y cómo responder de manera adecuada puede reducir considerablemente que se vuelva a traumatizar a la superviviente y crear confianza en las estructuras de reporte de una organización.
- Ofrecer unas definiciones claras sobre violencia sexual: informar al personal del significado, por ejemplo, de acoso sexual o de agresión sexual ayudará a establecer unas políticas más claras.

Véase "Herramienta II: Tipología de incidentes" para consultar definiciones relacionadas con la violencia sexual.

Respuesta inmediata

Cuando se reporta un incidente de violencia sexual, o terceros lo ponen en conocimiento de la organización, la primera forma de proceder debería ser siempre asegurar que la superviviente está en un lugar donde se sienta segura y que se están cubriendo sus necesidades físicas y emocionales. Una vez establecido esto, existen varias acciones recomendadas que deberían emprenderse para asegurar que la información sobre el incidente no se convierta en un rumor, empeore la situación ni ponga en peligro a la superviviente o a otro personal.

Se aconseja a los referentes que emprendan las siguientes acciones de inmediato:

- **Esclarecer los siguientes pasos:** aclarar con la superviviente qué forma de proceder querría que acometiese la organización. Esta postura debería comprobarse de manera rutinaria para ver si la superviviente sigue sintiéndose cómoda con ella.
- **Confidencialidad:** asegurar que el resto del personal que sabe del incidente no hablan de ello con quienes no lo saben. Se aconseja ofrecerles una respuesta estándar por si les preguntan; por ejemplo: "No puedo responder a esa pregunta, contacte con la dirección de la organización".
- **Comunicaciones:** establecer una línea directa de comunicación con un referente designado en sede. Las comunicaciones entre el terreno y la sede deberían gestionarlas y controlarlas solo aquellas personas designadas para ello. Dichas comunicaciones no deberían implicar varios intermediarios ni diversos sustitutos. No se debería hablar de la situación donde se pueda escuchar por casualidad dicha conversación.
- **Gestión de los medios:** actuar de forma proactiva hacia los medios de comunicación si parece que el incidente va a tener cobertura por parte de la prensa, persuadir a editores y periodistas de que utilicen, como máximo, las iniciales de la superviviente y no su nombre completo. Es conveniente acordar un nombre clave,

[20] Para obtener más información sobre los contextos de esta herramienta y sobre cómo Report the Abuse está ayudando a las organizaciones humanitarias a abordar la violencia sexual en sus lugares de trabajo, visite su página web o póngase directamente en contacto.

una palabra clave o un número de expediente para referirse a la superviviente. Toda actuación respecto a la prensa debe hablarse con detenimiento con la superviviente en el caso de que se la pueda identificar.

- **Gestión de informes:** las líneas de reporte deberían trazarse con claridad antes de que se produzca un incidente y, después, se deben seguir cuando se realice un informe. Esto debe incluir líneas de reporte alternativas en terreno, asegurándose de que existen varias personas a las que se puede informar, de distintos sexos, orientaciones sexuales (si fuera posible) y orígenes culturales. Dichas personas deben tener la formación adecuada para recibir informes de violencia sexual. También deberían existir líneas de reporte más allá del terreno para situaciones donde los cargos con más responsabilidades en terreno puedan estar implicados o no se pueda confiar en que aborden debidamente un incidente de violencia sexual.
- **Gestión de decisiones:** dado que se trata de información delicada, deben establecerse medidas específicas para asegurar que las estadísticas sobre incidentes de violencia sexual no se pierden, de forma que se incluyan medidas de mitigación y gestión en todos los ámbitos de las políticas y las prácticas de seguridad de una organización.

La información sobre cómo y a quién reportar debería estar disponible para todo el mundo con un lenguaje sencillo y claro en distintos lugares y en todas las operaciones de la organización. Eso puede comprender colocar copias físicas del proceso en cada oficina en terreno y asegurarse de que es accesible para aquellas personas sin acceso a ordenadores. Además, la información sobre el proceso de reporte debería estar disponible en todos los idiomas pertinentes para el entorno operativo. Si existe preocupación sobre el grado de alfabetización, deberían emplearse medios creativos para asegurar que todo el mundo entiende sus derechos y cómo reaccionar si se produce violencia sexual. Al desarrollar sistemas de reporte, estos deben reconocer las normas culturales del lugar y pueden ser distintos para distinto personal, por ejemplo, el nacional y el internacional.

Recopilación de información

Tras un informe inicial, debería recopilarse información adicional sobre el incidente. Seguramente, recabar la información sobre seguridad necesaria en estas circunstancias requerirá una formación y unas destrezas particulares para que se aborde el incidente con delicadeza, profesionalidad y exhaustividad, de una manera que no perjudique más a las personas involucradas.

Los siguientes consejos orientan al personal que recaba información sobre un incidente de violencia sexual:

- Al solicitar información sobre el incidente a la superviviente, hay que ir despacio y dejando tiempo para pausas y para reflexionar. Se empieza con preguntas generales abiertas hasta que se haya referido una vez una descripción íntegra de los acontecimientos. Se puede proseguir con preguntas sobre detalles concretos una vez se haya dado una explicación amplia.
- Hay que ser consciente de que solicitar esta información puede volver a ser traumático para la superviviente. Se puede facilitar el proceso concediendo el tiempo y el espacio necesarios para que la superviviente hable de su experiencia, eligiendo un lugar y un ambiente seguros y que fomenten el diálogo, y practicando la escucha activa.
- Las preguntas deberían plantearse en un entorno donde la superviviente se encuentre segura y cómoda. Se debería respetar y fomentar la opción de que la acompañe una compañera, amiga o referente de confianza. Aunque parezcan detalles menores, asegurarse de que hay agua y pañuelos ayudará a crear un entorno donde la superviviente se sienta respaldada.
- No deben formularse preguntas que perpetúen los mitos sobre la violación o la

actitud de culpar a la víctima, como serían: "¿Está segura de que eso fue lo que sucedió?", "¿Qué llevaba puesto?" o "¿Qué hizo para provocar eso?".

- Cuando sea posible, guardar la ropa o cualquier otro artículo de la superviviente puede servir para demostrar ante un tribunal que se produjo violencia sexual. Dichos artículos deberían almacenarse de la manera más limpia y cuidadosa que permitan las circunstancias.
- Si la superviviente no se ha duchado ni lavado, animarla a buscar asistencia médica, si estuviese disponible, e incluir la cuestión de que puede querer tomar la píldora del día después o la profilaxis post-exposición (PEP, por sus siglas en inglés). Hay que asegurarse de que en los SOP se incluye acceso a la píldora del día después y a la PEP y su uso.
- Tras realizar las preguntas a la superviviente, hay que asegurarse de que después va a estar en un lugar seguro con el apoyo apropiado. Aunque su función sea, principalmente, realizar las preguntas, debería de todas maneras confirmar que ella tiene acceso al apoyo psicosocial necesario o maneras de acceder a estas estructuras de apoyo; si fuera preciso, tome medidas para asegurar que pueda hacerlo.
- Mientras se realizan las preguntas, hay que reafirmar a la superviviente en todo momento de que la cree, de que se le informará sobre cada uno de los pasos siguientes y de que ni se merecía ni provocó lo que le ha sucedido.
- Tras recopilar todos los detalles pertinentes, hay que asegurarse de que esa información se almacena de forma segura en un lugar donde no será accesible ni se filtrará. Siempre que sea posible, hay que utilizar nombres clave, palabras clave o un número de expediente para referirse a la superviviente, incluso en las comunicaciones internas.

Tendemos a suponer que alguien va a estar más cómodo al tratar con una persona del mismo género. Sin embargo, ese no es siempre el caso y se deberían ofrecer opciones. Dichas opciones deberían incluir, si fuera posible, diversas orientaciones sexuales, nacionalidades, orígenes raciales, religiones y otros perfiles diversos.

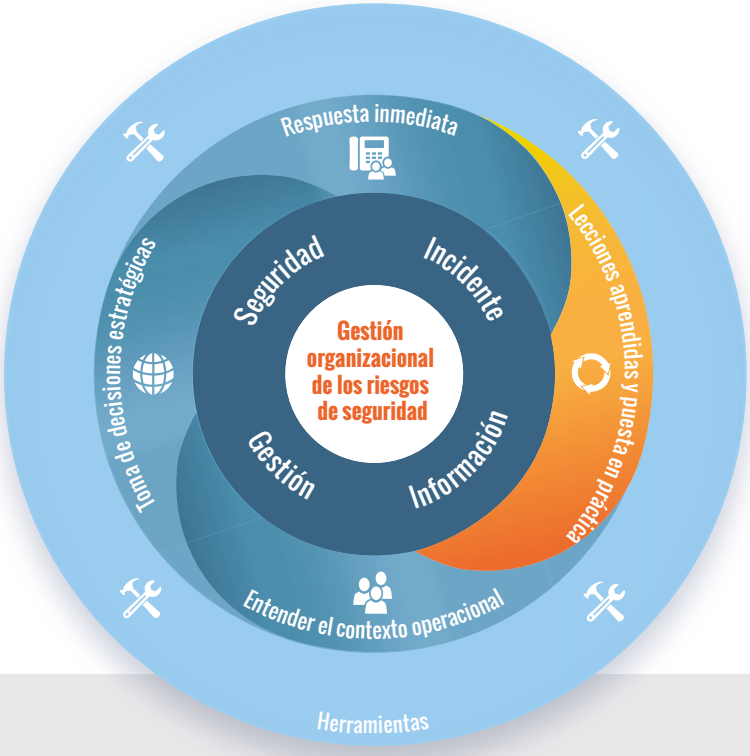
Cabe percatase desde el principio de que la recopilación de información sobre incidentes sobre situaciones delicadas, así como el reporte de dichos incidentes, deben proteger la identidad de aquellas personas involucradas, sin poner en peligro el intercambio de información ni la seguridad de la comunidad humanitaria y de desarrollo en general. En lo que respecta al informe, también existe una delgada línea entre mantener el incidente y la identidad de la superviviente en confidencialidad, y enviar el mensaje de que las supervivientes deberían sentirse avergonzadas sobre sus experiencias. Si se emplea un enfoque delicado y centrado en la superviviente, se pueden reducir las posibilidades de cruzar dicha línea.

Cabe también percatarse de que escuchar incidentes delicados puede ser un desencadenante para la persona que recaba la información como lo es para quien ha sobrevivido al incidente. Puede producirse trauma indirecto y se debería dar apoyo psicosocial si es necesario.

Véase "Herramienta VII Buenas prácticas para informar sobre incidentes degénero y mecanismos de denuncia para informar de explotación y abusos sexuales (EAS)".

Si existe la posibilidad de que la seguridad del personal de otra ONG en terreno esté en peligro, o vaya a estarlo, se debería compartir adecuadamente información sobre el incidente con otras organizaciones o a través de redes como el Departamento de Seguridad de Naciones Unidas (UNDSS) o en los foros de seguridad de ONG. La superviviente debe dar su consentimiento informado a que se comparta información de esta manera y se debería subrayar su función en asegurar que eso no le pasa a nadie más.

II. OBJETIVO DOS: LECCIONES APRENDIDAS Y EN PRÁCTICA



Este apartado trata acerca de la gestión de información sobre incidentes de seguridad a efectos de recopilar datos, procesarlos y analizarlos, transformarlos en información útil, extraer lecciones a partir del incidente y ejecutar acciones de seguimiento. Este apartado abarca:

- 2.1 Análisis posterior al incidente
- 2.2 Poner en práctica las lecciones aprendidas
- 2.3 Análisis y acciones de seguimiento de casos delicados

Herramientas pertinentes:

- Herramienta II: Matriz para analizar incidentes
- Herramienta VIII: Plan de acción para el seguimiento del incidente

El segundo objetivo principal de la gestión de información sobre incidentes de seguridad es poner en práctica las lecciones aprendidas tras un incidente de seguridad en las acciones de seguimiento y en prevención.

La finalidad es entender qué ha sucedido en vista a planificar y a ejecutar los cambios y los procedimientos necesarios que sirvan para prevenir, tratar el riesgo o mitigar las repercusiones de eventos parecidos. Esto suele producirse en el ámbito país / sede poco después de un evento de seguridad.

Después de que se considere "cerrado" un incidente, debería revisarse el incidente dentro de la organización. Una organización suele considerar cerrado un incidente cuando se han realizado el informe, el aprendizaje y la actualización de protocolos necesarios, y el incidente ha dejado de evolucionar. Definir el estado de un incidente respalda el análisis.

Estado del incidente frente al estado de gestión del incidente

Es ventajoso para las organizaciones definir una lista de estados del incidente que se puedan aplicar a eventos y a su gestión. Esto respalda el proceso de seguimiento de información sobre el incidente y, sobre todo, el análisis tras el incidente:

- Estado del incidente:
  - en curso: todavía se está produciendo;
  - finalizado: la organización considera que el evento principal ha terminado.
- Estado de gestión del incidente:
  - abierto: ha acabado el incidente principal, pero la gestión del impacto y su análisis todavía está en curso. Se está investigando el incidente.
  - cerrado: cuando se han puesto en práctica todas las lecciones aprendidas y se han ejecutado las acciones.

Para incidentes de larga duración, como un secuestro, resulta útil realizar una revisión intermedia "en tiempo real" de las acciones ejecutadas tras el evento inicial, de forma que no se pierda este aprendizaje.

Los análisis posteriores al incidente los puede llevar a cabo personal directamente afectado o involucrado en las respuestas y en las decisiones organizacionales que puedan haber influido en cómo se produjo el incidente.

Eso supone analizar información cualitativa para un diagnóstico sincero sobre los factores que contribuyeron a aumentar la vulnerabilidad y a influir en las reacciones concretas que se dieron según se desenvolvía el incidente. El proceso de recabar información debería realizarse en un ambiente de confidencialidad y confianza. Es importante evitar culpar al personal afectado tras un incidente.

2.1 Análisis posterior al incidente

El análisis posterior al incidente contempla cómo afectó directamente el incidente al personal y a la organización y si se les ha cuidado debidamente. Hay que examinar cómo las políticas organizacionales o la conducta personal pueden haber contribuido a que fuera posible el incidente y cuestionar qué mejores pautas han de desarrollarse. Además, hay que examinar cómo las respuestas organizacionales sirvieron para mitigar o resolver asuntos que surgieron a raíz del incidente (o lo obstaculizaron).

El análisis pretende entender los distintos "porqués" que hay detrás de los incidentes de seguridad: por qué se producen los incidentes de seguridad y entender los motivos que hay detrás de los mismos. Sin embargo, eso solo tiene valor si la organización en su conjunto emprende las acciones adecuadas para asegurar que sea menos probable que dichos incidentes vuelvan a producirse.

Se recomienda documentar el impacto real del incidente y las medidas que deben adoptarse para reducir la probabilidad de que un incidente así vuelva a producirse, al igual que su impacto si lo hiciera. Cuando se trata de incidentes críticos, el análisis también debería comprender una evaluación del proceso de gestión, es decir, qué decisiones se tomaron, cuándo y por qué. El proceso por escrito es imperativo si la organización quiere documentar de forma sistemática las lecciones aprendidas a raíz del incidente y reflejar dicho aprendizaje en operaciones y políticas futuras, a la vez que demostrar un aprendizaje organizacional que respalde las responsabilidades en deber de cuidado de la organización.

Se pueden contemplar algunos puntos importantes que tener en cuenta al planificar un análisis de incidentes de seguridad en tres grupos, como se muestra a continuación:

Los motivos para llevar a cabo un análisis de incidentes de seguridad:

- busca entender las causas raíz de los incidentes de seguridad;
- un análisis minucioso es la clave para identificar nuevas actuaciones para mitigar incidentes, o cómo mejorar las existentes, que se pueden emprender para reforzar los SOP y el grado general de seguridad de la organización, lo que permite un mejor acceso a poblaciones necesitadas;
- sirve para identificar lo que motiva el incidente; por ejemplo, si un ataque ha sido deliberado o no. Distinguirlo es importante para entender el contexto operacional. Si las pruebas indican que un incidente fue deliberado, también ayuda a identificar si la organización era el objetivo de una manera deliberada y por qué;
- al incluir elementos de análisis en cada informe sobre incidentes de seguridad, una organización puede constituir un banco de información que respaldará los análisis de tendencias.

Un análisis del incidente debería centrarse en las áreas siguientes:

- Mientras se gestaba el incidente, ¿se siguieron los procedimientos? ¿Son necesarios cambios?
- ¿El objetivo era la organización o una persona? ¿Se debe a que algo provocó un ataque? ¿El personal afectado parecía rico o un objetivo fácil?
- ¿Ya no se acepta a la organización en la zona?
- ¿Qué repercusiones tuvo el incidente en las actividades del programa?
- ¿Eran los procedimientos para tratar el incidente los apropiados?

Entre los factores más comunes que contribuyen a los incidentes de seguridad se encuentran:

- una gestión ineficaz de los riesgos de seguridad o que se han ignorado los procedimientos;
- carencia de una concienciación y una formación básica en seguridad;
- el perfil de la organización en el país y cómo la percibe la población del lugar (por ejemplo, el comportamiento, falta de sensibilidad cultural, etc.);

- relaciones interpersonales y problemas personales (incluso cuestiones internas de recursos humanos);
- un delito a causa de una riqueza patente o aparente;
- falta de información que lleva a malas decisiones sobre seguridad;
- asumir riesgos innecesarios;
- incidentes de seguridad relacionados con el estrés;
- personal que se extralimita o que se encuentra demasiado cómodo trabajando en un entorno inseguro.

Las organizaciones deberían sopesar si pueden compartir con otras agencias el análisis definitivo (o parte del mismo) de sus conclusiones sobre las causas de un incidente y cómo gestionar situaciones específicas.

Para más orientaciones, consúltense las distintas tablas en "Herramienta VI: Matriz para analizar incidentes".

Es importante analizar un incidente en su contexto general de seguridad (véase "Objetivo tres"), pero también a la luz de otros incidentes, ya se hayan producido en la zona o que sigan patrones parecidos. El registro sistemático de incidentes dentro de la organización hace que sea posible este análisis de tendencias. Este tema se trata con más detalle en "Objetivo cuatro".

2.2 Poner en práctica las lecciones aprendidas

La ventaja más evidente de recabar información a raíz de un incidente de seguridad es utilizarla de inmediato a efectos de los programas, como adaptar los planes de viajes y desplazamientos a terreno para mejorar la seguridad organizacional. El contenido del análisis contribuirá a determinar el acceso, los parámetros del proyecto, su ejecución, con vínculos a recursos humanos, presupuestación, monitoreo y evaluación en el ámbito operacional.

Entre otros ejemplos de lecciones aprendidas a raíz de la información sobre incidentes están:

- cambios inmediatos en operaciones y actualización de los SOP y los planes de contingencia; contemplar en su conjunto incidentes separados puede desencadenar decisiones en el ámbito del país;
- elaboración de nuevos indicadores para el seguimiento del contexto de seguridad y el diagnóstico de riesgos;
- compartir las lecciones aprendidas entre las oficinas de todo el mundo permitirá que esta información sea un aporte en las revisiones periódicas de procedimientos, políticas y planes de seguridad de país.

Un buen documento que analice los incidentes de seguridad incluirá un apartado para acciones recomendadas, vinculadas a las causas identificadas. Las buenas prácticas indican adjuntar un plan de acción de seguimiento al informe de análisis de incidentes, para reforzar que se ejecuten de hecho las acciones recomendadas.

Mediante el sistema informático de la organización, se puede enlazar el plan de acción a herramientas de planificación y enviar recordatorios automáticos y avisos al personal responsable.

Véase "Herramienta V: Matriz para analizar incidentes" para más ejemplos de acciones que se pueden poner en práctica tras analizar las causas de los incidentes

Véase "Herramienta VIII: Plan de acción" para saber qué información debería incluir un plan de acción de seguimiento.

2.3 Análisis y acciones de seguimiento de casos delicados

El análisis de un evento debe adherirse a los principios siguientes: confidencialidad, neutralidad y profesionalidad.

En el caso de violencia sexual dentro de una organización, la función primordial de la etapa de análisis, a efectos del presente manual, es determinar qué pasos han de seguirse, en términos administrativos o legales. Eso variará en gran medida entre organizaciones y contextos operacionales.

Si se puede hacer sin exponer detalles delicados sobre el evento o la superviviente, hay que consultar a aquellas personas en funciones parecidas en terreno para reunir información sobre la situación general de seguridad y sobre otros incidentes de violencia sexual en terreno.

Utilizar esta herramienta y cualquier otra para realizar un análisis de seguridad que determine si otros integrantes del personal, la organización o de la comunidad de ONG en su conjunto también corren el riesgo de experimentar violencia sexual u otras formas de violencia.

Al analizar este tipo de eventos, se debería incluir un análisis de impacto, que comprenda los traumas directos y los indirectos, así como formación y otras acciones reactivas que sean necesarias para prevenir esos incidentes en un futuro.

Consultar a los referentes que sea preciso —en terreno y en sede— para identificar qué acciones de seguimiento se necesitan y asegurarse de que se emprenden. Puede que se tengan que realizar otras consultas a recursos humanos y a los servicios jurídicos, éticos, laborales o médicos, como convenga a la organización. La información se compartirá según la necesidad de acceder a ella y se deben adoptar las medidas para facilitar una acción legal si la superviviente lo solicita y con su consentimiento informado. La posibilidad de emprender acciones legales en un contexto determinado puede variar enormemente, en función del perfil de una persona y del entorno jurídico operacional. Cualquier acción legal se regirá por la necesidad y el deseo de la superviviente de llevar el asunto a los tribunales. Hay que consultar con el personal nacional y con otros agentes para recabar distintas perspectivas sobre si se puede dar justicia legal en ese contexto y sobre los riegos a los que puede exponerse la superviviente si toma ese camino. En algunos lugares, puede no ser una opción realista y, en ese caso, se tendrán que gestionar las expectativas.

Incluso si se sabe que alguien en la organización ha experimentado violencia sexual, o si una superviviente ha emprendido las acciones para reportar, existen varios elementos que

no deben perderse de vista. Primero, dar el paso de reportar no implica directamente que una superviviente quiera que se difundan ampliamente y comenten los detalles. En todo momento durante el proceso de reporte, se debe informar a la superviviente de a quién se le cuenta su experiencia y esta debe dar su consentimiento. Es responsabilidad del personal involucrado, del responsable y de la organización proteger la identidad de la superviviente y la confidencialidad de los detalles del caso.[21]

Si una superviviente quiere que se informe de su identidad o que se comparta este u otros datos que la identifiquen, también se debería respetar. El enfoque centrado en la superviviente para abordar los incidentes de violencia sexual dispone que las decisiones y los deseos de la superviviente dictan el curso del proceso de reporte y su cuidado.

Se debería comunicar la información sobre confidencialidad a la superviviente de una manera que deje claro que, si bien se respetará que desee no desvelar elementos que la puedan identificar, no debería sentirse obligada a ello por algún tipo de vergüenza relacionada con haber sido sujeta a violencia sexual. También hay que asegurarse de que la superviviente sabe que puede dar a conocer su identidad más tarde, si esa fuera su decisión.

Antes de trasladar ninguna información, se debería consultar a la superviviente sobre qué información se va a comunicar y a quién, y esta tiene que dar su consentimiento informado. En algunos casos, no existe más opción que ofrecer detalles sobre el incidente a otros, pero al permitir que la superviviente participe en el proceso, podemos asegurar que empieza a recuperar el poder perdido durante el incidente de violencia sexual.

Solo se desvelarán detalles pertinentes a las personas que se considere necesario, para evitar las posibilidades de daños adicionales.

Si fuera preciso para garantizar la protección de otras integrantes de la organización, puede que se tenga que compartir información sobre el evento con otras empleadas. Se debería hacer con delicadeza y protegiendo a la superviviente todo lo posible. Escuchar sobre incidentes de violencia sexual puede ser un desencadenante, así que hay que asegurarse de que otro personal no está experimentando traumas indirectos y de que todas las personas de la organización tienen acceso a apoyo psicológico.

Al tiempo que mantiene el enfoque centrado en la superviviente, la organización también debe encontrar la manera de asegurar que tanto en país como en sede se conoce la realidad de este tipo de incidentes. El acoso y la violencia sexuales constan muy poco en los planes de seguridad de país o en los registros de riesgos de la organización, aun cuando se reconoce de manera anecdótica como un problema.

[21] K. Van Brabant, "Capítulo 12: Agresión sexual" en *GPR8 – Gestión de la seguridad de las operaciones en entornos violentos, Nueva Edición*, Humanitarian Practice Network/ Overseas Development Institute (ODI), 2010.

III. OBJETIVO TRES: ENTENDER EL CONTEXTO OPERACIONAL

Este apartado trata de las ventajas de entender el contexto operacional y de los medios para hacerlo. En concreto, subraya cómo colaborar con otras organizaciones a efectos de compartir información sobre incidentes, al igual que recursos para conseguir información sobre el contexto. Este apartado abarca:

- 3.1 Aspectos prácticos de compartir información sobre seguridad
- 3.2 Compartir información sobre incidentes externamente
- 3.3 Foros para compartir información sobre incidentes de seguridad
- 3.4 Recursos externos para analizar tendencias en el contexto

Herramienta pertinente:

- Herramienta II: Tipología de incidentes

El tercer objetivo primordial de la gestión de información sobre incidentes de seguridad es entender el contexto operacional de seguridad de una organización. Un buen conocimiento del contexto permite a las organizaciones adoptar decisiones operacionales sensatas sobre seguridad en el ámbito de país, región y sede. Los análisis de patrones de incidentes que reportan las organizaciones son la fuente de información más eficaz sobre el contexto de seguridad específico.

No obstante, para conseguir entender un contexto en su integridad y hacer un uso más estratégico de la información sobre un incidente de seguridad, en los análisis de seguridad se debería incluir la información sobre el incidente proveniente de más de una organización y de fuentes múltiples.

> *"Se puede obtener información sobre el contexto general de seguridad a partir de varias fuentes, entre ellas otras organizaciones, los medios de comunicación (incluso los centrados en materia humanitaria y de desarrollo) y la información que ofrecen proveedores de servicios especializados que, a través de suscripciones, describen el panorama general por país u ofrecen previsiones de riesgos".*

Las ONG suelen encontrar útil comparar sus incidentes con los de organizaciones con parámetros similares, ya sea por el enfoque que tienen sus programas (humanitario, de desarrollo, de derechos humanos, etc.) o por el tamaño (p. ej., de su presencia o de su personal). Para organizaciones más pequeñas, puede resultar esencial tener acceso a información adicional sobre incidentes en ese mismo país antes de que se pueda señalar alguna tendencia.

Una de las fuentes de información más eficaces sobre el contexto específico de seguridad es el análisis de patrones en los incidentes que hayan reportado diversas organizaciones. Las organizaciones pueden utilizar las conclusiones analíticas que se desprenden de un panorama global de los incidentes de seguridad como referencias para sus propias tendencias y para fundamentar las estrategias y la comunicación con organizaciones y con el sector humanitario y de desarrollo en su conjunto.

El análisis de tendencias también puede resultar una herramienta útil para informar a los medios de comunicación y para influir en la opinión pública y en donantes gubernamentales.

3.1 Aspectos prácticos de compartir información sobre seguridad

Categorías de información: desde confidencial hasta pública

Algunas organizaciones pueden considerar una obligación y parte de sus políticas compartir cierta información. Dentro de la preparación operacional, las ONG deberían decidir qué información sobre incidentes quieren compartir externamente y con qué finalidad. La tabla que aparece a continuación ofrece un ejemplo de cómo puede afectar la delicadeza de la información al acceso a todas las etapas de la gestión de información sobre un incidente de seguridad, desde la ubicación del incidente hasta un ámbito más estratégico dentro de una organización, al igual que entre organizaciones.

Clasificación	Acceso
Confidencial: La información confidencial tiene un valor considerable para la organización y desvelarla o difundirla sin autorización puede conllevar daños graves a la reputación de la organización o efectos negativos sobre sus operaciones.	Se debería conceder acceso explícitamente solo a aquellas personas que lo necesiten imperativamente, y solo el mínimo necesario (los principios de "necesidad de conocer" y de "mínimos privilegios"). Cuando la información confidencial se mantenga fuera de las oficinas de la organización —por ejemplo en portátiles, tablets o móviles—, debería estar protegida por entradas de acceso específicas y quizás por dispositivos de encriptación o plataformas de correo electrónico encriptado. Eso se aplica concretamente a casos delicados, como los de violencia sexual. En esas circunstancias, se necesita el consentimiento informado explícito de la persona afectada para compartir la información.
Reservada: No se pretende divulgar ni difundir esta información, ya que puede afectar a la vida de las personas o crear publicidad negativa, daños limitados a la reputación o potenciales pérdidas económicas para la organización.	El acceso a la información reservada para un pequeño grupo de personal está sujeto a controles. Se debería mantener de forma que se evite el acceso sin autorización a ella, es decir, en un sistema que exija un usuario válido y adecuado para entrar antes de que se conceda el acceso.
De uso interno: Difundir la información a las partes interesadas pertinentes asegura un buen funcionamiento organizacional y buenas respuestas internas en la organización. Su publicación no provocará ningún daño a la organización ni a su personal, pero aun así se considera inconveniente.	La información de uso interno se puede revelar o difundir a los integrantes de la organización, los socios u otras personas que sean adecuadas, según consideren los dueños de la información, sin ninguna restricción sobre el contenido ni el momento de su publicación.
Pública: Difundir la información en las noticias, en los medios y a través de otros canales no supone ningún riesgo para la organización ni para su personal; su publicación se considera conveniente o, al menos, no se tienen objeciones a ello.	La información se puede divulgar o difundir sin ninguna restricción sobre su contenido. La divulgación o la difusión de la información no puede contravenir ninguna legislación ni normativa vigentes, como las normas sobre privacidad.

Al decidir en qué categoría encaja la información, también se debería contemplar el impacto que tendrá el "no saber" en otras partes interesadas.

Por ejemplo, se produce un secuestro en una carretera que utilizan con frecuencia varias ONG que operan en la zona. Se puede considerar información confidencial, porque divulgar los detalles sobre este incidente podría tener graves repercusiones en el bienestar del personal, la capacidad de ejecutar programas y la reputación de la organización. Sin embargo, no divulgar la información a tiempo podría llevar a que otras personas sean secuestradas. Por lo tanto, es importante saber cómo se puede compartir la información de una manera horizontal entre actores para permitir que parte de la información sobre el incidente sea reservada en lugar de confidencial.

Alguna información nunca debería divulgarse públicamente ni compartirse a través de ningún mecanismo para tal fin, como los datos personales de aquellas afectadas por un incidente, ni los datos de contacto de familiares, etc.

Compartir información sobre incidentes y las redes sociales

En los últimos años, las redes sociales se han convertido en un recurso pertinente y considerable a la hora de obtener o compartir información relativa a seguridad. Se puede encontrar gran abundancia de información sobre contexto y seguridad a través de los motores de búsqueda de Twitter o Facebook.

Las redes sociales, Twitter y Facebook incluidos, también se pueden utilizar para alertar a otros, incluso a grupos, sobre incidentes o situaciones peligrosas de una forma privada. Sin embargo, estas fuentes de información han de entenderse y gestionarse para asegurar una gestión segura de la información. Se pueden compartir con todo el personal dentro de la organización las recomendaciones que aparecen más abajo y aplicarlas a cada etapa del ciclo de GIIS.

Recomendaciones sobre redes sociales y reporte de incidentes:

- **Personalizar la configuración de privacidad:** ajustar la configuración de privacidad en el sitio y elegir las opciones que limitan quién puede ver la información.
- **Separar lo personal y lo profesional:** utilizar distintos nombres de usuario y fotos en sitios diferentes, ya que se pueden utilizar para buscar los vínculos entre información profesional y la personal.
- **Detenerse antes de publicar:** cuando se publica algo en línea, se queda ahí para siempre. A veces incluso se puede acceder al contenido que ha sido eliminado a través del sitio web o a través de capturas de pantalla de la publicación original. El contenido que incluye información personal, conducta o paradero puede suponer un riesgo de seguridad.
- **Desactivar la geolocalización:** muchos sitios de redes sociales o aplicaciones solicitarán acceso a la ubicación del dispositivo, pero en la mayoría de los casos no es necesario. Además de acceder a la ubicación del dispositivo, algunos sitios publicarán dicha información. Cuando las personas "entran" en sitios como Facebook, pueden estar compartiendo su ubicación exacta con otras.

Dada la naturaleza de las plataformas y la velocidad a la que se comparte información a través de las redes sociales, la información no está verificada y puede no ser fiable. Las organizaciones deben reflexionar sobre la fuente y la fiabilidad de la información relacionada con seguridad, y su confidencialidad, antes de tomar ninguna decisión o de compartirla.

"Un grupo de WhatsApp que se crea a fin de informar a cada referente de seguridad de una región sobre los incidentes que se producen en su área de responsabilidad debería gestionarse con atención. Solo debería poder añadir miembros al grupo el administrador. Toda inclusión debería ser validada y, al menos, comunicada a todos los miembros. Las normas y los códigos de comunicación deberían convenirse y las personas participantes deberían velar porque esté protegido el acceso a esa conversación de WhatsApp, en caso de que pierdan el teléfono o se lo roben".

3.2 Compartir información sobre incidentes externamente

Compartir con otras organizaciones

Compartir información sobre seguridad, informes de incidentes y de situación, y sondear las vulnerabilidades entre agencias no está exento de dificultades.[22] Sin embargo, cada vez está más aceptado que compartir información sobre seguridad dentro de un contexto operacional concreto y reportar incidentes con rapidez a otras ONG en la zona es una responsabilidad colectiva.[23]

Las organizaciones pueden compartir información directamente entre ellas, a través de foros o mediante plataformas para compartir información sobre seguridad de ONG (véase más adelante "Foros para compartir información sobre incidentes de seguridad" y "Recursos externos para analizar tendencias en el contexto").

Lamentablemente, existen muchas barreras potenciales a que las agencias compartan información sobre seguridad:

- Una puesta en común de datos para percibir patrones exclusivos de incidentes de seguridad en ONG exige que las organizaciones quieran compartir sus datos agregados sobre incidentes de seguridad basándose en acuerdos de confidencialidad.
- Un concepto erróneo de la estructura organizacional, de la misión, la cultura, los clanes, la región, la religión, la historia y la antropología puede obstaculizar la colaboración y que se comparta información pertinente de seguridad.
- Algunas organizaciones (o personas dentro de una organización) pueden percibir la seguridad como un inconveniente en las operaciones, mientras que otras pueden poner demasiada insistencia en su autonomía, sin asociarse ni colaborar con otras partes interesadas en la región.
- Los choques de personalidad entre actores clave en asuntos de seguridad puede entorpecer gravemente la cooperación y la colaboración. Aunque no se debe subestimar la importancia de las relaciones interpersonales para crear confianza, las redes formales ofrecen unos cimientos para construir unas estructuras más formales para compartir información, de manera que no dependan únicamente de determinadas personas y así perduren a pesar de los cambios de personal.

[22] J. Schafer y P. Murphy, *Security Collaboration: Best Practices Guide*. InterAction Security Unit – InterAction, 2010.

[23] K. Van Brabant, *GPR8 – Gestión de la seguridad de las operaciones en entornos violentos, Nueva Edición,* Humanitarian Practice Network/ Overseas Development Institute (ODI), 2010.

- Una falta generalizada de recursos humanos y económicos para seguridad suele ser una traba para las agencias a la hora de contribuir a esfuerzos colaborativos o de participar plenamente en ellos.
- El enfoque sobre la seguridad puede ser bastante distinto entre agencias. Esas diferencias pueden dificultar la colaboración en unos servicios de seguridad comunes; sin embargo coordinarse y compartir información y enfoques servirá para que todas las partes entiendan mejor el contexto y para que pongan en práctica unas medidas encaminadas a gestionar los riesgos de seguridad más informadas y eficaces.
- La preocupación sobre un uso indiscreto de información delicada que se comparte a través de mecanismos de coordinación a veces puede ser un obstáculo considerable a que se comparta información. Existen algunos ejemplos de información que se compartió en esos foros y que acabó en la prensa, aunque sean excepciones. Es importante estar plenamente informado de la naturaleza exacta de todo mecanismo de coordinación, cómo se trata la información, las expectativas y las responsabilidades al manejar la información y las consecuencias de incumplir las condiciones del acuerdo.
- La seguridad es solo una de las múltiples prioridades que tienen las organizaciones al realizar los programas. Sin embargo, se ha mostrado una y otra vez que unas malas prácticas y la carencia de coordinación por parte de una organización pueden tener repercusiones en la capacidad de toda la comunidad de obtener y mantener el acceso para operaciones humanitarias y de desarrollo.

Una vez identificadas las barreras a que se comparta la información, los colaboradores deberían confiar en su profesionalidad y en sus valores para encontrar un terreno común sobre el que trabajar para llegar a una solución de mutuo acuerdo.

Es importante recordar que la conducta de una organización puede tener repercusiones en la seguridad de todas. Si una organización no transmite información importante sobre incidentes, conatos incluidos, puede conllevar que otra organización sufra un evento de gran repercusión, en lugar de ser capaz de evitar o de minimizar el impacto de esa amenaza. La colaboración es elemental para conocer el contexto y la seguridad organizacional general.

Compartir con donantes

Algunas organizaciones mandan informes con análisis posteriores al incidente a los donantes, junto con los informes trimestrales o intermedios, si se ha producido alguna interrupción de los programas a causa de un aumento de la inseguridad o un mayor número de incidentes. Los informes sirven para informar a los donantes sobre la situación en terreno y para apoyar las decisiones de ampliar los programas. La organización debería decidir en términos estratégicos si quiere compartir sus informes de incidentes con donantes, al tiempo que se asegura de cumplir con los requisitos contractuales.

3.3 Foros para compartir información sobre incidentes de seguridad

Más abajo se detallan algunos de los foros y grupos dedicados a la coordinación y la colaboración en materia de seguridad que se especializan en recopilar, analizar y compartir información de seguridad sobre incidentes.

Cada uno tiene un mandato distinto y, por lo tanto, diferentes mecanismos para recopilar y compartir información. No obstante, todos ellos son magníficas fuentes de información y pueden ayudar a mejorar la gestión de riesgos de seguridad.

- **Plataformas de bases de datos mundiales sobre incidentes**
  - Aid Worker Security Database
  - Security in Numbers Database (SiND)
- **En ámbito de sede**
  - European Interagency Security Forum (EISF)
  - InterAction (Estados Unidos)
  - Dutch Security Network (Países Bajos)
  - UK NGO Security Focal Point Group (Reino Unido)
  - CINFO: Comunidad de Prácticas de Seguridad (Suiza)
  - Grupo de Trabajo de Seguridad de la Coordinadora (España)
  - Canadian Interagency Security Advisory Forum (Canadá)
- **En ámbito región**
  - MENA Region Humanitarian Safety & Security Forum
  - West Africa Regional Security Forum (África Occidental)
- **En ámbito país**
  - International NGO Safety Organisation (INSO) y sus oficinas regionales
  - Pakistan Humanitarian Forum
  - NGO Forum – Sudán del Sur
- **Otros**
  - Reuniones con agencias de la ONU, con arreglo al marco de Salvar Vidas entre odos (Saving Lives Together – SLT)

Parte de la información que aportan estos foros será pública (fuentes abiertas), mientras que otra requerirá membresía. Las organizaciones deberían acercarse a foros mundiales, regionales, locales o en terreno sobre coordinación e intercambio de información en materia de seguridad como sea necesario y donde esté disponible.

3.4 Recursos externos para analizar tendencias en el contexto

"Puede resultar útil para las ONG comparar sus tendencias en incidentes con las de organizaciones parecidas a ellas. Ese enfoque exige que se compartan entre organizaciones los datos clave de tendencias en formato anónimo que no permita identificar a una única agencia".

Los responsables y analistas de seguridad deberían contemplar los análisis de información interna sobre incidentes así como la información externa sobre seguridad recopilada, sobre todo mediante las redes para compartir información.

La información externa sobre incidentes permite conocer el contexto del entorno operacional de las ONG.

Utilizar unas clasificaciones estándar facilita comparar la información entre organizaciones. El proyecto Aid in Danger dispone las clasificaciones estándar.

Véase "Herramienta II: Tipología de incidentes".

A continuación, la tabla presenta una instantánea de cuatro recursos clave que ofrecen datos o tendencias en incidentes de seguridad a partir de la información sobre incidentes de seguridad recabados de diversas fuentes. Se incluye información más minuciosa sobre cada uno de los recursos.

Nombre	Características clave
Aid Worker Security Database (AWSD), dirigida por Humanitarian Outcomes	Describe incidentes donde el personal ha sido asesinado, herido o secuestrado. Un informe anual ofrece reflexiones y análisis de tendencias en todo el mundo.
Security in Numbers Database (SiND), parte del proyecto Aid in Danger (AiD) de Insecurity Insight	Ofrece un boletín mensual de eventos de fuentes abiertas, una panorámica de tendencias que incluyen un amplio abanico de incidentes (más allá de aquellos en los que el personal es asesinado, herido o secuestrado), y un análisis de los incidentes de seguridad que las agencias han reunido y compartido. También permite acceder a los datos a través de Humanitarian Data Exchange.
International NGO Safety Organisation (INSO)	Ofrece información sobre incidentes a sus organizaciones miembros en los países donde tiene presencia. INSO también dispone de un panel que muestra datos clave sobre incidentes.
Marco Salvar Vidas entre Todos (Saving Lives Together – SLT)	El marco Salvar Vidas entre Todos (SLT) es una iniciativa conjunta entre Naciones Unidas, organizaciones internacionales y ONG. Las organizaciones socias de SLT reciben diversos informes sobre incidentes del Departamento de Seguridad de Naciones Unidas (UNDSS).

Aid Worker Security Database

El Aid Worker Security Database (AWSD) es un proyecto de Humanitarian Outcomes que registra los incidentes graves de violencia contra personal de ayuda, con informes sobre incidentes desde 1997 hasta la actualidad. El AWSD, que empezó en 2005, constituye el único recurso mundial integral para estadísticas sobre ataques graves contra operaciones de ayuda a civiles y ofrece el fundamento para analizar el entorno cambiante de seguridad para la respuesta humanitaria.

Se recaban datos sobre incidentes de fuentes públicas, a través un filtro sistemático de medios de comunicación y redes sociales, y de información que las organizaciones de ayuda y entidades de seguridad operacional aportan directamente al proyecto. El proyecto también mantiene acuerdos con diversos consorcios de seguridad del ámbito regional y de terreno para compartir información directamente y verificar los incidentes. Los informes sobre incidentes se contrastan y verifican cada año con todas las organizaciones humanitarias pertinentes de una manera continua. Entre ellas están las Naciones Unidas, ONG locales e internacionales, además de los consorcios de seguridad de país.

Ahora que cumple cinco años en línea, el AWSD es la única base de datos interactiva accesible al público de este tipo. El AWSD permite a las organizaciones descargarse el conjunto de datos completo y ofrece una API para que se desarrollen aplicaciones externamente utilizando los datos de la AWSD.

El informe anual *Aid Worker Security Report* se basa en pruebas empíricas a partir de los datos y ofrece reflexiones y análisis sobre tendencias en todo el mundo, al igual que recomendaciones sobre cuestiones cruciales de seguridad operacional.

Para más información o para contribuir con información y cambios al AWSD, envíe un correo electrónico a info@humanitarianoutcomes.org.

Aid in Danger Project

El proyecto Aid in Danger, de Insecurity Insight, monitorea de forma sistemática los informes de fuentes abiertas buscando incidentes que afecten negativamente a la prestación de ayuda y trabaja en asociación con agencias de cooperación para recopilar y compaginar sus informes sobre incidentes de seguridad. Todos los datos se almacenan en la base de datos Security in Numbers Database (SiND) para analizarlos. El proyecto empezó en 2008 como derivación de la iniciativa Health Care in Danger del CICR. Aid in Danger procura monitorear el impacto de la violencia y de actuaciones deliberadas que interfieren en la prestación de ayuda. El proyecto Aid in Danger hace seguimiento de un abanico de incidentes que repercuten en la prestación de ayuda: desde amenazas de violencia hasta decisiones administrativas de denegar permisos o visados, o la destrucción de infraestructuras y el impacto de la delincuencia. El proyecto también monitorea secuestros, asesinatos y lesiones del personal.

Para respetar la preocupación sobre confidencialidad de las agencias participantes, la base de datos Security in Numbers Database no está disponible para el público. Los conjuntos de datos que contienen subconjuntos seleccionados de datos, de los que se ha eliminado la información que pueda identificar a alguien, están disponibles a través de la página de Insecurity Insight en el Humanitarian Data Exchange.

El proyecto Aid in Danger publica en abierto un resumen mensual de eventos reportados por fuentes abiertas, actualizaciones habituales de análisis de tendencias y una panorámica de los datos confidenciales de agencias en colaboración con el European Interagency Security Forum (EISF).

Para más información sobre cómo participar como agencia, envíe un correo electrónico a info@insecurityinsight.org.

International NGO Safety Organisation

La International NGO Safety Organisation (INSO) es el principal mecanismo de coordinación en materia de seguridad para ONG que operan en contextos de riesgo elevado, con más de 850 organizaciones miembro de INSO en todo el mundo.

La organización británica sin ánimo de lucro se fundó en 2011 con el propósito de ofrecer a las ONG que se registrasen una serie de servicios gratuitos, entre ellos el seguimiento de incidentes en tiempo real, informes analíticos, datos y mapeo sobre seguridad, apoyo en incidentes críticos y formación sobre seguridad personal, gestión de la seguridad y gestión de crisis.

Las plataformas de INSO están activas en la actualidad en Afganistán, Iraq, Siria, Palestina (Gaza), Somalia, Kenia, RDC, RCA, Camerún, Nigeria, Mali y Ucrania, así como nuevas que abren cada año.

El registro en INSO está estrictamente limitado a ONG locales e internacionales y debe solicitarse en el país donde se opera. Las plataformas de INSO funcionan conforme a un

severo código de conducta por el que los miembros comparten información entre ellos en total confidencialidad.

En términos mundiales, INSO ofrece datos oportunos y precisos sobre ONG a través de su Panel de Datos Clave [Key Data Dashboard] y a principios de 2018 lanzará el Centro de Datos de Conflictos y Humanitarios [Conflict & Humanitarian Data Centre (CHDC)], una base de datos centralizada que contiene todos los incidentes recopilados en toda su red de plataformas en terreno.

Con más de un millón de entradas iniciales, el CHDC será uno de los mayores repositorios del mundo de este tipo y respaldará investigaciones de largo alcance y entre distintos contextos, así como unos análisis tácticos más inmediatos.

Se invita a las ONG que sean aptas para registrarse y que todavía no lo hayan hecho a contactar con INSO a través de su página de registro o mediante info@ngosafety.org.

"En algunos países, se pueden ver los incidentes de seguridad en relación con los eventos de los que reporta INSO. En términos globales, las agencias pueden consultar la base de datos Aid Worker Security Database para ver eventos críticos de secuestro, lesiones o asesinato de personal; para una gama más amplia de incidentes, las organizaciones se pueden unir a la base de datos Security in Numbers Database de Aid in Danger".

Marco Salvar Vidas entre Todos (Saving Lives Together)

El marco Salvar Vidas entre Todos (SLT, por sus siglas en inglés) es una iniciativa conjunta entre las Naciones Unidas, organizaciones internacionales (OI) y ONG. El marco de SLT, que empezó en 2006 y se revisó en 2015, reconoce que la ONU y sus organizaciones socias —OI y ONG— viven en su conjunto amenazas de seguridad y destaca la importancia de colaborar "para asegurar la prestación segura de ayuda humanitaria y al desarrollo". El objetivo de SLT es "aumentar la capacidad de las organizaciones socias de tomar decisiones informadas y poner en práctica disposiciones eficaces de seguridad para mejorar la seguridad y la protección de la plantilla y de las operaciones".[24] Las organizaciones socias del marco de SLT reciben informes diarios sobre incidentes de UNDSS.

Las recomendaciones de SLT, aunque sobre todo velan por la colaboración entre la ONU y ONG internacionales, ofrecen pautas interesantes para que las organizaciones refuercen su colaboración en la gestión de información sobre incidentes.[25]

Se pueden descargar el marco y las notas de orientación de SLT (en inglés) aquí.

Para más información, póngase en contacto con UNDSS en el ámbito país o a nivel mundial con:

Don Lloyd Cederstrand, OCHA (Coordinación y enlace operacional): cederstrand@un.org

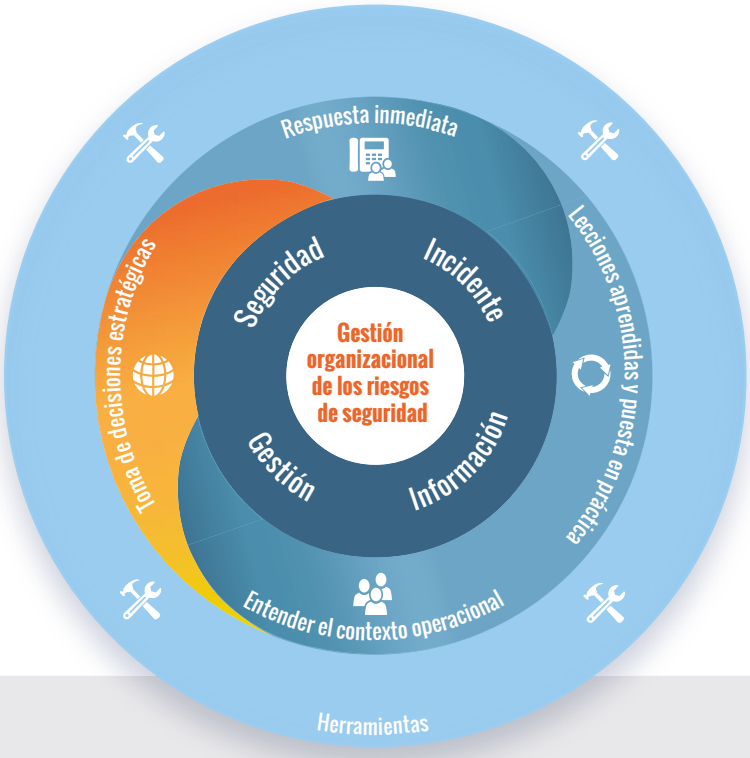
Centro de Comunicaciones del UNDSS (asistencia para comunicaciones en emergencias disponible las 24 horas): undsscomscen@un.org, Tel: +1 917 367 9438/9

Dirección ejecutiva del EISF: eisf-director@eisf.eu.

[24] Comité Permanente entre Organismos (IASC), "Saving Lives Together – A Framework for Improving Security Arrangements Among IGOs, NGOs and UN in the Field", IASC, 2015.

[25] La iniciativa SLT no implica que la ONU se responsabilice de la seguridad de toda la comunidad humanitaria. La ONU puede tener recursos —como aeronaves para evacuaciones y equipo de comunicaciones— que utilizará, cuando pueda, para respaldar a la comunidad de ONG, pero no se trata de una obligación y todo gasto en el que incurra tiene probabilidades de correr a cargo de la ONG. Las ONG deben responsabilizarse de su propia seguridad y asignarle los recursos convenientes. Lo mismo se puede decir de la gestión de información sobre incidentes.

IV. OBJETIVO CUATRO: TOMA DE DECISIONES ESTRATÉGICAS



Esta sección trata sobre la gestión de información sobre incidentes de seguridad en el contexto de las decisiones estratégicas, sobre todo en el ámbito regional o en sede. Lo que se pretende es ayudar a los referentes y analistas de seguridad a registrar información de incidentes de seguridad de manera sistemática, para usar la información de los análisis de tendencias y para comunicar las recomendaciones a personas clave tanto dentro como fuera de la organización. El propósito es dar información a las personas que toman las decisiones estratégicas para asegurar que la información de los incidentes se toma en cuenta en todos los ámbitos de la planificación, los procedimientos y los proyectos de la organización. En esta sección se tratará de:

- 4.1 Registro sistémico de incidentes: ¿qué sistema utilizar?
- 4.2 Análisis de tendencias para fundamentar las decisiones estratégicas
- 4.3 Estructuras organizacionales para tratar las cuestiones estratégicas de seguridad
- 4.4 Cómo utilizar información sobre incidentes de violencia sexual de una manera estratégica
- 4.5 Usar información sobre incidentes de seguridad para incidencia estratégica

Herramientas pertinentes:

- Herramienta II: Tipología de incidentes
- Herramienta IX: Sistemas de GIIS
- Herramienta X: Almacenamiento de incidentes
- Herramienta XI: Tecnología para reportar y registrar incidentes
- Herramienta XII: Analizar y comparar tendencias de datos
- Herramienta XIII: Preguntas estratégicas para decisiones referentes a la gestión de información sobre incidentes

El cuarto objetivo principal de la gestión de información sobre incidentes de seguridad es fundamentar las decisiones dentro de una organización.

Se deberían llevar a cabo análisis regulares en sede para determinar tendencias y patrones que fundamenten las decisiones estratégicas a largo plazo para toda la organización. La finalidad es hacer balance de la naturaleza cambiante de los incidentes de seguridad —para entender los entornos de trabajo que más desafíos suponen y la exposición general de la organización al riesgo— e identificar las mejores respuestas estratégicas.

Dadas las mejoras experimentadas en las tecnologías de la comunicación y la disponibilidad de información en todo el mundo, ha cobrado importancia tener una perspectiva mundial. Los incidentes ya no se pueden ver como un mero asunto específico de un país. Por ejemplo, la campaña de una organización en una región puede provocar manifestaciones ante sus oficinas en la otra punta del mundo.

Analizar la información sobre incidentes tiene implicaciones en una buena gestión a mayor escala, que puede incluir decisiones sobre:

- dónde operar;
- cómo comunicar sobre los programas;
- qué pólizas de seguros se necesita;
- en qué medida hay que presupuestar la gestión de riesgos de seguridad dentro de las operaciones en un país.

Los análisis de seguridad también se pueden utilizar para destacar preocupaciones generales sobre el mandato principal de una organización y las dificultades para acceder a las poblaciones beneficiarias.

Algunas organizaciones llevan a cabo este tipo de análisis una vez al año y otras lo hacen con más frecuencia. Se deberían realizar revisiones ad hoc, así como las revisiones previstas con antelación, cuando se produzca un cambio considerable en la misión, el perfil o los contextos operacionales de una organización. Es una ventaja para toda ONG tratar con regularidad su perfil de incidentes de seguridad. Ese análisis es posible gracias a un flujo de información eficaz entre oficinas en terreno y sede y un sistema eficaz y eficiente para registrar los incidentes de los que se reporta de una forma sistemática y estándar para facilitar un análisis comparativo y una toma de decisiones estratégica.

La toma de decisiones estratégica en relación con la información sobre incidentes de seguridad debería contemplar analizar información interna sobre incidentes al igual que información sobre seguridad recabada externamente, sobre todo a través de redes para compartir información. Comparar las tendencias internas con las externas puede alertar sobre vulnerabilidades y elementos de la gestión de riesgos de seguridad que han de abordarse dentro de la organización.

4.1 Registro sistémico de incidentes: ¿qué sistema utilizar?

Un buen sistema para registrar, almacenar, clasificar y extraer datos sobre incidentes de seguridad es una parte fundamental del análisis de incidentes de seguridad y de una toma de decisiones estratégica. Las organizaciones cuentan con distintos mecanismos para reportar, recopilar y registrar incidentes en el ámbito país en una ubicación centralizada. En lo que respecta a los sistemas en línea, existen diversas soluciones que van desde modelos gratuitos, de código abierto y que una puede adaptar a sus necesidades, hasta sistemas a medida que desarrollan sociedades mercantiles.

Independientemente del sistema que utilice una organización, es importante que el sistema de registro y mapeo esté diseñado para responder a las necesidades de quien lo utilice, desde para reportar hasta para analizar tendencias. Las nuevas tecnologías pueden ser de ayuda en esto.

Existen dos enfoques que una ONG puede adoptar sobre el uso de la tecnología para desarrollar un sistema de registro y mapeo:

- una solución independiente que se integra en los servidores y en los sistemas de la organización; o
- el "software como un servicio", donde un proveedor de servicios externo aloja el sistema.

La decisión sobre qué enfoque adoptar dependerá de factores como la estrategia tecnológica y el tamaño de la organización, las cifras probables de incidentes, los recursos y la capacidad para gestionar el sistema y la protección de datos. En la siguiente tabla se resumen algunos de los sistemas disponibles para reportar, almacenar y analizar a nivel central los incidentes de seguridad que afectan a una organización:

	Método para reportar y registrar incidentes	Sistema
Sistemas diseñados y gestionados internamente	Narración escrita del incidente, vinculada a una hoja de cálculo para registrar incidentes usando codificación sistemática	Se podría hacer a través de correos electrónios, documentos u hojas de Google, una plataforma Google compartida, SharePoint. Se puede utilizar una hoja de cálculo para clasificar la información que se presenta por escrito utilizando unos campos de datos concretos que haya que rellenar.
	Sistema en línea usando plataformas existentes de código abierto	Se puede construir el sistema para reportar incidentes como una extensión de plataformas existentes que se utilizan para el correo electrónico, como SharePoint. Se pueden adaptar plataformas de geolocalización en línea, como Ushahidi, para crear un sistema de gestión de información y reporte de incidentes mundial.
Sistemas externos	Suscribirse a una plataforma en línea para la gestión de datos	Algunas empresas privadas y organizaciones sin ánimo de lucro ofrecen plataformas en línea para la gestión de información sobre incidentes de seguridad.
	Sistema en línea personalizado	Algunas organizaciones han encargado sistemas en línea desarrollados específicamente para la organización.

Véase Herramienta IX: Sistemas de GIIS para encontrar una tabla más minuciosa que ilustra los sistemas disponibles para gestionar la información sobre incidentes y un resumen de las ventajas y desventajas de los distintos sistemas.

Organizaciones más pequeñas u ONG con recursos limitados pueden optar por los dos primeros métodos para registrar y reportar incidentes dado lo sencillo que es configurar y mantener dichos sistemas, además de su bajo coste relativo. Los sistemas más avanzados pueden convenir a organizaciones más grandes que experimentan un número elevado de incidentes y requieren de un sistema flexible que se corresponda con las necesidades específicas de la organización.[26]

Herramientas para el almacenamiento de incidentes

Una plantilla básica para almacenar incidentes debería incluir la información siguiente:

- **País, región y ubicación** – ser concreto.
- **Fecha y hora** – cuándo se produjo el incidente, cuánto duró y cuándo se cerró el incidente.
- **Qué sucedió** – una sinopsis breve y concisa sobre el incidente.
- **Categoría del incidente** – categorías analíticas para analizar las tendencias de datos (véanse las Herramientas II y X para opciones propuestas).
- **Qué personas estuvieron involucradas** – tanto en términos internos como externos, y tanto víctimas como apoyos en la gestión.
- **Actuaciones y decisiones adoptadas** – resumen de actuaciones y decisiones y quién las ha tomado.
- **Cambios operacionales** – panorámica de los cambios inmediatos realizados como reacción ante el incidente.
- **Análisis y comentarios** – resumen del documento de análisis tras el incidente.
- **Estado** – ¿está en curso el incidente? ¿Se ha documentado toda la información?

El presente manual ofrece ejemplos de herramientas de almacenamiento en Excel. Se pueden encontrar en "Herramienta II: Tipología de incidentes" y en "Herramienta X: Almacenamiento de incidentes".

Antes de diseñar la herramienta de almacenamiento, deberían identificarse las necesidades futuras de análisis y estadísticas; se deberían crear columnas para permitir que se elaboren análisis de tendencias y estadísticas utilizando la configuración de Excel.

Sistemas en línea

Funciones clave que una organización puede buscar en un sistema en línea:

- un repositorio único de incidentes en la web;
- que permita informes electrónicos desde un PC o dispositivos móviles conectados a internet;
- que notifique a distintos grupos en función de los datos que se presenten en el informe de incidentes;
- que vele por la seguridad de los datos (solo se puede acceder a la información entregada de una manera controlada y por la necesidad de conocer;
- que vele por la protección de los datos al transmitirse;
- que asegure que se hace copia de seguridad de los datos.

[26] G. de Palacios, "Managing security-related information: a closer look at incident reporting systems", EISF, próximamente.

Cuestiones esenciales que hay que decidir:

- cómo alimentarán el repositorio los usuarios finales;
- cómo asegurar que el acceso al repositorio está sujeto al principio de necesidad de conocer;
- cómo notificar a distintos grupos de personas en función de los datos presentados sobre el incidente;
- cómo asegurar que la información se capta de una manera íntegra y precisa a partir de la fuente del incidente;
- cómo validar electrónicamente la información captada;
- en qué medida se utilizará el sistema para hacer seguimiento del caso (¿será solo un repositorio o también tendrá la posibilidad de hacer seguimiento?);
- qué tipo de funciones de análisis crear sobre esa base.

Puntos clave que aclarar antes de embarcarse en el desarrollo de un sistema en línea:

- definición de categorías de incidentes;
- instrucciones claras para usuarios sobre las categorías.

Más allá de cuáles sean las herramientas y los sistemas, es importante definir, en términos técnicos, quién accede a los datos almacenados en el ámbito de terreno, país, región y sede. Algunos ejemplos de métodos que se pueden utilizar para velar por que la información se comparta con las partes interesadas adecuadas son contraseñas, encriptado, grupos cerrados, validación de acceso inter pares, etc. Véase Introducción: Seguridad de la información para saber más sobre la seguridad de la información.

Véase "Herramienta XI: Tecnología para reportar y registrar incidentes" para conocer ejemplos y descripciones de sistemas en línea para registrar y reportar incidentes.

4.2 Análisis de tendencias para fundamentar las decisiones estratégicas

Una vez consolidada la información sobre incidentes en un sistema central, incluyendo categorías analíticas, se puede analizar la información de seguridad de una manera más estratégica para fundamentar las decisiones.

Responsables, referentes y analistas de seguridad deberían transformar los datos en información útil. Dicha información se compartirá con determinado personal con más responsabilidades en forma de tendencias y estadísticas que respalden los procesos de toma de decisiones.

La mayoría de las organizaciones clasifican los incidentes de seguridad. La categorización sirve para el análisis y para extraer estadísticas.

Los datos se pueden desglosar en categorías clave ("Herramienta II: Tipología de incidentes") y presentar en forma de informes que resuman los análisis de tendencias ("Herramienta XI: Analizar y comparar tendencias de datos").

Las características de ese análisis estratégico dependen del número de incidentes de seguridad que se reporten dentro de una organización. Si son solo unos cuantos, un escrito donde se resumen los eventos cruciales puede ser el mejor método para presentar

las tendencias. Si aumenta el número de eventos reportados, será importante desarrollar un monitoreo de tendencias en cifras más sistemático.

La siguiente lista de preguntas puede ayudar a los referentes de seguridad a elaborar conclusiones estratégicas adicionales y recomendaciones de actuación tras un buen análisis de los incidentes de seguridad en eventos pasados:

- ¿Qué clase de incidentes de seguridad han vivido el personal y la organización?
- ¿En qué países se produjeron?
- Como referente de seguridad en sede, ¿cuál es su grado de satisfacción con la manera en la que las oficinas de país parecen haber utilizado los incidentes de seguridad, conatos incluidos, para aprender y para mejorar sus prácticas?
- ¿Qué incidentes de seguridad experimentan otras organizaciones en el mismo país y cómo se comparan con los incidentes de los que se ha reportado dentro de su organización?
- ¿Cómo han afectado los incidentes de seguridad en la prestación de ayuda?
- ¿Podemos costear el impacto de los incidentes de seguridad en la prestación de ayuda?
- ¿Cuáles han sido las principales causas de los incidentes de seguridad?
- ¿Se pueden clasificar las causas de los incidentes según la estrategia de respuesta que pueda ser precisa?
- ¿Podemos utilizar los datos para identificar un umbral de riesgo que nuestra organización esté dispuesta a aceptar?

Véase "Herramienta XIII: Preguntas estratégicas para decisiones referentes a la gestión de información sobre incidentes" para consultar una lista completa de preguntas y acciones recomendadas posibles.

Herramienta de visualización Google Earth Pro

El mapeo geográfico de eventos puede resultar útil para visualizar incidentes y así respaldar el análisis y el reporte a cuadros superiores dentro de la organización. Existen varias opciones para mostrar la información de forma visual. Si esta es la opción por la que se inclina, deben incluirse los datos necesarios sobre geolocalización y el tipo de incidente dentro del informe inicial, ya que no resulta tan eficaz ni preciso hacerlo a posteriori.

Si se dispone de la información correcta (p. ej., coordinadas GPS, códigos de colores, tipos de incidentes, etc.), una posibilidad sencilla para mostrar la ubicación de los incidentes puede ser convertir un documento Excel en un documento KML y luego vincular este a Google Earth Pro. Si el documento Excel-KML incluye la información adecuada, saldrán marcados los eventos automáticamente en un mapa de Google.[27]

Hay que asegurarse de que la configuración vela por la confidencialidad con un acceso limitado a la información.

[27] Para ver el proceso de conversión de un documento Excel a KML, consulte: https://www.earthpoint.us/ExcelToKml.aspx

4.3 Estructuras organizacionales para tratar las cuestiones estratégicas de seguridad

Las organizaciones pueden tratar cuestiones de seguridad desde una perspectiva estratégica en diversos formatos.

Por ejemplo, un comité de gestión de riesgos de seguridad puede reunirse con una periodicidad regular (p. ej., una vez al año o con más frecuencia) y unir a miembros designados de la junta, la dirección general, el referente de seguridad o el equipo de seguridad y, tal vez, a directoras regionales. El personal de seguridad suele tener que encargarse de preparar la reunión, donde después presenta las tendencias de seguridad y elabora el orden del día que se va a tratar.

En este tipo de reunión, puede ser ventajoso abordar:

- Tendencias de incidentes de seguridad durante los últimos años, que se presentan como:
  - una tabla de incidentes de seguridad por país;
  - una tabla de incidentes de seguridad por categoría;
  - una tabla sobre la gravedad del incidente (es decir, repercusiones);
  - una tabla sobre las causas de los incidentes.
- Un análisis de las consecuencias de los incidentes de seguridad reportados, por ejemplo:
  - consecuencias para las personas, con repercusiones psicológicas o físicas,
  - consecuencias operacionales,
  - consecuencias para la organización, como las que afectan a la reputación de la ONG,
  - consecuencias para la gestión de riesgos de seguridad.
- Recomendaciones sobre cómo asegurar la continuidad del trabajo en esos entornos.
- Calificaciones del contexto y niveles de seguridad operacionales.
- Obstáculos al reporte de incidentes en la organización.
- Un caso práctico que ilustre un tema importante que ha de tratarse con todo el equipo y que lleve a desarrollar un plan de acción para casos parecidos en un futuro (p. ej., un plan de comunicación en caso de incidentes, si establecer relaciones con las autoridades del lugar o no, etc.).
- Espacio para abordar las preguntas que tengan quienes deciden entre los presentes para el personal de seguridad.

Para ver más ejemplos sobre cómo elaborar análisis de seguridad para reuniones de revisión, consúltese "Herramienta XII: Analizar y comparar tendencias de datos".

En toda reunión debería incluirse un punto en el orden del día que sea revisar los documentos de seguridad —como el umbral organizacional de riesgos de seguridad, el marco de gestión de riesgos de seguridad, la estrategia de seguridad, la política de seguridad, el plan de gestión de crisis, etc.—, aunque el punto de acción sea "no es preciso actuar". Eso es importante para documentar el proceso debido para el deber de cuidado.

4.4 Cómo utilizar información sobre incidentes de violencia sexual de una manera estratégica

La mejor manera en la que las organizaciones pueden enfocar los incidentes de violencia sexual contra su personal es aprendiendo de la experiencia para asegurarse de que la organización cumple mejor su función de proteger a su personal y de responder a estos tipos de incidentes en el futuro. Sigue siendo un tema que a las personas les cuesta tratar, así que la organización debería volcarse, de una manera activa, en crear confianza y apertura para tratar estos temas internamente.

Se debería analizar si sería estratégico y beneficioso ser abiertos acerca de incidentes de violencia sexual con los medios de comunicación o dentro de foros mundiales con otros integrantes de la comunidad de ONG.

> *"Ser abiertos en una plataforma más grande también puede crear el espacio para que otras ONG emprendan cambios parecidos dentro de sus organizaciones, lo que contribuye a un aumento generalizado de la seguridad del personal de ONG".*

Si se van a utilizar datos sobre un evento concreto para subrayar la cuestión y las lecciones globales extraídas, la superviviente debe dar su consentimiento informado. Cuando sea posible, debería involucrarse a la superviviente en este proceso y así aportar una voz que guíe la creación de una narrativa en torno al incidente y a las lecciones aprendidas.

Si la superviviente ha dado su consentimiento informado para que se comparta información sobre su experiencia —en terreno o en general—, hay que asegurarse de que recibe apoyo adicional en el momento que se haga pública la información, incluso un permiso por razones humanitarias, apoyo psicológico, etc.

Se puede compartir información sobre tendencias y los aprendizajes organizacionales sin poner en riesgo los derechos de las personas, y eso debería fomentarse.

4.5 Usar la información sobre incidentes de seguridad para incidencia estratégica

Una organización debería decidir, en términos estratégicos, si utilizar información sobre incidentes obtenida internamente, y puede que también externamente, a efectos de incidencia.

Muchas organizaciones informan sobre que cada vez es más difícil garantizar el paso seguro y la prestación de ayuda a civiles que la necesitan. Sin embargo, sin datos consolidados de todo el sector sobre tales incidentes y sin una estrategia colectiva eficaz para abordar las obstrucciones deliberadas o la impunidad de los culpables, la mayoría de las agencias solo pueden llevar casos individuales por sí mismas.

Las ONG han realizado grandes progresos en el desarrollo de estrategias de gestión de riesgos de seguridad para responder a unos contextos de seguridad en constante cambio. No obstante, eso no ha ido acompañado de una incidencia humanitaria común para abordar las preocupaciones que van más allá de la estrategia de gestión de riesgos

de seguridad de una organización concreta. Por ello, la magnitud de la inseguridad para la acción humanitaria permanece oculta, se trata cada caso en silencio y, en la mayor parte de las situaciones, los responsables no son llevados ante la justicia. Existen posibilidades de desarrollar una estrategia de incidencia de todo el sector para abordar las cuestiones complejas.

Algunos incidentes de seguridad van más allá de lo que una organización puede controlar y se puede precisar de una campaña conjunta de incidencia con otras organizaciones. Por ejemplo, que se utilicen cada vez más armas explosivas en zonas pobladas afecta a la seguridad del personal y se interpone en la prestación de ayuda. Cuando las autoridades nacionales no toman las medidas precisas contra los autores, las organizaciones pueden tener que buscar respaldo internacional con investigaciones o presionar para que se les lleve a juicio.

En términos más globales, para el sector de la cooperación es importante velar por que la información sobre los desafíos que crean contextos de seguridad volátiles se ponga con regularidad a disposición de partes interesadas clave, como donantes, responsables políticos, los medios y el público en general. Se necesitan pruebas documentadas de violencia contra cooperantes o de los incidentes que afectan a la prestación de ayuda para respaldar los esfuerzos generales por proteger al personal de ayuda y sus operaciones, y para que así se pueda acceder sin trabas a las poblaciones que lo necesitan. En términos colectivos, el sector humanitario y de desarrollo podría hacer más por recordar al público donante y a los responsables políticos las dificultades y los peligros a los que se enfrenta el personal de ayuda al prestarla en entornos inseguros.

Sin embargo, cuando las organizaciones contemplan si realizar una campaña de incidencia, deben considerar las consecuencias que puede tener para la seguridad del personal y para la realización de los programas.

¿Qué datos se necesitan para la incidencia?

Existe una tendencia entre los medios y otras partes interesadas de preguntar primero por las cifras que reflejan la magnitud del problema. Por lo tanto, se ha hecho mucho hincapié en intentar cuantificar las personas que han sido afectadas. No obstante, eso no es imprescindible a la hora de tratar sobre las políticas. Campañas anteriores han mostrado que describir la índole de un problema puede tener el poder suficiente para impulsar cambios. Por ejemplo, la campaña contra las minas antipersona empezó centrándose en presentar contextos particulares con datos de los programas en Camboya y Angola del Comité Internacional de la Cruz Roja (CICR) que ilustraban un problema, en lugar de cuantificarlo. Como muchas personas se sintieron interpeladas por la vívida descripción del impacto que tenían las minas en la vida de las personas, la campaña logró conseguir unos resultados impresionantes.[28]

Los incidentes que afectan a la seguridad de las ONG se pueden utilizar para describir el carácter y el impacto de un problema, aunque se desconozca su frecuencia. Existen posibilidades para que la comunidad de ayuda llegue a un público más amplio y a responsables políticos clave con narrativas sólidas sobre cómo su labor y su personal se ven afectados por los contextos en los que trabajan.

[28] Para ver una descripción general de los elementos que contribuyeron al éxito de la campaña para prohibir las minas antipersona, consulte el artículo siguiente aquí. Uno de los primeros artículos del CICR, que tuvo gran repercusión, admitía que no se conocían las cifras totales, pero describía el impacto y el efecto general de las minas sobre la población civil. Véase el artículo aquí.

Una de las fuentes más convincentes que demuestran el impacto de la inseguridad en la prestación de ayuda son los informes de incidentes que generan las organizaciones para su propia gestión de los riesgos de seguridad. La mera existencia de los datos pone de manifiesto el problema mejor que ningún otro dato recabado específicamente a efectos de incidencia. Podría ser una oportunidad perdida no aprovechar ese recurso para defender una mejor protección o, al menos, más financiación para las políticas en materia de seguridad o una mejor formación sobre seguridad para el personal.

Generar dichos datos de una forma colectiva, como sector, puede contribuir a una incidencia más sólida en la protección del personal de ayuda y los programas, y a que los donantes acepten mejor que la gestión de riesgos de seguridad es un gasto directo que debería incluirse en las propuestas.

Es importante no exponer a personas o casos concretos a efectos de apuntarse un tanto político. Los datos colectivos reducen dicho riesgo.

Los cuadros superiores de las organizaciones pueden avanzar en esta línea si contribuyen a compartir datos con otras organizaciones y reforzando los vínculos entre el personal de seguridad y el de políticas e incidencia dentro de sus organizaciones. Eso ayuda a velar por que el personal de políticas e incidencia utilice de forma estratégica los aportes de los análisis sobre incidentes de seguridad de múltiples organizaciones.

Caso práctico: Asistencia de salud en peligro, CICR

En 2008, el CICR encargó un estudio en 16 países para documentar cómo afectaba la violencia a la prestación de atención médica, mediante los datos sobre incidentes de contextos seleccionados.[29] Ese estudio se convirtió en la primera base empírica para empezar a abordar la violencia contra el personal sanitario, que desde entonces ha sido reflejada por muchos otros casos prácticos.[30] A partir de ahí, el CICR ha llevado el proyecto Asistencia de salud en peligro, que combina la sensibilización con directrices prácticas sobre cómo mejorar la seguridad del personal sanitario.[31]

Otras organizaciones han empezado también a asumir esta cuestión. Desde 2014, diez integrantes de la Safeguarding Health in Conflict Coalition han publicado informes anuales conjuntos sobre ataques contra la atención médica, donde combinan datos e información de distintas organizaciones para que el tema se mantenga en la agenda global.[32] Más de veinte integrantes de la coalición, incluso varias organizaciones humanitarias, ayudan a difundir la información para fomentar que se proteja mejor la atención médica.[33]

En 2016, la Organización Mundial de la Salud (OMS) publicó datos relativos a ataques contra la atención médica en su página web.[34]

29 ICRC, *A sixteen-country study: health care in danger.* ICRC, 2011.
30 Para más información, véase: http://healthcareindanger.org/resource-centre/
31 Para más información, véase: http://healthcareindanger.org/hcid-project/
32 Para más información, véase: https://www.safeguardinghealth.org/
33 Puede ver una lista de las organizaciones humanitarias que apoyan a la Safeguarding Health in Conflict Coalition en la segunda página aquí.
34 Véase: http://www.who.int/emergencies/attacks-on-health-care/en/. Este sitio se actualizará próximamente. Véase también Lieberman, A., "WHO readies to launch online database tracking health worker attacks", 2017, *Devex*.

En mayo de 2016, el Consejo de Seguridad de la ONU adoptó la Resolución 2286, que establece una hoja de ruta para la protección de la atención médica en conflictos.[35]

Estos ejemplos muestran cómo un uso eficaz de los datos puede servir para incluir, y mantener, esta importante cuestión en la agenda.

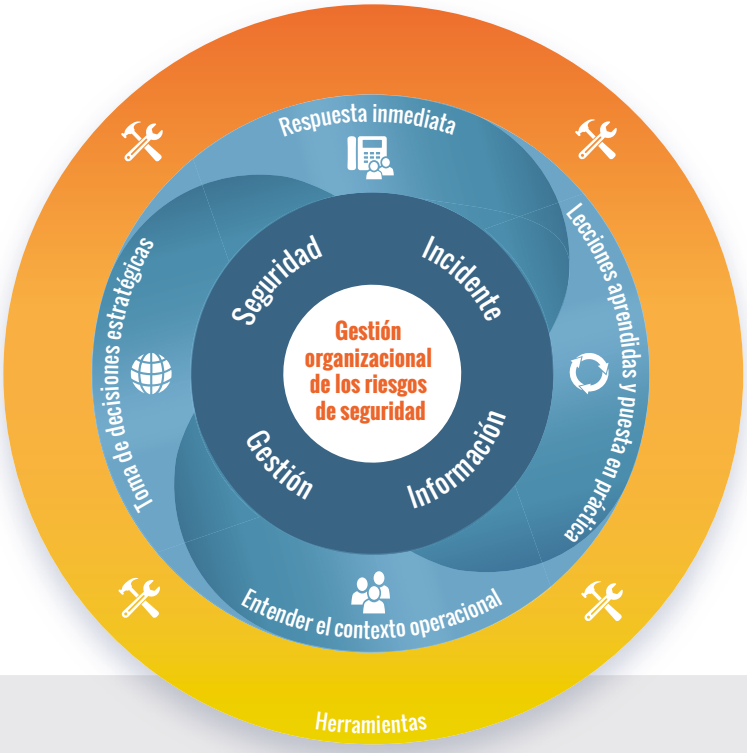
El grupo de trabajo para la protección de la acción humanitaria
El Grupo de trabajo para la protección de la acción humanitaria [Working Group for the Protection of Humanitarian Action] está sopesando las opciones para una acción colectiva y mundial a fin de proteger al personal de ayuda . El grupo de trabajo reúne a profesionales de organizaciones operacionales humanitarias, expertos en seguridad, expertos en incidencia y políticas, y académicas, y lo dirigen conjuntamente el Advanced Training Programme on Humanitarian Action, de la Harvard Humanitarian Initiative, y Acción contra el Hambre. Su objetivo es traspasar la tendencia de las organizaciones humanitarias de trabajar aisladas, responder a este entorno cada vez más desafiante a través de una reflexión colectiva, una incidencia más fuerte y más coherente en todo el sector humanitario, y acciones conjuntas para reiterar que se respete el derecho internacional humanitario (DIH) y se proteja la acción humanitaria. Dado que el DIH es responsabilidad de los Estados, la comunidad humanitaria solo puede defender a escala global cambios en un contexto que, a estas alturas, es cada vez menos propicio a que la ayuda humanitaria llegue a la población civil que la necesita.

Uno de los descubrimientos iniciales del grupo de trabajo fue la necesidad de compartir información de manera sistemática sobre incidentes de seguridad para que se puedan identificar tendencias y prioridades clave. El grupo de trabajo también identificó una carencia de cooperación y comunicación directa entre los responsables de riesgos de seguridad y los departamentos de incidencia en muchas organizaciones como una traba para una labor más eficaz. El grupo de trabajo procura que los referentes de seguridad y el personal de políticas dentro de las organizaciones participen en identificar casos donde la incidencia común puede respaldar la respuesta a problemas de seguridad.

Para obtener más información sobre el grupo de trabajo, póngase en contacto con:
Lise Fouquat: lfouquat@actioncontrelafaim.org
Pauline Chetcuti: pchetcuti@actioncontrelafaim.org
Julia Brooks: jbrooks@hsph.harvard.edu

[35] Naciones Unidas "Adopción de Resolución Nº 2286 del Consejo de Seguridad de Naciones Unidas relativa a la protección de hospitales y personal humanitario en situaciones de conflictos armados", 2016, *Naciones Unidas*.
[36] ATHA. (2016). "Policy Project: Protection of Humanitarian Action", *ATHA*.

CAPÍTULO III: HERRAMIENTAS



El presente apartado ofrece unas herramientas orientativas que respaldan la gestión de información sobre incidentes. Deben leerse y utilizarse conjuntamente con el contenido escrito de este manual.

Las herramientas están organizadas de la siguiente manera (se accede a la herramienta al hacer click sobre el elemento):

- I: Matriz de autodiagnóstico en GIIS
- II: Tipología de incidentes
- III: Incidentes organizacionales o externos
- IV: Plantilla para reportar incidentes
- V: Matriz para analizar incidentes
- VI: Cómo llevar a cabo una reunión informativa sobre los hechos
- VII: Buenas prácticas para informar sobre incidentes de género y mecanismos de denuncia para informar de explotación y abusos sexuales (EAS)
- VIII: Plan de acción para el seguimiento del incidente
- IX: Sistemas de GIIS
- X: Almacenamiento de incidentes
- XI: Tecnología para reportar y registrar incidentes
- XI: Analizar y comparar tendencias de datos
- XIII: Preguntas estratégicas para decisiones referentes a la gestión de información sobre incidentes

HERRAMIENTA I: MATRIZ DE AUTODIAGNÓSTICO EN GIIS

Utilícese la presente tabla como una guía de los elementos habituales de un sistema de gestión de información sobre incidentes.

PREGUNTAS GENERALES	
¿Cuántas oficinas en terreno / país / región están operativas en la actualidad en la organización?	
Número de empleados (plantilla internacional, nacional, voluntarios, etc.)	
En la actualidad, ¿cuántos referentes de seguridad están trabajando con usted?	
En sede, ¿la responsabilidad de aplicar el marco de gestión de riesgos de seguridad es compartida? Si es así, ¿con quién (cargo)?	
MARCO DE GESTIÓN DE LOS RIESGOS DE SEGURIDAD	**Se aplica en mi organización (sí/no/en parte)**
¿Las responsabilidades decisorias sobre la gestión de riesgos de seguridad están establecidas con claridad en todos los ámbitos?	
¿Usa la organización información sobre el contexto de seguridad a otros efectos políticos, como serían la incidencia, la comunicación con donantes o la programación?	
GESTIÓN DE INCIDENTES Y DE CRISIS	
¿Cuenta la organización con una política sobre gestión de incidentes / crisis?	
¿Se dispone de un marco de gestión de incidentes en terreno / país (procedimientos)?	
¿Se aplica un marco de gestión de incidentes en sede (procedimientos)?	
¿El marco de gestión de incidentes incluye un árbol de comunicaciones?	
¿El marco de gestión de incidentes aborda los incidentes que son conatos?	
¿Se forma al personal sobre la gestión de incidentes o crisis y se llevan a cabo simulacros?	
¿La organización utiliza un sistema en línea para gestionar los incidentes?	

¿Utiliza la organización un programa de procesamiento de textos u hojas de cálculo como base de su sistema de gestión de incidentes?	
¿Se ha convenido en un procedimiento de comunicaciones relativas a incidentes con la aseguradora de la organización?	
¿Existen vínculos entre las políticas de gestión de riesgos de seguridad y las políticas de recursos humanos en la organización?	
RECOPILACIÓN DE INFORMACIÓN SOBRE INCIDENTES	
¿Existe una definición organizacional del término "incidente"?	
¿Utiliza la organización categorías definidas para describir distintos tipos de incidentes? Si lo hace, ¿se corresponden con las categorías que utilizan otras ONG con las que esté asociada?	
¿Existe una plantilla de informe de incidentes en terreno / país? Si es así, ¿está unificada con las de otras ONG con las que esté asociada?	
¿Existe un procedimiento para afrontar emociones (ventilación) en terreno?	
¿Existe un procedimiento para reuniones posteriores sobre hechos en terreno?	
¿Existe en terreno un sistema de almacenamiento seguro para la información recabada?	
¿Existe en país / región un sistema de almacenamiento seguro para la información recabada?	
¿Existe en sede un sistema de almacenamiento seguro para la información recabada?	
¿Recopila información su organización sobre incidentes externos (es decir, los que no tienen repercusiones en su organización)?	
REPORTE Y REGISTRO DE INFORMACIÓN SOBRE INCIDENTES	
¿Existe un procedimiento para reportar incidentes?	
¿Existen directrices de apoyo a la plantilla de informe de incidentes?	
¿Existe un árbol de reporte claro para cada oficina en terreno?	
¿Existe una lista de contactos disponible en terreno / país?	
¿Se aplica un sistema de registro en terreno / país?	
¿Se aplica un sistema de registro en región?	
¿Se aplica un sistema de registro en sede?	
¿Se registran daños y pérdidas en infraestructura o equipo?	
¿Se registran amenazas verbales, escritas o virtuales a la organización?	

¿Se registran las trabas administrativas?	
¿Se registra la violencia sexual (acoso incluido)?	
¿Se reportan los incidentes relacionados con violencia sexual mediante el marco habitual de gestión de incidentes?	
¿Se registran los conatos?	
¿El sistema es seguro en todos los ámbitos? ¿Los datos están seguros?	
ANÁLISIS DE INFORMACIÓN SOBRE INCIDENTES	
¿Existe una segunda plantilla para reportar incidentes que ofrezca orientación sobre la información que ha de recopilarse a efectos analíticos (por ejemplo, 72 horas después del evento)?	
¿Alguien se encarga en terreno / país de analizar los incidentes?	
¿Alguien se encarga desde la región de analizar los incidentes?	
¿Alguien se encarga en sede de analizar / verificar los resultados de los análisis en región y en terreno / país?	
¿Se forma al personal para mejorar sus destrezas analíticas (no necesariamente solo en materia de seguridad)?	
¿Se dispone de un sistema en el ámbito país para mapear (p. ej., mediante una hoja de cálculo) y analizar incidentes?	
En terreno / país, ¿se consultan fuentes externas (partes interesadas o información) durante el análisis?	
En la región, ¿se consultan fuentes externas (partes interesadas o información) durante el análisis?	
En sede, ¿se consultan fuentes externas (partes interesadas o información) durante el análisis?	
COMPARTIR INFORMACIÓN SOBRE INCIDENTES	
¿Existen unas directrices o unas políticas generales sobre clasificación de la información en la organización?	
¿Se dispone de unas políticas sobre comunicaciones internas en terreno / país?	
¿Se dispone de unas políticas regionales sobre comunicaciones internas?	
¿Se dispone de unas políticas sobre comunicaciones internas en sede?	
¿La organización forma parte de un grupo en materia de seguridad de ONG en terreno / país? (ejemplos)	
¿La organización forma parte de un grupo regional en materia de seguridad de ONG? (ejemplos)	
¿La organización forma parte de un grupo en materia de seguridad de ONG en sede? (ejemplos)	

¿Existe una política sobre comunicaciones externas en terreno / país?	
¿Existe una política regional sobre comunicaciones externas?	
¿Existe una política sobre comunicaciones externas en sede?	
¿La organización utiliza las redes sociales para comunicaciones generales?	
¿La organización tiene vínculos firmes con partes interesadas de medios?	
¿Tiene la organización un sistema de mapeo de actores en terreno / país?	
¿Tiene la organización un sistema regional de mapeo de actores?	
¿Tiene la organización un sistema de mapeo de actores en sede?	
¿Las comunicaciones internas suelen ser verbales o por escrito?	
¿Las comunicaciones externas suelen ser verbales o por escrito?	
¿Existe un documento de traspaso para referentes en terreno que incluya la información sobre incidentes?	
¿Se ha formado al personal para compartir información de incidentes y las políticas organizacionales?	
¿El personal directivo y de la junta aprovecha este intercambio de información?	
USO DE LA INFORMACIÓN SOBRE INCIDENTES	
¿Se ha nombrado a alguien en terreno / país para que se encargue de las acciones de seguimiento (a medio plazo)?	
¿Existe una comunicación de seguimiento un mes después del incidente (los ámbitos pueden variar)?	
¿Existe una comunicación de seguimiento tres meses después del incidente (los ámbitos pueden variar)?	
¿La sede hace seguimiento de que se apliquen las lecciones aprendidas?	
¿Su organización hace análisis cuantitativo?	
¿Su organización hace análisis cualitativo?	
¿Se dispone en país de un sistema para hacer análisis de datos cuantitativos sobre incidentes?	
¿Se dispone en sede de un sistema para hacer análisis de datos cuantitativos sobre incidentes?	
¿Se celebran reuniones en terreno para presentar las tendencias de datos al personal?	

¿Se celebran reuniones en país para presentar las tendencias de datos al personal?	
¿Se celebran reuniones regionales para presentar las tendencias de datos al personal?	
¿Se celebran reuniones en sede para presentar las tendencias de datos al personal?	
¿El personal de programas consulta a los referentes de seguridad de terreno / país?	
¿El personal de programas consulta al responsable / asesor de seguridad de sede?	
¿Se presentan los análisis (p. ej., de tendencias) al personal directivo y de la junta?	
¿Se comparte la información sobre tendencias de datos con partes interesadas externas?	
¿Se utilizan para incidencia las tendencias de datos de la organización?	

HERRAMIENTA II: TIPOLOGÍA DE INCIDENTES

A continuación se ofrecen definiciones de distintos tipos de incidentes a modo ilustrativo. Las organizaciones no tienen que utilizar todas las categorías en su gestión de información sobre incidentes de seguridad. No obstante, se anima a que utilicen las definiciones establecidas que se proponen para facilitar el intercambio de datos y las comparaciones con otras agencias.

Se definen los incidentes dentro de categorías amplias (tales como accidente, actuación de las autoridades, delito, etc.) y subcategorías asociadas. Las agencias pueden elegir usar solo las categorías amplias, determinadas subcategorías o combinar categorías amplias y subcategorías.

Las categorías amplias cumplen distintas funciones: algunas clasifican el evento por sus repercusiones (p. ej., muertes o daños); otras describen el propio carácter del evento (p. ej., violencia sexual), mientras que otras contienen información sobre el autor además de describir la naturaleza del evento (p. ej., delitos o actuación de las autoridades); otras clasifican el contexto en el que se produjo el evento (p. ej., inseguridad generalizada), mientras que otras categorías describen los medios (p. ej., uso de armas); y otras clasifican la respuesta de la agencia.

La adecuación de una categorización u otra dependerá del enfoque analítico. Un único evento se puede contemplar desde diversas perspectivas.

Para la mayoría de los eventos es pertinente más de una de las categorías amplias. Se puede considerar que las subcategorías se excluyen mutuamente, lo que significa que normalmente solo corresponde una de las subcategorías.

Véanse también las definiciones de categorías de eventos que se utilizan en el análisis de tendencias y los datos de Insecurity Insight en Humanitarian Data Exchange.

CATEGORÍA AMPLIA	SUBCATEGORÍAS	DEFINICIONES
Accidente Enfermedad Catástrofe natural Accidentes de tráfico donde hay personal o vehículos de la agencia involucrados y otros incidentes que no son intencionados, como accidentes, catástrofes o enfermedades repentinas.	**Accidente: Muerte**	No se pueden atribuir todas las muertes involuntarias a causas naturales. Las causas de muerte accidental pueden ser accidentes automovilísticos, complicaciones por lesiones, etc.
	Accidente: Otros	Un incidente fortuito que conlleva perjuicio para el personal o daños a propiedades de la organización.
	Accidente: Vehículo	Un accidente que implique un vehículo de la organización. Vehículo se refiere a cualquier tipo de medio de transporte, entre otros: coches, camiones, autobuses, motocicletas, etc.
	Accidente: Incendio natural	Todo incendio por causas naturales o involuntarias que dañe los bienes o que ponga en peligro al personal (como fuegos eléctricos o fugas de gas, etc.).
	Enfermedad	Toda enfermedad grave de una persona empleada.
	Catástrofe natural	Catástrofe natural real o prevista que sucede, o se prevé que suceda, en una ciudad o país donde la organización tiene una oficina. Entre las catástrofes naturales, se pueden incluir los terremotos, los volcanes, los huracanes, los tornados, tormentas que causan daños (granizo, inundaciones instantáneas), inundaciones, tsunamis, etc.
Actuación de las autoridades (AA) Acciones directas o indirectas por parte de actores estatales o no estatales que impiden la prestación de ayuda.	**AA: Abuso de poder**	El uso de poderes legislativos, ejecutivos u otros autorizados por parte de funcionarios gubernamentales en beneficio propio ilícito. Un acto ilegal por parte de un funcionario supone abuso de poder solo si el acto está directamente relacionado con sus obligaciones oficiales.
	AA: Acceso denegado	Actuaciones que a) impiden que una organización llegue a beneficiarios o beneficiarios potenciales para un diagnóstico de necesidades o prestación directa de servicios; o actuaciones que b) impiden que los beneficiarios lleguen a servicios que presta una organización.
	AA: Acusaciones	Una imputación de prácticas indebidas por parte de las autoridades del país de destino.
	AA: Aplicación de las leyes	Aplicación de legislación, órdenes ejecutivas, decretos o normativas existentes o de reciente aprobación que, al aplicarse, tengan un efecto real en la prestación de ayuda. Eso puede incluir la confiscación del equipo, poner a las personas / organización en listas de vigilancia, etc.
	AA: Arrestos ***(Véase también cargos, detención y encarcelamiento)***	Arresto del personal. Quien arreste debe estar operando en capacidad gubernamental (como la policía) para distinguir este incidente de uno de toma de rehenes. Unos cargos formales suelen anteceder a los arrestos.
	AA: Cargos	Cargos legales formales realizados por una autoridad gubernamental que afirman que un integrante del personal o la organización han cometido un delito.

GORÍA AMPLIA	SUBCATEGORÍAS	DEFINICIONES
Actuación de las autoridades (AA) Acciones directas o indirectas por parte de actores estatales o no estatales que impiden la prestación de ayuda.	**AA: Puesto de control**	Un puesto de control no fronterizo erigido en zonas bajo el control de militares, paramilitares o banda armada para vigilar o controlar el movimiento de personas y mercancías que afecten a la prestación de ayuda.
	AA: Denegación de visado	Retraso o denegación de un timbre oficial, visado u otro permiso obligatorio que permita entrar en un país o territorio dentro de un país para prestar ayuda.
	AA: Detención	Mantener en custodia a personal antes de que se presenten cargos oficiales o sin cargos oficiales; incluye detención temporal durante horas o días.
	AA: Expulsión	Acto de forzar a personal o a una organización a abandonar un país o territorio.
	AA: Multa	La organización tiene que pagar dinero como castigo por no haber acatado una norma o ley.
	AA: Cierre forzoso	Orden gubernamental o de otras autoridades de detener las operaciones en un país o territorio; incluye cierre de un solo programa o varios.
	AA: Actuación gubernamental	Actuación del Gobierno anfitrión o donante que tiene una repercusión directa o indirecta sobre la capacidad económica de una agencia para prestar ayuda; incluye la congelación de fondos, la introducción de impuestos o el fin de ayudas.
	AA: Encarcelamiento	Mantener retenido a personal en un lugar oficial conocido o desconocido, como una cárcel, a menudo tras cargos oficiales.
	AA: Introducción de leyes	Se refiere a la elaboración de borradores o a la votación de leyes, órdenes ejecutivas, decretos o normativas que, una vez vigentes, tendrán un efecto potencial o real sobre la prestación de ayuda. Eso puede incluir, entre otros, procedimientos restrictivos de registro, normativa sobre importación o transparencia sobre las fuentes de financiación.
	AA: Investigación	El proceso o el acto de examinar hechos relativos a alegaciones contra el personal o la organización.
	AA: Registro de bienes	Registro de las instalaciones por autoridades externas.
Criminalidad Incidentes a raíz de delitos que afectan a los bienes del personal o de la agencia	**Criminalidad: Robo a mano armada**	Un robo a punta de pistola o donde los que cometen el robo llevan armas de fuego que afectan al personal o a los bienes.
	Criminalidad: Incendio provocado	Todo incendio que dañe los bienes o ponga en peligro al personal y que no sea fortuito. En el incendio provocado se incluye, entre otros, el uso de dispositivos incendiarios, el sabotaje intencionado de los sistemas eléctricos o los conductos / depósitos de gas, y el uso de acelerantes de combustión para destruir bienes.

CATEGORÍA AMPLIA	SUBCATEGORÍAS	DEFINICIONES
Criminalidad Incidentes a raíz de delitos que afectan a los bienes del personal o de la agencia	**Criminalidad: Chantaje**	Amenazas, extorsión o manipulación a alguien para obligarle a hacer algo; incluye conseguir algo, sobre todo dinero, por la fuerza o mediante amenazas.
	Criminalidad: Allanamiento	El acto de entrar por medios ilícitos a las instalaciones o los vehículos de una agencia de cooperación, con intención de cometer un robo.
	Criminalidad: Robo con escalamiento	Allanamiento de morada del personal, normalmente con intención de cometer un robo. Se usa si las personas estaban durmiendo o si no eran conscientes del allanamiento.
	Criminalidad: Asalto / secuestro de vehículo	Todo incidente en el que se incaute a la fuerza un vehículo con personal o que sea propiedad de la organización.
	Criminalidad: Ciberataque	Uso deliberado de sistemas informáticos, iniciativas tecnológicas y redes que conlleve consecuencias perjudiciales que puedan poner en riesgo datos y que lleven a delitos cibernéticos.
	Criminalidad: Fraude	Engaño ilícito o delictivo encaminado a obtener beneficios económicos o personales.
	Crime: Intrusión	La entrada de delincuentes o civiles (que no sean autoridades estatales) por medios ilícitos o sin autorización en las instalaciones, los vehículos o los domicilios del personal de agencias de ayuda.
	Criminalidad: Saqueo	Robo durante disturbios, violencia, revueltas u otros levantamientos.
	Criminalidad: Piratearía	Atacar y robar naves en el mar o barcos en los ríos.
	Criminalidad: Atraco	Evento en el que a) el autor no iba armado, b) el personal estaba presente durante el incidente y plenamente consciente de que le estaban robando; y c) se apropiaron de activos.
	Criminalidad: Hurto	Toda situación en la que se roben bienes personales de un empleado o de un lugar sin que la víctima del delito sea consciente de que se están sustrayendo los artículos.
	Criminalidad: Robo de bienes de la organización	Toda situación en la que se roben bienes (por encima de un valor predefinido) de una organización sin que nadie de la plantilla sea testigo de cómo se sustraen los bienes.
	Criminalidad: Vandalismo	Destrucción o daños deliberados a bienes de la organización o del personal.
Daños Daños a los bienes de la agencia.	**Daños materiales**	Todo daño o perjuicio, por encima de una cantidad predefinida, que se haga a los bienes de la organización, bien de manera involuntaria (p. ej., catástrofes naturales, accidentes y similares), bien voluntaria (p. ej., disturbios que provocan daños materiales y similares).

CATEGORÍA AMPLIA	SUBCATEGORÍAS	DEFINICIONES
Muerte La muerte de personal por la causa que sea.	**Muerte: Accidente**	(Véase Accidente)
	Muerte: Intencionada (homicidio)	(Véase ALS)
	Muerte: Natural	Toda muerte que se pueda atribuir a causas naturales, como infarto, enfermedad o apoplejía.
	Muerte: Suicidio	El fallecimiento voluntario e intencionado de alguien del personal por sus propios medios. Se define el suicidio como quitarse la vida de forma voluntaria e intencionada.
Inseguridad general (IG) Incidentes relativos al contexto general que provocan inseguridad y afectan, directa o indirectamente, a la prestación de ayuda. Puede que no afecten directamente a la agencia, su personal o su infraestructura.	**IG: Actividad armada**	Actuaciones por parte de entidades estatales, no estatales o grupos armados organizados que impliquen el uso de armas.
	IG: Ataque a otra agencia	Ataque a otra agencia sobre el que se informa y que no ha afectado a la agencia directamente.
	IG: Golpe de Estado	Golpe de Estado, motín y otras rebeliones por parte de fuerzas armadas. Se define un golpe de Estado como un intento (armado, por lo general) de retirar y reemplazar un gobierno, ya tenga éxito o no, sea violento o no; un intento de golpe puede desestabilizar las fuerzas políticas.
	IG: Fuego cruzado / enfrentamientos activos	Toda situación en la que personal o bienes de la agencia están atrapados en un ataque o tiroteo entre dos o más partes armadas. En dicha situación, la plantilla y los bienes involucrados no son el objetivo del ataque.
	IG: Manifestación	Toda manifestación (incluso protestas, marchas, sentadas, piquetes y similares) que sea no violenta. Reunión masiva de personas con fines políticos o sociales.
	IG: Tiroteo	Tiroteo deliberado de personas que no sean personal de la agencia (véase también ALS: homicidio y UA: armas de fuego).
	IG: Huelga / no presentarse	Decisiones deliberadas por parte del personal de no ir a trabajar por otras razones que no sean enfermedad.
	IG: Disturbios	Disturbios civiles o políticos, así como un comportamiento que se presente como tumultuoso o de muchedumbre. En este comportamiento se incluye el saqueo, los motines en cárceles, multitudes prendiendo fuego, enfrentamientos generales con la policía (normalmente, por parte quienes protestan).
Asesinato, lesión o secuestro (ALS): Incidentes que conlleven el asesinato, las lesiones o el secuestro del personal. Normalmente, eventos críticos.	**ALS: Rapto / secuestro / toma de rehenes / captura**	Todo incidente en el que se capture a personal a la fuerza. Este incidente puede involucrar una petición de rescate o no.
	ALS: Paliza	Incidente en el que se ataca a personal, normalmente con partes del cuerpo (puños, pies) u objetos (palos u objetos contundentes).
	ALS: Muerte: Intencionada (homicidio) / asesinato	Toda muerte que haya sido provocada, por ejemplo por tiroteo, agresión física, envenenamiento, etc. En las muertes intencionadas no se incluyen los suicidios.

CATEGORÍA AMPLIA	SUBCATEGORÍAS	DEFINICIONES
Asesinato, lesión o secuestro (ALS): Incidentes que conlleven el asesinato, las lesiones o el secuestro del personal. Normalmente, eventos críticos.	**ALS: Desaparición**	Incidente en el que desaparece alguien del personal. Diferencias entre desaparición y secuestro: a) por el actor: agentes no estatales suelen secuestrar mientras que los agentes estatales suelen "desaparecer" personas a quienes después se denomina "desaparecidas"; b) por cómo el autor comunica la acción de haber tomado a alguien del personal: los secuestradores suelen presentar demandas (p. ej., rescate) mientras que normalmente no se suele volver a oír de las personas desaparecidas; c) por los motivos: el secuestro suele responder a una demanda concreta mientras que las desapariciones suelen llevarse a cabo para silenciar a alguien del personal, a menudo por motivos políticos.
	ALS: Tortura	Mutilación / lesiones intencionadas que se caracterizan, explícitamente, como tortura del personal. Incidente donde sufre lesiones alguien del personal.
	ALS: Lesiones	La mayor parte de las lesiones que se consideran heridas se infligen con amas, al contrario que en la paliza.
Motivo Clasificación del motivo de los autores.	**Motivo: Ataque**	Ataques directamente dirigidos contra la agencia.
	Motivo: Lugar equivocado en el momento equivocado	Ataques que no iban directamente dirigidos contra la agencia ni contra su personal y que los sufren el personal o los bienes de la agencia por estar cerca de un ataque general o de un ataque dirigido contra otra entidad o persona.
Conato Incidentes que podrían haber provocado perjuicio o haber afectado de otra manera a la prestación de ayuda. Incluye cualquier situación en la que casi se produce un incidente de seguridad, pero que no se produce, cerca de personal / agencia / programa de ayuda, o donde las personas que se vieron afectadas consiguieron evitar perjuicios graves (si se provocan perjuicios, el evento se incluye en ALS).	**Conato: Criminalidad**	El conato se produjo en el contexto de un evento delictivo.
	Conato: Armas explosivas	El conato se produjo en el contexto de la detonación de un arma explosiva (p. ej., bomba de un edificio aledaño o bomba en un restaurante al que suele ir el personal de la agencia). Registra eventos concretos, al contrario que el uso generalizado de armas explosivas en un entorno inseguro.
	Conato: ALS	El incidente evitó por poco que se asesinase, hiriese o secuestrase a personal.

CATEGORÍA AMPLIA	SUBCATEGORÍAS	DEFINICIONES
Medidas de seguridad (MS) Actuaciones por parte de agencias para responder a la inseguridad generalizada o a un incidente de seguridad	**MS: Evacuación: médica**	Evacuación del alguien del personal por motivos médicos, en general con presencia de lesiones o enfermedades que no se pueden tratar adecuadamente en el hospital local ni en la consulta del médico ni en el centro de tratamientos.
	MS: Evacuación: no médica	Evacuación del alguien del personal por motivos de seguridad. Hay que señalar que evacuación se refiere a la retirada del personal del país de operaciones. El traslado de personal a otra ubicación dentro del país por motivos de seguridad se llama reubicación.
	MS: Hibernación	Proceso de resguardarse en el lugar hasta que pase el peligro o se reciba más asistencia.
	MS: Toque de queda impuesto	La imposición de un toque de queda en una ciudad o país donde la organización tenga oficinas.
	MS: Cierre de oficinas	Decisión de cerrar una oficina en respuesta al contexto general de seguridad o a un evento concreto.
	MS: Monitoreo en curso	Proceso de monitorear de forma activa una situación de seguridad con vistas a un cambio potencial de las medidas de seguridad.
	MS: Suspensión del programa	Proceso de modificar de forma considerable las actividades del plan, normalmente deteniendo una actividad o un programa concreto.
	MS: Reubicación	El traslado de personal a otra ciudad u oficina dentro del país de operaciones por motivos de seguridad.
	MS: Viajes limitados, sin toque de queda	Toda limitación sobre viajes que afecte al personal. Este tipo de evento es parecido a un aviso de seguridad para viajes y puede ser la consecuencia de altercados políticos o sociales, brotes de epidemia o catástrofes naturales.
Violencia sexual Incidentes donde personal sufra cualquier tipo de violencia sexual.	**Violencia sexual: Comportamiento sexual agresivo**	Un comportamiento violento en potencia para satisfacer anhelos sexuales.
	Violencia sexual: Intento de agresión sexual	Intento de contacto sexual con el cuerpo de otra persona sin su consentimiento.
	Violencia sexual: Violación	Relación sexual (oral, vaginal o penetración anal) contra la voluntad de la persona y sin su consentimiento.
	Violencia sexual: Agresión sexual	Acto de contacto sexual con el cuerpo de otra persona sin su consentimiento.
	Violencia sexual: Comentarios sexuales no deseados	Insinuaciones verbales, que incluyen silbidos, gritos o enunciar frases o propuestas sexuales implícitas o explícitas que son no deseadas.
	Violencia sexual: Tocamientos sexuales no deseados	Tocamientos de carácter sexual no deseado, independientemente de la intensidad de los tocamientos. Puede incluir masajes, manoseo, agarre o roce de cualquier parte del cuerpo de otra persona.

CATEGORÍA AMPLIA	SUBCATEGORÍAS	DEFINICIONES
Violencia sexual Incidentes donde personal sufra cualquier tipo de violencia sexual.	**Violencia sexual: Acoso sexual**	Insinuaciones sexuales no deseadas, solicitud de favores sexuales y otras conductas verbales o físicas de carácter sexual que afecten al empleo de la persona a la que van dirigidas. Por ejemplo: a) se pone como condición, explícita o implícita, el sometimiento a dicha conducta para contratar a la persona a la que va dirigida, o b) se utiliza que una persona se someta o rechace dicha conducta como pilar para decisiones sobre su trabajo; o c) tal conducta tiene la finalidad o el efecto de interferir de manera no razonable con el rendimiento de una persona en el trabajo o de crear un entorno laboral intimidante, hostil u ofensivo.
Amenaza Amenazas directas o indirectas emitidas por un actor estatal o no estatal que impiden la prestación de ayuda.	**Amenaza: Acoso cara a cara**	Eventos donde una persona o un grupo acosa directamente a alguien del personal (p. ej., acoso a causa de las actividades de un programa de la agencia o de los programas).
	Amenaza: Intimidación cara a cara	Eventos donde una persona o un grupo intimida directamente a alguien del personal (p. ej., personal que se siente intimidado por agentes armados que patrullan cerca de un punto donde se distribuyen alimentos).
	Amenaza: Amenazas cara a cara	Eventos donde una persona o un grupo amenaza directamente a alguien del personal; debería incluir algún tipo de consecuencia si no se obedece (p. ej., una amenaza de represalias por no incluir a alguien en una actividad de la organización).
	Amenaza: Amenaza en remoto contra la agencia	Eventos donde la agencia o su personal reciben una amenaza que no es cara a cara, sino a través de algún mecanismo remoto (p. ej., correo electrónico, SMS, teléfono o amenazas generales publicadas en una página web o en redes sociales (Twitter, Facebook). Pueden incluir amenazas directas que gritan civiles durante manifestaciones).
	Amenaza: Riesgo para la reputación	Eventos que implican un riesgo percibido o real, presente o potencial, para el logo / distintivo de la marca de la agencia, su imagen o su reputación.
	Amenaza: Amenaza de cierre	Eventos que implican la amenaza de cierre forzoso de una actividad, programa o agencia.
	Testigo	Eventos donde el personal es testigo de un ataque o un delito contra otros integrantes del personal, familiares o beneficiarios.
Uso de armas (UA) Registra el tipo de arma que se utilizó en el incidente que afectó a personal, infraestructura o a la prestación de ayuda.	**UA: Explosivos: Bombas aéreas**	Armas explosivas que se lanzan desde el aire, incluso armas incendiarias, salvo bombas de racimo, y misiles tierra - tierra.
	UA: Explosivos: Bombas de racimo	Armas explosivas lanzadas desde el aire o desde tierra que a su vez sueltan munición más pequeña.
	UA: Explosivos: Granada de mano	Artefacto explosivo pequeño que se lanza con la mano, diseñado para detonar tras el impacto o después de un tiempo establecido.

CATEGORÍA AMPLIA	SUBCATEGORÍAS	DEFINICIONES
Uso de armas (UA) Registra el tipo de arma que se utilizó en el incidente que afectó a personal, infraestructura o a la prestación de ayuda.	**UA: Explosivos: Minas**	Toda explosión de minas que involucre al personal.
	UA: Explosivos: Otros	Cualquier otra arma explosiva que no se haya mencionado o sea una combinación de las anteriores.
	UA: Explosivos: RCIED (por sus siglas en inglés)	Artefacto explosivo improvisado a control remoto, como una bomba que se haya dejado a orillas de la carretera y que se detona cuando el objetivo está cerca.
	UA: Explosivos: De tierra	Incluye misiles, morteros o proyectiles que se lanzan desde un sistema móvil o estático, entre otros, granadas propulsadas por cohetes.
	UA: Explosivos: SVIED (por sus siglas en inglés)	Artefacto explosivo improvisado que lleva puesto una persona, p. ej., cinturón explosivo suicida, explosivos en una mochila.
	UA: Explosivos: VBIED (por sus siglas en inglés)	Artefacto explosivo improvisado que va en un vehículo, p. ej., coche bomba o un coche que lleve un artefacto explosivo.
	UA: Biológicas	Todo uso de armas biológicas en una ciudad o país donde la organización tenga oficinas.
	UA: Químicas	Todo uso de armas químicas en una ciudad o país donde la organización tenga oficinas.
	UA: Nucleares	Todo uso de armas nucleares, ya sean explosivas o no, en una ciudad o país donde la organización tenga oficinas.
	UA: Radiológicas	Todo uso de armas radiológicas, normalmente referidas como "bombas sucias", en una ciudad o país donde la organización tenga oficinas. Los incidentes que se pueden producir por armas radiológicas van desde ataques contra centrales nucleares hasta ataques con artefactos nucleares improvisados que se pueden haber construido a partir de material radiológico robado.
	WU: Fuego de armas ligeras	Todo uso de armas de fuego o de mano que involucre a la plantilla o los bienes de la organización.
Ocupación	**Ocupación de las oficinas de la organización**	Confiscar y ocupar cualquier edificio, almacén o recinto de la organización por parte de civiles o agentes gubernamentales.
Otros	**Otros incidentes**	Un incidente que ninguna de las categorías de incidentes predefinidas en esta lista describe adecuadamente. Cabe percatarse de que, en caso de seleccionar esta categoría, quien informa debe dar una descripción completa del incidente en el campo "descripción del incidente".

HERRAMIENTA III: INCIDENTES ORGANIZACIONALES O EXTERNOS

A menudo, las organizaciones se centrarán en el reporte y el registro de incidentes organizacionales (es decir, incidentes que tienen repercusiones para la organización, su personal, sus bienes y su reputación) y no incluyen los incidentes externos (es decir, incidentes que repercuten en otras organizaciones) en su sistema de reporte y registro. La organización debe definir qué constituye un incidente que repercute en la organización y decidir si también se deberían reportar y registrar los incidentes externos.

A continuación se muestra un ejemplo de un cuadro elaborado por una organización como ayuda en el diagnóstico de cuál se considerará un incidente organizacional y cuál no. Se puede adaptar y cambiar, en función de la política y los procedimientos de seguridad de una organización. Más abajo puede encontrar un cuadro sin rellenar.

PERSONA INVOLUCRADA	HORARIO LABORAL		BIENES AFECTADOS DE LA ORGANIZACIÓN		CLASIFICACIÓN
	Sí	No	Sí	No	
Personal que no está en su país de origen (puestos internacionales)	X		X		Incidente organizacional
	X			X	Incidente organizacional
		X	X		Incidente organizacional
		X		X	Si no hubo violencia: No Si fue con violencia: Sí
Personal que está en su país de origen	X		X		Incidente organizacional
	X			X	Incidente organizacional
		X	X		Incidente organizacional
		X		X	No organizacional
Parte interesada externa contratada por la organización	X		X		Incidente organizacional
	X			X	No organizacional
		X	X		En función del tipo de incidente y de bienes, así como de las repercusiones del incidente: sí o no
		X		X	No organizacional

PERSONA INVOLUCRADA	HORARIO LABORAL		BIENES AFECTADOS DE LA ORGANIZACIÓN		CLASIFICACIÓN
	Sí	No	Sí	No	
Personal que no está en su país de origen (puestos internacionales)					
Personal que está en su país de origen					
Parte interesada externa contratada por la organización					

HERRAMIENTA IV: PLANTILLA PARA REPORTAR INCIDENTES

La presente plantilla abarca la información más inmediata que se necesita para gestionar los incidentes de seguridad y para los análisis preliminares.

NÚMERO DE REFERENCIA DEL INCIDENTE:	
Estimación sobre la fiabilidad de la fuente y la validez de la información (según la matriz aprobada):[37]	

1. DATOS DE CONTACTO DEL AUTOR	
Autor del informe:	Nombre completo, puesto (relación con la organización, si es alguien ajeno)
¿Es la persona que hace el informe la involucrada en el incidente?	Sí / No
Fecha del informe:	Fecha de entrega (y versión del informe si no es el primero que se entrega)
2. INFORMACIÓN GENERAL SOBRE EL INCIDENTE	
Ubicación:	Datos exactos de la ubicación del incidente (incluso coordenadas de GPS, si fuera posible)
Fecha del incidente:	Fecha del incidente (si es único) o secuencia detallada de los incidentes si son eventos múltiples.
Hora del incidente:	Hora exacta del incidente (si es único) o secuencia / horario detallado de los incidentes si fueron varios (hora del día / noche).
Programa nacional:	Datos exactos sobre los programas afectados de la ONG
3. CATEGORÍA DEL INCIDENTE	
Tipo de incidente:	Intencionado o accidental; interno de la organización o externo; secuestro, hurto, robo, extorsión, accidente de tráfico, etc.

[37] Se puede indicar al inicio de cada informe o como nota dentro del contenido del informe.

4. INDICAR LA GRAVEDAD DEL INCIDENTE	
Conato	Toda situación donde casi se produce un incidente de seguridad, pero no se produce, cerca de un trabajador, una agencia o un programa de ayuda, o donde aquellos afectados consiguieron evitar perjuicios graves.
No crítico	Las personas no han estado amenazadas física ni psicológicamente. Sin lesiones.
Leve	Las personas han estado amenazadas física o psicológicamente. Lesiones menores que no requieren de un seguimiento médico prolongado.
Grave	Lesiones graves que requieren de un seguimiento médico prolongado. Amenaza grave contra la integridad física o psíquica.
Mortal	Ha fallecido personal como consecuencia directa del incidente.
Todavía se desconoce	
5. DESCRIPCIÓN DEL INCIDENTE	
Un panorama breve pero conciso del evento	
6. VÍCTIMA(S)	
Nombre completo:	Indicar si la víctima es personal nacional o internacional.
Personal nacional / internacional:	¿Qué nacionalidad tiene?
Sexo:	Hombre, mujer u otros
Edad:	¿Qué edad tiene la víctima?
Otros datos pertinentes para el caso:	¿Padecía la persona alguna discapacidad o enfermedad que pudiera tener repercusión en el evento?
Antigüedad y cargo en la organización:	¿Cuánto tiempo llevaba trabajando en el programa? Cargo / responsabilidad de la víctima dentro de la organización.
Estado actual de la víctima:	Ilesa, herida (concretar la gravedad, física o psicológica) o muerta.
7. TESTIGOS	
Indicar el nombre completo y los datos personales de contacto de las personas presentes cuando se produjo el incidente y que puedan ayudar a aclarar los hechos.	

8. ACTUACIÓN INMEDIATA ADOPTADA TRAS EL ACCIDENTE	
Contactos internos:	¿A quién se ha informado dentro de la organización sobre el incidente (en el programa o la misión)?
Contactos externos: *Donantes:* *Otras organizaciones humanitarias / de desarrollo:* *Medios de comunicación:* *Otros:*	¿Con qué autoridades externas (locales o nacionales, administrativas, judiciales o militares) se ha contactado a raíz del incidente?
Actuaciones emprendidas que afectan a los programas:	El incidente tiene consecuencias para el programa, tales como la reducción de plantilla o el cese de actividades o del programa en su conjunto.
Actuaciones emprendidas que afectan al personal involucrado:	Fue necesario realizar un seguimiento / una reunión informativa / un asesoramiento para el personal involucrado en el incidente
9. ANÁLISIS PRELIMINAR: RIESGOS PARA EL PROGRAMA	
Operacionales:	Si el incidente conlleva nuevos riesgos o eleva un riesgo preexistente para las operaciones de la organización, hay que especificarlo aquí. ¿Qué actuaciones para mitigarlos se han emprendido?
Recursos humanos:	Si el incidente conlleva nuevos riesgos o eleva un riesgo preexistente para el personal de la organización, especificarlo. ¿Qué actuaciones para mitigarlos se han emprendido?
Económicos / Materiales:	Si el incidente conlleva nuevos riesgos o eleva un riesgo preexistente en materia económica o para los bienes de la organización, hay que especificarlo aquí. ¿Qué actuaciones para mitigarlos se han emprendido?
Jurídicos / De reputación:	Si el incidente conlleva nuevos riesgos o eleva un riesgo preexistente en materia jurídica o para la imagen de la organización, hay que especificarlo aquí. ¿Qué actuaciones para mitigarlos se han emprendido?
Otros:	¿Qué actuaciones para mitigarlos se han emprendido?
10. APOYO DE SEDE	
Indicar si es necesario el apoyo de sede y, si así fuera, qué tipo de apoyo se necesita.	

HERRAMIENTA V: MATRIZ PARA ANALIZAR INCIDENTES

Esta matriz será de ayuda para analizar las repercusiones y las causas de un incidente y cómo se han realizado la gestión y el seguimiento durante y después de este análisis inicial.

1. IDENTIFICAR LAS REPERCUSIONES DEL INCIDENTE

Duración del incidente	¿Cuánto ha durado el incidente?
Tipo de contexto	Según las categorías de contexto, y tipo y grado de violencia que utiliza la organización.
Fase de seguridad	Según se definen en los documentos sobre seguridad de la organización.
Estimación de pérdidas	
Organizacionales	
Dinero	Indique cuál ha sido el coste directo del incidente para la organización a raíz del mismo (cifras).
Equipo	Indique si se han dañado equipos / bienes y su valor.
Documentación	Indique si faltan documentos sensibles (por ejemplo, una lista de personal) o algo que se utilice para certificar documentos (por ejemplo, sellos).
Otros	
Personales	
Dinero	Indique la cantidad de dinero que el personal ha perdido durante el incidente.
Equipos	Indique si se han dañado durante el incidente equipos que pertenecían al personal y su valor.
Documentación	Indique si faltan documentos personales que pertenecían al personal.
Otros	
Afrontar emociones	Indique si se ha realizado una sesión para afrontar emociones o no. Especificar la fecha.

2. IDENTIFICAR LAS CAUSAS DEL INCIDENTE

FACTORES QUE HAN PODIDO CONTRIBUIR (POSIBILIDAD DE RESPUESTA MÚLTIPLE) ¿EL INCIDENTE ESTABA RELACIONADO CON …?		
Tipo de actividad	El incidente está vinculado al tipo de labor que realiza la organización.	Detallar
Falta de aceptación de nuestro programa	El incidente es fruto de falta de aceptación del programa.	Detallar
Insuficientes medidas de protección	El incidente es fruto de la falta de medidas de protección.	Detallar
Incumplimiento de las normas de seguridad o SOP	El incidente es fruto de incumplir las normas o los procedimientos de seguridad.	Detallar
Imprudencia / falta de vigilancia	El incidente es fruto de la imprudencia o la falta de vigilancia del equipo humano.	Detallar
Carencia de equipos de comunicación	El incidente es fruto de la carencia (por no tener o no funcionar) de los equipos de comunicación necesarios para la seguridad del equipo humano.	Detallar
Conflictos dentro del equipo humano	El incidente es fruto de un conflicto entre dos o más integrantes del equipo humano.	Detallar
Conducción negligente / sin control del vehículo	El incidente es fruto de la falta de capacidad del conductor de manejar el vehículo implicado en el incidente.	Detallar
Comportamiento inadecuado	El incidente es fruto del comportamiento inadecuado de uno o varios integrantes del equipo (infracción del código de conducta, vestimenta inadecuada, etc.)	Detallar
Cambio de contexto	El incidente es fruto del cambio de la situación general (es decir, del contexto).	Detallar
Conflicto cultural externo	El incidente es fruto de conflictos preexistentes entre la comunidad, tales como enfrentamientos étnicos o religiosos.	Detallar
Otros	Describa factores que no se han mencionado que hayan podido contribuir al incidente.	

3. IDENTIFICAR PATRONES Y ACCIONES POTENCIALES

PREGUNTA / PROCESO	RES-PUESTA	IMPLICACIONES POTENCIALES (SEGÚN DIAGNÓSTICO)	ACTUACIONES POTENCIALES DE LA AGENCIA
1. ¿Este incidente se ha producido antes y qué parecido guardan?	Sí	Amenaza pronunciada (que prueba la documentación justificativa).	Comunicar diagnósticos, seguir usándolos como fundamento de las decisiones sobre seguridad.
	No	Amenaza malograda (que prueba la documentación justificativa).	Cambiar diagnósticos y las prácticas de seguridad basadas en ellos.
	No	Amenaza obsoleta (que prueba la documentación justificativa).	Cambiar diagnósticos y las prácticas de seguridad basadas en ellos.
2. Si se siguieron los procedi-mientos adecuados, ¿cuál fue el resultado?	Positivo	Se siguieron los procedimientos adecuados.	Consolidar procedimientos.
		El personal tuvo suerte.	Reconsiderar procedimientos.
	Negativo	Prácticas de seguridad defectuosas.	Reconsiderar prácticas de seguridad.
		Propensión muy elevada al riesgo.	Comunicación con el personal. Formar / volver a formar al personal.
3. Si no se siguieron los procedi-mientos adecuados, ¿cuál fue el resultado?	Positivo	Procedimientos inadecuados.	Reconsiderar procedimientos o aplicabilidad de los mismos en todas las situaciones
		El personal tuvo suerte.	Reconsiderar procedimientos.
	Negativo	Falta de conocimiento de los procedimientos, posiblemente por una de las razones siguientes: • no se realizan sesiones infor-mativas sobre seguridad con el personal nuevo; • carencia de un plan de seguridad (SOP y planes de contingencia); • no se atiende suficiente a proveer al personal con sesiones infor-mativas sobre seguridad y acceso al plan de seguridad; • falta de tiempo y motivación para que el personal lea el plan de seguridad.	Contemplar maneras de comunicar mejor los procedimientos al personal.
		Intento fallido de seguir los procedimientos, posiblemente por una de las razones siguientes: • los procedimientos son demasi-ado complicados para recordar-los y seguirlos; • no se ha impartido la formación necesaria; • el equipamiento necesario no ha estado siempre disponible o en funcionamiento.	Reconsiderar procedimientos, formación, suficiencia del equipo.

PREGUNTA / PROCESO	RES-PUESTA	IMPLICACIONES POTENCIALES (SEGÚN DIAGNÓSTICO)	ACTUACIONES POTENCIALES DE LA AGENCIA
3. Si no se siguieron los procedimientos adecuados, ¿cuál fue el resultado?	Negativo	El personal disiente de los procedimientos, posiblemente por una de las razones siguientes: • procedimientos inadecuados; • se necesita más formación para convencer al personal de la importancia de los procedimientos; • prácticas de contratación inadecuadas; • carencia de mecanismos de cumplimiento dentro de la agencia.	Reconsiderar prácticas adecuadas en materia de seguridad.

4. ANÁLISIS DE LA GESTIÓN DEL INCIDENTE

Reporte a los responsables del programa	¿Se transmitió correctamente la información? ¿Se cumplieron los plazos temporales de la organización?
Árbol de comunicaciones	¿Se transmitió correctamente la información en la ubicación en terreno en su conjunto? ¿Funcionó bien el árbol de comunicaciones?
Funciones y responsabilidades	¿Los responsables supieron qué hacer en función de sus responsabilidades y tareas?
Identificación previa al incidente de personas que sean recursos clave	¿Habíamos identificado previamente y con claridad a personas clave (tanto externas como internas) que nos han ayudado a gestionar el incidente? ¿Hemos intentado contactar con una institución / autoridad para ayudarnos? ¿Identificamos a personas que eran recursos clave? Indicar las personas de contacto.
Comunicación entre terreno y sede	¿Cómo ha ido la comunicación entre sede y terreno? ¿Qué hay que mejorar?
Otros	

HERRAMIENTA VI: CÓMO LLEVAR A CABO UNA REUNIÓN INFORMATIVA SOBRE LOS HECHOS

El proceso de informar sobre los hechos debería empezar tras organizar los primeros auxilios o el tratamiento médico (físico y psicológico) de las personas involucradas. Al organizar una reunión informativa sobre hechos a efectos de recopilar información, aun es importante mantener en mente los principios básicos de los primeros auxilios psicológicos (PAP): realizar la reunión cuando se haya asegurado la seguridad física y psicológica, crear un espacio seguro, el empoderamiento de la persona superviviente, claridad sobre el proceso, las expectativas y las acciones de seguimiento, etc.[38]

Una reunión informativa sobre los hechos no debería confundirse con afrontar las emociones (a menudo denominada ventilación emocional). Un acontecimiento traumático deberían abordarlo profesionales y personal formado que presten primeros auxilios psicológicos.

Al La información que consta a continuación no pretende formar a la persona que la lea sobre primeros auxilios psicológicos ni convertirlas en investigadoras profesionales. Se trata de una lista de consejos para realizar entrevistas seguras y útiles a fin de averiguar los hechos, dentro del marco de reportar el incidente.

Al empezar una reunión informativa sobre los hechos, hay que recordar a toda persona que participe que la finalidad de la reunión es aprender y prevenir, no encontrar culpables.

Preparación para una reunión informativa:

- Identificar quién va a liderar la sesión.
- Identificar quién va a relatar los hechos; los procedimientos organizacionales deberían definir si el personal involucrado en el incidente debería participar en la reunión conjuntamente o por separado. El procedimiento puede establecer si eso es una decisión que se puede contemplar caso por caso, en función del carácter del evento y las limitaciones logísticas. Aunque organizar una reunión colectiva ofrece unas ventajas claras (logísticas, pero también para captar la narrativa), también puede derivar en que se "reescriba" el incidente y se alteren los hechos (testigos y víctimas se influyen mutuamente, varía su percepción, el personal puede

[38] Para más información sobre los primeros auxilios psicológicos, véanse las directrices de la Organización Mundial de la Salud aquí.

temer dar su opinión sobre las causas y las responsabilidades ante otras personas, etc.).

- Informar a las personas que van a relatar los hechos sobre quién va a estar presente.
- Identificar un espacio seguro para celebrar la reunión. Escoger una ubicación segura y adecuada para la persona, como una sala de conferencias o un despacho privado.
- Permitir que la persona que ha de explicar los hechos proponga el mejor momento para celebrar la reunión (teniendo en cuenta otras limitaciones), conforme a los procedimientos de reporte de la organización.
- Hay que preparar las preguntas; las preguntas pueden seguir la plantilla de reporte de incidentes y cubrir los mismos puntos. Puede que no se tengan que formular durante la entrevista, pero pueden servir de guía si se necesita. Deben ser preguntas abiertas.
- Hay que ser consciente de los propios sesgos potenciales y dejarlos a un lado mientras celebra la reunión. El análisis vendrá después.

Pasos durante la reunión:

1. Celebrar la entrevista en un lugar tranquilo y con privacidad. Intentar que la persona se sienta cómoda al llegar, ofreciendo un vaso de agua, té o café. Hay que asegurarse de que no está cansada y de que ya ha realizado la ventilación emocional.
2. Hay que señalar que la finalidad de la reunión es averiguar los hechos, no buscar culpables.
3. No se debe prometer confidencialidad, pero sí contar a la persona que solo se compartirá la información con quienes necesiten conocerla.
4. Se debe ofrecer a la persona un cálculo aproximado del tiempo que va a llevar la reunión.
5. Hay que pedir a la persona que cuente su versión de lo que ha sucedido sin interrumpirla. Se pueden tomar notas o grabar sus respuestas.
6. Pedir aclaraciones a través de preguntas que cubran la información que falta, utilizando preguntas abiertas.
7. Se debe relatar a la persona entrevistada la información que esta ha dado, corrigiendo las incoherencias.
8. Hay que preguntar a la persona qué piensa que podría haber evitado el incidente, centrándose en las condiciones y los acontecimientos previos al evento. Eso puede servir para el análisis.
9. Se debe evitar expresar los propios pensamientos, opiniones o conclusiones sobre el incidente o sobre lo que dice la persona.
10. Hay que informar a la persona entrevistada sobre los pasos siguientes.
11. Se debe agradecer a la persona su participación.
12. Acabar la documentación de la reunión rellenando la plantilla de reporte de incidentes.

Ejemplos de preguntas abiertas:

- ¿Dónde estaba cuando se produjo el incidente?
- ¿Qué estaba haciendo en ese momento?
- ¿Qué observó que podía haber sido inusual?
- ¿Qué vio o escuchó?

- ¿Cuáles eran las condiciones del entorno en ese momento (clima, luz, ruido, etc.)?
- ¿Qué estaba haciendo el personal herido en ese momento?
- En su opinión, ¿qué provocó el incidente?
- En su opinión, ¿cómo se pueden prevenir incidentes parecidos en un futuro?
- ¿Hubo otros testigos? ¿Sabe los nombres de otros testigos?
- ¿Qué relación tiene con otras personas involucradas en el incidente?
- ¿Qué otros detalles querría compartir?

Qué se debe evitar:

- Intimidar, interrumpir o juzgar a la persona.
- Ayudar a la persona en sus respuestas a las preguntas.
- Formular preguntas tendenciosas.
- Formular varias preguntas al mismo tiempo.
- Involucrarse emocionalmente.
- Sacar conclusiones precipitadas.
- Difundir los descubrimientos de la investigación.
- Hacer promesas que no se pueden cumplir.

Análisis:

Se sugiere que durante la reunión se pregunte a la persona por su análisis del incidente para que esté empoderada y tenga la ocasión de compartir comentarios esclarecedores. No obstante, se debe recordar que su criterio puede haberse visto afectado por el evento traumático. Las causas del incidente tendrá que analizarlas la persona que cumplimente el informe del incidente. La finalidad de la reunión informativa para averiguar los hechos es determinar todos los factores que han contribuido a que se produjese el incidente.

Las preguntas siguientes pueden servir para analizar los factores que han contribuido:

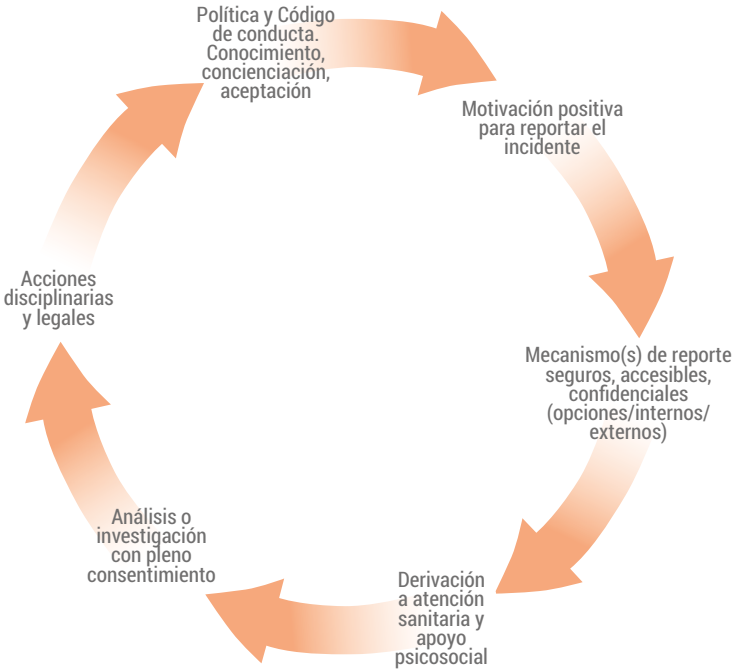
- ¿Han contribuido las condiciones peligrosas?
- ¿Ha contribuido la ubicación?
- ¿Ha contribuido el procedimiento?
- ¿Ha contribuido la falta de equipo de protección personal o de emergencias?
- ¿Han contribuido los SOP? ¿Deberían actualizarse para plasmar una nueva realidad en terreno?
- ¿Han contribuido las dinámicas del equipo? ¿Cómo podríamos mejorar eso?

Expresiones como “el personal fue descuidado” o “el empleado no siguió los procedimientos de seguridad”, “momento inadecuado en el lugar inoportuno” no llegan a la raíz que provoca un incidente. Para evitar estas conclusiones engañosas, hay que centrarse en por qué se ha producido el incidente, p. ej.: “¿Por qué el empleado no siguió los procedimientos de seguridad?”.

HERRAMIENTA VII: BUENAS PRÁCTICAS PARA INFORMAR SOBRE INCIDENTES DE GÉNERO Y MECANISMOS DE DENUNCIA PARA INFORMAR DE EXPLOTACIÓN Y ABUSOS SEXUALES (EAS)

Esta herramienta provee un resumen de buenas prácticas al reportar y hacer seguimiento de incidentes delicados en materia de género y EAS. Debería orientar a las organizaciones en el desarrollo y la adaptación de sus sistemas.

Ciclo para reportar incidentes delicados[39]



Políticas:
Las políticas están en los cimientos de un buen reporte de incidentes y deberían incluir una cláusula sobre denuncia. Se debería hacer especial hincapié en alentar a que se reporten los incidentes. Debería ser obligatorio reportar determinados incidentes, salvo cuando sea la decisión de la persona, como sucede en los casos de acoso o violencia de género. A la explotación y los abusos sexuales (EAS) le corresponde un código de conducta y políticas distintas. El personal tiene el deber de

[39] Esta herramienta se ha extraído de C. Persaud, *Género y Seguridad: Directrices para la transversalización del género en la gestión de riesgos de seguridad,* EISF, 2012.

reportar incidentes de explotación y abusos sexuales o enfrentarse a posibles medidas disciplinarias. Véase más información al respecto más adelante).

Concienciación:
El personal debería ser consciente de lo que constituye un incidente y deberían destacarse las situaciones de las que menos se habla, como son el acoso, la violencia de género, conatos o incidentes pequeños. Se puede sensibilizar sobre el tema al tiempo que se crear un entorno propicio y confianza para alentar a que se reporten los incidentes durante la iniciación, en formaciones, reuniones, etc. El personal debe conocer sus derechos y sus opciones.

Procedimientos / opciones para reportar incidentes:
Se deberían establecer varios canales para reportar incidentes. Eso ofrece más opciones para el personal en función de la comodidad que sientan o la confidencialidad que necesiten. Entre las opciones están: reportar en línea a través de la intranet de la agencia, teléfono de emergencia (gratuito o a cobro revertido), referentes, canales que sortean a algunos cuadros superiores (en casos donde se esté reportando sobre ellos), etc.

Utilidad de referentes:
Los referentes han de ser seleccionados y formados con sumo cuidado según su perfil personal, su aptitud, su capacidad para mantener la confidencialidad y la objetividad. Contar con varios coordinadores diversos (internacionales y nacionales, mujeres y hombres) puede aumentar la comodidad y el acceso a la hora de reportar.

Análisis / investigaciones:
El seguimiento de los incidentes fundamentará a su vez los análisis de riesgos, las medidas de reducción de riesgos o el grado de concienciación del personal. Puede que sea necesario realizar algún tipo de investigación interna, llevada a cabo por personas con una excelente formación, en casos donde se violen las políticas internas. Eso garantizará que se notifique a las autoridades locales / la policía para que realice una investigación externa si se confirma una violación de la legislación del lugar.

Procedimientos disciplinarios:
Si se produce una falta de conducta por parte del personal (en función de la gravedad del incidente y de la legislación local, laboral incluida), se deben adoptar medidas disciplinarias y se deben ejecutar de forma coherente entre personal local / nacional / internacional / masculino / femenino.

Memoria institucional:
Evítese contratar a personas con un historial de cualquier tipo de incidente grave, entre ellos, corrupción, acoso o violencia sexual, incluso explotación sexual, abuso sexual y violencia doméstica. Puede parecer obvio, pero se han dado muchos casos, con pruebas circunstanciales, de volver a contratar a autores de estos hechos en las oficinas de un país distinto —a veces incluso por la misma agencia—. Si la legislación pertinente que rija a empleadores y empleados lo permite, se deben establecer mecanismos de coordinación con otras agencias para crear un sistema a fin de compartir información sobre empleados cuyos contratos

hayan sido rescindidos por haber cometido acoso, violencia sexual o explotación y abusos sexuales. Son imperativas unas prácticas de contratación que incluyan comprobar y examinar referencias.

Marco sobre explotación y abusos sexuales

A continuación, los principios sobre explotación y abusos sexuales que definió el Comité Permanente entre Organismos (IASC):

- La explotación y los abusos sexuales por los trabajadores humanitarios constituyen faltas de conducta graves y son, por tanto, motivo para la rescisión del contrato;
- Los actos sexuales con niños (personas menores de 18 años) están prohibidos independientemente de cuáles sean los criterios locales para la edad de mayoría y la edad de consentimiento. La evaluación equivocada de la edad del niño no es atenuante;
- El ofrecimiento de dinero, empleo, bienes o servicios a cambio de relaciones sexuales, incluidos favores sexuales u otras formas de comportamiento humillante, degradante o abusivo, está prohibido. Esto incluye el ofrecimiento de la asistencia debida a los beneficiarios;
- Las relaciones sexuales entre los trabajadores humanitarios y los beneficiarios deben evitarse, pues se basan en una relación de poder inherentemente desigual y menoscaban la credibilidad y la integridad de la labor de ayuda humanitaria;
- Cuando un trabajador humanitario teme o sospecha explotación o abusos sexuales por parte de otro trabajador humanitario, en el mismo organismo o en otro, debe informar de la situación a través de los mecanismos previstos por el organismo;
- El personal humanitario tiene la obligación de crear y mantener un ambiente que evite la explotación y los abusos sexuales y promueva la aplicación de su código de conducta. El personal directivo a todos los niveles tiene la responsabilidad especial de apoyar y elaborar sistemas para tal fin.

Ciclo para reportar explotación y abusos sexuales[40]

40 InterAction, *InterAction Step by Step Guide to Addressing Sexual Exploitation and Abuse.* InterAction, 2010.

HERRAMIENTA VIII: PLAN DE ACCIÓN PARA EL SEGUIMIENTO DEL INCIDENTE

Esta herramienta presenta preguntas que hay que incluir en el plan de seguimiento que debería ponerse en marcha para cada incidente, independientemente de su gravedad.

Número de referencia del incidente: #

Actuación que debe emprenderse (una línea por cada actuación)	Descripción concisa de la actuación que debe emprenderse
Quién debe hacerlo	Cuál es su ámbito, nombre o puesto
Con quién	Quién va a participar, tanto de dentro como de fuera de la organización
Logística necesaria y presupuesto	Gastos y necesidades estimadas, procedimiento de contratación dentro de la organización
Para cuándo	¿Cuándo ha de ejecutarse la actuación? ¿Fecha fijada o revisión periódica?
Quién se responsabiliza de que se ejecute la actuación	¿Se encargará el responsable? ¿El referente? ¿Otra persona?
Revisión y validación	Quién las hace y cuándo
Revisión y validación	Firma del personal involucrado en su ejecución y control

Estado del incidente:
Estado de la gestión del incidente:

HERRAMIENTA IX: SISTEMAS DE GIIS

Sistemas disponibles para reportar, registrar, almacenar y analizar incidentes de seguridad que afectan a la organización en la esfera central.

MÉTODO PARA REGISTRAR Y REPORTAR INCIDENTES	SISTEMA	VENTAJAS	DESVENTAJAS	FACTORES EN LOS COSTES DE INSTALACIÓN Y FUNCIONA-MIENTO
Narración escrita del incidente	• E-mails • Documento de Google • Plataforma compartida de Google • SharePoint	Costes muy bajos de configuración	Solo funciona bien si se utiliza sistemáticamente. Riesgos: • Se pierde el saber hacer e incluso a veces el acceso en algunos momen-tos cuando se va el personal. • Reportes muy dispares; con implicaciones para poder comparar la información. Requiere dedicarle bastante tiempo	Coste en tiempo del personal que instala el sistema. Coste en tiempo del personal que escribe los informes narrativos. Coste en tiempo del personal que traslada la información a un formato sistemático. Coste en tiempo del personal que lleva a cabo el análisis, lo que puede llevar mucho tiempo ya que el propio sistema no soporta el análisis.

MÉTODO PARA REGISTRAR Y REPORTAR INCIDENTES	SISTEMA	VENTAJAS	DESVENTAJAS	FACTORES EN LOS COSTES DE INSTALACIÓN Y FUNCIONA-MIENTO
Hoja de cálculo de Excel para registrar incidentes mediante una codifi-cación sistemática	Hoja de cálculo de Excel configu-rada para que se registren los campos. Se puede utilizar la hoja de cálculo de Excel para clasificar sistemática-mente la información presentada por escrito.	Bajos costes de configuración No se requieren costes de consultoría, ya que el trabajo se puede hacer internamente con facilidad. Puede funcionar muy bien para organizaciones que empiezan a registrar incidentes y cuyo volumen de incidentes para registrar y gestionar es limitado.	Puede ser difícil de gestionar cuando se rastrean demasiadas categorías y tipos de eventos. Demanda un análisis de tendencias muy manual que puede llevar mucho tiempo. Habitualmente, solo la persona que tiene acceso a la hoja de cálculo conoce y entiende el sistema. Fomenta menos los reportes del personal, ya que puede seguir sin ser conscientes del sistema de registro.	Coste en tiempo del personal para desarrollar un sistema adecuado en Excel. Coste de personal para traducir la información por escrito a categorías codificadas. Coste de personal para llevar a cabo el análisis.
Suscripción a una plataforma en línea para la gestión de datos	Algunas empresas privadas y algunas organi-zaciones sin ánimo de lucro ofrecen plataformas en línea para gestionar la información sobre inci-dentes de seguridad.	Sistemas eficientes respecto a las funciones integra-das de análisis. La mayoría de los sistemas permite distintos niveles de acceso, lo que permite un acceso a medida para el personal en terreno y para el personal directivo. Se externalizan las cuestiones técnicas. El acceso directo para el personal en terreno alienta a que se reporte.	Costes mensuales de funcionamiento. Puede resultar complicado o costoso solicitar cambios para adaptar el sistema a los requisitos específicos de la organización	Tarifa de suscripción.

MÉTODO PARA REGISTRAR Y REPORTAR INCIDENTES	SISTEMA	VENTAJAS	DESVENTAJAS	FACTORES EN LOS COSTES DE INSTALACIÓN Y FUNCIONA-MIENTO
Suscripción a una plataforma en línea para la gestión de datos		Reduce la carga de trabajo para el personal de análisis en sede, ya que el análisis puede ser una función integrada.		
Sistema en línea a medida	Algunas organizaciones han encargado el desarrollo de sistemas en línea específicos para la organización. Algunas organi-zaciones han sido capaces de utilizar sistemas existentes y crear la parte de reportes como una extensión de plataformas existentes que se utilizan	El sistema se corresponde con las necesidades y las definiciones internas de la organización. Si se vincula a sistemas existentes, el personal puede aprender a utilizarlo con mucha más rapidez.	Costes elevados de desarrollo si se precisa de especia-listas externos en informática. Si las organi-zaciones pueden utilizar sus departa-mentos de informática, se reducen los costes. Los costes de mantenimiento pueden ser elevados si se precisa de consultores de informática exter-nos, pero pueden reducirse si lo lleva a cabo el departa-mento interno de informática.	Costes de desarrollo y mante-nimiento.

HERRAMIENTA X: ALMACENAMIENTO DE INCIDENTES

Estructuras básicas al utilizar hojas de cálculo de Excel para almacenar incidentes

Diseñar la estructura perfecta para almacenar información sobre incidentes de seguridad en una hoja de cálculo de Excel es un gran desafío. El amplio abanico de distintos eventos que deberían contemplarse de cara a unas decisiones estratégicas sobre el contexto de seguridad y la información minuciosa que se necesita sobre algunos aspectos imposibilita contar con una estructura sencilla que se adecue a todas las situaciones. El desafío consiste en encontrar el equilibrio adecuado entre mantenerla dentro de una sencillez y funcionalidad y que aun así almacene la información clave que se necesita, lo suficientemente detallada como para que la información sea significativa al recomendar unas políticas u otras.

El presente manual orientativo ofrece ejemplos de dos formatos distintos para almacenar información sobre incidentes en una hoja de cálculo de Excel. Se anima a las organizaciones que diseñan su propia hoja de cálculo a mirar ambos ejemplos y a combinar y acoplar los elementos que sean más apropiados en función de sus prioridades. Se aconseja consultar otras herramientas para ver las definiciones que se proponen de los distintos campos.

Se puede acceder a las dos hojas de cálculo de Excel de ejemplo y descargarlas desde la página del proyecto de RedR. Consulte los elementos que se presentan a continuación:

- Hoja de cálculo con Categorías de Evento SiND
- Plantilla de documento de registro de incidentes

A continuación se muestran los principios básicos que se deben tener en cuenta al diseñar una hoja de cálculo de Excel destinada a información sobre incidentes de seguridad.

Unidades de análisis

En una hoja de cálculo de Excel, cada fila almacena una unidad de información clave. En la mayoría de los casos, esta será el evento. Cada fila es un único evento. Las columnas se utilizan para dar detalles sobre el evento.

Para almacenar otras unidades de información, como tratar al personal como unidades individuales (en lugar de como un número asociado a un evento) o para registrar datos sobre el material que se ha perdido o rastrear una respuesta, se puede hacer lo siguiente:

- Crear una segunda / tercera / cuarta hoja en el libro de Excel para "personal", "material" o "respuesta". En estas nuevas hojas de cálculo, cada fila almacena la información particular sobre cada persona, cada artículo dañado o perdido, o cada respuesta, etc. Así, cada hoja de cálculo cuenta una unidad distinta. Si a cuatro personas de la plantilla les afectó un evento, la hoja de cálculo del evento tendrá una fila (una unidad) para el evento, pero cuatro filas (cuatro unidades) sobre personal (véanse ejemplos más abajo). Si se dañaron dos coches en el evento, la "hoja de material" tendrá dos filas, una por cada uno de los coches. Cada persona de la plantilla y cada coche, por lo tanto, se convierte en una unidad en sí misma. Esas hojas se pueden utilizar para almacenar detalles con los que es útil contar para el análisis general.

    - La ventaja de este sistema reside en las facilidades que da para un análisis minucioso más allá de la descripción del evento. También se pueden utilizar menús desplegables de categorías múltiples y exclusivas que se eligen para cada elemento. La hoja incluye más información de una manera más condensada. La desventaja es que los datos se hacen más complejos.
    - Si se abren hojas de cálculo adicionales, es esencial utilizar números de identificación únicos para cada evento en la primera columna, como garantía de que se puede vincular de nuevo la información al evento.

- Integrar una unidad distinta (como personal, material, etc.) en la hoja donde la unidad de análisis es el evento. Eso se puede hacer creando una serie de columnas adicionales cada vez que la unidad de cálculo cambia de evento a personal, material o respuesta. Se pueden utilizar distintos colores para señalarlo.

    - Por ejemplo, las columnas podrían incluir el número de personas de la plantilla a las que ha afectado el evento mediante tantas columnas adicionales como sean necesarias para clasificar a todo el personal con información adicional, que entonces debe dividirse en columnas de opciones múltiples (véase la hoja de cálculo de Aid Worker Security Database como ejemplo de hasta qué punto de detalle se puede registrar información en paralelo sobre personal).

Algunas diferencias en la información de hojas de Excel únicas o múltiples

A continuación, los ejemplos muestran la misma información sobre cuatro personas a las que afectó un único evento almacenada por unidad de análisis "evento" y por unidad de análisis "personal". Almacenar la información sobre el personal en una hoja de cálculo donde la unidad de análisis es el evento requiere más columnas para almacenar menos detalles. Tampoco se pueden almacenar datos sobre individuos (sería todo un reto añadir información sobre el puesto o si el seguro ha cubierto el asesoramiento posterior al incidente). Si se pone el personal como unidad de análisis, es fácil registrar información más detallada. Esos detalles adicionales podrían servir para advertir tendencias o para identificar recomendaciones de actuación concretas, por ejemplo en referencia a la cobertura del seguro.

Hoja única para unidades de evento:

UNIDAD DE ANÁLISIS	NÚMERO DE PERSONAS EMPLEADAS AFECTADAS	MUJER	HOMBRE	PERSONAL INTERNACIONAL	PERSONAL NACIONAL	OTROS	MUERTOS	HERIDOS
Evento 1	4	1	3	1	2	1	1	3

Hojas múltiples para unidades distintas (p. ej., personal, material o respuesta):

UNIDAD DE ANÁLISIS	IDENTIFICACIÓN ÚNICA DE EVENTO	SEXO	ESTATUS	PUESTO	IMPACTO	ASESORAMIENTO CUBIERTO POR SEGURO
Personal 1	Evento 1	Mujer	Personal internacional	Técnica	Heridas	Cubierto
Personal 2	Evento 1	Hombre	Personal nacional	Conductor	Muerte	No aplicable
Personal 3	Evento 1	Hombre	Personal nacional	Técnico	Heridas	Sin cobertura
Personal 4	Evento 1	Hombre	Voluntario	Voluntario	Heridas	Sin cobertura

Opciones múltiples o mutuamente excluyentes
Se puede registrar la información con opciones múltiples (que se aplica más de una descripción) o con opciones mutuamente excluyentes (que solo se puede aplicar una opción).

- **Las opciones múltiples** se presentan en columnas, una al lado de la otra. Cada columna representa una característica concreta y se utiliza la hoja de cálculo para indicar que se aplica al evento la opción específica. Se puede hacer eligiendo "sí", un número (p. ej., 1) o una opción de una lista desplegable. Las opciones que no se aplican se dejan en blanco (menos trabajo de codificación) o se indica que no se aplican eligiendo "no aplicable" o "0" (esto facilita la comprobación que las cifras totales son correctas y descubrir errores).
- **Las opciones mutuamente excluyentes** se presentan en forma de opciones, enunciadas en una lista desplegable, que se pueden elegir al rellenar la información en una columna determinada. Las listas desplegables permiten registrar información adicional y aseguran una coherencia en la ortografía. No obstante, deberían utilizarse únicamente cuando solo se puede aplicar una opción. Véase Hoja de cálculo con Categorías de Evento SiND para ejemplos de desplegables.
- **Las opciones múltiples y las mutuamente excluyentes** se pueden combinar en la gestión de datos. Una hoja de cálculo bien diseñada puede contener una serie de columnas con opciones múltiples (p. ej., pueden aplicarse todas o algunas de las opciones a cada evento y se rellenan las columnas como convenga). A estas opciones se asocia una lista de opciones mutuamente excluyentes en forma de lista desplegable (p. ej., cada vez que se elija una de las opciones, el sistema no solo indica "sí" o un número, sino que especifica la subcategoría debajo de la opción). Para ver un ejemplo de dicho sistema, consulte la Hoja de cálculo con Categorías de Evento SiND.

HERRAMIENTA XI: TECNOLOGÍA PARA REPORTAR Y REGISTRAR INCIDENTES

Cada uno de los sistemas para reportar y registrar es distinto y tiene sus propias ventajas y desventajas. El modelo más adecuado para una organización potencial dependerá del grado de capacidad tecnológica que tenga la agencia, la magnitud de sus operaciones, tamaño y recursos económicos, etc.

Véase la tabla a continuación, donde se comparan algunos sistemas en línea para reportar incidentess.[41]

	TARIFA	CÓDIGO ABIERTO (GRATIS)	CON LICENCIA	INDEPENDIENTE	SOFTWARE COMO SERVICIO	NORMAL	A MEDIDA	GRÁFICOS INTEGRADOS	GRADO DE PROTECCIÓN DE LOS DATOS
Ushahidi		•		•		•			••
SIMSON	•		•		•	•		•	••
Open DataKit		•		•		•		•	••
SharePoint	•		•	•	•	•		•	••
NAVEX Global™	•		•		•		•	••	••
IRIS	•		•				•	•	••
RIMS			•				•	•	••

•• Sin analizar

El apartado siguiente presenta las ventajas y las desventajas de los sistemas que utilizan en la actualidad las organizaciones que han contribuido al presente manual. Para saber más sobre uno de los sistemas, siga los enlaces que aparecen.

[41] Parte de la información que se comparte en esta herramienta se ha extraído de un artículo todavía sin publicar: G. de Palacios, "*Managing security-related information: a closer look at incident reporting systems*", EISF, próximamente.

SharePoint
Es una aplicación web integrada en Microsoft Office. Se vende principalmente como un sistema de gestión y almacenamiento de documentos; sin embargo, el producto se puede configurar de muchas maneras y su uso varia considerablemente entre una organización y otra. Aunque exige comprar una licencia para su uso, algunos de los productos de Microsoft Office 365 son gratuitos para las organizaciones sin ánimo de lucro. SharePoint es un sistema que se puede utilizar para compartir información de distintas maneras; se pueden crear formularios en línea a los que solo pueden acceder usuarios autorizados.

VENTAJAS	LIMITACIONES
Al ser un producto Microsoft, es compatible con software de ofimática, como Word, Excel, PowerPoint, etc. Eso permite a una organización exportar con facilidad los datos desde el sistema hasta estas aplicaciones y compartir y analizar la información utilizando un software conocido. Puede que no se necesite instalar nuevo software ni formar al personal sobre el uso de la nueva plataforma. Se puede gestionar internamente el desarrollo del sistema, puesto que se puede encargar el equipo informático que ya desarrolla y mantiene SharePoint.	Aunque se pueden hacer encuestas a través de SharePoint, no es un software especialmente diseñado para reportar ni para recopilar datos. La representación de datos en un mapa no está incorporada por defecto en el sistema y tendría que hacerse instalando un complemento adicional.

Ushahidi
Ushahidi se desarrolló para mapear informes de violencia en Kenia durante la violencia postelectoral de 2008 y después de la misma. Se pueden enviar los informes a través de varias plataformas con un formulario en línea, correo electrónico, mensaje de texto o redes sociales, como Twitter. Cuando se reciben estos informes, un administrador puede revisarlos para así validar y aprobar el contenido, de forma que puedan aparecer en el mapa de su página principal.

Ushahidi es un software gratuito y de código abierto para recopilar, visualizar y mapear interactivamente información. Se puede adaptar el formulario del informe para que una organización pueda recabar la información que le sea importante; una vez se hayan validado los informes, se pueden ver reflejados en un mapa agrupados por categorías predefinidas de incidentes. La plataforma se puede programar para alertar a los responsables de seguridad cuando se reporte un nuevo incidente, para que puedan dar apoyo a las víctimas y validar el informe. Ushahidi también puede alertar a otros usuarios una vez se haya validado el informe.

VENTAJAS	LIMITACIONES
La principal ventaja de Ushahidi es que se puede descargar gratis desde internet. No es complicado instalar el sistema y desde que la organización decide en qué servidores instalar el software, los datos permanecen bajo el control de la organización.	La principal desventaja de Ushahidi es que la representación estadística de la información que se incluye en la base de datos no está integrada en el sistema, y han de combinarse soluciones externas a estos efectos. Es una solución magnífica para recopilar datos, pero se necesitan otros recursos para analizar los datos. La plataforma de Ushahidi ya no está en desarrollo, lo que podría causar problemas dado que otras tecnologías relacionadas siguen evolucionando. El personal de informática podría resolver estas cuestiones potenciales.

SIMSON

El sistema SIMSon fue diseñado por el Centre for Safety and Development (CSD) para ONG, específicamente. SIMSon es un sistema en línea para reportar incidentes de seguridad donde los usuarios pueden ver representados en un mapa los incidentes sobre los que se ha reportado. Las ONG que utilizan SIMSon no tienen que instalar, programar ni escribir el código de ningún software. El Centre for Safety and Development (CSD) también da soporte con el funcionamiento de la plataforma y la gestión de copias de seguridad. Se pueden filtrar los incidentes por categorías, organización, ubicación, marco temporal y otras informaciones e indicadores relacionados con la seguridad. Los usuarios reciben alertas por correo electrónico de nuevos informes de incidentes, en función de su lugar en la organización y de sus derechos de acceso derivados. Se pueden analizar los incidentes dentro de SIMSon mediante el uso de gráficos y tablas. Los datos sobre incidentes también se pueden descargar como un archivo de Excel. Se pueden cargar los documentos y los informes de incidentes y, a discreción de la organización, se pueden compartir con otras partes interesadas (por ejemplo, aseguradoras u otras ONG). Existe un procedimiento especial para "incidentes sensibles", que solo informa a personal designado dentro de la organización. Esto es pertinente cuando se trata de incidentes de agresión sexual, por ejemplo.

Para saber más, se puede descargar un resumen de funcionalidades de SIMSon de la página web del CSD siguiendo este enlace.

VENTAJAS	LIMITACIONES
El sistema está preparado para su uso y dirigido a ONG, con el apoyo del CSD. Por lo tanto, las organizaciones no tienen que invertir recursos en su desarrollo, mantenimiento ni copias de seguridad. Los datos sobre incidentes se pueden analizar dentro de SIMSon o exportando los datos a un archivo Excel.	Aunque el CSD garantiza a las organizaciones que utilizan el sistema que, si así lo eligen, son las únicas que pueden ver sus informes sobre incidentes, las ONG pueden querer controlar sus datos de seguridad e incidentes y pueden ser reacias a delegar dicha responsabilidad en terceros. Puede que no sea fácil adaptar el formulario de reporte a las necesidades específicas de la organización.

World Vision International y NAVEX Global

World Vision International (WVI), en colaboración con el proveedor internacional de informes sobre riesgos NAVEX Global, han creado un sistema en línea para reportar incidentes que comunica incidentes, quejas, acoso y otros eventos. Este sistema va más allá de la mera comunicación de incidentes de seguridad y abarca otros elementos de la gestión de riesgos, como son la corrupción, las demandas, la reputación, etc., en varios idiomas. NAVEX Global adapta su sistema de reporte a las necesidades y las características de la organización que lo utiliza. El sistema para reportar incidentes permite incluir información de diversas fuentes y todo el personal de WVI puede reportar a la plataforma, ya que también sirve como sistema de denuncia.

Para saber más sobre el sistema de reporte de incidentes de World Vision International, véase el siguiente documento.

VENTAJAS	LIMITACIONES
Al combinar el formulario para reportar incidentes con el canal para denuncias, los mecanismos de quejas de beneficiarios, etc., se reduce la posibilidad de utilizar varios sistemas para fines parecidos. Contar tras el sistema con el respaldo de una empresa dedicada a cuestiones éticas y a la gestión de cumplimiento puede servir para poner los datos del reporte de incidentes en perspectiva con otros campos de la gestión de riesgos.	El formulario puede ser muy minucioso, en comparación, lo que, a pesar de sus ventajas, puede desalentar a reportar a causa del largo proceso que implica. Además, es probablemente una solución que solo se pueden permitir organizaciones grandes.

IRIS

Basada en Ushahidi, IRIS es una plataforma que se puede utilizar para reportar incidentes a través de una interfaz en línea y para visualizar en un mapa dónde se han producido dichos incidentes. Se puede adaptar la plantilla de informe de incidentes para incluir las necesidades al reportar de la organización que utiliza el sistema.

Se puede utilizar la plataforma como "software como servicio" (SaaS, por sus siglas en inglés), así como instalarla en los servidores de una organización, lo que permite un control absoluto de los datos que se reporten. Solo pueden acceder a la interfaz usuarios registrados y se pueden configurar distintos privilegios en función del perfil del usuario. Se pueden entregar los informes a través de la interfaz en línea o a través de una conexión de ancho de banda pequeño.

La plataforma es plurilingüe y se pueden filtrar los informes por defecto o por campos a medida. Los responsables y otros usuarios pueden recibir alertas cuando se reporten nuevos incidentes, de forma que se pueda ofrecer apoyo inmediato a las víctimas mientras que se informa al resto del equipo para actuar como convenga.

Se pueden extraer datos de la plataforma y usarlos para alimentar el software de visualización de datos para que se puedan utilizar las estadísticas sobre incidentes para extraer lecciones aprendidas, dar recomendaciones, ofrecer información, tener información de fondo sobre análisis de riesgos, etc.

VENTAJAS	LIMITACIONES
Fácil de instalar y de utilizar, con un aspecto y una forma de recabar información muy a medida. IRIS se basa en la versión 2 de Ushahidi, que, al ser una plataforma de código abierto, puede desarrollarse para incorporar las necesidades respecto al reporte que tengan las organizaciones que la utilizan, adaptarla a nuevos desarrollos y tecnologías, y hacerla compatible con otros sistemas existentes. Los usuarios son ilimitados y funciona sin licencia, de forma que las organizaciones solo pagan por la instalación y la adaptación. Se pueden importar los datos existentes sobre incidentes al sistema una vez instalado.	Habría que desarrollar la conexión entre la lista de usuarios y el directorio activo de la organización, pero se pueden crear los usuarios uno por uno y otorgar el acceso a la información durante el proceso. Se concibió el software original para compartir información reportada, en términos amplios. Aunque se puede tener un perfil de usuario que sea "solo para reportar", ha de planificarse con atención cómo limitar el acceso a la información.

RIMS

El servicio de gestión de incidentes de la Risk Management Society (RIMS) ofrece un sistema sencillo, fácil de utilizar que se basa sobre todo en descripciones de incidentes en forma de test. Permite categorías a medida para codificar aspectos de los eventos. Se pueden instalar gráficos. La plataforma solo existe en inglés.

En el ejemplo que se contempla, fue principalmente el departamento de Recursos Humanos quien utilizó el sistema respecto a seguros. El uso del sistema para análisis de incidentes de seguridad fue limitado. Por lo tanto, no se pudo juzgar cómo habría funcionado este sistema si se hubiera configurado por completo para atender las necesidades de gestión de la información sobre incidentes de seguridad más allá de las descripciones sobre incidentes en forma de test y, en concreto, las necesidades de análisis.

VENTAJAS	LIMITACIONES
Es fácil de usar. El personal puede utilizar el sistema para reportar incidentes sin mucha formación. Es fácil configurar campos a medida y navegar por el sitio. Es un sistema fácil y muy accesible para almacenar descripciones de incidentes de seguridad.	Los ejemplos revisados usaban principalmente descripciones de eventos en forma de texto. El sistema no envía recordatorios.

HERRAMIENTA XII: ANALIZAR Y COMPARAR TENDENCIAS DE DATOS

Orientaciones para comparar los datos de tendencias de la organización con datos sobre incidentes de seguridad más amplios.

Preguntas y consideraciones clave

- ¿Cuáles son los parecidos y las diferencias en las tendencias entre la organización y las que aparecen dentro de los datos unificados?
- ¿Por qué existen parecidos y diferencias? Pensar sobre cada aspecto observado por separado y preguntarse:
  - ¿Por qué se ven parecidos o diferencias en esta subcategoría de tipos de incidentes?
  - ¿Se debe al entorno externo general?
  - ¿Cómo afectan a estas tendencias los países en los que trabaja la organización o los programas que realiza la organización?
  - ¿Alguna de las diferencias podría ser el resultado de las prácticas de reporte (de la organización o de otras)?
  - ¿Dónde tiene la organización más incidentes de un tipo concreto?
  - ¿Dónde tiene la organización menos incidentes de un tipo concreto?
- Buscar parecidos en las tendencias e intentar explicarlos.
- Observar las diferencias. Intentar proponer una explicación de las diferencias.
- Ser preciso. Si se sabe que algo es un hecho, ha de manifestarse. Si se piensa pero no se tienen pruebas, hay que utilizar un lenguaje que lo señale, como “los datos indican” o “a partir de la información disponible, parece que…”.
- Identificar tendencias clave:
  - ¿Qué tendencias clave se pueden detectar?
  - ¿Sugieren los datos tendencias emergentes que deberían tener en cuenta las organizaciones?
- Describir las tendencias de la forma más concisa posible:
  - ¿Son tendencias mundiales?
  - ¿Existen tendencias en un país concreto?
  - ¿A qué categoría de eventos de seguridad se refieren?
  - Ser todo lo concreto que se pueda nombrando tipos de incidentes que se vea aumentar y dónde puede estar sucediendo eso. Si se puede, dar detalles de quién o qué puede verse especialmente afectado.

- Pensar en las tendencias generales del contexto amplio de la ayuda como se muestran en el análisis de tendencias o como se ven por los datos, ya sean mundiales o de país. Intentar describir el contexto general de prestación de ayuda, cambios recientes y amenazas o tendencias emergentes.
- Pensar en las diferencias en tendencias entre los datos de la organización y los de otras agencias (sin incluir las que son producto de diferencias en el modo de reportar). Considerar los países en los que trabaja la organización, qué programas presta la organización y los puntos flacos o fuertes en el marco de la gestión de riesgos de seguridad de la organización.
- Si se está haciendo por segunda o tercera vez, pensar en las diferencias entre los datos más recientes y análisis previos. Describir los cambios y proponer explicaciones a los mismos.
- Identificar actuaciones que haya que adoptar:
  - ¿Surge alguna pregunta al contemplar los datos que se pueda seguir de cerca?
  - ¿Quién puede ayudar a averiguar más cosas?
- Contactar con la oficina de país / región / el proveedor de servicios de información con preguntas para examinar la realidad tras las tendencias de datos.
- Pensar en qué incluir en el plan de acción para ponerlo en marcha en las próximas semanas / meses.

Desarrollar el plan de acción

- ¿Sugieren los datos que el referente de seguridad debería adoptar medidas concretas?
- ¿Sugieren los datos que deberían añadirse nuevos riesgos emergentes o situaciones que van en aumento a los formularios de consentimiento informado para tratarlos con el personal?
- ¿Sugieren los datos que debería hacerse especial hincapié en un tipo de evento específico durante la formación para un contexto concreto?
- ¿Destacan los datos riesgos específicos que deberían tratarse más minuciosamente con los referentes de seguridad de país y región para ver si se necesitan cambios en las políticas?
- A raíz de los datos, ¿destacan asuntos que tienen que llevarse ante el personal directivo de la organización?
- ¿El análisis de los datos sugiere que la organización necesita mejoras en la gestión de información sobre incidentes de seguridad en algún ámbito dentro de la organización?

Cuestiones posibles que remarcar a compañeros en terreno o de cargos directivos / junta

- Nombrar tendencias concretas que deberían observarse de cerca. Proponer que se incluyan en un plan de revisión habitual.
- Destacar un riesgo concreto y específico y proponer que se hable internamente de un umbral de riesgo aceptable para un tipo concreto de evento en un contexto concreto para ayudar a formular políticas claras.
- Proponer actividades específicas para mejorar la gestión de información sobre incidentes de seguridad y, así, la capacidad de la organización de detectar tendencias y solicitar luz verde para ejecutar elementos específicos (véase la matriz de autodiagnóstico para consultar elementos concretos que se pueden mejorar).

Comunicar las conclusiones definitivas y el plan de acción

Elaborar el borrador de un documento claro y conciso que:

- cite las fuentes y los métodos utilizados;
- muestre que se han considerado los datos y que se confía en los hallazgos (se puede incluir que se ha desechado la idea de investigar más sobre un aspecto concreto porque se piensa que es producto de sesgo en el reporte);
- presente una lista clara con las tendencias que se considere que son preocupantes; de ahí, se elige un máximo de tres y, si se trata de algo que se haga con regularidad, se incluyen las tendencias clave del análisis anterior;
- presente una lista con las actuaciones que se recomiendan:
- para la persona que elabora el documento, aclarando qué ha estado haciendo, qué está haciendo actualmente o qué hará en los próximos meses para abordar las necesidades identificadas;
- para otros compañeros (en terreno o en cargos superiores). Se mantienen estas tareas para otras personas como una tarea única, proponiendo cómo se estará facilitando el proceso y qué se va a necesitar de ellos, como su opinión, su apoyo, etc.

Comparar los datos con los que ha unificado Insecurity Insight mediante la Security in Numbers Database de Aid in Danger utilizando análisis de tendencias publicados o consultando Humanitarian Data Exchange, además de los datos anteriores sobre incidentes de seguridad que tenga la organización.

Véase un ejemplo de informe que analiza las tendencias de datos de múltiples agencias aquí.

HERRAMIENTA XIII: PREGUNTAS ESTRATÉGICAS PARA DECISIONES REFERENTES A LA GESTIÓN DE INFORMACIÓN SOBRE INCIDENTES

Tras una buena visión de conjunto de qué tipo de incidentes de seguridad se producen cuándo, cabe observar los datos y pensar si indican alguna acción necesaria de seguimiento. Hay que buscar información adicional y finalizar el informe sobre incidentes de seguridad con recomendaciones específicas.

La lista de preguntas siguiente puede servir a los referentes de seguridad para elaborar conclusiones estratégicas y recomendaciones de actuación adicionales después de un buen análisis de incidentes de seguridad de eventos pasados.

PREGUNTAS QUE PLANTEARSE AL OBSERVAR LOS DATOS ANALIZADOS SOBRE INCIDENTES DE SEGURIDAD	POSIBLE ACTUACIÓN DE SEGUIMIENTO	POSIBLE RECOMENDACIÓN DE ACTUACIÓN QUE AÑADIR AL FINAL DEL INFORME SOBRE EL ANÁLISIS
1. ¿Qué clase de incidentes de seguridad vivieron el personal y la organización? **2. ¿En qué países se produjeron?**		
¿Nuestra organización prepara debidamente al personal para la clase de eventos que puede vivir?	Averiguar en qué medida las personas han sido bien preparadas para los tipos de eventos que se producen. Averiguar los costes de cursos pertinentes y añadir un presupuesto estimado.	Proponer que se necesita una formación específica o cursos de sensibilización para el personal que trabaja en contextos que se ven afectados por tipos concretos de incidentes.
¿Cubre el seguro las respuestas necesarias, bien para el personal, bien para asumir los daños materiales?	Averiguar de mano del personal afectado si ha recibido o querría recibir asesoramiento profesional tras el incidente. Averiguar si el seguro cubre dicho asesoramiento. Averiguar cuán fácil o caro fue sustituir los artículos perdidos (seguro u otros).	Indicar cualquier fallo en la cobertura del seguro. Indicar una estrategia para solucionar las pérdidas materiales en los contextos de los países donde esto parece ser un riesgo más agudo.

PREGUNTAS QUE PLANTEARSE AL OBSERVAR LOS DATOS ANALIZADOS SOBRE INCIDENTES DE SEGURIDAD	POSIBLE ACTUACIÓN DE SEGUIMIENTO	POSIBLE RECOMENDACIÓN DE ACTUACIÓN QUE AÑADIR AL FINAL DEL INFORME SOBRE EL ANÁLISIS
3. Como referente de seguridad en sede, ¿cuál es el grado de satisfacción con la forma en la que las oficinas en país parecen haber utilizado los incidentes de seguridad y los conatos para aprender y mejorar sus prácticas? **4. ¿Cuáles son los incidentes de seguridad que otras organizaciones sufren en el mismo país y cuál es la comparación con los incidentes de los que se ha reportado dentro de la propia organización?**		
¿Existen oficinas de país que pueden no estar reportando de forma sistemática a sede?	Intentar conversar con personal clave para averiguar por qué no se reportaron incidentes o por qué solo se reportaron unos pocos.	Recomendar que se revisen las instrucciones sobre cómo y cuándo reportar. Recomendar cambios en el sistema de reporte de forma que aliente a reportar sistemáticamente Recomendar un mayor respaldo por parte de la directiva al remarcar los beneficios de reportar de manera sistemática.
¿Existen oficinas de país que sufran determinados tipos de incidentes? ¿Qué comparación guardan dichos incidentes con los que viven otras organizaciones?	Intentar conversar con personal clave para averiguar por qué determinados incidentes se producen con frecuencia o nunca.	
5. ¿Cómo afectaron los incidentes de seguridad a la prestación de ayuda? **6. ¿Podemos evaluar el coste que tienen las repercusiones de los incidentes de seguridad sobre la prestación de ayuda?**		
¿Los compañeros han reportado en qué medida los incidentes trastornaron su labor?	Intentar conversar con compañeros sobre la mejor manera de describir las repercusiones de los incidentes de seguridad en la prestación de ayuda	Añadir declaraciones sobre cómo los incidentes de seguridad han afectado a la prestación de ayuda.
¿Los compañeros han evaluado los costes de la pérdida de tiempo de la plantilla y las pérdidas materiales?	Intentar conversar con el personal sobre la mejor manera de evaluar los costes de la pérdida de tiempo de la plantilla y de las pérdidas materiales.	Añadir declaraciones sobre los costes de los incidentes de seguridad para las operaciones.
¿Los compañeros han reportado en qué medida ha afectado el incidente de seguridad al acceso?	Intentar conversar con el personal y que se describa cómo afecta la seguridad al acceso a poblaciones beneficiarias y a cuántas personas no se consiguió llegar a causa de los problemas de seguridad.	Añadir declaraciones sobre cómo afectan los incidentes de seguridad al acceso a poblaciones.

PREGUNTAS QUE PLANTEARSE AL OBSERVAR LOS DATOS ANALIZADOS SOBRE INCIDENTES DE SEGURIDAD	POSIBLE ACTUACIÓN DE SEGUIMIENTO	POSIBLE RECOMENDACIÓN DE ACTUACIÓN QUE AÑADIR AL FINAL DEL INFORME SOBRE EL ANÁLISIS
7. ¿Cuáles fueron los principales contextos de los incidentes de seguridad? **8. ¿Se puede clasificar el contexto de los incidentes por la estrategia de respuesta que estos demandan?**		
¿Cuántos de los incidentes pueden haberse producido por errores en una buena estrategia de aceptación? ¿En qué zonas falló la aceptación? ¿Entre actores no estatales, autoridades, beneficiarios, personal, subcontratistas u otros?	Intentar conversar dentro de la organización sobre la mejor estrategia de aceptación y cómo aplicarla de forma efectiva.	Nombrar la zona o la población meta para las que debe desarrollarse una mejor estrategia de aceptación. Proponer una formación mejorada sobre estrategia de aceptación para el personal que vaya a un país concreto o que trate con un tipo de actor concreto.
¿Cuántos incidentes pueden haberse producido porque el personal no respetó las normas o las normativas o se comportó de una manera irresponsable?	Intentar conversar dentro de la organización sobre cómo potenciar el código de conducta ética con el personal y asegurar que se cumplen los procedimientos de seguridad.	Hacer una lista de aspectos de conducta que se deberían incluir en un código de conducta de obligado cumplimiento para el personal. Hacer una lista de áreas de conducta donde el personal no respetó las normas y proponer mecanismos para hacer que se cumplan mejor.
¿Cuántos de los incidentes se pueden haber producido por factores personales relativos a los orígenes, al pasado o a las relaciones familiares del miembro del personal?	Intentar conversar dentro de la organización sobre cómo abordar los factores de riesgo relativos a la vida doméstica, orígenes étnicos u otros factores privados.	Hacer una lista de contextos y países donde se pueden necesitar políticas o procedimientos específicos, que podrían incluir, entre otros: • cómo responder si alguien del personal sufre violencia doméstica; • cómo responder cuando existe riesgo de discriminación o violencia por perfil étnico; • qué código de conducta ética se puede esperar del personal local allí donde intereses empresariales o políticos de su familia amplia podrían afectar al personal.

PREGUNTAS QUE PLANTEARSE AL OBSERVAR LOS DATOS ANALIZADOS SOBRE INCIDENTES DE SEGURIDAD	POSIBLE ACTUACIÓN DE SEGUIMIENTO	POSIBLE RECOMENDACIÓN DE ACTUACIÓN QUE AÑADIR AL FINAL DEL INFORME SOBRE EL ANÁLISIS
¿Cuántos incidentes se produjeron porque el personal o la organización estaban en el lugar equivocado en el momento equivocado?	Intentar conversar dentro de la organización sobre hasta qué punto la organización está preparada para aceptar riesgos generales relacionados con el terrorismo, la delincuencia u otros incidentes que no vayan específicamente dirigidos contra la organización.	Hacer una lista de países con un riesgo agudizado de incidentes que se escapan al control de incluso las mejores políticas de seguridad.
¿Cuántos incidentes se produjeron a causa de la actuación de actores estatales?	Identificar los actores estatales responsables en documentos internos y procurar identificar caminos para establecer un diálogo con ellos. Hablar con el departamento de incidencia y sopesar lanzar una campaña conjunta de sensibilización con otras ONG.	Proponer caminos posibles para iniciar conversaciones que seguirán los representantes de país o el personal directivo con más responsabilidades mediante canales diplomáticos o el respaldo de otras agencias (p. ej., el CICR). Identificar áreas donde una organización podría considerar una campaña de incidencia con otras, como el bombardeo de infraestructuras o la impunidad en el enjuiciamiento.
9. ¿Podemos utilizar los datos para identificar un umbral de riesgo que nuestra organización está dispuesta a aceptar?		
¿Qué tipo de decisiones se adoptaron durante el periodo que se está analizando que indiquen el umbral de riesgo que la organización está dispuesta a aceptar?	Pensar en términos críticos sobre las decisiones de uno mismo sobre los riesgos de seguridad. ¿En qué principios y umbrales se basan? Intentar conversar con otro personal de la organización y sopesar si se utilizan los mismos principios y umbrales.	Recomendar que se elabore un umbral de riesgos articulado con claridad para comunicárselo al personal.
¿Cuál ha sido la coherencia del proceso de decisión en distintos contextos?		
¿Parece haber una relación entre los incidentes de seguridad de los que se ha reportado y las decisiones concretas que se han adoptado?		

REFERENCIAS Y BIBLIOGRAFÍA

ATHA, "Policy Project: Protection of Humanitarian Action", *ATHA*. 2016. Disponible en inglés en: http://www.atha.se/policy-project-protection-of-aid-workers

R. Ayre, *The Information Management Challenge: A Briefing on Information Security for Humanitarian Non-Governmental Organisations in the Field*. EISF, 2010. Disponible en inglés en: https://www.eisf.eu/wp-content/uploads/2014/09/0119-Ayre-EISF-2010-The-Information-Management-Challenge-A-Briefing-on-Information-Security-for-Humanitarian-Non-Governmental-Organisations-in-the-Field.pdf

S. Bickley, *Security Risk Management: a basic guide for smaller NGOs*. EISF, 2017. Disponible en inglés en: https://www.eisf.eu/library/security-risk-management-a-basic-guide-for-smaller-ngos/

P. Buth, *Crisis management of critical incidents*. EISF, 2010. Disponible en inglés en: https://www.eisf.eu/wp-content/uploads/2014/09/0121-Buth-2010-Crisis-Management-of-Critical-incident-2010.pdf

S. Davidson, *Managing the message: Communication and media management in a security crisis*. EISF, 2013. Disponible en inglés en: https://www.eisf.eu/wp-content/uploads/2014/09/1140-Davidson-2013-Managing-the-Message-Communication-and-media-management-in-a-security-crisis.pdf

Davis, J. et al. *Seguridad en práctica: herramientas de gestión de riesgos para organizaciones de ayuda humanitaria. Segunda edición.* EISF, 2017. Disponible en: https://www.eisf.eu/wp-content/uploads/ 2017/03/2124-EISF-2017-Security-to-go_a-risk-management-toolkit-for-humanitarian-aid-agencies-2nd-edition.pdf

G. de Palacios, Forthcoming publication "Managing security-related information: a closer look at incident reporting systems", EISF, 2017.

A. Dick, *Creating Common NGO Security Terminology: A comparative study*. Security Management Initiative, 2010. Disponible en inglés en: https://www.eisf.eu/wp-content/uploads/2014/09/0647-Dick-2010-Creating-Common-NGO-Security-Terminology-A-Comparative-Study.pdf

Earth Point. (desconocido). "Excel To KML - Display Excel files on Google Earth", *Earth Point*. Disponible en inglés en: https://www.earthpoint.us/ExcelToKml.aspx

K. Hoelscher, J. Miklian, y H. M. Nygård, *Understanding Attacks on Humanitarian Aid Workers*. Peace Research Institute Oslo (PRIO) Conflict Trends, 2015. Disponible en inglés en: http://file.prio.no/publication_files/prio/Hoelscher,%20Miklian,%20Nyg%C3%A5rd%20-%20Understanding%20Attacks%20on%20Humanitarian%20Aid%20Workers,%20Conflict%20Trends%206-2015.pdf

ICRC, *Asistencia de salud en peligro: estudio realizado en dieciséis países*. ICRC, 2011. Disponible en: https://www.icrc.org/eng/assets/files/reports/report-hcid-16-country-study-2011-08-10.pdf?__hstc=163349155.76b9edd98545ef10cf2630f8704dd68b.1500037719517.1500037719517.1500838137193.2&__hssc=163349155.2.1500838137193&__hsfp=520750989

InterAction, *InterAction Step by Step Guide to Addressing Sexual Exploitation and abuse*. InterAction, 2010. Disponible en inglés en: https://www.interaction.org/sites/default/files/2010.6%20-%20Step%20by%20Step%20Guide%20-%20Comments%20Version.pdf

Comité Permanente entre Organismos (IASC), *Orientación operacional sobre las responsabilidades de los líderes de grupo / sector y la OCAH en la gestión de la información*. OMS, 2008. Disponible en: http://www.who.int/hac/network/global_health_cluster/iasc_operational_guidance_on_information_management_v3.pdf

Comité Permanente entre Organismos (IASC), "Saving Lives Together – A Framework for Improving Security Arrangements Among IGOs, NGOs and UN in the Field", IASC, 2015. Disponible en inglés: https://interagencystandingcommittee.org/collaborative-approaches-field-security/content/saving-lives-together-framework-improving-security-0

Comité Permanente entre Organismos (IASC), *Guidelines for Integrating Gender-Based Violence Interventions in Humanitarian Action: Reducing risk, promoting resilience and aiding recovery*, IASC, 2015. Disponible en: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/femm/dv/gbv_toolkit_book_01_20_2015_/gbv_toolkit_book_01_20_2015_en.pdf

Comité Permanente entre Organismos (IASC), *Protección contra la explotación y los abusos sexuales. Guía de mejores prácticas. Mecanismos interinstitucionales de denuncia comunitaria*, IASC, 2016. Disponible en: http://reliefweb.int/report/world/protection-sexual-exploitation-and-abuse-psea-inter-agency-cooperation-community-based

Organización Internacional de Normalización (ISO), ISO 31000:2009: Gestión del riesgo. Principios y directrices, 2009.

Organización Internacional de Normalización (ISO), ISO/IEC 27000:2014: ITecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión de conjunto y vocabulario, 2014.

Irish Aid, *Irish Aid Guidelines for NGO Professional Safety & Security Risk Management*, ALNAP, 2013. Disponible en inglés en: http://www.alnap.org/resource/11229

E. Kemp y M. Merkelbach, "Can you get sued? Legal liability of international humanitarian aid organisations towards their staff", *Security Management Initiative*, 2011. Disponible en inglés en: https://www.eisf.eu/library/can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/

E. Kemp y M. Merkelbach, "Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications", *EISF*, 2016. Disponible en inglés en: https://www.eisf.eu/library/duty-of-care-a-review-of-the-dennis-v-norwegian-refugee-council-ruling-and-its-implications/

A. Lieberman, "WHO readies to launch online database tracking health worker attacks", *Devex*, 2017. Disponible en inglés en: https://www.devex.com/news/who-readies-to-launch-online-database-tracking-health-worker-attacks-90331#.WWYjVPrtmqh.twitter

J. Martinsson, "Important Lessons from the Landmine Campaign", *The World Bank*, 2010. Available from: https://blogs.worldbank.org/publicsphere/important-lessons-landmine-s-campaign%20

M. Merkelbach, *Voluntary Guidelines on the Duty of Care to Seconded Civilian Personnel*. Swiss Federal Department of Foreign Affairs (FDFA), Stabilisation Unit (SU) and Center for International Peace Operations (ZIF), 2017. Disponible en inglés en: http://www.zif-berlin.org/fileadmin/uploads/experten-einsaetze/Voluntary_Guidelines_on_the_Duty_of_Care_to_Seconded_Civilian_Personnel_Final_170420.pdf

M. Nobert, *Prevention, Policy and Procedure Checklist: Responding to Sexual Violence in Humanitarian and Development Settings*. Report the Abuse, 2016. Disponible en inglés en: http://www.reporttheabuse.org/take-action/preventing-sexual-violence/

M. Nobert, "Why should we address sexual violence in humanitarian workplaces?", *EISF*, 2017. Disponible en inglés en: https://www.eisf.eu/news/why-should-we-address-sexual-violence-in-humanitarian-workplaces/

A. Parlov, "Toward a global ban on landmines", *International Review of the Red Cross*, 1995. Disponible en inglés en: https://www.icrc.org/eng/resources/documents/article/other/57jmmj.htm

C. Persaud, *Género y seguridad: directrices para transversalización del género en la gestión de riesgos de seguridad*. EISF, 2013. Disponible en: https://www.eisf.eu/wp-content/uploads/2014/09/1137-Persaud-2012-Gender-and-Security-Guidelines-for-Mainstreaming-Gender-in-Security-Risk-Management.pdf

RedR UK y EISF, *Report: Inclusion and security of LGBTI aid workers*. RedR UK, 2016. Disponible en: https://www.eisf.eu/wp-content/uploads/2016/08/2091-RedR-and-EISF-2016-REPORT-INCLUSION-AND-SECURITY-OF-LGBTI-AID-WORKERS-WORKSHOP-22-01-2016.pdf

Safeguarding Health in Conflict Coalition, *Impunity must end: attacks on health in 23 countries in conflict in 2016*, 2017. Disponible en inglés en: https://www.safeguardinghealth.org/sites/shcc/files/SHCC2017final.pdf

Saving Lives Together, "Guidelines for the Implementation of the "Saving Lives Together" Framework", *Saving Lives Together*. July 2016, 2016. Disponible en inglés en: https://www.eisf.eu/library/guidelines-for-the-implementation-of-the-saving-lives-together-framework/

J. Schafer y P. Murphy, *Security Collaboration: Best Practices Guide*. InterAction Security Unit – InterAction, 2010. Disponible en inglés en: https://acceptanceresearch.files.wordpress.com/2010/10/interaction_security-collaboration-best-practices-guide-201111.pdf

Naciones Unidas, "Adopción de Resolución Nº 2286 del Consejo de Seguridad de Naciones Unidas relativa a la Protección de hospitales y personal humanitario en situaciones de conflictos armados", Naciones Unidas, 2016. Disponible en: https://www.un.org/press/en/2016/sc12347.doc.htm

Ejército de Estados Unidos, *Field Manual No. 2-22.3. Human Intelligence Collector Operations*, 2006. Disponible en: https://fas.org/irp/doddir/army/fm2-22-3.pdf

K. Van Brabant, *HPG Report 9: Mainstreaming the Organisational Management of Safety and Security*. Humanitarian Policy Group/ODI, 2001. Disponible en: https://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/297.pdf

K. Van Brabant, *GPR8 – Operational Security Management in Violent Environments, Revised Edition*. Humanitarian Practice Network/Overseas Development Institute (ODI), 2010. Disponible en: https://odihpn.org/wp-content/uploads/2011/04/GPR8_revised_edition_Spanish.pdf

A. Wansbrough-Jones y M. Dixon, *"Saving Lives Together": A Review of existing NGO and United Nations Security Coordination Practices in the Field*. Coordination Toolkit, 2014. Disponible en: http://www.coordinationtoolkit.org/wp-content/uploads/Saving-Lives-Together-Review-of-NGO-and-UN-Security-Coordination-Practices.pdf

OMS, War Trauma Foundation y Visión Mundial Internacional, *Primera ayuda psicológica: Guía para trabajadores de campo*. OMS, 2011. Disponible en: http://www.who.int/mental_health/publications/guide_field_workers/en/

OMS, página web, *Attacks on Health Care*, 2017. Disponible en inglés en: http://www.who.int/emergencies/attacks-on-health-care/en/

C. Wille, "Lessons from the Aviation Industry: What Can We Learn for Humanitarian Security Risk Management?", *EISF*, 2016. Disponible en inglés en: https://www.eisf.eu/news/lessons-from-the-aviation-industry-what-can-we-learn-for-humanitarian-security-risk-management/

C. Williamson, "Gestión de personal" en Seguridad en práctica: herramientas de gestión de riesgos para organizaciones de ayuda humanitaria. *EISF*, 2017. Disponible en: https://www.eisf.eu/news/people-management-and-security-risk-management/

INFORMACIÓN ADICIONAL

ORGANIZACIONES

RedR UK es una ONG humanitaria internacional que apoya a actores humanitarios de todo el mundo mediante formación y soporte técnico. Fundada en 1980 como una lista de socios, RedR se ha convertido en una agencia líder en la capacitación del sector que llega a miles de profesionales humanitarios y a cientos de organizaciones. Tenemos presencia internacional con oficinas en Reino Unido, Sudán, Kenia y Jordania y ofrecemos formación a personal humanitario de todo el globo desde estos centros regionales.

RedR UK es uno de los principales proveedores de formación y apoyo a la capacitación en el sector humanitario, que forma a más de 7.000 personas del sector en más de 55 países cada año. Tras trabajar durante más de 35 años en la capacitación de personal humanitario, apoyando a decenas de miles de personas, RedR ha desarrollado unos conocimientos que nos convierten en líderes de educación para adultos dentro del sector. Tenemos experiencia en impartir programas de capacitación que incluyen formación presencial, coaching y mentoring, simulacros virtuales y en terreno, despliegues, consultorías de corta duración y aprendizaje en línea. Además de nuestros programas educativos de gran calidad, hemos hecho contribuciones considerables para que se imparta formación de una manera eficaz en el sector. La experiencia de RedR UK en impartir y gestionar innovadores programas de capacitación humanitaria coloca a RedR UK en un lugar bien posicionado para gestionar el proyecto de Gestión de la Información sobre Incidentes de Seguridad.

Insecurity Insight es uno de los principales grupos de expertos dedicado a generar y analizar "datos sobre personas en peligro" con un historial en desarrollo avanzado de sistemas para monitorear incidentes para la comunidad humanitaria. Desde 2009, Insecurity Insight ha trabajado en colaboración con agencias humanitarias para elaborar un mecanismo para compartir y analizar incidentes de agencias en confidencialidad.

European Interagency Security Forum es una red independiente de referentes de seguridad que representa en la actualidad a 85 ONG humanitarias con sede en Europa y operaciones internacionales. Su compromiso es mejorar la seguridad de las operaciones de ayuda y del personal. Pretende aumentar el acceso seguro para las agencias humanitarias a personas afectadas por emergencias. En su labor, resulta esencial el desarrollo de investigación y herramientas que velen por la concienciación, la preparación y las buenas prácticas. El EISF facilita intercambios entre organizaciones miembros y otros órganos como la ONU, donantes internacionales, instituciones académicas y de investigación, el sector privado y un amplio abanico de ONG internacionales. La idea del EISF es convertirse en un punto de referencia mundial para las prácticas aplicadas y el conocimiento colectivo y en su labor es crucial desarrollar investigaciones prácticas para la gestión de riesgos de seguridad en el sector humanitario.

CONTACTOS

Para compartir recursos y para saber más sobre el proyecto, se puede contactar con:

RedR UK	Marine Menier: marine.menier@redr.org.uk
Insecurity Insight	Christina Wille: christina.wille@insecurityinsight.org
EISF	Lisa Reilly: eisf-director@eisf.eu