ACADEMIA HUMANITARIA · HUMANITAIRES JOBS

Mini MBA humanitario: dirigir una organización humanitaria

Material del curso · Semana 10 : Gestión de riesgos de la organización y de la seguridad

Programa de dirección de exactamente 3 meses (12 semanas, 144 horas): liderazgo, estrategia, ciclo de proyecto, MEAL, finanzas y presupuestos de donantes, cumplimiento y fraude, movilización de recursos, cadena de suministro, RR. HH. y salvaguarda, riesgos y seguridad, negociación e incidencia, cambio y gobernanza. Ejercicios numéricos corregidos, tres exámenes mensuales exigentes con estudios de caso y un diploma verificable de la Academia Humanitaria.

https://humanitairejobs.org/es/academia/mini-mba-humanitaire/semaine-10/

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

Semana 10 : Gestión de riesgos de la organización y de la seguridad

Objetivos

- Implantar una gestión de riesgos a escala de la organización: registro, apetito de riesgo, riesgos residuales, reparto de riesgos con donantes y socios.
- Dirigir la gestión de riesgos de seguridad: análisis de contexto, amenazas, vulnerabilidades, estrategias de aceptación, protección y disuasión.
- Preparar y conducir la gestión de incidentes críticos: célula de crisis, comunicación, continuidad de las actividades.

La gestión de riesgos de la organización

La norma **ISO 31000** define el riesgo como el efecto de la incertidumbre sobre los objetivos. Una organización humanitaria afronta riesgos de varias naturalezas: **de seguridad**, **fiduciarios** (fraude, corrupción, desvío), **jurídicos y de cumplimiento** (sanciones, derecho laboral, protección de datos), **operativos** (acceso, ruptura de suministro), **reputacionales**, **éticos** (abusos, vulneración de los principios) y **financieros** (tipo de cambio, tesorería, dependencia de los donantes).

El **registro de riesgos** describe cada riesgo (causa, evento, consecuencia), su probabilidad y su impacto (a menudo en una escala de 1 a 5), las medidas existentes, el **riesgo residual**, el responsable y la fecha de revisión. El nivel de riesgo suele calcularse como probabilidad × impacto: un riesgo de probabilidad 4 e impacto 5 obtiene 20 sobre 25, por encima de un umbral de escalamiento fijado, por ejemplo, en 15.

El **apetito de riesgo**, aprobado por el consejo de administración, indica qué riesgos acepta la organización para cumplir su misión. Una ONG médica puede aceptar un riesgo de seguridad elevado para atender en zona de conflicto, pero no aceptar ningún riesgo de tolerancia hacia la explotación sexual. Sin un apetito de riesgo formalizado, cada decisión depende de la personalidad del director de turno.

> La **transferencia de riesgos** a los socios locales es una deriva denunciada por numerosos estudios: la ONG internacional se queda a resguardo mientras su socio soporta el peligro sin medios. El **reparto de riesgos** supone financiar la seguridad de los socios, compartir la información y decidir juntos qué es aceptable.

Análisis de riesgos de seguridad

La gestión de riesgos de seguridad sigue un ciclo: **análisis de contexto** (actores, dinámicas del conflicto, criminalidad, percepción de la organización), **identificación de amenazas** (secuestro, ataque armado, asalto en carretera, artefactos explosivos, violencia sexual,

detención arbitraria, disturbios civiles, desastres naturales, enfermedades), **análisis de vulnerabilidades** y capacidades, y luego evaluación del riesgo y elección de medidas.

Una fórmula pedagógica resume la lógica: **riesgo = amenaza × vulnerabilidad / capacidades**. Casi nunca se controla la amenaza; se actúa sobre la vulnerabilidad (exposición, perfil, rutinas previsibles) y sobre las capacidades (formación, comunicaciones, procedimientos, red).

El **umbral de riesgo aceptable** se decide sopesando el riesgo residual frente a la **criticidad del programa**: cuanto más salva vidas una actividad, más riesgo puede aceptarse, con medidas reforzadas. El marco de criticidad de programas del sistema de la ONU (Programme Criticality) y el enfoque del GISF (Global Interagency Security Forum) formalizan este razonamiento.

Las fuentes de información deben cruzarse: red de contactos locales, foros de seguridad de ONG y organizaciones de asesoría en seguridad, agencias de la ONU, medios locales, datos públicos sobre conflictos (por ejemplo el programa de datos sobre conflictos de Uppsala, UCDP). La información sensible recibida de socios o terceros no se difunde sin su acuerdo.

Estrategias: aceptación, protección, disuasión

El **triángulo de la seguridad** distingue tres estrategias complementarias:

- **Aceptación**: reducir o eliminar la amenaza obteniendo el consentimiento de los actores (comunidades, autoridades, grupos armados) gracias a la calidad, la imparcialidad percibida, la transparencia y el diálogo. Es la estrategia preferida de las ONG, pero se construye con el tiempo y puede derrumbarse rápido si un actor considera parcial a la organización.
- **Protección**: reducir la vulnerabilidad mediante medidas físicas y de procedimiento (muros, guardias, vehículos adecuados, procedimientos de desplazamiento, hibernación, reducción de la visibilidad).
- **Disuasión**: oponer una contraamenaza (escoltas armadas, retirada condicional, presión política). Las escoltas armadas son en principio un último recurso, enmarcado por las directrices del IASC sobre el uso de escoltas armadas, porque pueden comprometer la neutralidad percibida y crear nuevos riesgos.

El **plan de seguridad** de un país incluye: análisis de riesgos, niveles de seguridad e indicadores para pasar de un nivel a otro, procedimientos operativos estándar (desplazamientos, comunicaciones, gestión del efectivo, visitantes), planes de contingencia (hibernación, reubicación, evacuación) y organigrama de crisis. Debe ser conocido, comprendido y puesto a prueba mediante ejercicios; de lo contrario, no sirve para nada.

> Indicadores de activación: decida de antemano qué eventos hacen pasar de un nivel a otro (por ejemplo dos incidentes armados a menos de 20 km de la base en una semana). Sin indicadores, la decisión de reubicar llega a menudo demasiado tarde.

Gestión de incidentes críticos

Un **incidente crítico** (secuestro, fallecimiento, agresión grave, ataque a una oficina, desaparición) supera las capacidades normales de gestión. Lo gestiona un **equipo de gestión de crisis** en la sede o a nivel regional, distinto del equipo sobre el terreno, con roles definidos de antemano: responsable de la crisis, enlace con la familia, comunicación, seguridad, jurídico y seguros, recursos humanos, apoyo psicológico.

Principios para las primeras horas: **poner a salvo** a las personas aún expuestas, **verificar** los hechos, **activar** la célula de crisis, **llevar un diario** cronológico de todas las decisiones e informaciones, **controlar la comunicación** (ninguna declaración pública ni publicación en redes sociales por parte del personal, un único portavoz), **informar a la familia** antes que a cualquier otro público y **coordinar** con las autoridades y las demás organizaciones.

En caso de secuestro, las organizaciones se apoyan en especialistas y en sus seguros; las políticas varían sobre el pago de rescates, prohibido o fuertemente desaconsejado por varios Estados y contrario a los regímenes de sanciones en algunos casos. La política de la organización debe estar clara antes del incidente, no improvisarse durante él.

Después del incidente: apoyo psicológico para las personas afectadas y el equipo, revisión de lecciones aprendidas sin buscar chivos expiatorios, actualización del análisis de riesgos y, si procede, revisión de la presencia en la zona.

Continuidad de las actividades y reputación

La **continuidad de las actividades** prepara a la organización para mantener sus funciones esenciales pese a una perturbación: pérdida de una oficina, corte de las comunicaciones o de los bancos, epidemia, ciberataque, suspensión del registro. El plan identifica las **funciones críticas** (nómina, pagos a los beneficiarios, suministros vitales, comunicación con los donantes), su tiempo máximo de interrupción aceptable y las soluciones alternativas (copias de seguridad fuera del sitio, cuentas bancarias alternativas, delegaciones de firma, gestión a distancia).

La **gestión a distancia** (programas conducidos por equipos nacionales o socios cuando el personal directivo ya no puede acceder a la zona) exige una atención especial: transferencia real de los medios de seguridad, sistemas de seguimiento por terceros, llamadas de verificación a los beneficiarios y vigilancia para no transferir el riesgo sin transferir los medios.

El **riesgo reputacional** suele derivarse de los demás riesgos: un escándalo de abusos, un fraude ocultado o un incidente mal gestionado cuestan mucho más que sus pérdidas directas. La mejor protección es la transparencia: informar a los donantes y, cuando proceda, al público, de forma factual y rápida, mostrando las medidas adoptadas.

La **ciberseguridad** y la protección de datos son ahora riesgos importantes: autenticación de dos factores, copias de seguridad, actualizaciones, formación contra el phishing y cifrado de los datos sensibles de los beneficiarios.

Ejercicio: registro de riesgos y decisión de reubicación

Parte 1. Elabore un registro de cinco riesgos de su organización (al menos uno de seguridad, uno fiduciario, uno reputacional, uno de protección de datos y uno financiero): descripción causa-evento-consecuencia, probabilidad e impacto sobre 5, puntuación, medidas existentes, riesgo residual, responsable. Indique cuáles superan un umbral de escalamiento de 15.

Parte 2. Su base de Morongo está en el nivel de seguridad 3 de 4. En diez días: dos asaltos a vehículos de ONG en el eje principal, panfletos hostiles a las organizaciones extranjeras y el anuncio de una operación militar en los próximos 15 días. La base gestiona un programa nutricional que trata a 600 niños con desnutrición aguda grave. Analice la situación (amenazas, vulnerabilidades, criticidad) y proponga una decisión argumentada: mantenimiento con medidas, reducción de personal, gestión a distancia o reubicación. Precise los indicadores que activarían la etapa siguiente y cómo asegurar la continuidad de los tratamientos.

Elementos de solución. La criticidad es muy alta (tratamiento vital de niños), lo que justifica aceptar un riesgo más elevado, pero no exponerse sin medidas. Una respuesta sólida reduce la exposición (personal no esencial reubicado, desplazamientos limitados y no previsibles, visibilidad reducida), refuerza la aceptación (diálogo con los líderes sobre los panfletos), preposiciona tres meses de productos nutricionales, transfiere progresivamente la continuidad de los tratamientos a las estructuras de salud y a los agentes comunitarios, y fija indicadores claros de reubicación completa (combates a menos de una distancia determinada, amenaza directa contra la organización, imposibilidad de comunicarse).

Para recordar

- Registro de riesgos: causa, evento, consecuencia, probabilidad × impacto, riesgo residual, responsable, revisión.
- Apetito de riesgo aprobado por el consejo; compartir los riesgos con los socios, no transferirlos.
- Riesgo = amenaza × vulnerabilidad / capacidades; el umbral aceptable depende de la criticidad del programa.
- Aceptación, protección, disuasión; escoltas armadas como último recurso.
- Incidente crítico: célula de crisis, diario de decisiones, un único portavoz, la familia informada en primer lugar.

Cuestionario

1. Un riesgo de fraude tiene una probabilidad de 3 y un impacto de 4; un riesgo de secuestro, una probabilidad de 2 y un impacto de 5. Se escalan los riesgos cuya puntuación alcanza o supera 12. ¿Cuáles?
   A. Ninguno
   B. Solo el fraude (12); el secuestro está en 10
   C. Solo el secuestro
   D. Los dos

2. Organizar reuniones periódicas con los líderes comunitarios para explicar los criterios de focalización forma parte de la estrategia de:
   A. Disuasión
   B. Protección
   C. Aceptación
   D. Transferencia del riesgo

3. Tras un secuestro, a quien hay que informar primero, antes de cualquier comunicado público, es:
   A. A los periodistas
   B. A la familia de la persona secuestrada, por medio de la persona designada de la célula de crisis
   C. A los donantes
   D. A las redes sociales de la organización

4. ¿Por qué fijar de antemano indicadores para pasar de un nivel de seguridad a otro?
   A. Para satisfacer a los donantes
   B. Para que la decisión de reducir o reubicar no dependa del ánimo del momento y no se tome demasiado tarde
   C. Para evitar formar al personal
   D. Porque lo exige la ley

5. Una ONG internacional confía a un socio local las actividades de una zona que se ha vuelto demasiado peligrosa para su propio personal, sin presupuesto de seguridad adicional. Esto es:
   A. Una buena práctica de localización
   B. Una transferencia de riesgo, contraria al reparto equitativo de los riesgos
   C. Una estrategia de disuasión
   D. Una obligación de los donantes

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