ACADEMIA HUMANITARIA · HUMANITAIRES JOBS

Mini MBA Seguridad y gestión de riesgos: proteger a los equipos y mantener el acceso

Manual completo

Programa de exactamente 3 meses (12 semanas, 144 horas) para gestionar la seguridad y los riesgos de una organización humanitaria: deber de cuidado, análisis del contexto, evaluación de riesgos, planes y procedimientos, aceptación y negociación del acceso, incidentes, gestión de crisis y secuestro, salud y bienestar del personal, seguridad digital y protección de datos, riesgos de la organización y cumplimiento, reparto del riesgo con los socios, gobernanza y continuidad de las actividades. Ejercicios numéricos corregidos, tres exámenes mensuales con estudios de caso y un diploma verificable de la Academia Humanitaria.

https://humanitairejobs.org/es/academia/mini-mba-securite-risques/

Documento gratuito de la Academia Humanitaria. Puede imprimirse y compartirse libremente con fines de formación, sin modificaciones.

-

Índice

1. Semana 1 : Deber de cuidado y gestión de riesgos de seguridad: el marco
2. Semana 2 : Analizar el contexto: actores, dinámicas y tendencias de la violencia
3. Semana 3 : Evaluar los riesgos: amenazas, vulnerabilidades, probabilidad e impacto
4. Semana 4 : Planes de seguridad, procedimientos, desplazamientos y comunicaciones
5. Semana 5 : Construir la aceptación y negociar el acceso
6. Semana 6 : Incidentes: notificar, analizar, aprender
7. Semana 7 : Gestionar una crisis: célula de crisis, hibernación, reubicación, evacuación, secuestro
8. Semana 8 : Salud, bienestar psicosocial, salvaguarda interna y seguros
9. Semana 9 : Seguridad digital y protección de la información
10. Semana 10 : Gestionar todos los riesgos de la organización: registro, apetito, cumplimiento y reputación
11. Semana 11 : Compartir el riesgo con los socios y financiar la seguridad
12. Semana 12 : Gobernanza, cultura de seguridad, continuidad de las actividades y proyecto final

Semana 1 : Deber de cuidado y gestión de riesgos de seguridad: el marco

Objetivos

- Explicar el deber de cuidado (duty of care) de una organización humanitaria y sus consecuencias jurídicas, éticas y operativas.
- Describir el ciclo de gestión de riesgos de seguridad y las tres estrategias: aceptación, protección, disuasión.
- Situar la seguridad al servicio del acceso y de los programas: permanecer y actuar, en lugar de huir o exponerse.

Por qué la seguridad es una función de dirección

Cada año, cientos de trabajadores humanitarios mueren, resultan heridos o son secuestrados; la gran mayoría son **personal nacional**. Las bases de datos públicas sobre la seguridad de los trabajadores humanitarios muestran que la violencia se concentra en un pequeño número de contextos, pero que ninguna organización que trabaje en zonas de crisis está a salvo.

La seguridad no es, ante todo, una cuestión de guardias y muros. Es una **función de dirección** que permite llegar a las personas necesitadas manteniendo los riesgos para el personal en un nivel aceptable. Una organización que gestiona mal sus riesgos pierde su acceso, sus equipos, su financiación y, a veces, su reputación.

> Objetivo de la gestión de riesgos de seguridad: permitir un acceso sostenible a las poblaciones, no eliminar todo riesgo. La única forma de eliminar todo riesgo es no hacer nada.

El deber de cuidado

El **deber de cuidado** (duty of care) es la obligación, jurídica y moral, de una organización de adoptar todas las medidas razonables para proteger a su personal contra los daños previsibles. Se extiende, en distintos grados, a los consultores, los voluntarios, los visitantes y los socios.

En la práctica, exige:

- **evaluar** los riesgos antes de exponer a alguien;
- **informar** claramente al personal de los riesgos (consentimiento informado);
- **formar** y equipar;
- establecer **medidas** proporcionadas (procedimientos, comunicaciones, seguros, apoyo psicosocial);
- **responder** a los incidentes y aprender.

Decisiones judiciales en varios países han reconocido la responsabilidad de organizaciones humanitarias que no habían adoptado medidas razonables frente a un riesgo conocido. El deber de cuidado no puede delegarse por completo: una organización sigue siendo responsable incluso cuando se apoya en un proveedor o en un dispositivo común.

Debe ser **equitativo**: históricamente, el personal nacional ha recibido menos formación, equipamiento y opciones de evacuación que el personal internacional ante un riesgo igual o mayor. Las buenas prácticas actuales exigen abordar esta desigualdad de forma explícita.

El ciclo de gestión de riesgos de seguridad

El marco más utilizado en el sector (formalizado en particular por la revisión de buenas prácticas n.º 8 de la Humanitarian Practice Network y las guías del Global Interagency Security Forum, GISF) sigue un ciclo:

- **1. Análisis del contexto**: actores, dinámicas, tendencias de la violencia.
- **2. Evaluación de riesgos**: amenazas, vulnerabilidades, probabilidad, impacto.
- **3. Elección de estrategias y medidas**: aceptación, protección, disuasión.
- **4. Planes y procedimientos**: plan de seguridad, procedimientos operativos, planes de contingencia.
- **5. Implementación**: formación, equipamiento, presupuesto, responsabilidades.
- **6. Seguimiento, incidentes y revisión**: notificación, análisis, actualización periódica.

El ciclo gira de forma continua: cualquier cambio significativo del contexto (elecciones, ofensiva militar, incidente grave) desencadena una revisión, sin esperar a la fecha prevista.

Aceptación, protección, disuasión

Se combinan tres estrategias, con una dosificación propia de cada contexto:

- **Aceptación**: obtener el consentimiento de las comunidades, de las autoridades y de las partes en conflicto a la presencia y a las actividades de la organización, mediante la pertinencia de los programas, el respeto de los principios, el diálogo y el comportamiento del personal. Es la estrategia básica de los humanitarios.
- **Protección**: reducir la vulnerabilidad mediante medidas y equipos (procedimientos de desplazamiento, muros, guardias no armados, comunicaciones, vehículos adaptados, refugios). Protege, pero puede alejar a la organización de las comunidades («búnkerización»).
- **Disuasión**: oponer una amenaza para disuadir de una agresión (guardias armados, escoltas armadas, suspensión condicional de las actividades). Se reserva para casos excepcionales porque puede comprometer la neutralidad y la aceptación.

Ejemplo. En una zona donde la organización está bien aceptada pero la delincuencia urbana es elevada, la combinación típica es: aceptación en las comunidades de intervención, protección reforzada de las residencias y de los desplazamientos en la ciudad (no caminar de noche, vehículos cerrados con seguro) y suspensión de las actividades como palanca de disuasión en caso de ataque dirigido.

El umbral de riesgo aceptable y el programa crítico

Toda exposición debe estar **justificada por el valor del programa**. Cuanto mayor es el riesgo, más crítica debe ser la actividad para las personas (salvar vidas) y más debe la organización disponer realmente de los medios para gestionarlo.

Las herramientas de **criticidad de los programas** (por ejemplo, el marco de las Naciones Unidas) clasifican las actividades de la más crítica (actividad vital inmediata, u ordenada por el Secretario General) a la menos crítica. Una actividad poco crítica no justifica un riesgo elevado; una actividad vital puede justificar un riesgo elevado, pero no un riesgo inaceptable.

Ejemplo de decisión. Una formación en gestión de proyectos de tres días, en una ciudad donde el riesgo de secuestro se considera elevado, puede trasladarse o impartirse en línea. Una campaña de vacunación contra una epidemia en la misma ciudad puede mantenerse con medidas reforzadas, porque el beneficio vital justifica un riesgo residual más alto, dentro del límite fijado por la dirección.

> El umbral de riesgo aceptable lo fija la dirección de la organización, por escrito, y no el equipo más valiente sobre el terreno.

Funciones y responsabilidades

La seguridad es asunto de todos, pero las responsabilidades deben estar claras:

- **Junta directiva y dirección general**: política de seguridad, umbral de riesgo aceptable, recursos, supervisión de los incidentes graves.
- **Director de país**: responsable de la seguridad en el país; es una función de dirección que no se delega por completo en el asesor de seguridad.
- **Responsable o asesor de seguridad**: análisis, asesoramiento, procedimientos, formación, seguimiento de incidentes.
- **Puntos focales de seguridad** en las bases sobre el terreno.
- **Cada miembro del personal**: respetar los procedimientos, notificar, adoptar un comportamiento que proteja la aceptación y decir no a una misión considerada demasiado peligrosa.

El **derecho de retirada**: toda persona puede negarse a ir a un lugar o abandonar un lugar si considera que el riesgo es demasiado alto, sin sanción. A la inversa, la dirección puede prohibir un desplazamiento aunque la persona sea voluntaria.

Ejercicio: un director de país ante una solicitud de misión

Situación. Un donante solicita una visita de seguimiento de un proyecto de educación en un distrito donde, el mes pasado, tres vehículos de ONG fueron asaltados. El personal nacional de la base pregunta por qué los internacionales tienen un chaleco de protección y una opción de evacuación por avión, mientras que ellos no tienen ni seguro adecuado ni formación. Un joven coordinador internacional se ofrece voluntario para la visita «porque no tiene miedo».

Trabajo solicitado. 1) ¿Está justificado el nivel de riesgo por la criticidad de la actividad? 2) ¿Qué problemas de deber de cuidado observa? 3) ¿Qué decisión y qué medidas?

Solución. 1) Una visita de seguimiento de un proyecto de educación no es una actividad vital: no justifica un riesgo elevado. Se buscan alternativas: seguimiento a distancia (llamadas, fotos geolocalizadas, socio local), verificación por un tercero mejor aceptado, aplazamiento o reunión en un lugar más seguro. 2) Desigualdad de trato entre personal nacional e internacional (seguro, formación, equipamiento, opciones de reubicación); decisión dejada al voluntariado individual en lugar de una evaluación de riesgos y una decisión de la dirección. 3) Rechazar la misión en esta forma y explicar al donante la solución de seguimiento alternativa; iniciar una revisión de las medidas para el personal nacional (formación, seguro, plan de reubicación para quienes están expuestos debido a su empleo); recordar que el umbral de riesgo lo fija la dirección y no el voluntariado.

Para recordar

- La gestión de riesgos de seguridad sirve al acceso a las poblaciones; no persigue el riesgo cero.
- Deber de cuidado: evaluar, informar, formar, equipar, responder y aprender, de forma equitativa entre el personal.
- Ciclo: contexto, evaluación, estrategias, planes, implementación, seguimiento y revisión.
- Primero la aceptación; protección según las necesidades; disuasión como último recurso.
- El riesgo aceptable depende de la criticidad del programa y lo fija la dirección, por escrito.

Cuestionario

1. La estrategia de seguridad básica de las organizaciones humanitarias es:
   A. La disuasión
   B. La aceptación
   C. La protección
   D. La evitación total

2. El deber de cuidado se aplica:
   A. A todo el personal y, en distintos grados, a consultores, voluntarios y visitantes
   B. Solo al personal internacional
   C. Solo al personal armado
   D. Únicamente en tiempo de guerra

3. ¿Quién fija el umbral de riesgo aceptable?
   A. Las autoridades locales
   B. El miembro del personal con más experiencia
   C. El donante
   D. La dirección de la organización, por escrito

4. Unos guardias armados alrededor de un almacén corresponden a:
   A. La aceptación
   B. La protección no armada
   C. La disuasión
   D. La evitación

5. Un miembro del personal rechaza una misión que considera demasiado peligrosa. Esa persona:
   A. Debe ser sancionada
   B. Ejerce su derecho de retirada, sin sanción
   C. Debe dimitir
   D. Debe encontrar un sustituto

Respuestas del cuestionario : 1. B · 2. A · 3. D · 4. C · 5. B

Semana 2 : Analizar el contexto: actores, dinámicas y tendencias de la violencia

Objetivos

- Realizar un análisis de contexto estructurado (político, económico, social, de seguridad) útil para la toma de decisiones.
- Cartografiar a los actores según su influencia, sus intereses y su actitud hacia la organización.
- Leer datos de incidentes (frecuencias, tasas, tendencias) sin errores de interpretación y producir indicadores de alerta.

Por qué analizar el contexto

Todas las decisiones de seguridad se basan en una comprensión del contexto. Un análisis débil produce dos errores simétricos: **subestimar** una amenaza (y exponer al personal) o **sobrestimarla** (y abandonar a poblaciones que podrían haber recibido ayuda).

Un buen análisis responde a unas cuantas preguntas: ¿quién controla el territorio y las carreteras? ¿Cuáles son los intereses de los actores y cómo les afecta la acción humanitaria? ¿Qué tipos de violencia existen, contra quién, dónde, cuándo y por qué? ¿Qué está cambiando?

Fuentes: personal nacional (la primera fuente, a menudo la más fina), comunidades, autoridades, otras organizaciones, foros de coordinación de la seguridad de las ONG, Naciones Unidas (UNDSS), medios de comunicación locales, redes sociales (con prudencia), bases de datos públicas sobre conflictos. Toda información se **contrasta** y se califica según la fiabilidad de la fuente y la credibilidad de la información.

Las matrices de análisis

Dos matrices sencillas estructuran el análisis:

- **PESTEL adaptado**: político, económico, social, tecnológico, ambiental, legal, a los que se añade la seguridad (grupos armados, delincuencia, fuerzas de seguridad).
- **Análisis histórico**: línea de tiempo de los acontecimientos principales de los últimos años, para detectar los ciclos (temporadas de combates, periodos electorales, cosechas, trashumancia).

El análisis desemboca en **escenarios**: el más probable, el más peligroso y, eventualmente, un escenario de mejora, cada uno con **indicadores** observables que señalan que nos acercamos a él.

Ejemplo de indicadores. Escenario «reanudación de los combates alrededor de la ciudad»: desplazamiento de familias hacia el sur, cierre de los mercados semanales, subida repentina del precio del combustible, salida de los comerciantes extranjeros, movimientos de tropas

notificados, discursos hostiles en las radios locales. Tres indicadores de seis observados desencadenan una reunión de crisis y la revisión del nivel de seguridad.

Cartografiar a los actores

La **cartografía de actores** identifica a quienes pueden influir en la seguridad y el acceso: autoridades nacionales y locales, fuerzas armadas y policiales, grupos armados no estatales, líderes tradicionales y religiosos, milicias, redes criminales, comerciantes, medios de comunicación, comunidades de acogida y desplazadas, otras organizaciones.

Para cada uno: **influencia** (de débil a fuerte), **actitud** hacia la organización (hostil, neutral, favorable), **intereses** y **relación** actual.

Actor	Influencia	Actitud	Acción
Jefe de la principal milicia	Fuerte	Neutral, desconfiado	Diálogo regular a través de un intermediario aceptado; explicar los principios y los criterios de focalización
Prefecto	Fuerte	Favorable	Información regular, respeto de los procedimientos administrativos
Jóvenes desempleados de la ciudad	Media	Hostil (contrataciones consideradas injustas)	Transparencia en las contrataciones, mecanismo de quejas, empleos por día equitativos

> Un actor hostil con mucha influencia es una prioridad del análisis y de la estrategia de aceptación, no solo una amenaza que evitar.

Leer los datos de incidentes

Los datos de incidentes ayudan a objetivar la amenaza, siempre que se lean correctamente:

- **Frecuencia bruta**: número de incidentes por periodo.
- **Tasa**: incidentes en relación con la exposición (número de empleados, de desplazamientos, de días-persona). Sin denominador, un aumento puede reflejar simplemente un incremento de la actividad.
- **Sesgo de notificación**: un aumento puede deberse a una mejor notificación, no a un agravamiento.
- **Tipología**: un mismo total puede ocultar un descenso de los robos y un aumento de los secuestros, mucho más graves.

Ejemplo. Año 1: 24 incidentes para 300 empleados. Año 2: 36 incidentes para 600 empleados. Tasa: 8 frente a 6 incidentes por cada 100 empleados al año. A pesar de un aumento bruto del 50 %, la tasa ha bajado un 25 %. Pero si los incidentes graves (violencia contra las personas) pasan de 3 a 9, su tasa pasa de 1 a 1,5 por cada 100 empleados: la gravedad aumenta. La lectura combina tasa y gravedad.

Comprender la violencia contra los humanitarios

Los ataques contra los humanitarios responden a varias lógicas, que hay que distinguir porque requieren respuestas diferentes:

- **Criminal**: beneficio económico (robos, asaltos, secuestros con rescate). Las medidas de protección y la discreción sobre los bienes de valor son eficaces.
- **Política o militar**: la organización se percibe como aliada de un bando, o su acción molesta a una estrategia. La aceptación, la neutralidad percibida y la comunicación son centrales.
- **Vinculada al propio trabajo**: conflictos de focalización, contrataciones impugnadas, despidos, quejas no atendidas. La calidad y la rendición de cuentas de los programas son medidas de seguridad.
- **Incidental**: encontrarse en el lugar equivocado en el momento equivocado (fuego cruzado, bombardeos, minas). Análisis de las zonas y los horarios, procedimientos de movimiento.

Muchos incidentes graves que afectan a ONG están vinculados a **tensiones internas o de vecindad** (personal despedido, proveedor descartado, beneficiario excluido): el análisis de seguridad también debe examinar a la propia organización.

Producir un análisis útil

Un análisis útil cabe en **dos páginas**, se actualiza periódicamente (mensualmente en un contexto inestable, tras cualquier acontecimiento importante) y termina con implicaciones concretas:

- zonas y carreteras accesibles, accesibles con condiciones o prohibidas;
- horarios y modos de desplazamiento;
- actores con los que reunirse y mensajes clave;
- indicadores que vigilar y umbrales de revisión;
- consecuencias para los programas (calendario, modalidades, gestión a distancia).

Se comparte con las personas que lo necesitan, respetando la **confidencialidad**: un análisis que nombra a actores armados o a informantes puede poner a personas en peligro si circula. Tampoco debe utilizar información confidencial procedente de otras organizaciones sin su acuerdo explícito.

Ejercicio: una ciudad que cambia

Situación. Una ONG trabaja desde hace 3 años en una ciudad de guarnición. Datos: año 1, 18 incidentes para 150 empleados (de ellos 2 contra las personas); año 2, 27 incidentes para 300 empleados (de ellos 6 contra las personas). Desde hace un mes: un candidato local no contratado amenaza públicamente a la organización; dos mercados semanales han cerrado; los alquileres bajan porque se marchan familias acomodadas; una radio local acusa a «las ONG» de ayudar a los rebeldes; el foro de seguridad de las ONG informa de movimientos de tropas.

Trabajo solicitado. 1) Calcule e interprete las tasas de incidentes. 2) Clasifique las señales según la lógica de violencia. 3) Proponga tres implicaciones prácticas.

Solución. 1) Tasa global: 12 y luego 9 incidentes por cada 100 empleados (descenso del 25 %). Tasa de incidentes contra las personas: 1,33 y luego 2 por cada 100 empleados (aumento del 50 %). La situación se agrava en gravedad pese al descenso de la tasa global. 2) Amenaza del candidato no contratado: lógica vinculada al trabajo; acusaciones radiofónicas: lógica política (percepción de parcialidad); mercados cerrados, salidas, movimientos de tropas: indicadores de un escenario de reanudación de los combates (riesgo incidental y político). 3) Tratar la queja sobre la contratación (mecanismo formal, transparencia, seguridad del personal de RR. HH.); emprender una iniciativa de aceptación (reuniones con las autoridades y los líderes, programa de radio sobre los principios y los criterios de ayuda); revisar el escenario y el nivel de seguridad, preparar la reubicación y la gestión a distancia si se confirman los indicadores militares.

Para recordar

- Un análisis débil subestima o sobrestima; contrastar y calificar la fiabilidad y la credibilidad de las fuentes.
- Escenarios con indicadores observables y umbrales que desencadenan una revisión.
- Cartografiar la influencia, la actitud y los intereses de los actores; priorizar a los actores hostiles influyentes.
- Siempre un denominador: tasas de incidentes por exposición, leídas junto con la gravedad.
- Muchos incidentes graves tienen un origen vinculado al trabajo: la calidad de los programas es una medida de seguridad.

Cuestionario

1. 30 incidentes para 500 empleados. La tasa por cada 100 empleados es:
   A. 30
   B. 16,7
   C. 6
   D. 0,6

2. Los incidentes pasan de 20 a 30 mientras el personal pasa de 200 a 400. La tasa:
   A. Aumenta un 50 %
   B. Baja un 25 %
   C. Se mantiene estable
   D. Se duplica

3. Un despido mal gestionado seguido de amenazas corresponde sobre todo a una violencia:
   A. Vinculada al trabajo de la organización
   B. Incidental
   C. Criminal
   D. Militar

4. Un análisis de seguridad que nombra a informantes debe:
   A. Publicarse por transparencia
   B. Compartirse con todos los socios
   C. Enviarse a los medios de comunicación
   D. Circular de forma estrictamente restringida para no ponerlos en peligro

5. Un actor hostil y muy influyente debe ser:
   A. Ignorado
   B. Denunciado ante la prensa
   C. Una prioridad del análisis y de la estrategia de aceptación
   D. Esquivado sin establecer nunca contacto

Respuestas del cuestionario : 1. C · 2. B · 3. A · 4. D · 5. C

Semana 3 : Evaluar los riesgos: amenazas, vulnerabilidades, probabilidad e impacto

Objetivos

- Identificar las amenazas y evaluar la vulnerabilidad de la organización y de cada perfil de personal ante ellas.
- Calificar los riesgos en una matriz probabilidad × impacto, calcular el riesgo residual tras las medidas y compararlo con el umbral aceptable.
- Redactar una evaluación de riesgos clara, fechada y revisable, que conduzca a decisiones.

Amenaza, vulnerabilidad, riesgo

Tres nociones que no deben confundirse:

- **Amenaza**: lo que puede causar un daño (asalto a un vehículo, secuestro, bombardeo, artefacto explosivo, disturbio, enfermedad, accidente de tráfico).
- **Vulnerabilidad**: el grado de exposición de la organización o de una persona a esa amenaza, según su ubicación, sus desplazamientos, su perfil, sus bienes, sus procedimientos, su aceptación.
- **Riesgo**: la combinación de la probabilidad de que una amenaza se materialice contra nosotros y del impacto si se materializa.

Una misma amenaza no crea el mismo riesgo para todos. **Ejemplo:** la amenaza de secuestro con rescate pesa más sobre los perfiles percibidos como «rentables» (personal internacional de determinadas nacionalidades, cuadros nacionales de alto nivel, personas cuya familia se percibe como acomodada). La vulnerabilidad también depende de los procedimientos: unos desplazamientos previsibles, siempre a las mismas horas, aumentan la vulnerabilidad de todos.

La matriz probabilidad × impacto

El método más extendido califica cada riesgo en dos escalas de 1 a 5:

- **Probabilidad**: 1 muy improbable, 2 improbable, 3 posible, 4 probable, 5 muy probable (en un periodo definido, por ejemplo 12 meses).
- **Impacto**: 1 insignificante, 2 menor (daños materiales limitados), 3 moderado (heridas leves, interrupción breve), 4 grave (heridas graves, pérdida de bienes importantes, suspensión), 5 crítico (fallecimiento, secuestro, retirada del país).

Puntuación = probabilidad × impacto, de 1 a 25. Niveles habituales: de 1 a 4 bajo, de 5 a 9 medio, de 10 a 16 alto, de 20 a 25 muy alto (los umbrales varían según las organizaciones y deben ponerse por escrito).

Amenaza	Probabilidad	Impacto	Puntuación	Nivel
Asalto a un vehículo en el eje norte	4	4	16	Alto
Robo con allanamiento en la oficina	3	2	6	Medio
Secuestro de un empleado	2	5	10	Alto
Accidente de tráfico grave	3	5	15	Alto

Observación: el accidente de tráfico tiene a menudo una puntuación tan alta como las amenazas vinculadas a la violencia, y es más fácil de reducir.

Riesgo residual y umbral aceptable

El **riesgo inherente** es el riesgo antes de las medidas; el **riesgo residual** es el que queda tras las medidas previstas. La decisión se toma sobre el riesgo residual, comparado con el umbral aceptable fijado por la dirección para la actividad considerada.

Ejemplo. Asalto en el eje norte: inherente 4 × 4 = 16. Medidas: desplazamientos en dos vehículos, horarios variables, nada de dinero ni de bienes de valor visibles, comunicación con control de llamada cada hora, actualización diaria del estado de la carretera por el foro de ONG, regla de no resistencia. Probabilidad estimada reducida a 2 (la vulnerabilidad baja), impacto reducido a 3 (no resistencia, asistencia rápida). Residual: 2 × 3 = 6, nivel medio.

Si el umbral aceptable para las actividades de distribución es «medio», la actividad puede continuar con estas medidas. Si las medidas no permiten bajar por debajo del umbral, hay que cambiar la actividad (modalidad, lugar, socio) o suspenderla.

> Una medida escrita pero no aplicada no reduce ningún riesgo. La evaluación debe decir quién aplica qué y cómo se verifica.

Los límites de la calificación

La matriz es útil, pero engañosa si se toma por una medida exacta:

- Las calificaciones son **juicios**, no medidas. Dos personas pueden calificar de forma distinta; se busca un consenso argumentado, con el personal nacional.
- Los **acontecimientos raros y catastróficos** (ataque a un hotel, atentado contra una base) tienen una probabilidad baja pero un impacto extremo: una puntuación de 1 × 5 = 5 los clasifica como «medios» cuando exigen planes específicos.
- Los riesgos **acumulados**: varios riesgos medios combinados pueden constituir una situación inaceptable.
- Los riesgos evolucionan: una evaluación sin fecha o de hace ocho meses en un contexto inestable ya no tiene valor.

Buena práctica: vigilar de forma especial cualquier amenaza de impacto 5, sea cual sea su probabilidad, y prever para cada una un plan de contingencia (secuestro, ataque armado,

evacuación médica).

Perfiles y seguridad inclusiva

Las personas no están expuestas de la misma manera según su **perfil**: nacionalidad, origen étnico o clan, religión, género, orientación sexual e identidad de género, discapacidad, edad, apariencia, idioma. Un mismo lugar puede ser seguro para una persona y peligroso para otra.

Un enfoque **inclusivo** de la seguridad (desarrollado en particular por el GISF) consiste en:

- tener en cuenta los perfiles en la evaluación de riesgos, sin obligar a nadie a revelar información personal;
- permitir que cada persona comunique de forma confidencial preocupaciones relacionadas con su perfil;
- adaptar las medidas (alojamiento, desplazamientos, destinos), sin excluir automáticamente a personas de determinados puestos;
- formar a los responsables en estas cuestiones.

Ejemplo. Un empleado nacional de un grupo étnico minoritario no puede cruzar determinados puestos de control sin riesgo. En lugar de excluirlo del proyecto, el equipo adapta los itinerarios, lo asigna a zonas donde su perfil no está expuesto y prevé un alojamiento seguro en caso de tensión.

Redactar la evaluación

Una evaluación de riesgos de seguridad útil contiene:

- la **zona** y el **periodo** cubiertos, la fecha y los autores;
- un resumen del contexto (remisión al análisis);
- la tabla de amenazas con probabilidad, impacto y puntuación inherente;
- para cada riesgo alto o muy alto: medidas, responsables, riesgo residual;
- la comparación con el umbral aceptable por tipo de actividad;
- las decisiones y recomendaciones (continuación, adaptación, suspensión);
- la fecha de la próxima revisión y los desencadenantes de una revisión anticipada.

La **valida** el director de país (y la sede por encima de cierto nivel de riesgo) y se **explica** al personal afectado. También sirve de base para el presupuesto de seguridad y para el consentimiento informado del personal.

Ejercicio: evaluar y decidir

Situación. Una ONG quiere abrir una base en una ciudad a 120 km de la capital regional. Amenazas identificadas: asalto a vehículo (probabilidad 4, impacto 4); ataque armado contra la base (probabilidad 2, impacto 5); secuestro (probabilidad 2, impacto 5); accidente de tráfico (probabilidad 4, impacto 4); enfermedad grave sin acceso a atención médica (probabilidad 3, impacto 4). Umbral aceptable fijado por la dirección para actividades de salud vitales: residual «alto» como máximo (≤ 16), con plan de contingencia para toda amenaza de impacto 5. Medidas propuestas: convoyes de dos vehículos y control de llamada (asalto reducido a 2 × 3), consignas viales y conductores formados (accidente reducido a 2 × 4), guardias no armados, muro y refugio (ataque reducido a 1 × 5), evacuación médica mediante un servicio aéreo contratado y botiquines (enfermedad reducida a 2 × 3). Ninguna medida específica para el secuestro.

Trabajo solicitado. 1) Puntuaciones inherentes y residuales. 2) ¿Es aceptable la apertura? 3) ¿Qué falta?

Solución. 1) Inherentes: asalto 16, ataque 10, secuestro 10, accidente 16, enfermedad 12. Residuales: asalto 6, ataque 5, secuestro 10 (sin cambios), accidente 8, enfermedad 6. 2) Todos los residuales son ≤ 16, por tanto dentro del umbral, pero dos amenazas de impacto 5 (ataque, secuestro) exigen un plan de contingencia. 3) Faltan medidas y un plan para el secuestro: análisis de los perfiles expuestos, discreción de los desplazamientos, variación de los horarios, normas sobre los visitantes, preparación de una célula de crisis y de una política de gestión de secuestros; y un plan de contingencia en caso de ataque (refugio, comunicaciones de emergencia, procedimiento de reubicación). La apertura puede decidirse una vez establecidos estos planes, validados por la dirección.

Para recordar

- Riesgo = probabilidad × impacto de una amenaza, según la vulnerabilidad de la organización y de las personas.
- Decidir sobre el riesgo residual, comparado con el umbral aceptable de la actividad.
- Una medida no aplicada no reduce nada: responsables y verificación obligatorios.
- Toda amenaza de impacto 5 exige un plan de contingencia, sea cual sea su probabilidad.
- Seguridad inclusiva: integrar los perfiles sin excluir ni forzar la divulgación.

Cuestionario

1. Probabilidad 3, impacto 5. La puntuación es:
   A. 8
   B. 35
   C. 2
   D. 15

2. Tras las medidas, un riesgo pasa de 4 × 4 a 2 × 3. El riesgo residual es:
   A. 16
   B. 10
   C. 6
   D. 8

3. Una amenaza de probabilidad 1 e impacto 5 (puntuación 5):
   A. Puede ignorarse
   B. Exige un plan de contingencia específico
   C. Es automáticamente aceptable
   D. Debe calificarse con 25

4. La decisión de continuar una actividad se toma sobre:
   A. El riesgo residual comparado con el umbral aceptable
   B. El riesgo inherente
   C. La opinión del donante
   D. El número de incidentes del año pasado

5. En un enfoque de seguridad inclusiva:
   A. Se excluyen automáticamente determinados perfiles
   B. Se obliga a cada persona a declarar su orientación sexual
   C. Se ignoran los perfiles
   D. Se permiten las comunicaciones confidenciales y se adaptan las medidas

Respuestas del cuestionario : 1. D · 2. C · 3. B · 4. A · 5. D

Semana 4 : Planes de seguridad, procedimientos, desplazamientos y comunicaciones

Objetivos

- Redactar un plan de seguridad de país o de zona, con niveles de seguridad y medidas asociadas.
- Diseñar procedimientos operativos estándar realistas, en particular para los desplazamientos y los sitios.
- Establecer un sistema de comunicaciones y de seguimiento de movimientos que funcione cuando todo lo demás falla.

El plan de seguridad

El **plan de seguridad** traduce la evaluación de riesgos en normas y responsabilidades. Es breve, práctico, conocido por todos y se revisa periódicamente. Contenido tipo:

- resumen del contexto y de las principales amenazas;
- estrategia (combinación de aceptación, protección y disuasión);
- niveles de seguridad y medidas asociadas;
- procedimientos operativos estándar (desplazamientos, sitios, comunicaciones, visitantes, dinero en efectivo, incidentes);
- planes de contingencia (evacuación médica, hibernación, reubicación, evacuación, secuestro, ataque);
- organigrama de seguridad y contactos de emergencia;
- anexos: mapas, listas de personal, inventario de los equipos de comunicación.

Cada persona recién llegada recibe una **sesión informativa de seguridad** a su llegada y firma que ha leído el plan. Un plan de 80 páginas que nadie ha leído no protege a nadie.

Los niveles de seguridad

La mayoría de las organizaciones utilizan 4 o 5 **niveles de seguridad** por zona, cada uno asociado a medidas automáticas, lo que agiliza las decisiones en periodos de tensión:

Nivel	Situación	Medidas tipo
1. Normal	Riesgos bajos y estables	Procedimientos estándar
2. Vigilancia	Tensiones, incidentes aislados	Desplazamientos limitados en horario, control de llamada reforzado, revisión de los planes
3. Restricción	Violencia en aumento, posibles amenazas dirigidas	Solo desplazamientos esenciales, con autorización; reducción del personal no esencial; actividades adaptadas
4. Hibernación o reubicación	Violencia generalizada o dirigida	Reagrupamiento en un lugar seguro, o salida del personal más expuesto; actividades suspendidas o a distancia
5. Evacuación y suspensión	Riesgo inaceptable	Salida de la zona o del país según el plan; mantenimiento del contacto con el personal que se queda

El paso de un nivel a otro lo decide el director de país, sobre la base de **indicadores** definidos de antemano (véase la semana 2), y se comunica inmediatamente a todos.

Los procedimientos de desplazamiento

Los desplazamientos son el momento en que el personal está más expuesto. Procedimiento tipo:

- **Autorización** previa según el nivel de seguridad, sobre la base de un plan de desplazamiento: itinerario, horarios, pasajeros, vehículos, contactos.
- **Verificación de la carretera** esa misma mañana: foro de seguridad, autoridades, transportistas, personal local.
- **Vehículo** revisado y equipado: combustible, rueda de repuesto, botiquín, comunicaciones.
- **Control de llamada** (check-in) a intervalos fijados y en cada punto clave; procedimiento claro si falta una llamada.
- **Toque de queda interno**: llegada antes de una hora fijada, con margen.
- **Comportamiento** en los puestos de control y en caso de asalto (no resistirse, no hacer fotos, calma, cooperación).

Cálculo de la salida. Trayecto de 180 km, velocidad media realista de 40 km/h: 4 h 30. Toque de queda interno a las 17 h, margen de una hora: llegada prevista a más tardar a las 16 h. Salida a más tardar a las 11 h 30. Con un control de llamada cada hora y a la llegada: 5 llamadas. Si falta una llamada, la base intenta restablecer el contacto durante 15 minutos y luego activa el procedimiento de vehículo desaparecido.

Seguridad de los sitios

Oficinas, residencias, almacenes y sitios de distribución son objeto de una evaluación y de medidas adaptadas:

- **Elección del sitio**: barrio, vecindad (evitar la proximidad de posibles objetivos: edificios militares, ministerios sensibles), dos vías de acceso, distancia de las zonas con riesgo de inundación.
- **Perímetro**: muro o valla, portón, iluminación, guardias no armados formados, control de visitantes.
- **Edificio**: puertas y ventanas sólidas, habitación segura o refugio según las amenazas (habitación reforzada contra intrusiones, refugio contra fuego indirecto).
- **Seguridad contra incendios y eléctrica**: extintores, detectores, salidas de emergencia.
- **Reservas**: agua, alimentos, combustible, medicamentos para la hibernación (a menudo de 7 a 14 días).

Cálculo de reservas. 12 personas, hibernación de 10 días: agua a 4 litros por persona y día para beber y un uso mínimo = 480 litros; con un 20 % de margen, unos 580 litros. Alimentos: 12 × 10 = 120 raciones diarias. Combustible para un generador a 2 litros por hora, 8 horas al día: 160 litros.

Las comunicaciones

El sistema de comunicaciones debe funcionar **cuando la red móvil está cortada**, algo que ocurre a menudo justo cuando más se necesita. Principio de redundancia: al menos dos medios independientes.

- **Teléfono móvil**: práctico, pero frágil y susceptible de vigilancia.
- **Radio HF**: larga distancia, independiente de las redes, pero requiere operadores formados y licencias.
- **Radio VHF**: corto alcance, ideal en ciudad y en convoy, con repetidores.
- **Teléfono satelital** y terminales satelitales de datos: independientes, pero costosos y a veces regulados o mal vistos por las autoridades.
- **Balizas de seguimiento** GPS con botón de alerta.

Normas: indicativos de llamada, lenguaje claro pero sin información sensible (nada de nombres, sumas de dinero ni itinerarios detallados por radio), árbol de llamadas (cada responsable llama a un número definido de personas), pruebas periódicas, cargadores y baterías de repuesto. Las comunicaciones también son una cuestión de aceptación: utilizar una radio o un teléfono satelital allí donde las autoridades lo prohíben puede hacer sospechar de espionaje.

Procedimientos que realmente se aplican

Los procedimientos fracasan a menudo por razones sencillas: demasiado numerosos, poco conocidos, imposibles de aplicar o eludidos por costumbre. Buenas prácticas:

- Redactar **pocos** procedimientos, breves, adaptados al contexto real, con el personal que los aplicará.
- **Explicarlos** (el porqué) y no solo imponerlos.

- **Ejercitarlos**: simulacros de vehículo desaparecido, de hibernación, de evacuación médica, al menos dos veces al año.
- **Verificarlos**: controles puntuales de los cuadernos de a bordo, de los controles de llamada, de los registros de visitantes.
- Tratar el incumplimiento como una cuestión de **gestión**: un responsable que elude los procedimientos da ejemplo a todo el equipo.

> La complacencia es un riesgo en sí misma: tras meses sin incidentes, los procedimientos se relajan precisamente cuando el contexto puede dar un vuelco.

Ejercicio: planificar una misión sobre el terreno

Situación. Un equipo de 4 personas debe desplazarse desde la base hasta un sitio a 210 km para una distribución. Velocidad media realista: 35 km/h. Toque de queda interno: 17 h 30, con un margen de una hora. La distribución dura 3 horas. El sitio no tiene red móvil en los últimos 80 kilómetros. El nivel de seguridad de la zona es «vigilancia». El conductor propone salir a las 9 h «como de costumbre».

Trabajo solicitado. 1) ¿Puede hacerse la misión de ida y vuelta en el día? 2) Si no, ¿qué organización? 3) ¿Qué medios de comunicación y qué controles de llamada?

Solución. 1) Trayecto: 210 / 35 = 6 horas. Ida y vuelta 12 horas + 3 horas de distribución = 15 horas; llegada a más tardar a las 16 h 30: salida a la 1 h 30 de la madrugada, imposible (no se circula de noche). La misión no puede hacerse en el día. 2) Noche en el lugar o en una ciudad de etapa segura, en un alojamiento evaluado de antemano; o dividirla: día 1 trayecto (salida a las 9 h, llegada hacia las 15 h), día 2 distribución y regreso parcial, o distribución por un socio local con seguimiento. Variar la hora de salida habitual, que hace previsibles los movimientos. 3) Teléfono móvil donde haya red, teléfono satelital o radio HF para los 80 km sin red, baliza de seguimiento; control de llamada cada hora y en cada punto clave (salida, entrada en la zona sin red, llegada, inicio y fin de la distribución); procedimiento de vehículo desaparecido conocido por la base.

Para recordar

- Un plan de seguridad breve, conocido, firmado a la llegada y revisado periódicamente.
- Niveles de seguridad con medidas automáticas e indicadores de cambio de nivel definidos de antemano.
- Desplazamientos: autorización, verificación de la carretera, control de llamada, toque de queda con margen, no resistencia.
- Comunicaciones redundantes, probadas, sin información sensible en claro.
- Pocos procedimientos, explicados, ejercitados y verificados; la complacencia es un riesgo.

Cuestionario

1. Trayecto de 160 km a 40 km/h, llegada a más tardar a las 16 h. Salida a más tardar:
   A. 12 h
   B. 10 h
   C. 14 h
   D. 11 h

2. 10 personas, 7 días de hibernación, 4 litros de agua por persona y día. Agua mínima:
   A. 70 litros
   B. 400 litros
   C. 40 litros
   D. 280 litros

3. ¿Por qué exigir dos medios de comunicación independientes?
   A. Para reducir costes
   B. Porque los donantes lo exigen
   C. Porque la red móvil falla a menudo en el momento crítico
   D. Para comunicarse con la prensa

4. Por radio se evita mencionar:
   A. Los indicativos de llamada
   B. Los nombres, las sumas de dinero y los itinerarios detallados
   C. La hora
   D. El nivel de seguridad

5. Tras seis meses sin incidentes, el equipo relaja los controles de llamada. Esto es:
   A. Complacencia, un riesgo que la dirección debe corregir
   B. Normal y sin riesgo
   C. Una buena adaptación
   D. Una decisión del conductor

Respuestas del cuestionario : 1. A · 2. D · 3. C · 4. B · 5. A

Semana 5 : Construir la aceptación y negociar el acceso

Objetivos

- Construir una estrategia de aceptación basada en los principios, la calidad de los programas y el diálogo con todos los actores.
- Medir la aceptación con indicadores concretos en lugar de suponerla.
- Preparar y conducir una negociación de acceso humanitario con un actor armado, fijando las propias líneas rojas.

La aceptación no es algo adquirido

La **aceptación** es el consentimiento, activo o pasivo, de los actores que pueden perjudicar a la organización. No se decreta: se construye y se mantiene, y puede perderse en un solo día.

Se basa en varios pilares:

- **Los principios**: humanidad, neutralidad, imparcialidad, independencia, comprendidos y percibidos como reales.
- **La calidad y la pertinencia** de los programas: una ayuda útil, justa y bien focalizada.
- **La rendición de cuentas**: las comunidades saben qué pueden esperar y pueden presentar quejas.
- **El comportamiento** del personal: respeto, discreción, ausencia de arrogancia, ni explotación ni abusos.
- **El diálogo** con todos los actores que tienen influencia, incluidos los grupos armados no estatales.
- **La coherencia**: los mismos criterios en todas partes, el mismo discurso ante todos.

La aceptación es a menudo **local y personal**: depende de un equipo, de un responsable respetado. No se transfiere automáticamente de una zona a otra ni de una persona a otra.

Lo que destruye la aceptación

Las pérdidas de aceptación provienen a menudo de la propia organización:

- Focalización percibida como injusta o acaparada por una élite o un grupo.
- Contrataciones percibidas como favorables a un clan o excluyentes de la población local.
- Promesas incumplidas, programas interrumpidos sin explicación.
- Asociación visible con una parte en el conflicto (escoltas militares, logotipos de fuerzas armadas, presencia en reuniones militares mediatizadas).
- Comportamiento personal: conducción peligrosa, consumo ostentoso de alcohol en un contexto conservador, relaciones consideradas inapropiadas.

- Comunicación pública imprudente: un comunicado de la sede o un mensaje en las redes sociales leído localmente como una toma de posición.

> Un tuit de la sede puede anular meses de trabajo de aceptación sobre el terreno: la comunicación externa forma parte de la gestión de riesgos.

Medir la aceptación

La aceptación se da por supuesta con demasiada frecuencia («la gente nos quiere»). Se puede **medir** con indicadores:

- ¿Conocen las comunidades y los líderes a la organización, sus actividades y sus principios? (encuestas de percepción, entrevistas)
- ¿Recibe la organización **alertas** espontáneas («no pasen por ahí mañana»)?
- ¿Se conceden sus solicitudes de acceso, y en qué plazos?
- ¿Las quejas recibidas se refieren a la calidad de la ayuda o a la presencia misma de la organización?
- ¿Los incidentes la afectan más o menos que a otras organizaciones comparables?

Ejemplo. Encuesta de percepción a 300 personas en dos distritos: distrito A, el 78 % conoce a la organización y el 70 % considera la ayuda «justa»; distrito B, el 41 % la conoce y el 35 % considera la ayuda «justa». La aceptación es claramente más débil en B, donde sin embargo el equipo se sentía «bien aceptado». Acciones: reuniones comunitarias, difusión de los criterios de focalización, revisión de las listas con los comités, contratación local más equilibrada.

Negociar el acceso: preparación

La **negociación humanitaria** busca obtener el acceso a las poblaciones, la seguridad de los equipos y el respeto de los principios, en un diálogo a menudo asimétrico. Los métodos estructurados (por ejemplo, los del Centro de Competencias en Negociación Humanitaria, CCHN) insisten en la preparación:

- **Análisis del interlocutor**: intereses, motivaciones, normas, limitaciones, red, a quién debe convencer él mismo.
- **Análisis del propio mandato**: lo que se puede ofrecer y lo que no.
- **Líneas rojas** fijadas y validadas de antemano por la jerarquía: ningún pago, ningún desvío de la ayuda, ninguna lista de beneficiarios impuesta, ninguna escolta del grupo armado si compromete la neutralidad.
- **Zona de negociación**: los puntos abiertos al intercambio (calendario, modalidades, comunicación, elección de los sitios).
- **Equipo**: quién negocia (persona aceptada, idioma, perfil), quién apoya, quién decide.
- **Plan B**: ¿qué se hace en caso de fracaso? (mejor alternativa a un acuerdo negociado)

Negociar el acceso: conducción y seguimiento

Principios de conducción:

- Empezar por establecer la **relación** y la confianza; escuchar antes de pedir.
- Hablar de las **necesidades de las poblaciones** que el interlocutor dice defender: muchos actores armados quieren ser vistos como protectores de «su» población.
- Explicar los principios en términos concretos: imparcialidad = ayuda según las necesidades, para todos; neutralidad = no tomar partido, tampoco contra él.
- No prometer nunca lo que no se puede cumplir; no ceder nunca en una línea roja bajo presión: pedir tiempo y consultar con la jerarquía.
- Dejar **constancia** de lo acordado e informar a los demás actores interesados si es necesario, sin poner a nadie en peligro.

Seguimiento. Un acuerdo de acceso se verifica con el uso: ¿pasan realmente los equipos? ¿Se cumplen los compromisos por ambas partes? Toda violación (cobro de tasas, desvío, amenaza) se analiza y recibe una respuesta proporcionada: recordatorio, suspensión parcial, suspensión total, coordinación con las demás organizaciones para evitar que un grupo enfrente a unas ONG con otras.

Coordinación y posiciones comunes

Negociar en solitario expone a la organización a exigencias que no puede rechazar sin riesgo, o que otra organización aceptará. La **coordinación** refuerza la posición de todos:

- **Normas operativas comunes** (ground rules) entre las organizaciones de una zona: ningún pago en los puestos de control, ninguna escolta armada salvo excepción, rechazo colectivo de las listas impuestas.
- **Grupos de trabajo sobre el acceso** coordinados por OCHA, que hacen el seguimiento de las restricciones de acceso y llevan a cabo una incidencia común.
- **Foros de seguridad de las ONG** que comparten la información y los análisis.

Límites: la coordinación no debe hacer perder la **independencia** de cada organización ni asociarla a posiciones políticas. Algunas organizaciones, como el CICR, llevan a cabo sus propias negociaciones confidenciales. La coordinación se hace sobre principios y prácticas, no mediante un alineamiento ciego.

Ejercicio: un puesto de control que «cobra tasas»

Situación. Un grupo armado controla la carretera hacia 3 campos de desplazados (25 000 personas). Desde hace dos semanas exige 50 USD por camión de ayuda y pide que el 10 % de los víveres se «entregue a los combatientes que protegen los campos». Dos ONG han empezado a pagar «para no abandonar a la gente». Su organización distribuye víveres y gestiona un centro de salud. Una encuesta de percepción reciente muestra que el 74 % de los habitantes de los campos les conoce y considera justa su ayuda.

Trabajo solicitado. 1) ¿Cuáles son sus líneas rojas? 2) ¿Qué palancas e intereses del grupo puede movilizar? 3) ¿Qué plan si la negociación fracasa?

Solución. 1) Ningún pago ni parte de la ayuda a una parte en el conflicto (violación de los principios, de las normas de los donantes y a menudo de las leyes antiterroristas); ninguna distribución bajo control del grupo; lista de beneficiarios establecida por la organización según las necesidades. 2) Palancas: la fuerte aceptación en los campos (el grupo quiere ser visto como protector de los desplazados); la importancia del centro de salud, incluso para las familias de los combatientes (atención imparcial a todos); una posición común con las demás organizaciones a través del grupo de trabajo sobre el acceso; la intervención de líderes religiosos o tradicionales respetados por el grupo. 3) Coordinarse con OCHA y las ONG para que los pagos cesen de forma colectiva; si el acceso sigue condicionado, suspender temporalmente los convoyes de víveres explicando el motivo a las comunidades y al grupo; considerar modalidades alternativas (transferencias monetarias si los mercados lo permiten, compras locales en los campos); mantener el centro de salud si su acceso no depende de los convoyes; documentar e informar a los donantes.

Para recordar

- La aceptación se construye, se mantiene, se mide y puede perderse en un día.
- Focalización, contratación, comportamiento y comunicación pública: primeras causas de pérdida de aceptación.
- Negociar: analizar al interlocutor, fijar las líneas rojas, conocer la propia zona de intercambio y el plan B.
- Ningún pago ni parte de la ayuda a una parte en el conflicto: línea roja común.
- Las normas comunes entre organizaciones refuerzan a cada una, sin sacrificar la independencia.

Cuestionario

1. ¿Qué señal indica una aceptación real?
   A. El personal se siente bien
   B. La comunidad da alertas espontáneas sobre los peligros
   C. El donante está satisfecho
   D. Las oficinas están bien protegidas

2. Una línea roja de negociación debe estar:
   A. Fijada y validada de antemano por la jerarquía
   B. Improvisada durante la reunión
   C. Abierta a negociación si el interlocutor insiste
   D. En secreto incluso para el equipo

3. Un grupo armado exige el 5 % de la ayuda. La respuesta conforme a los principios:
   A. Aceptar para mantener el acceso
   B. Pagar en efectivo en lugar de en víveres
   C. Aceptar en secreto
   D. Negarse, buscar una posición común y otras palancas, y suspender si es necesario

4. ¿Por qué coordinar normas comunes entre organizaciones?
   A. Para compartir los presupuestos
   B. Para suprimir la independencia de cada una
   C. Para evitar que un actor enfrente a las organizaciones entre sí
   D. Para evitar hablar con las comunidades

5. En una encuesta, el 40 % de los habitantes conoce a la organización en un distrito donde el equipo se cree bien aceptado. Conclusión:
   A. La encuesta es falsa
   B. La aceptación probablemente está sobrestimada; reforzar la información y el diálogo
   C. Hay que abandonar el distrito
   D. No hay nada que hacer

Respuestas del cuestionario : 1. B · 2. A · 3. D · 4. C · 5. B

Semana 6 : Incidentes: notificar, analizar, aprender

Objetivos

- Establecer un sistema de notificación de incidentes y cuasi incidentes que fomente la transmisión de información.
- Analizar un incidente con un método estructurado (cronología, causas, factores contribuyentes) sin cultura de la culpa.
- Aprovechar los datos de incidentes para ajustar las medidas y rendir cuentas a la dirección y a los donantes.

Por qué notificar

Un **incidente de seguridad** es todo acontecimiento que ha causado o podría haber causado un daño al personal, a los bienes, a la reputación o a los programas. El **cuasi incidente** (near miss) es un acontecimiento que podría haber causado un daño pero no lo causó: disparos oídos cerca de un convoy, falso puesto de control evitado por poco, amenaza verbal.

Notificar sirve para:

- **prestar asistencia** inmediata a las personas afectadas;
- **alertar** a los demás equipos y organizaciones;
- **comprender** las tendencias y adaptar las medidas;
- **rendir cuentas** a la dirección, a la junta, a los donantes y a las aseguradoras;
- **demostrar** que la organización ejerce su deber de cuidado.

La pirámide de incidentes (observada en numerosos sectores) muestra que antes de un incidente grave suele haber muchos cuasi incidentes e incidentes menores. No notificarlos es privarse de las alertas tempranas.

El sistema de notificación

Un sistema eficaz consta de tres niveles:

- **Alerta inmediata** (en la hora siguiente): llamada o mensaje a la persona designada, con la información esencial: quién, qué, dónde, cuándo, estado de las personas, necesidad de ayuda.
- **Informe de incidente** (en un plazo de 24 a 48 horas): formulario estándar con cronología, consecuencias y acciones emprendidas.
- **Análisis** (en un plazo de 1 a 2 semanas para los incidentes significativos): causas, lecciones, recomendaciones.

Para fomentar la notificación:

- formulario sencillo, disponible sin conexión y en los idiomas del personal;

- **ninguna sanción** por notificar un error de buena fe (cultura «justa», que distingue el error honesto de la negligencia grave o de la infracción deliberada);
- canal **confidencial** para los incidentes sensibles (violencia sexual, acoso, incidentes que implican a un colega);
- **retroalimentación**: los equipos ven qué cambia gracias a sus notificaciones.

> Si un equipo nunca notifica nada, casi nunca es porque no ocurra nada. Es una señal de alerta sobre la cultura de seguridad.

Clasificar los incidentes

Una **tipología** común hace comparables los datos: violencia contra las personas (asesinato, herida, secuestro, agresión sexual, detención arbitraria), robo y asalto, intrusión, amenaza, incidente vinculado al conflicto (disparos, bombardeos, artefactos explosivos), accidente de tráfico, incidente de salud, incidente de seguridad digital, disturbios civiles.

Cada incidente recibe también un **nivel de gravedad**, por ejemplo de 1 (menor, sin heridos ni pérdidas significativas) a 4 (crítico: fallecimiento, secuestro, herida grave, retirada de una zona).

Ejemplo de tabla trimestral. 42 incidentes notificados: 15 robos menores, 9 amenazas, 6 accidentes de tráfico (de ellos 2 graves), 5 asaltos a vehículos, 4 cuasi incidentes vinculados a los combates, 2 detenciones arbitrarias de corta duración, 1 agresión física. Los incidentes de gravedad 3 y 4 son 8, es decir, el 19 %. Los 5 asaltos se produjeron todos en el mismo eje, entre las 15 h y las 17 h: la tendencia es aprovechable (cambio de horarios, revisión de las autorizaciones en ese eje).

Analizar un incidente

El análisis de un incidente significativo busca comprender, no castigar. Método en cuatro pasos:

- **Cronología** precisa, reconstruida a partir de varias fuentes (personas implicadas, testigos, comunicaciones, GPS).
- **Hechos y consecuencias**: daños, reacciones, asistencia prestada.
- **Causas y factores contribuyentes**: contexto (amenaza), vulnerabilidades (procedimientos, comportamiento, equipamiento), decisiones tomadas y sus razones, lo que funcionó bien.
- **Recomendaciones**: medidas concretas, responsables, plazos y verificación de su aplicación.

Preguntas útiles: ¿se conocía la amenaza? ¿Eran adecuados los procedimientos? ¿Eran conocidos y se aplicaban? Si no, ¿por qué (imposibles, desconocidos, eludidos)? ¿Fue rápida y adecuada la respuesta al incidente? ¿Qué deberíamos haber visto venir?

Las personas afectadas deben estar **protegidas** durante el análisis: apoyo psicológico, respeto de su ritmo, confidencialidad y ningún interrogatorio repetido que las vuelva a traumatizar.

Utilizar los datos

Los datos de incidentes alimentan:

- el **análisis de contexto** y la evaluación de riesgos (frecuencias, lugares, horarios, autores, modos de operar);
- las **decisiones** sobre las medidas (lo que funciona, lo que no funciona);
- los **informes** a la dirección (cuadro de mando trimestral) y a la junta;
- el **intercambio** con los foros de seguridad y las bases de datos sectoriales, de forma anonimizada y con el acuerdo de la organización.

Indicadores útiles. Número de incidentes por cada 100 empleados; proporción de incidentes graves; plazo medio de notificación; proporción de recomendaciones aplicadas en plazo.
Ejemplo: 24 recomendaciones derivadas de los análisis del año; 15 aplicadas en plazo, 5 con retraso, 4 sin iniciar. Tasa de aplicación en plazo: 62,5 %. La dirección examina con prioridad las 4 sin iniciar: una recomendación no aplicada deja el riesgo intacto.

Rendir cuentas y comunicar

Tras un incidente grave, varios públicos esperan información, con necesidades diferentes:

- **Familia** de las personas afectadas: información rápida, humana, a cargo de una persona designada, antes de cualquier comunicación pública.
- **Personal**: información factual, medidas adoptadas, apoyo disponible, para evitar los rumores.
- **Donantes**: según los contratos, notificación rápida de los incidentes graves y de sus consecuencias para los programas.
- **Aseguradoras**: declaración en plazo de los daños y los gastos médicos.
- **Otras organizaciones**: alerta a través del foro de seguridad.
- **Medios de comunicación**: solo a través del portavoz designado; en caso de secuestro, la comunicación pública puede poner en peligro a la víctima y la decide la célula de crisis.

Una comunicación torpe puede agravar un incidente: publicar el nombre de una víctima antes de informar a su familia, acusar públicamente a un actor armado o revelar información que comprometa una negociación.

Ejercicio: analizar un asalto

Situación. Un vehículo de la organización fue asaltado a las 16 h 40 en el eje sur, a 25 km de la base; el conductor y dos empleados no resultaron heridos, pero se llevaron el vehículo, dos ordenadores y 4 000 USD de dietas en efectivo. Hechos: la autorización de movimiento preveía la llegada antes de las 16 h; la distribución se había retrasado; el control de llamada de las 16 h no se hizo (sin red); el responsable de base no activó el procedimiento de vehículo desaparecido hasta las 17 h 30. El trimestre anterior se habían notificado 3 cuasi incidentes en el mismo eje al final de la tarde, sin cambios en los procedimientos. Las dietas en efectivo se transportaban «para simplificar».

Trabajo solicitado. 1) Factores contribuyentes. 2) Lo que funcionó bien. 3) Recomendaciones.

Solución. 1) Salida tardía sin reevaluación (procedimiento de toque de queda no aplicado ante el retraso); zona sin red sin medio de comunicación alternativo; plazo de 90 minutos antes de activar el procedimiento de vehículo desaparecido; cuasi incidentes anteriores no aprovechados; transporte de dinero en efectivo visible e innecesario. 2) No resistencia del personal, sin heridos; notificación inmediata tras el incidente. 3) Norma clara: en caso de retraso, quedarse en el lugar, en un sitio seguro evaluado de antemano, en lugar de circular por ese eje al final de la tarde; teléfono satelital o baliza para las zonas sin red; procedimiento de vehículo desaparecido activado a más tardar 15 minutos después de una llamada fallida; análisis sistemático de los cuasi incidentes; pago de las dietas por dinero móvil o transferencia, y límite máximo para el transporte de efectivo; apoyo psicológico para los tres empleados; responsables y plazos para cada recomendación, con seguimiento del director de país.

Para recordar

- Notificar incidentes y cuasi incidentes: la base de la pirámide previene la cúspide.
- Tres niveles: alerta inmediata, informe en 48 horas, análisis de los incidentes significativos.
- Cultura justa: ninguna sanción por el error honesto notificado; canales confidenciales.
- Analizar para comprender: cronología, causas, factores contribuyentes, recomendaciones con seguimiento.
- Tras un incidente grave: primero la familia, un portavoz único, prudencia absoluta en caso de secuestro.

Cuestionario

1. Unos disparos oídos cerca de un convoy, sin heridos ni daños, constituyen:
   A. Nada que notificar
   B. Un incidente grave
   C. Un cuasi incidente que hay que notificar
   D. Un incidente de salud

2. 48 incidentes, de ellos 12 de gravedad 3 o 4. La proporción de incidentes graves es:
   A. 12 %
   B. 25 %
   C. 36 %
   D. 4 %

3. 30 recomendaciones, 21 aplicadas en plazo. Tasa:
   A. 70 %
   B. 30 %
   C. 21 %
   D. 63 %

4. En una cultura justa, un empleado que notifica un error honesto:
   A. Es sancionado para dar ejemplo
   B. Es trasladado
   C. Debe reembolsar los daños
   D. No es sancionado, y el error sirve para aprender

5. Tras el secuestro de un empleado, ¿quién decide la comunicación pública?
   A. El servicio de comunicación de la sede por sí solo
   B. Cada colega en las redes sociales
   C. La célula de crisis
   D. Los medios de comunicación locales

Respuestas del cuestionario : 1. C · 2. B · 3. A · 4. D · 5. C

Semana 7 : Gestionar una crisis: célula de crisis, hibernación, reubicación, evacuación, secuestro

Objetivos

- Organizar una célula de crisis y sus primeras horas: funciones, información, decisiones, diario.
- Planificar y decidir una hibernación, una reubicación o una evacuación, incluido para el personal nacional.
- Conocer los principios de gestión de un secuestro o una detención y el papel de cada persona.

¿Qué es una crisis?

Una **crisis** es una situación que amenaza gravemente a las personas, la capacidad de la organización para funcionar o su reputación, y que supera los procedimientos ordinarios: secuestro, muerte violenta, ataque a una base, evacuación de un país, catástrofe que afecta al personal, escándalo grave.

La gestión de crisis se apoya en una estructura preparada de antemano:

- **Célula de gestión de crisis** (en la sede o a nivel regional): decide la estrategia, moviliza los recursos, gestiona las relaciones con las familias, las autoridades, los donantes y los medios de comunicación.
- **Equipo de gestión del incidente** (a nivel de país): gestiona la situación sobre el terreno y aplica las decisiones.

Esta separación permite que el terreno se concentre en la acción mientras la célula gestiona el entorno y las decisiones estratégicas. Ambos deben tener mandatos escritos, miembros designados y suplentes, y haber realizado al menos un ejercicio de simulación.

Las primeras horas

Las primeras horas determinan a menudo el desenlace de una crisis. Lista de acciones tipo:

- **Activar** la célula según los criterios previstos; designar a un responsable y a un secretario que lleve el **diario de crisis** (hora, información, fuente, decisión, responsable).
- **Establecer los hechos**: distinguir lo confirmado, lo probable y los rumores.
- **Proteger a las personas**: poner a salvo al resto del personal, asistencia médica, reagrupamiento.
- **Informar** a las familias (a través de una persona designada), al personal, a la dirección; controlar la comunicación externa (ningún comentario público sin decisión de la célula).
- **Tomar las decisiones** urgentes: nivel de seguridad, suspensión de actividades, movimientos.

- **Planificar** las próximas horas y los relevos: una crisis puede durar semanas, y el cansancio es un riesgo.

> El diario de crisis no es una formalidad: conserva la memoria de las decisiones, protege jurídicamente a la organización y evita repetir las mismas discusiones en cada relevo.

Hibernación, reubicación, evacuación

Tres opciones cuando la situación se deteriora, descritas en el plan de seguridad:

- **Hibernación**: permanecer en el lugar, reagrupados en un sitio seguro, a la espera de que pase el peligro inmediato (combates en la ciudad, disturbios). Exige reservas (agua, alimentos, combustible, medicamentos), comunicaciones y una decisión sobre la duración máxima.
- **Reubicación**: trasladar a una parte del personal a una zona más segura del mismo país (capital, otra región), generalmente al personal más expuesto o no esencial.
- **Evacuación**: sacar al personal del país. Para el personal internacional, suele ser el regreso al país de origen; para el personal nacional, una evacuación fuera del país es jurídica y prácticamente compleja, y rara vez posible.

El **punto de no retorno**: pasado cierto momento (aeropuerto cerrado, carreteras cortadas), la evacuación ya no es posible. Por tanto, hay que decidir **pronto**, sobre la base de los indicadores, en lugar de esperar a tener certeza.

Cálculo de evacuación. 46 personas que reubicar en un avión de 12 plazas; 2 plazas reservadas al personal de la compañía y al material de comunicación: 10 plazas útiles por rotación. Se necesitan 5 rotaciones. Si cada rotación dura 3 horas y el aeródromo cierra al anochecer, solo pueden hacerse 3 rotaciones al día: 2 días como mínimo. La lista de prioridad (personas más expuestas, enfermas, no esenciales) se establece de antemano.

El personal nacional en las crisis

El personal nacional suele ser el más expuesto y el menos protegido durante las crisis. Las buenas prácticas:

- Hablar de antemano con cada empleado de sus riesgos propios (perfil, lugar de origen, familia) y de las opciones realistas.
- Prever opciones de **reubicación interna** para quienes estén amenazados debido a su empleo.
- Garantizar la **continuidad de los salarios** en caso de suspensión (anticipos de salario antes de una evacuación, medios de pago a distancia).
- Mantener el **contacto** y el apoyo tras la salida del personal internacional.
- No transferir la responsabilidad de los programas al personal nacional o a los socios sin recursos ni acuerdo, exponiendo así a quienes se quedan.

Ejemplo. Antes de una evacuación, una organización abona tres meses de anticipo de salario a sus 60 empleados nacionales, organiza un árbol de llamadas diario y acuerda con ellos un

protocolo sencillo: no se mantiene ninguna actividad sin evaluación y acuerdo de cada persona, y ningún empleado conserva bienes de la organización que lo pongan en peligro.

Secuestro y detención

El secuestro es una de las crisis más graves y más largas. Principios generalmente admitidos (que deben adaptarse a la política de cada organización y al derecho aplicable):

- **Prevención**: análisis de los perfiles expuestos, discreción, variación de los itinerarios y los horarios, control de la información publicada (incluidas las redes sociales del personal).
- **Preparación**: política escrita (incluida la posición de la organización sobre los rescates, que varía según las organizaciones y las leyes), formularios confidenciales de «prueba de vida» rellenados de antemano por el personal expuesto (preguntas cuya respuesta solo conoce la persona), seguro especializado si procede, consultores especializados identificados.
- **Gestión**: célula de crisis dedicada, comunicación estrictamente controlada, coordinación con la familia y, según el caso, con las autoridades y los gobiernos interesados, apoyo de especialistas.
- **Después**: apoyo médico y psicológico de larga duración para la persona liberada y su familia, así como para los colegas.

La **detención arbitraria** por parte de autoridades o de grupos armados exige una reacción rápida: localizar a la persona, contactos con las autoridades, apoyo jurídico, visitas si es posible, información a la familia.

Ejercitarse y extraer lecciones

Una célula de crisis que nunca se ha ejercitado pierde horas preciosas. Los **ejercicios** van desde el debate en torno a un escenario (ejercicio de mesa de 2 a 3 horas) hasta la simulación completa con inyecciones de información en tiempo real.

Un buen ejercicio pone a prueba: la activación (quién llama a quién, en cuánto tiempo), el reparto de funciones, la circulación de la información, el mantenimiento del diario, las decisiones difíciles (por ejemplo: informar o no a los medios, evacuar o hibernar) y el relevo.

Indicador sencillo. Plazo de activación de la célula: objetivo inferior a 2 horas. Durante un ejercicio, la alerta se da a las 22 h; se contacta con el primer miembro a las 22 h 20 y la célula completa se reúne a las 0 h 45: 2 h 45, por encima del objetivo. Causa: la lista de contactos no estaba actualizada y no se habían designado dos suplentes. Acción: actualización trimestral de la lista, suplentes nombrados, prueba de llamada mensual.

Tras toda crisis real, una **revisión** (al cabo de al menos unas semanas) examina lo que funcionó y lo que debe cambiar, con la misma cultura de aprendizaje que para los incidentes.

Ejercicio: la ciudad está cercada

Situación. Los combates se acercan a una ciudad donde la organización tiene 8 empleados internacionales y 54 empleados nacionales, de los cuales 12 son originarios de otra región y están amenazados por su grupo étnico. El aeropuerto sigue funcionando; un avión de 14 plazas (12 plazas útiles) puede hacer 2 rotaciones al día hacia la capital. Se cumplen 4 de los 6 indicadores del escenario «cerco». La carretera hacia la capital está cortada. Las reservas de la residencia principal permiten 5 días de hibernación para 20 personas.

Trabajo solicitado. 1) ¿Hibernar, reubicar o evacuar, y a quién? 2) ¿Cuántos días se necesitan para reubicar por avión a las personas prioritarias? 3) ¿Qué medidas para el personal nacional que se queda?

Solución. 1) Con 4 indicadores de 6 y una carretera cortada, el punto de no retorno se acerca: reubicar ahora en la capital a las personas más expuestas (los 12 empleados amenazados, con su acuerdo) y al personal internacional no esencial; mantener un pequeño equipo esencial solo si la hibernación es posible y segura. 2) Personas prioritarias: 12 empleados amenazados + 8 internacionales = 20 personas, es decir, 2 rotaciones de 12 plazas, posibles en 1 día. Si se añaden familiares a cargo de los empleados amenazados (por ejemplo, 16 personas), 36 personas = 3 rotaciones, es decir, 2 días. 3) Anticipo de salario de varios meses, contacto diario mediante árbol de llamadas, ninguna actividad mantenida sin evaluación y acuerdo, retirada de los bienes de la organización que pudieran exponerlos, información clara sobre las opciones y apoyo psicológico; plan de reanudación en cuanto la situación lo permita.

Para recordar

- Célula de crisis (estrategia, entorno) y equipo sobre el terreno (acción): mandatos, suplentes, ejercicios.
- Primeras horas: activar, establecer los hechos, proteger, informar, decidir, planificar; llevar un diario.
- Hibernar, reubicar, evacuar: decidir antes del punto de no retorno, sobre la base de indicadores.
- El personal nacional, a menudo el más expuesto, tiene derecho a opciones y a un apoyo reales.
- Secuestro: prevención, política escrita, pruebas de vida preparadas, comunicación controlada, especialistas.

Cuestionario

1. 30 personas que reubicar, avión de 10 plazas útiles. Número de rotaciones:
   A. 2
   B. 30
   C. 4
   D. 3

2. Hibernación de 15 personas durante 8 días a 4 litros de agua por persona y día:
   A. 120 litros
   B. 32 litros
   C. 480 litros
   D. 600 litros

3. El diario de crisis sirve sobre todo para:
   A. Informar a los medios de comunicación
   B. Dejar constancia de la información y las decisiones, y facilitar los relevos
   C. Evaluar al personal
   D. Calcular los costes

4. ¿Por qué preparar formularios de «prueba de vida» de antemano?
   A. Para verificar, en caso de secuestro, que la persona está viva mediante preguntas cuya respuesta solo ella conoce
   B. Para el seguro médico
   C. Para los visados
   D. Para los recursos humanos

5. Una célula de crisis se reúne 3 h 10 después de la alerta, con un objetivo de 2 horas. Acción prioritaria:
   A. Suprimir el objetivo
   B. No hacer nada, era un ejercicio
   C. Cambiar de director
   D. Actualizar los contactos, designar suplentes y hacer pruebas periódicas

Respuestas del cuestionario : 1. D · 2. C · 3. B · 4. A · 5. D

Semana 8 : Salud, bienestar psicosocial, salvaguarda interna y seguros

Objetivos

- Organizar la protección de la salud del personal: prevención, atención médica, evacuación médica y primeros auxilios.
- Prevenir y atender el estrés, el agotamiento y el trauma, y medir el bienestar de los equipos.
- Tratar el acoso, la violencia sexual contra el personal y las necesidades de seguro como riesgos en sí mismos.

La salud, primer riesgo

En muchos contextos, las **enfermedades** (paludismo, infecciones digestivas, enfermedades crónicas mal controladas) y los **accidentes** causan más bajas laborales, repatriaciones y a veces fallecimientos que la violencia. La protección de la salud forma, por tanto, parte de la gestión de riesgos.

Medidas esenciales:

- **Antes de la partida o del destino**: reconocimiento médico, vacunaciones, profilaxis antipalúdica adaptada, sesión informativa de salud sobre el contexto.
- **En el lugar**: cartografía de los centros de atención (calidad, distancia, horarios, idiomas), contratos con clínicas, botiquines de primeros auxilios, personal formado en primeros auxilios (al menos una persona por equipo o por vehículo en zona aislada).
- **Evacuación médica**: procedimiento escrito, contrato con un proveedor o una aseguradora, criterios de activación, plazos realistas.
- **Personal nacional**: cobertura sanitaria equivalente en la práctica, incluida la de las familias según la política de la organización.

Plazo crítico. La «primera hora» tras un traumatismo grave es decisiva. Si el hospital quirúrgico más cercano está a 6 horas por carretera y no es posible ninguna evacuación aérea antes del día siguiente, el riesgo de accidente grave pesa mucho más en la evaluación, y la formación en primeros auxilios avanzados pasa a ser prioritaria.

Estrés, agotamiento y trauma

Los trabajadores humanitarios están expuestos a tres tipos de estrés:

- **Estrés básico y acumulativo**: carga de trabajo, condiciones de vida, aislamiento, conflictos de equipo, inseguridad permanente. Si no se trata, conduce al **agotamiento** (burn-out).
- **Estrés traumático**: exposición a un acontecimiento violento o a la muerte.
- **Trauma vicario**: a fuerza de escuchar y ver el sufrimiento de los demás.

Varias encuestas realizadas a trabajadores humanitarios han puesto de manifiesto tasas elevadas de síntomas de ansiedad, depresión y agotamiento, a menudo superiores a las de la población general, y más elevadas aún entre el personal nacional expuesto a las mismas violencias que su propia familia.

Medidas: carga de trabajo razonable, vacaciones y pausas de recuperación respetadas (descanso y recuperación, R&R, según el contexto, por ejemplo cada 6 a 12 semanas en contextos difíciles), acceso confidencial a apoyo psicológico, formación de los responsables para detectar las señales, primeros auxilios psicológicos tras un incidente, cultura que no estigmatice la petición de ayuda.

> Un responsable que nunca se toma vacaciones envía un mensaje a todo su equipo. El bienestar también es una cuestión de ejemplo.

Medir el bienestar

El bienestar de los equipos se mide, como cualquier riesgo:

- **Tasa de utilización de las vacaciones** y de los R&R: días disfrutados / días correspondientes.
- **Horas extraordinarias** medias y número de personas por encima de un umbral.
- **Bajas por enfermedad** y rotación del personal (salidas anticipadas).
- **Encuestas anónimas** breves y periódicas (escalas validadas de estrés o de agotamiento, preguntas sobre el apoyo percibido).
- Uso del **apoyo psicológico** (en número, nunca con nombres).

Ejemplo. Equipo de 40 personas: 1 200 días de vacaciones correspondientes en el año, 690 disfrutados, es decir, el 57,5 %. 14 personas trabajan habitualmente más de 55 horas semanales. Rotación: 11 salidas en el año, es decir, el 27,5 %. Estas cifras señalan un riesgo de agotamiento elevado: plan de acción (planificación obligatoria de las vacaciones, refuerzos, reducción de reuniones, seguimiento por la dirección).

Acoso y violencia sexual contra el personal

El **acoso** (laboral y sexual), la discriminación y la **violencia sexual** contra el personal, incluso por parte de colegas, son riesgos infradeclarados. Corresponden a la vez a la seguridad, a los recursos humanos y a la salvaguarda (safeguarding) interna.

Un dispositivo mínimo incluye:

- un **código de conducta** claro y firmado, que prohíba también la explotación y el abuso sexuales contra las poblaciones;
- **canales de denuncia** múltiples y confidenciales (incluidos canales fuera de la jerarquía y externos);
- un enfoque **centrado en la persona superviviente**: seguridad, confidencialidad, respeto de sus decisiones, atención médica rápida (profilaxis posexposición al VIH y anticoncepción de emergencia dentro de plazo), apoyo psicológico;

- **investigaciones** realizadas por personas formadas, independientes de la cadena jerárquica afectada;
- **sanciones** efectivas e intercambio de información entre organizaciones para evitar la contratación de personas sancionadas (mecanismos interinstitucionales de verificación de referencias).

Los kits de profilaxis posexposición deben estar disponibles y el personal designado debe estar formado en su uso, porque los plazos de eficacia son cortos (idealmente en las primeras horas y, como máximo, en 72 horas).

Los seguros

Los seguros transfieren una parte del riesgo financiero. Coberturas habituales:

- **Salud** (incluso en el extranjero) y **evacuación médica**;
- **Accidente, invalidez y fallecimiento**, incluidos los riesgos de guerra y terrorismo, a menudo excluidos de los contratos estándar;
- **Responsabilidad civil** de la organización;
- **Bienes**: vehículos, equipos, existencias, dinero en efectivo;
- **Secuestro y rescate** (kidnap and ransom), que financia sobre todo a los consultores especializados y cuya existencia debe mantenerse confidencial.

Puntos de atención: exclusiones (zonas, actividades, guerra), límites máximos, plazos de declaración, cobertura equitativa del personal nacional y coherencia con el derecho local (seguros obligatorios).

Cálculo sencillo. Prima del 4 % de la masa salarial para una cobertura de accidente y fallecimiento que incluye los riesgos de guerra, sobre una masa salarial de 2 400 000 USD: 96 000 USD al año. Si la organización solo asegura a los 30 internacionales (masa salarial de 1 500 000 USD) y deja a 120 nacionales (900 000 USD) sin cobertura equivalente, el ahorro de 36 000 USD crea una desigualdad grave y un riesgo jurídico y reputacional.

Los primeros auxilios y la preparación médica

La preparación médica sobre el terreno se planifica como todo lo demás:

- **Formación**: primeros auxilios básicos para todos, primeros auxilios avanzados en zona aislada o de conflicto (control de hemorragias, torniquete, posición lateral, quemaduras).
- **Equipamiento**: botiquín individual (en zonas de conflicto, con torniquete), botiquín de vehículo, botiquín de la base.
- **Fichas médicas confidenciales** del personal (grupo sanguíneo, alergias, tratamientos, contactos de emergencia), accesibles solo en caso de urgencia.
- **Plan de evacuación médica** por zona: centro de primera línea, centro de referencia, medios de transporte, plazos, números, coste.

Cálculo de necesidades de formación. 85 empleados en zona aislada, objetivo: al menos 2 personas formadas en primeros auxilios avanzados por equipo de 5 en desplazamiento. Si 17

equipos pueden estar sobre el terreno al mismo tiempo, se necesitan al menos 34 personas formadas; con un 30 % de margen para las ausencias y la rotación, unas 45 personas.

Ejercicio: un equipo al límite

Situación. Una base de 25 personas (5 internacionales, 20 nacionales) en zona de conflicto. En 6 meses: 3 salidas anticipadas de internacionales, 4 bajas por enfermedad largas entre los nacionales; 210 días de vacaciones disfrutados de 450 correspondientes; el jefe de base no ha tomado ningún día de vacaciones; una empleada nacional ha comentado a una colega las insinuaciones repetidas de un supervisor, pero no quiere «armar un escándalo». El hospital quirúrgico más cercano está a 5 horas por carretera; nadie está formado en primeros auxilios avanzados. El seguro de fallecimiento e invalidez solo cubre a los internacionales.

Trabajo solicitado. 1) Calcule la tasa de utilización de las vacaciones. 2) Identifique los riesgos. 3) Proponga medidas prioritarias.

Solución. 1) 210 / 450 = 46,7 %. 2) Agotamiento colectivo (pocas vacaciones disfrutadas, salidas y bajas, ejemplo del jefe de base); acoso sexual comunicado de manera informal, con riesgo de escalada y de silencio; riesgo médico grave (a 5 horas del hospital, ningún socorrista avanzado); desigualdad de cobertura del seguro. 3) Planificación obligatoria de las vacaciones y los R&R, empezando por el jefe de base; apoyo psicológico accesible y confidencial; informar a la empleada, sin presionarla, de los canales de denuncia confidenciales y de sus opciones, garantizar su seguridad y la ausencia de represalias, y hacer intervenir a la función de salvaguarda según la política (una alerta recibida por un responsable no puede ignorarse); formar rápidamente al menos a 2 personas por equipo en primeros auxilios avanzados y revisar el plan de evacuación médica; extender el seguro al personal nacional.

Para recordar

- Las enfermedades y los accidentes pesan a menudo más que la violencia: prevención, atención y evacuación médica planificadas.
- Estrés acumulativo, traumático y vicario: vacaciones, R&R, apoyo confidencial, ejemplo de los responsables.
- Medir el bienestar: vacaciones disfrutadas, horas, bajas, rotación, encuestas anónimas.
- Acoso y violencia sexual: canales confidenciales, enfoque centrado en la persona superviviente, PEP en un plazo de 72 horas.
- Seguros adaptados a los riesgos de guerra y equitativos entre personal nacional e internacional.

Cuestionario

1. Un equipo ha disfrutado 540 días de vacaciones de 900 correspondientes. Tasa de utilización:
   A. 60 %
   B. 40 %
   C. 54 %
   D. 90 %

2. La profilaxis posexposición al VIH debe iniciarse como máximo en un plazo de:
   A. 7 días
   B. 2 semanas
   C. 30 días
   D. 72 horas

3. Masa salarial de 1 800 000 USD, prima del 3 %. Coste anual:
   A. 5 400 USD
   B. 18 000 USD
   C. 54 000 USD
   D. 540 000 USD

4. El trauma vicario está causado por:
   A. Un accidente de tráfico
   B. La exposición repetida al sufrimiento de los demás
   C. Un exceso de vacaciones
   D. El desfase horario

5. Un responsable recibe una alerta informal de acoso sexual. Debe:
   A. Informar a la víctima de sus opciones y de los canales confidenciales y activar el procedimiento de salvaguarda
   B. Esperar a una denuncia por escrito
   C. Confrontar públicamente al presunto autor
   D. No hacer nada si la víctima no quiere armar un escándalo

Respuestas del cuestionario : 1. A · 2. D · 3. C · 4. B · 5. A

Semana 9 : Seguridad digital y protección de la información

Objetivos

- Identificar las amenazas digitales propias de las organizaciones humanitarias: phishing, fraude en transferencias, vigilancia, fuga de datos.
- Establecer medidas básicas proporcionadas: autenticación, copias de seguridad, cifrado, gestión de accesos, dispositivos.
- Proteger los datos de las personas asistidas y del personal, y reaccionar ante un incidente digital.

Por qué lo digital es un riesgo de seguridad

Las organizaciones humanitarias poseen información muy sensible: listas de beneficiarios (a veces con biometría y localización), testimonios de violaciones, datos médicos, información sobre el personal, análisis de seguridad, movimientos. Una fuga o un ataque informático puede poner en peligro **vidas**, no solo datos.

Varios ciberataques conocidos han tenido como objetivo a organizaciones humanitarias, incluido el robo de datos de cientos de miles de personas vulnerables. Las organizaciones también son blanco del fraude financiero en línea y de la **vigilancia** de las comunicaciones por parte de actores estatales o no estatales.

Principales amenazas:

- **Suplantación de identidad** (phishing): correos o mensajes falsos que roban credenciales o instalan programas maliciosos.
- **Fraude en transferencias**: falso proveedor, falso director que solicita un pago urgente, cambio fraudulento de datos bancarios.
- **Ransomware**: cifrado de los datos a cambio de un rescate.
- **Robo o incautación de dispositivos** (ordenadores, teléfonos) en los puestos de control o durante asaltos.
- **Vigilancia** de las comunicaciones y de las redes sociales.
- **Errores internos**: compartir por error, archivo enviado al destinatario equivocado, contraseña a la vista.

Las medidas básicas

Unas pocas medidas sencillas bloquean la gran mayoría de los ataques comunes:

- **Autenticación multifactor** (MFA) en el correo electrónico, el almacenamiento en línea, el banco y el programa de contabilidad.
- **Gestor de contraseñas** y contraseñas largas y únicas.
- **Actualizaciones** automáticas de los sistemas y las aplicaciones.

- **Copias de seguridad** periódicas, una de ellas sin conexión o aislada, y pruebas de restauración (regla 3-2-1: tres copias, dos soportes diferentes, una copia fuera de las instalaciones).
- **Cifrado** de los discos de los ordenadores portátiles y de los teléfonos.
- **Gestión de accesos**: cada persona solo accede a lo que necesita; retirada de los accesos el día de la salida de un empleado.
- **Formación** periódica, con ejercicios de phishing simulados.

Ejemplo de ejercicio. Se envía un correo de phishing falso a 120 empleados: 38 hacen clic en el enlace (31,7 %), 14 introducen sus credenciales (11,7 %), 9 notifican el correo al servicio informático (7,5 %). Tras una formación específica, un segundo ejercicio da 12 clics (10 %), 3 introducciones de credenciales (2,5 %) y 41 notificaciones (34,2 %). El aumento de las notificaciones es tan importante como el descenso de los clics: convierte al personal en un sistema de alerta.

Fraude en transferencias y procedimientos financieros

El **fraude del CEO** y el fraude de datos bancarios cuestan cada año sumas importantes a las organizaciones, incluidas las humanitarias. Los procedimientos financieros son la mejor defensa:

- Toda **modificación de los datos bancarios** de un proveedor o de un empleado se verifica mediante una llamada a un número ya conocido, nunca al indicado en la solicitud.
- Ningún pago urgente fuera de procedimiento, ni siquiera a petición aparente de un director: la doble validación sigue siendo obligatoria.
- Los accesos a la banca en línea utilizan dispositivos y cuentas dedicados, con doble firma electrónica.
- El personal sabe que contará con **respaldo** si rechaza un pago sospechoso, aunque lo pida un superior.

> La urgencia y la confidencialidad son las dos palancas favoritas de los estafadores: «Estoy en una reunión, haz esta transferencia ahora mismo y no se lo digas a nadie».

Dispositivos, puestos de control y vigilancia

Sobre el terreno, los riesgos digitales también son **físicos**:

- En los puestos de control, los teléfonos pueden ser registrados. Un teléfono que contiene fotos de posiciones militares, mensajes críticos con una parte o listas de beneficiarios puede dar lugar a una detención. Norma: llevar solo lo necesario, borrar los datos sensibles de los dispositivos de terreno, utilizar dispositivos dedicados al trabajo.
- Las **redes sociales** del personal revelan información aprovechable: localización en tiempo real, opiniones políticas, fotos de colegas, signos de riqueza. Una política sobre el uso de las redes sociales, explicada y no punitiva, reduce estos riesgos.

- Las **mensajerías** cifradas de extremo a extremo protegen el contenido, pero no el hecho de que se esté comunicando, ni el propio teléfono si se incauta desbloqueado.
- El uso de ciertas herramientas (satélites, VPN, drones) puede estar prohibido o resultar sospechoso: verificar la legislación y la aceptación.

Proteger los datos de las personas

La **protección de datos** de los beneficiarios y del personal se basa en principios reconocidos (en particular, el manual del CICR y del Brussels Privacy Hub sobre la protección de datos en la acción humanitaria):

- **Licitud y finalidad**: base legítima y finalidad precisa para cada recogida.
- **Minimización**: recoger solo lo necesario.
- **Consentimiento informado** cuando esa es la base elegida, teniendo en cuenta las relaciones de poder (un hogar que necesita ayuda no es libre de negarse).
- **Seguridad**: cifrado, accesos limitados, registro de actividad.
- **Conservación limitada** y supresión al término de la finalidad.
- **Intercambio regulado** mediante acuerdos de intercambio de datos, con un análisis de riesgos (incluidas las solicitudes de autoridades o de partes en el conflicto).
- **Evaluación de impacto** antes de todo nuevo sistema (biometría, pago móvil, plataforma compartida).

Ejemplo de minimización. Para una distribución de kits, hay que identificar el hogar y verificar que no haya recibido ya el kit. La pertenencia étnica o religiosa no es necesaria y no debe recogerse; la foto y la huella dactilar generalmente tampoco lo son.

Reaccionar ante un incidente digital

Un incidente digital (cuenta pirateada, ordenador robado, ransomware, archivo enviado por error) se trata como un incidente de seguridad:

- **Contener**: cambiar las contraseñas, revocar las sesiones, aislar el dispositivo infectado, borrar a distancia un dispositivo robado.
- **Evaluar**: ¿qué datos, qué personas, qué riesgo para ellas?
- **Informar**: dirección, responsable de protección de datos, personas afectadas si están expuestas a un riesgo, autoridades de control según el derecho aplicable, donantes según los contratos.
- **Restaurar** a partir de las copias de seguridad; no pagar un rescate sin decisión de la dirección y análisis jurídico.
- **Aprender**: análisis, correcciones, formación.

Ejemplo. Un ordenador portátil sin cifrar que contiene la lista de 3 200 hogares con sus números de teléfono y su localización es robado durante un asalto. El riesgo para las personas depende del contexto: si algunos hogares pertenecen a un grupo perseguido, es elevado. Acciones: evaluación inmediata, información a las comunidades afectadas por canales seguros

si están expuestas, cambio de las modalidades de contacto, cifrado obligatorio de todos los ordenadores portátiles.

Ejercicio: un correo urgente del director

Situación. Un viernes a las 17 h, la contable recibe un correo aparentemente del director de país, que está de viaje: «Confidencial. Tenemos que pagar hoy el anticipo de 48 000 USD al nuevo proveedor de combustible o perderemos el contrato. Datos bancarios adjuntos. No estoy localizable, reunión con el ministro». La dirección de envío difiere en una letra de la dirección habitual. El mismo día, un proveedor habitual ha pedido por correo cambiar sus datos bancarios. El correo de la organización no tiene autenticación de dos factores.

Trabajo solicitado. 1) Señales de alerta. 2) Conducta inmediata. 3) Medidas duraderas.

Solución. 1) Urgencia, confidencialidad, indisponibilidad del solicitante, nuevo proveedor sin expediente de compra, dirección de envío ligeramente diferente, solicitud paralela de cambio de datos bancarios. 2) No pagar; llamar al director a su número conocido (o a su adjunto); no modificar los datos del proveedor habitual sin una llamada de verificación a un número ya conocido; informar al responsable informático y a finanzas; conservar los correos como pruebas. 3) Autenticación de dos factores en todo el correo; norma escrita: ningún pago fuera de procedimiento, doble validación, verificación telefónica de toda modificación bancaria; formación y ejercicios de phishing; filtrado de los dominios parecidos; mensaje claro de la dirección: rechazar un pago sospechoso siempre contará con respaldo.

Para recordar

- Los datos humanitarios son sensibles: una fuga puede poner vidas en peligro.
- MFA, contraseñas únicas, actualizaciones, copias de seguridad 3-2-1, cifrado, accesos mínimos, formación.
- Fraude en transferencias: verificación a través de un número conocido, doble validación, respaldo a quien se niega.
- Terreno: dispositivos con lo mínimo en los puestos de control, política sobre las redes sociales.
- Protección de datos: finalidad, minimización, seguridad, conservación limitada, evaluación de impacto.

Cuestionario

1. 150 empleados reciben un correo falso; 24 hacen clic. Tasa de clics:
   A. 24 %
   B. 16 %
   C. 6,25 %
   D. 15 %

2. La regla de copias de seguridad 3-2-1 significa:
   A. 3 copias, 2 soportes diferentes, 1 copia fuera de las instalaciones
   B. 3 contraseñas, 2 factores, 1 cuenta
   C. 3 días, 2 semanas, 1 mes
   D. 3 servidores, 2 países, 1 nube

3. Un proveedor pide por correo cambiar sus datos bancarios. Usted:
   A. Los cambia inmediatamente
   B. Paga en efectivo
   C. Responde al correo
   D. Lo verifica con una llamada al número ya conocido

4. Para una distribución de kits, recoger la pertenencia étnica de los hogares es:
   A. Obligatorio
   B. Recomendable
   C. Contrario al principio de minimización si no es necesario
   D. Inocuo

5. Roban un ordenador sin cifrar que contiene listas de beneficiarios. Primer paso:
   A. Comprar otro ordenador
   B. Evaluar los datos expuestos y el riesgo para las personas, y después informar
   C. No decir nada
   D. Publicar un comunicado

Respuestas del cuestionario : 1. B · 2. A · 3. D · 4. C · 5. B

Semana 10 : Gestionar todos los riesgos de la organización: registro, apetito, cumplimiento y reputación

Objetivos

- Construir y mantener un registro de riesgos de la organización (de seguridad, fiduciarios, operativos, jurídicos, reputacionales, éticos).
- Definir el apetito de riesgo y traducirlo en umbrales y decisiones, incluso mediante la pérdida esperada.
- Integrar el cumplimiento (sanciones, antiterrorismo, fraude, protección contra la explotación y el abuso sexuales) en un enfoque único.

De los riesgos de seguridad a los riesgos de la organización

La gestión de los riesgos de la organización (a menudo llamada ERM, enterprise risk management) extiende la lógica de la seguridad a todos los riesgos que amenazan la misión:

- **Seguridad**: violencia, accidentes, salud del personal.
- **Fiduciarios**: fraude, corrupción, desvío, mal uso de los fondos.
- **Operativos**: ruptura del abastecimiento, fallo de un socio, pérdida de acceso.
- **Jurídicos y de cumplimiento**: sanciones, antiterrorismo, derecho laboral, fiscalidad, protección de datos.
- **Éticos y de salvaguarda**: explotación y abuso sexuales, acoso, vulneración de los principios.
- **Reputacionales**: pérdida de confianza de las comunidades, de los donantes y del público.
- **Financieros y estratégicos**: dependencia de un donante, crisis de tesorería, pérdida de pertinencia.

Estos riesgos están **vinculados**: un desvío de ayuda por parte de un grupo armado es a la vez un riesgo fiduciario, jurídico (sanciones), operativo (suspensión), reputacional y de seguridad (represalias si la organización lo denuncia). Por eso es necesario un enfoque integrado.

El registro de riesgos

El **registro de riesgos** recoge los principales riesgos, con, para cada uno: descripción (causa, acontecimiento, consecuencia), categoría, propietario, probabilidad, impacto, puntuación inherente, medidas existentes, puntuación residual, medidas adicionales previstas, plazo.

Riesgo	Propietario	Inherente	Residual	Acción
Desvío de ayuda alimentaria por una autoridad local en la provincia X	Director de programas	4 × 5 = 20	3 × 4 = 12	Verificación por terceros, llamadas a los beneficiarios, distribución directa
Fraude en las compras de combustible	Director financiero	4 × 3 = 12	2 × 3 = 6	Tarjetas de combustible, conciliaciones mensuales
Pérdida del primer donante (55 % de los ingresos)	Director general	3 × 5 = 15	3 × 4 = 12	Plan de diversificación, reservas
Explotación sexual por parte de un empleado o un socio	Responsable de salvaguarda	3 × 5 = 15	2 × 5 = 10	Formación, verificación de referencias, canales de quejas comunitarios

La dirección revisa el registro cada trimestre, y la junta o su comité de auditoría y riesgos, cada año. Los **diez principales riesgos** son objeto de un seguimiento particular.

El apetito de riesgo

El **apetito de riesgo** es el nivel de riesgo que la organización acepta asumir para cumplir su misión. Lo fija la junta, por categoría:

- **Seguridad**: apetito moderado, elevado solo para las actividades vitales (véase la criticidad de los programas).
- **Fiduciario**: apetito bajo para el fraude, pero aceptación de un riesgo residual en los contextos difíciles, siempre que se detecte y se notifique.
- **Explotación y abuso sexuales**: tolerancia cero para los comportamientos, lo que no impide reconocer que el riesgo existe y debe gestionarse activamente.
- **Programático**: apetito más elevado para la innovación y el acceso a zonas difíciles.

El apetito de riesgo no es un eslogan: se traduce en **umbrales** (puntuación residual máxima por categoría), en **delegaciones** (quién puede aceptar qué nivel de riesgo) y en **decisiones** documentadas. Un apetito demasiado bajo impide trabajar allí donde las necesidades son mayores; un apetito no definido deja que cada responsable decida en solitario.

La pérdida esperada

Para ciertos riesgos financieros, la matriz puede completarse con la **pérdida esperada**: probabilidad anual × coste en caso de materializarse. Esto ayuda a comparar el coste de una medida con la pérdida que evita.

Ejemplo. Riesgo de robo de la caja de una oficina sobre el terreno: probabilidad anual estimada en el 20 %, pérdida media de 15 000 USD (efectivo y gastos). Pérdida esperada: 0,2 × 15 000 = 3 000 USD al año. Pasar a los pagos por dinero móvil cuesta 1 800 USD al año y reduce la probabilidad al 5 % y la pérdida media a 4 000 USD: pérdida esperada de 200 USD.

Ganancia neta: 3 000 − 200 − 1 800 = 1 000 USD al año, sin contar la reducción del riesgo para la seguridad del cajero.

Límites: la pérdida esperada no sirve para los riesgos que afectan a vidas o cuyo impacto es catastrófico. Nadie decide aceptar un secuestro porque su «pérdida esperada» sea baja. Para estos riesgos se razona en términos de umbral aceptable y de planes de contingencia.

Cumplimiento: sanciones, antiterrorismo, fraude

Las obligaciones de cumplimiento vienen impuestas por las leyes nacionales, los regímenes de sanciones y los contratos de los donantes:

- **Sanciones y antiterrorismo**: prohibición de poner fondos o recursos a disposición de personas o entidades incluidas en las listas. Medidas: verificación de proveedores, socios y empleados según el riesgo; cláusulas contractuales; vigilancia de los pagos en las zonas controladas por grupos incluidos en las listas; uso de las exenciones humanitarias existentes, documentando su aplicación.
- **Antifraude y anticorrupción**: política, línea de denuncia, investigaciones, notificación a los donantes en plazo (véase la parte de finanzas).
- **Verificación del beneficiario final**: en general, los donantes no exigen cotejar a cada beneficiario de la ayuda con las listas, y los principios humanitarios se oponen a ello; los controles se refieren a los socios, proveedores y personal.

El diálogo con los donantes y los bancos es esencial: la **retirada de los bancos** (de-risking), que se niegan a operar con organizaciones que trabajan en zonas sancionadas, puede bloquear operaciones enteras. Documentar la propia diligencia ayuda a mantener las cuentas abiertas.

Protección contra la explotación y el abuso sexuales

La **protección contra la explotación y el abuso sexuales** (PSEA) de las poblaciones asistidas es una obligación fundamental. Los seis principios fundamentales del Comité Permanente entre Organismos (IASC) prohíben en particular toda relación sexual con niños y niñas (menores de 18 años) y todo intercambio de dinero, empleo, bienes o servicios por favores sexuales, e imponen notificar cualquier preocupación.

El dispositivo:

- código de conducta y formación de todo el personal y de los socios;
- verificación de referencias en la contratación (mecanismos interinstitucionales);
- **mecanismos comunitarios de quejas** accesibles, seguros y adaptados a las mujeres y a la infancia;
- asistencia a las víctimas (médica, psicosocial, jurídica) según sus decisiones;
- investigaciones rápidas e independientes, sanciones, notificación a los donantes;
- cláusulas de PSEA en los acuerdos con los socios.

Indicador engañoso: **cero quejas** no significa cero abusos. En la mayoría de los contextos, la ausencia de quejas indica más bien que las comunidades no conocen los mecanismos o no los

consideran seguros.

Ejercicio: el comité de riesgos de la junta

Situación. Usted presenta al comité de riesgos de una ONG los siguientes elementos. Fraude en el combustible: probabilidad anual del 30 %, pérdida media de 25 000 USD; medida propuesta (tarjetas de combustible y conciliaciones) con un coste de 4 000 USD al año, que reduciría la probabilidad al 10 % y la pérdida a 10 000 USD. Desvío de ayuda en una provincia: inherente 4 × 5, residual 3 × 4; umbral de apetito fiduciario de la junta: residual ≤ 9. Mecanismo de quejas de PSEA: ninguna queja en 2 años en 5 provincias; una encuesta de conocimiento muestra que el 18 % de las mujeres entrevistadas conoce el mecanismo. Un socio local nunca ha sido cotejado con las listas de sanciones.

Trabajo solicitado. 1) ¿Está justificada la medida sobre el combustible? 2) ¿Está el riesgo de desvío dentro del apetito? ¿Qué hacer? 3) ¿Qué concluir sobre la PSEA? 4) ¿Y el socio?

Solución. 1) Pérdida esperada actual: 0,3 × 25 000 = 7 500 USD; tras la medida: 0,1 × 10 000 = 1 000 USD; ganancia neta: 7 500 − 1 000 − 4 000 = 2 500 USD al año: justificada. 2) Residual 12 > 9: fuera del apetito. Opciones: medidas adicionales (verificación por terceros, distribución directa, transferencias monetarias), reducción del volumen en la provincia, o aceptación explícita y documentada por la junta de un rebasamiento temporal con un plan. 3) Cero quejas con un 18 % de conocimiento indica un mecanismo ineficaz, no una ausencia de abusos: campaña de información, canales adaptados a las mujeres, puntos focales mujeres, verificación de la confianza de las comunidades. 4) Cotejo inmediato con las listas de sanciones e integración sistemática de esta verificación en el procedimiento de selección de socios.

Para recordar

- Los riesgos de la organización están vinculados: de seguridad, fiduciarios, operativos, jurídicos, éticos, reputacionales, financieros.
- Registro de riesgos con propietarios, puntuaciones inherentes y residuales, acciones y plazos, revisado por la dirección y la junta.
- Apetito de riesgo fijado por la junta, por categoría, traducido en umbrales y delegaciones.
- Pérdida esperada = probabilidad × coste: útil para los riesgos financieros, no para las vidas.
- PSEA: cero quejas no es cero abusos; sanciones: verificar socios, proveedores y personal.

Cuestionario

1. Probabilidad anual del 25 %, pérdida de 12 000 USD. Pérdida esperada:
   A. 12 000 USD
   B. 4 800 USD
   C. 3 000 USD
   D. 300 USD

2. Una medida cuesta 2 000 USD al año y reduce la pérdida esperada de 5 000 a 1 500 USD. Ganancia neta anual:
   A. 3 500 USD
   B. 1 500 USD
   C. 5 000 USD
   D. −500 USD

3. ¿Quién fija el apetito de riesgo de la organización?
   A. La junta directiva
   B. Cada jefe de proyecto
   C. El donante principal
   D. El auditor externo

4. Un mecanismo de quejas de PSEA no recibe ninguna queja en dos años. Conclusión más probable:
   A. No hay ningún abuso
   B. Hay que suprimir el mecanismo
   C. El personal es ejemplar
   D. Probablemente el mecanismo no se conoce ni se considera seguro

5. Los cotejos con las listas de sanciones se refieren en general a:
   A. Cada beneficiario de la ayuda
   B. Los periodistas
   C. Los socios, proveedores y personal según el riesgo
   D. Nadie

Respuestas del cuestionario : 1. C · 2. B · 3. A · 4. D · 5. C

Semana 11 : Compartir el riesgo con los socios y financiar la seguridad

Objetivos

- Analizar la transferencia de riesgo hacia los socios nacionales y locales y construir un reparto equitativo de los riesgos.
- Presupuestar la seguridad de forma completa y defenderla ante los donantes.
- Organizar la seguridad en los consorcios, la gestión a distancia y la coordinación interinstitucional.

La transferencia del riesgo

Cuando el acceso se vuelve difícil, las organizaciones internacionales se apoyan cada vez más en **socios nacionales y locales**, mejor aceptados y a menudo los únicos presentes. Es una fortaleza para la respuesta y para la localización, pero puede convertirse en una **transferencia de riesgo**: la organización internacional reduce su exposición exponiendo más al socio, sin darle los medios para hacerle frente.

Señales de una transferencia injusta:

- el socio trabaja en zonas a las que la organización internacional prohíbe ir a su propio personal, sin evaluación conjunta de los riesgos;
- el presupuesto del socio no contiene ninguna partida de seguridad (comunicaciones, seguros, formación, vehículos adaptados);
- el socio asume en solitario el riesgo fiduciario (pérdidas y robos reembolsados por él) y el riesgo jurídico (sanciones);
- no se prevé ninguna asistencia en caso de incidente grave que afecte al personal del socio.

Hacia un reparto equitativo

El **reparto del riesgo** (risk sharing) es un enfoque que reconoce que los riesgos deben distribuirse según la capacidad de cada parte para gestionarlos, y financiarse. Los trabajos interinstitucionales sobre este tema (en particular en el marco del Grand Bargain y de las redes de ONG) proponen:

- una **evaluación conjunta** de los riesgos con el socio, antes del acuerdo;
- **costes de seguridad subvencionables** en el presupuesto del socio, en la medida de las necesidades reales;
- acceso del socio a la **formación**, a los análisis de seguridad y a los dispositivos de emergencia (evacuación médica, seguro);
- un reparto claro del **riesgo fiduciario**: qué pérdidas se aceptan si se han seguido los procedimientos y cuáles se reembolsan;

- **compromisos recíprocos** en caso de incidente grave: asistencia, comunicación, apoyo a las familias.

> Pregunta de control: si este incidente le ocurriera a nuestro propio personal, ¿qué haríamos? ¿Merece menos el socio?

Presupuestar la seguridad

La seguridad cuesta, y sus costes deben figurar claramente en los presupuestos; de lo contrario, se cubren con otras partidas o se ignoran. Partidas típicas:

- **Personal**: asesor de seguridad, puntos focales, guardias, operadores de radio.
- **Equipos**: comunicaciones (radios, teléfonos satelitales, balizas), vehículos adaptados, protección de los sitios, equipos de protección individual según el contexto.
- **Formación**: seguridad básica, formaciones avanzadas, primeros auxilios, ejercicios de crisis.
- **Servicios**: suscripciones a servicios de análisis, foros de seguridad, evacuación médica, seguros específicos.
- **Reservas para contingencias**: hibernación, reubicación, evacuación.

Ejemplo de presupuesto anual de un país (8 millones USD de programas, 150 empleados). Asesor de seguridad y 3 puntos focales: 140 000; guardias (6 sitios): 90 000; comunicaciones: 45 000; formación y ejercicios: 35 000; adaptación de los sitios: 40 000; seguros específicos y evacuación médica: 60 000; contingencias: 30 000. Total: 440 000 USD, es decir, el 5,5 % de los programas y unos 2 933 USD por empleado. Este porcentaje varía mucho según los contextos, a menudo entre el 2 y el 15 %.

Defender el presupuesto de seguridad

Los donantes suelen aceptar los costes de seguridad si están **justificados, son proporcionados y están vinculados al acceso**. Argumentos eficaces:

- vincular cada coste a un riesgo identificado en la evaluación de riesgos y a una actividad;
- mostrar lo que la seguridad permite: acceso a zonas concretas, continuidad de las actividades, protección de las personas asistidas;
- presentar los costes como costes directos del proyecto (prorrateados, según claves justificables) en lugar de diluirlos en los costes indirectos;
- mostrar los datos: incidentes evitados o mejor gestionados, días de actividad mantenidos.

Ejemplo de argumento cifrado. El año pasado, sin teléfonos satelitales, los equipos de dos bases suspendieron sus desplazamientos 45 días en total cada vez que se cortaba la red móvil. Equipar estas bases cuesta 12 000 USD; los 45 días de suspensión retrasaron actividades por valor de 300 000 USD. La inversión es pequeña en comparación con la continuidad que permite.

Consorcios, gestión a distancia y coordinación

En un consorcio, cada miembro sigue siendo responsable de su personal, pero el líder debe asegurarse de que todos evalúen y gestionen los riesgos: evaluación común, intercambio de información, procedimientos de alerta comunes, presupuesto de seguridad para cada miembro.

En la gestión a distancia, la seguridad de los equipos sobre el terreno (personal nacional, socios) pasa a ser prioritaria: análisis local por parte de quienes están expuestos, derecho a rechazar una actividad, comunicaciones, medios de reubicación y contactos regulares.

Coordinación interinstitucional:

- Los **foros de seguridad de las ONG** (plataformas nacionales de intercambio de información y análisis, a menudo financiadas por donantes): alertas, informes de incidentes, formaciones, análisis.
- El marco **«Saving Lives Together»**, que organiza la cooperación entre el sistema de gestión de la seguridad de las Naciones Unidas y las ONG asociadas.
- El **Global Interagency Security Forum** (GISF) a nivel internacional: guías, investigaciones, intercambios entre responsables de seguridad.

El intercambio de información exige normas: confidencialidad, anonimización, acuerdo previo para cualquier dato que no pertenezca a la organización.

Medir la madurez de la gestión de riesgos

Una organización puede evaluar su **madurez** en gestión de riesgos de seguridad en unas pocas dimensiones, calificadas de 1 (inexistente) a 4 (integrada y en mejora continua):

- política y gobernanza (umbral de riesgo, responsabilidades);
- evaluación de riesgos y planes actualizados;
- formación y competencias;
- incidentes y aprendizaje;
- gestión de crisis;
- deber de cuidado equitativo (personal nacional, socios);
- recursos y presupuesto.

Ejemplo. Calificaciones de una organización: 3, 2, 2, 1, 3, 1, 2. Media: 14 / 7 = 2. Las dos calificaciones de 1 (incidentes y aprendizaje; deber de cuidado equitativo) son las prioridades: afectan a la capacidad de aprender y a la equidad, sobre las que descansan las demás dimensiones. Una autoevaluación anual, debatida en la junta, permite seguir los progresos.

Ejercicio: un socio en primera línea

Situación. Su organización financia a una ONG local para actividades de protección de la infancia en una provincia a la que su personal ya no está autorizado a ir. El presupuesto del socio (600 000 USD) no prevé ningún coste de seguridad. El socio tiene 40 empleados sobre el terreno; dos de ellos estuvieron detenidos 3 días el mes pasado; no tiene ni seguro de accidentes ni teléfono satelital. El acuerdo establece que toda pérdida de bienes, incluso debida a un saqueo, la reembolsa el socio.

Trabajo solicitado. 1) Identifique los problemas. 2) Proponga un presupuesto de seguridad realista para el socio (comunicaciones 6 000; formación 8 000; seguro de accidentes del 3 % de una masa salarial de 240 000; reserva para contingencias 10 000; punto focal de seguridad a media jornada 9 000). 3) ¿Qué modificaciones del acuerdo?

Solución. 1) Transferencia de riesgo injusta: zona considerada demasiado peligrosa para su personal, sin evaluación conjunta; ningún coste de seguridad; detención sin apoyo previsto; riesgo fiduciario totalmente transferido, incluso en caso de fuerza mayor. 2) Comunicaciones 6 000 + formación 8 000 + seguro 7 200 + contingencias 10 000 + punto focal 9 000 = 40 200 USD, es decir, el 6,7 % del presupuesto; que se financiará adicionalmente o por reasignación, justificándolo ante el donante. 3) Evaluación conjunta de los riesgos y derecho del socio a suspender una actividad peligrosa; partida presupuestaria de seguridad; acceso a las formaciones, a los análisis y a la evacuación médica de su organización; cláusula de reparto del riesgo fiduciario (pérdidas debidas a saqueo aceptadas si se siguieron los procedimientos y se notificó el incidente); compromiso de asistencia en caso de detención o de incidente grave.

Para recordar

- Trabajar con socios no debe convertirse en una transferencia injusta del riesgo.
- Reparto del riesgo: evaluación conjunta, presupuesto de seguridad, acceso a formaciones y dispositivos, pérdidas compartidas.
- Presupuestar la seguridad como costes directos, vinculados a los riesgos y a las actividades, a menudo entre el 2 y el 15 % según el contexto.
- Defender la seguridad por el acceso y la continuidad que permite, con cifras.
- Foros de seguridad de las ONG, Saving Lives Together, GISF: coordinación con normas de confidencialidad.

Cuestionario

1. Presupuesto de seguridad de 360 000 USD para 6 000 000 USD de programas. Proporción:
   A. 3,6 %
   B. 0,6 %
   C. 16,7 %
   D. 6 %

2. Mismo presupuesto para 120 empleados. Coste por empleado:
   A. 300 USD
   B. 50 000 USD
   C. 3 000 USD
   D. 30 000 USD

3. Un socio reembolsa en solitario toda pérdida debida a un saqueo, aunque se hayan seguido los procedimientos. Esto es:
   A. Un reparto equitativo
   B. Una transferencia injusta del riesgo fiduciario
   C. Una buena práctica
   D. Una exigencia de todos los donantes

4. Calificaciones de madurez 2, 3, 1, 2, 2 en 5 dimensiones. Media:
   A. 2
   B. 2,5
   C. 1,8
   D. 10

5. En un consorcio, la seguridad del personal de cada miembro corresponde:
   A. Solo al líder
   B. A las autoridades locales
   C. Al donante
   D. A cada miembro, con un dispositivo coordinado por el líder

Respuestas del cuestionario : 1. D · 2. C · 3. B · 4. A · 5. D

Semana 12 : Gobernanza, cultura de seguridad, continuidad de las actividades y proyecto final

Objetivos

- Organizar la gobernanza de los riesgos: política, funciones de la junta y de la dirección, informes, auditorías.
- Desarrollar una cultura de seguridad en la que cada persona notifica, aprende y protege la aceptación.
- Construir un plan de continuidad de las actividades y realizar el proyecto final: un marco de gestión de riesgos para un país.

La política de seguridad y de gestión de riesgos

La **política**, adoptada por la junta, fija el marco que aplican todos los países y servicios:

- principios (deber de cuidado, aceptación, derecho de retirada, igualdad de trato, ningún pago a las partes en el conflicto);
- apetito de riesgo y umbrales por categoría;
- funciones y responsabilidades, desde la dirección hasta los puntos focales;
- requisitos mínimos: evaluación de riesgos, plan de seguridad, formación, notificación de incidentes, gestión de crisis;
- posición sobre las cuestiones sensibles (escoltas armadas, guardias armados, rescates, comunicación en caso de secuestro);
- seguimiento: informes, auditorías, revisiones.

Unas **normas mínimas** por nivel de riesgo hacen operativa la política. **Ejemplo:** en todo país clasificado como de riesgo alto, un asesor de seguridad dedicado, un plan revisado cada 6 meses, una formación avanzada para todo el personal expuesto, un ejercicio de crisis anual y comunicaciones satelitales en cada base.

La función de la junta y de la dirección

La **junta directiva** no gestiona la seguridad en el día a día, pero tiene la responsabilidad última sobre ella:

- adopta la política y el apetito de riesgo;
- recibe un informe periódico (al menos anual, trimestral para los riesgos principales);
- se le informa sin demora de los incidentes graves y de las crisis;
- verifica que los recursos sean suficientes y que se dé seguimiento a las auditorías.

La **dirección** rinde cuentas con un cuadro de mando sencillo: incidentes por categoría y gravedad, tasa por cada 100 empleados, países por encima del umbral, cumplimiento de las

normas mínimas (planes actualizados, formaciones, ejercicios), recomendaciones con retraso, madurez.

Ejemplo de lectura. 12 países; 10 tienen un plan de seguridad actualizado (83 %); 7 han realizado un ejercicio de crisis en el año (58 %); 3 países tienen riesgos residuales por encima del apetito. La junta pide para esos 3 países una decisión explícita: medidas adicionales, reducción de actividades o aceptación motivada y temporal del rebasamiento.

Auditar la seguridad

Las **auditorías de seguridad** (internas, entre pares o externas) verifican que el dispositivo existe y funciona:

- documentos: evaluación de riesgos, plan, procedimientos, listas de contactos, registro de incidentes;
- prácticas: controles de llamada efectivos, cuadernos de movimientos, registros de visitantes, pruebas de radio;
- conocimientos: entrevistas con el personal (¿conocen el plan, el nivel de seguridad, el procedimiento en caso de incidente?);
- equipos: estado de los vehículos, comunicaciones, botiquines, reservas de hibernación;
- equidad: medidas reales para el personal nacional y los socios.

Ejemplo de muestra. El auditor entrevista a 30 empleados: 27 conocen el nivel de seguridad actual (90 %), 18 saben qué hacer si un colega no responde a un control de llamada (60 %), 9 han participado en un ejercicio en el año (30 %). Los procedimientos escritos existen, pero su apropiación es baja: la formación y los ejercicios pasan a ser prioritarios.

La cultura de seguridad

Los procedimientos mejor redactados fracasan sin una **cultura de seguridad**: un conjunto de comportamientos compartidos en el que la seguridad se ve como un medio para hacer el trabajo, no como un obstáculo.

Sus señales:

- los incidentes y los cuasi incidentes se notifican, y los errores se debaten sin miedo;
- los responsables aplican las normas que imponen;
- cada persona puede decir «no» o «alto» sin que se burlen de ella ni la sancionen;
- el personal nacional participa en los análisis y en las decisiones;
- la seguridad se trata en las reuniones de programa, no solo entre especialistas;
- la calidad de los programas y el comportamiento personal se reconocen como medidas de seguridad.

> La cultura se ve en lo que ocurre cuando un responsable con prisa quiere saltarse una norma. Si nadie se atreve a decir nada, la cultura de seguridad es débil.

La continuidad de las actividades

El **plan de continuidad de las actividades** prepara a la organización para mantener sus funciones esenciales pese a una perturbación grave: pérdida de una oficina, corte prolongado de Internet, ciberataque, pandemia, evacuación, salida repentina de personas clave.

Etapas:

- **Identificar las funciones críticas**: pago de los salarios, de los proveedores y de las transferencias a los beneficiarios, abastecimiento de los centros de salud, comunicaciones con los equipos, informes a los donantes con vencimiento.
- **Fijar para cada una un plazo máximo de interrupción**: por ejemplo, 24 horas para las comunicaciones de emergencia, 7 días para la nómina, 30 días para los informes a los donantes.
- **Prever las soluciones alternativas**: oficina alternativa, acceso a distancia, copias de seguridad, delegaciones de firma, proveedores de reserva, existencias.
- **Designar suplentes** para las funciones clave y documentar los accesos esenciales (sin compartir contraseñas en claro).
- **Probar** el plan al menos una vez al año.

Ejemplo. El sistema de nómina está alojado en un servidor de la oficina de la capital. Plazo máximo tolerado: 7 días. Si la oficina queda inaccesible, la restauración a partir de la copia de seguridad externa tarda 3 días, lo que respeta el plazo, siempre que la copia sea reciente y esté probada: la última es de hace 5 semanas. Acción: copia de seguridad diaria automatizada, prueba trimestral de restauración.

Proyecto final: un marco de gestión de riesgos para un país

El proyecto final del Mini MBA Seguridad y gestión de riesgos consiste en redactar, para un país o una zona reales (solo con datos públicos, nunca con información confidencial de una organización) o ficticios pero realistas, un **marco de gestión de riesgos** de 6 a 10 páginas:

- **1. Análisis del contexto**: actores, dinámicas, escenarios, indicadores.
- **2. Evaluación de riesgos**: amenazas, vulnerabilidades por perfil, matriz, riesgos inherentes y residuales, comparación con el umbral.
- **3. Estrategia**: combinación de aceptación, protección y disuasión, y estrategia de acceso y de negociación.
- **4. Plan de seguridad resumido**: niveles, procedimientos clave, comunicaciones, planes de contingencia (evacuación médica, hibernación, reubicación, secuestro).
- **5. Personas**: deber de cuidado equitativo, salud, bienestar, salvaguarda interna, seguros.
- **6. Riesgos de la organización**: extracto del registro (fiduciario, cumplimiento, PSEA, digital, reputación).
- **7. Socios, presupuesto y gobernanza**: reparto del riesgo, presupuesto de seguridad, cuadro de mando, continuidad de las actividades.

Criterios de evaluación: calidad del análisis, coherencia entre riesgos y medidas, realismo y proporcionalidad, equidad entre personal y socios, respeto de los principios humanitarios,

claridad. El proyecto forma parte del examen del tercer mes.

Ejercicio: preparar el informe anual a la junta

Situación. Datos del año: 9 países; 210 incidentes para 1 400 empleados (año anterior: 168 para 1 200); incidentes graves: 21 (año anterior: 12); planes actualizados en 7 países; ejercicios de crisis en 4 países; 2 países con un riesgo residual por encima del apetito; 38 recomendaciones derivadas de incidentes, de ellas 22 aplicadas en plazo; plan de continuidad probado: ninguno. Los socios locales han notificado 35 incidentes, pero no están incluidos en las estadísticas oficiales.

Trabajo solicitado. 1) Calcule las tasas y los porcentajes clave. 2) ¿Qué debe retener la junta? 3) ¿Qué decisiones pedirle?

Solución. 1) Tasa de incidentes: 15 por cada 100 empleados frente a 14 el año pasado (+7 %). Tasa de incidentes graves: 1,5 frente a 1,0 por cada 100 empleados (+50 %). Planes actualizados: 7 / 9 = 78 %; ejercicios: 4 / 9 = 44 %; recomendaciones en plazo: 22 / 38 = 58 %. 2) La gravedad aumenta claramente más que la frecuencia; la preparación es insuficiente (planes, ejercicios, continuidad nunca probada); el aprendizaje es lento; dos países están fuera del apetito; los riesgos de los socios son invisibles en los informes. 3) Decisiones: para los 2 países fuera del apetito, elegir entre medidas adicionales, reducción de actividades o aceptación motivada y temporal; exigir planes actualizados y un ejercicio de crisis en todos los países en un plazo de 6 meses; probar el plan de continuidad en el año; integrar los incidentes de los socios en los informes y presupuestar su seguridad; hacer un seguimiento trimestral de las recomendaciones con retraso.

Para recordar

- Una política adoptada por la junta, desglosada en normas mínimas por nivel de riesgo.
- La junta tiene la responsabilidad última: apetito, informes, información inmediata sobre las crisis, recursos.
- Auditar los documentos, las prácticas, los conocimientos, los equipos y la equidad.
- Cultura de seguridad: notificar sin miedo, poder decir alto, ejemplaridad de los responsables.
- Continuidad de las actividades: funciones críticas, plazos máximos, soluciones alternativas, suplentes, pruebas periódicas.

Cuestionario

1. 9 países, 6 con un plan actualizado. Porcentaje:
   A. 67 %
   B. 60 %
   C. 75 %
   D. 54 %

2. Incidentes graves: 18 para 1 200 empleados. Tasa por cada 100 empleados:
   A. 18
   B. 15
   C. 0,15
   D. 1,5

3. En una auditoría, 12 de 40 empleados saben qué hacer si falta un control de llamada. Esto indica:
   A. Una buena apropiación
   B. Un problema de radio
   C. Una apropiación baja (30 %): formación y ejercicios prioritarios
   D. Nada en particular

4. En un plan de continuidad, el plazo máximo de interrupción sirve para:
   A. Calcular los salarios
   B. Dimensionar las soluciones alternativas de cada función crítica
   C. Evaluar al personal
   D. Fijar el presupuesto de comunicación

5. Una señal clara de una buena cultura de seguridad es:
   A. Cada persona puede decir «alto» sin ser sancionada
   B. Ningún incidente notificado
   C. Procedimientos muy largos
   D. Guardias armados

Respuestas del cuestionario : 1. A · 2. D · 3. C · 4. B · 5. A