ACADEMIA HUMANITÁRIA · HUMANITAIRES JOBS

Mini MBA humanitário: dirigir uma organização humanitária

Material do curso · Semana 10 : Gestão dos riscos da organização e da segurança

Programa de direção de exatamente 3 meses (12 semanas, 144 horas): liderança, estratégia, ciclo de projeto, MEAL, finanças e orçamentos de doadores, conformidade e fraude, mobilização de recursos, cadeia de abastecimento, RH e salvaguarda, riscos e segurança, negociação e advocacia, mudança e governação. Exercícios numéricos corrigidos, três exames mensais exigentes com estudos de caso e um diploma verificável da Academia Humanitária.

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

Documento gratuito da Academia Humanitária. Pode ser impresso e partilhado livremente para fins de formação, sem modificações.

Semana 10 : Gestão dos riscos da organização e da segurança

Objetivos

- Implementar uma gestão de riscos à escala da organização: registo, apetite pelo risco, riscos residuais, partilha de riscos com doadores e parceiros.
- Dirigir a gestão dos riscos de segurança: análise de contexto, ameaças, vulnerabilidades, estratégias de aceitação, proteção e dissuasão.
- Preparar e conduzir a gestão de incidentes críticos: célula de crise, comunicação, continuidade das atividades.

A gestão dos riscos da organização

A norma **ISO 31000** define o risco como o efeito da incerteza sobre os objetivos. Uma organização humanitária enfrenta riscos de várias naturezas: **de segurança**, **fiduciários** (fraude, corrupção, desvio), **jurídicos e de conformidade** (sanções, direito do trabalho, proteção de dados), **operacionais** (acesso, rutura de abastecimento), **reputacionais**, **éticos** (abusos, violação dos princípios) e **financeiros** (câmbio, tesouraria, dependência dos doadores).

O **registo de riscos** descreve cada risco (causa, evento, consequência), a sua probabilidade e o seu impacto (muitas vezes numa escala de 1 a 5), as medidas existentes, o **risco residual**, o responsável e a data de revisão. O nível de risco é muitas vezes calculado como probabilidade × impacto: um risco de probabilidade 4 e impacto 5 obtém 20 em 25, acima de um limiar de escalada fixado, por exemplo, em 15.

O **apetite pelo risco**, aprovado pelo conselho de administração, diz que riscos a organização aceita para cumprir a sua missão. Uma ONG médica pode aceitar um risco de segurança elevado para prestar cuidados em zona de conflito, mas não aceitar nenhum risco de tolerância em relação à exploração sexual. Sem um apetite pelo risco formalizado, cada decisão depende da personalidade do diretor em funções.

> A **transferência de riscos** para os parceiros locais é um desvio denunciado por numerosos estudos: a ONG internacional fica abrigada enquanto o seu parceiro suporta o perigo sem meios. A **partilha de riscos** pressupõe financiar a segurança dos parceiros, partilhar a informação e decidir em conjunto o que é aceitável.

Análise dos riscos de segurança

A gestão dos riscos de segurança segue um ciclo: **análise de contexto** (atores, dinâmicas do conflito, criminalidade, perceção da organização), **identificação das ameaças** (rapto, ataque armado, assalto na estrada, engenhos explosivos, violência sexual, detenção arbitrária,

distúrbios civis, catástrofes naturais, doenças), **análise das vulnerabilidades** e das capacidades, e depois avaliação do risco e escolha das medidas.

Uma fórmula pedagógica resume a lógica: **risco = ameaça × vulnerabilidade / capacidades**. Quase nunca se controla a ameaça; atua-se sobre a vulnerabilidade (exposição, perfil, rotinas previsíveis) e sobre as capacidades (formação, comunicações, procedimentos, rede).

O **limiar de risco aceitável** decide-se pesando o risco residual face à **criticidade do programa**: quanto mais uma atividade salva vidas, mais risco pode ser aceite, com medidas reforçadas. O quadro de criticidade dos programas do sistema da ONU (Programme Criticality) e a abordagem do GISF (Global Interagency Security Forum) formalizam este raciocínio.

As fontes de informação devem ser cruzadas: rede de contactos locais, fóruns de segurança de ONG e organizações de aconselhamento em segurança, agências da ONU, media locais, dados públicos sobre conflitos (por exemplo o programa de dados sobre conflitos de Uppsala, UCDP). As informações sensíveis recebidas de parceiros ou de terceiros não se divulgam sem o seu acordo.

Estratégias: aceitação, proteção, dissuasão

O **triângulo da segurança** distingue três estratégias complementares:

- **Aceitação**: reduzir ou eliminar a ameaça obtendo o consentimento dos atores (comunidades, autoridades, grupos armados) graças à qualidade, à imparcialidade percebida, à transparência e ao diálogo. É a estratégia preferida das ONG, mas constrói-se ao longo do tempo e pode ruir depressa se um ator considerar a organização parcial.
- **Proteção**: reduzir a vulnerabilidade através de medidas físicas e processuais (muros, guardas, viaturas adequadas, procedimentos de deslocação, hibernação, redução da visibilidade).
- **Dissuasão**: opor uma contra-ameaça (escoltas armadas, retirada condicional, pressão política). As escoltas armadas são em princípio um último recurso, enquadrado pelas diretrizes do IASC sobre o uso de escoltas armadas, porque podem comprometer a neutralidade percebida e criar novos riscos.

O **plano de segurança** de um país inclui: análise de riscos, níveis de segurança e indicadores de passagem de um nível a outro, procedimentos operacionais padrão (deslocações, comunicações, gestão de numerário, visitantes), planos de contingência (hibernação, relocalização, evacuação) e organigrama de crise. Deve ser conhecido, compreendido e testado através de exercícios; caso contrário, de nada serve.

> Indicadores de ativação: decida antecipadamente que eventos fazem passar de um nível a outro (por exemplo dois incidentes armados a menos de 20 km da base numa semana). Sem indicadores, a decisão de relocalizar chega muitas vezes tarde demais.

Gestão de incidentes críticos

Um **incidente crítico** (rapto, morte, agressão grave, ataque a um escritório, desaparecimento) ultrapassa as capacidades normais de gestão. É gerido por uma **equipa de gestão de crise** na sede ou a nível regional, distinta da equipa no terreno, com papéis definidos antecipadamente: responsável da crise, ligação com a família, comunicação, segurança, jurídico e seguros, recursos humanos, apoio psicológico.

Princípios para as primeiras horas: **pôr em segurança** as pessoas ainda expostas, **verificar** os factos, **ativar** a célula de crise, **manter um diário** cronológico de todas as decisões e informações, **controlar a comunicação** (nenhuma declaração pública nem publicação nas redes sociais por parte do pessoal, um único porta-voz), **informar a família** antes de qualquer outro público e **coordenar** com as autoridades e as outras organizações.

Em caso de rapto, as organizações apoiam-se em especialistas e nos seus seguros; as políticas variam quanto ao pagamento de resgates, proibido ou fortemente desencorajado por vários Estados e contrário aos regimes de sanções em alguns casos. A política da organização deve estar clara antes do incidente, e não ser improvisada durante.

Depois do incidente: apoio psicológico para as pessoas afetadas e para a equipa, retorno de experiência sem procura de bodes expiatórios, atualização da análise de riscos e, se for o caso, revisão da presença na zona.

Continuidade das atividades e reputação

A **continuidade das atividades** prepara a organização para manter as suas funções essenciais apesar de uma perturbação: perda de um escritório, corte das comunicações ou dos bancos, epidemia, ciberataque, suspensão do registo. O plano identifica as **funções críticas** (salários, pagamentos aos beneficiários, abastecimentos vitais, comunicação com os doadores), o seu tempo máximo de interrupção aceitável e as soluções de recurso (cópias de segurança fora do local, contas bancárias alternativas, delegações de assinatura, gestão remota).

A **gestão remota** (programas conduzidos por equipas nacionais ou parceiros quando o pessoal de direção já não pode aceder à zona) exige uma atenção especial: transferência real dos meios de segurança, sistemas de acompanhamento por terceiros, chamadas de verificação aos beneficiários e vigilância para não transferir o risco sem transferir os meios.

O **risco reputacional** decorre muitas vezes dos outros riscos: um escândalo de abusos, uma fraude dissimulada ou um incidente mal gerido custam muito mais do que as suas perdas diretas. A melhor proteção é a transparência: informar os doadores e, quando apropriado, o público, de forma factual e rápida, mostrando as medidas tomadas.

A **cibersegurança** e a proteção de dados são agora riscos importantes: autenticação de dois fatores, cópias de segurança, atualizações, formação contra o phishing e encriptação dos dados sensíveis dos beneficiários.

Exercício: registo de riscos e decisão de relocalização

Parte 1. Elabore um registo de cinco riscos da sua organização (pelo menos um de segurança, um fiduciário, um reputacional, um de proteção de dados e um financeiro): descrição causa-evento-consequência, probabilidade e impacto em 5, pontuação, medidas existentes, risco residual, responsável. Indique quais ultrapassam um limiar de escalada de 15.

Parte 2. A sua base de Morongo está no nível de segurança 3 em 4. Em dez dias: dois assaltos a viaturas de ONG no eixo principal, panfletos hostis às organizações estrangeiras e o anúncio de uma operação militar nos próximos 15 dias. A base gere um programa nutricional que trata 600 crianças com desnutrição aguda grave. Analise a situação (ameaças, vulnerabilidades, criticidade) e proponha uma decisão fundamentada: manutenção com medidas, redução de efetivos, gestão remota ou relocalização. Precise os indicadores que desencadeariam a etapa seguinte e a forma de assegurar a continuidade dos cuidados.

Elementos de correção. A criticidade é muito elevada (tratamento vital de crianças), o que justifica aceitar um risco mais elevado, mas não expor-se sem medidas. Uma resposta sólida reduz a exposição (pessoal não essencial relocalizado, deslocações limitadas e não previsíveis, visibilidade reduzida), reforça a aceitação (diálogo com os líderes sobre os panfletos), pré-posiciona três meses de produtos nutricionais, transfere progressivamente a continuidade dos cuidados para as estruturas de saúde e os agentes comunitários, e fixa indicadores claros de relocalização completa (combates a menos de uma distância determinada, ameaça direta contra a organização, impossibilidade de comunicar).

A reter

- Registo de riscos: causa, evento, consequência, probabilidade × impacto, risco residual, responsável, revisão.
- Apetite pelo risco aprovado pelo conselho; partilhar os riscos com os parceiros, não transferi-los.
- Risco = ameaça × vulnerabilidade / capacidades; o limiar aceitável depende da criticidade do programa.
- Aceitação, proteção, dissuasão; escoltas armadas como último recurso.
- Incidente crítico: célula de crise, diário das decisões, um único porta-voz, a família informada em primeiro lugar.

Quiz

1. Um risco de fraude tem probabilidade 3 e impacto 4; um risco de rapto tem probabilidade 2 e impacto 5. São escalados os riscos cuja pontuação atinge ou ultrapassa 12. Quais?
   A. Nenhum
   B. Apenas a fraude (12); o rapto está em 10
   C. Apenas o rapto
   D. Os dois

2. Organizar encontros regulares com os líderes comunitários para explicar os critérios de seleção faz parte da estratégia de:
   A. Dissuasão
   B. Proteção
   C. Aceitação
   D. Transferência do risco

3. Após um rapto, quem deve ser informado primeiro, antes de qualquer comunicado público, é:
   A. Os jornalistas
   B. A família da pessoa raptada, pela pessoa designada da célula de crise
   C. Os doadores
   D. As redes sociais da organização

4. Porque fixar antecipadamente indicadores de passagem de um nível de segurança a outro?
   A. Para satisfazer os doadores
   B. Para que a decisão de reduzir ou relocalizar não dependa do humor do momento e não seja tomada tarde demais
   C. Para evitar formar o pessoal
   D. Porque a lei o exige

5. Uma ONG internacional confia a um parceiro local as atividades de uma zona que se tornou demasiado perigosa para o seu próprio pessoal, sem orçamento de segurança adicional. Isto é:
   A. Uma boa prática de localização
   B. Uma transferência de risco, contrária à partilha equitativa dos riscos
   C. Uma estratégia de dissuasão
   D. Uma obrigação dos doadores

Respostas do quiz : 1. B · 2. C · 3. B · 4. B · 5. B