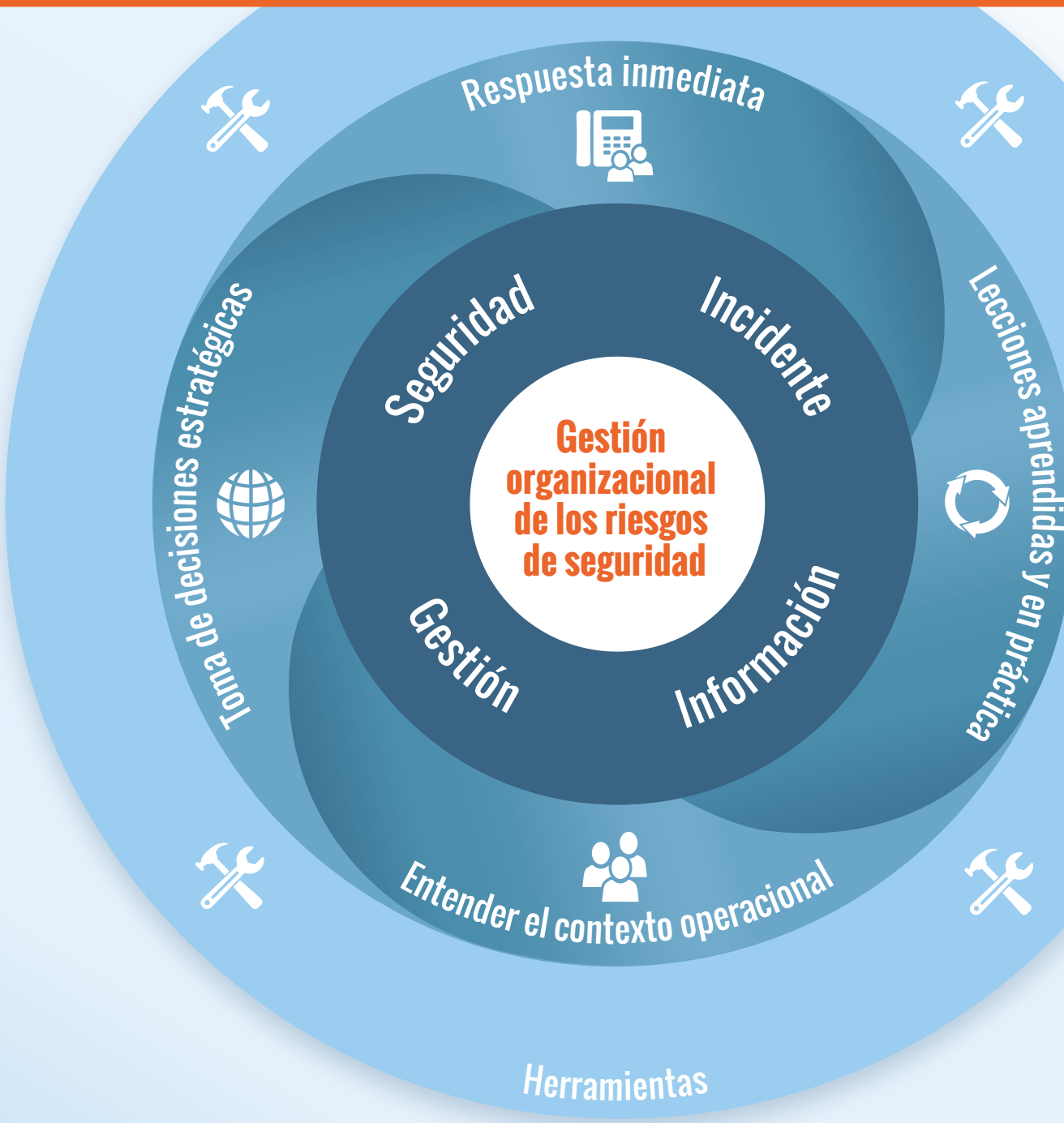
MANUAL DE GESTIÓN DE LA INFORMACIÓN SOBRE INCIDENTES DE SEGURIDAD

TRECE HERRAMIENTAS PARA SU ORGANIZACION



Funded by European Union Humanitarian Aid

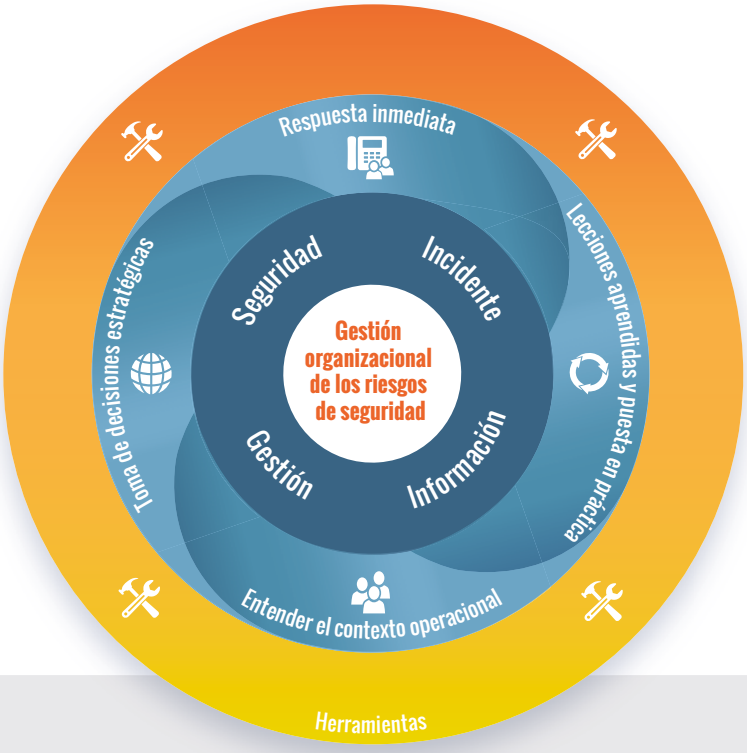
eisf

redr uk
people and skills for disaster relief

Aid in Danger

Insecurity Insight
Data on People in Danger

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 procedimientos 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 procedimientos 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 informativas 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 informativas 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 demasiado complicados para recordarlos 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:

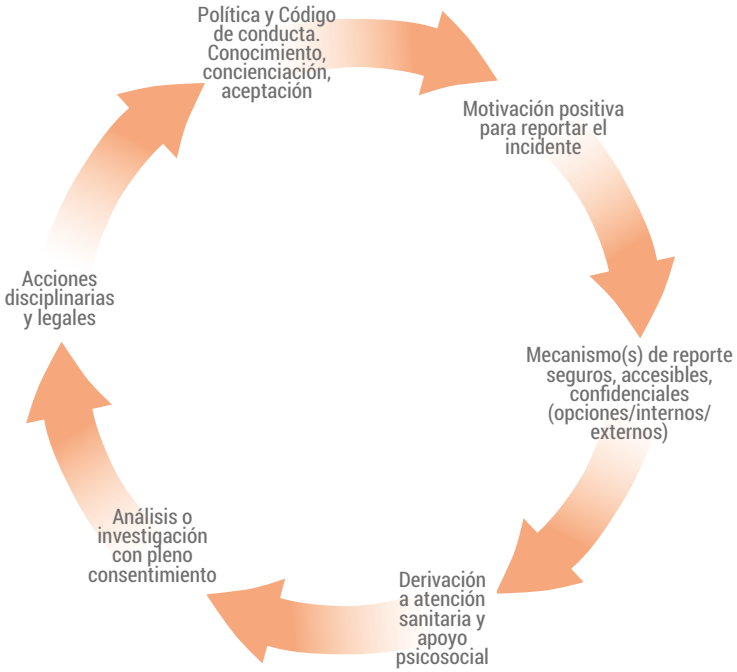
- ¿Han contribuido las condiciones peligrosas?
- ¿Ha contribuido la ubicación?
- ¿Ha contribuido el procedimiento?
- ¿Ha contribuido la falta de equipo de protección personal o de emergencias?
- ¿Han contribuido los SOP? ¿Deberían actualizarse para plasmar una nueva realidad en terreno?
- ¿Han contribuido 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	HOM-BRE	PERSONAL INTER-NACIONAL	PERSONAL NACIONAL	OTROS	MUER-TOS	HERI-DOS
Evento 1	4	1	3	1	2	1	1	3

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

UNIDAD DE ANÁLISIS	IDENTIFI-CACIÓN ÚNICA DE EVENTO	SEXO	ESTATUS	PUESTO	IMPACTO	ASESORA-MIENTO 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?		