ACADEMIA HUMANITÁRIA · HUMANITAIRES JOBS

Mini MBA Segurança e gestão de riscos: proteger as equipas e manter o acesso

Manual completo

Programa de exatamente 3 meses (12 semanas, 144 horas) para gerir a segurança e os riscos de uma organização humanitária: dever de proteção, análise do contexto, avaliação dos riscos, planos e procedimentos, aceitação e negociação do acesso, incidentes, gestão de crise e rapto, saúde e bem-estar do pessoal, segurança digital e proteção de dados, riscos da organização e conformidade, partilha do risco com os parceiros, governação e continuidade de atividade. Exercícios numéricos corrigidos, três exames mensais com estudos de caso e um diploma verificável da Academia Humanitária.

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

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

-

Índice

1. Semana 1 : Dever de proteção e gestão dos riscos de segurança: o quadro
2. Semana 2 : Analisar o contexto: atores, dinâmicas e tendências da violência
3. Semana 3 : Avaliar os riscos: ameaças, vulnerabilidades, probabilidade e impacto
4. Semana 4 : Planos de segurança, procedimentos, deslocações e comunicações
5. Semana 5 : Construir a aceitação e negociar o acesso
6. Semana 6 : Incidentes: comunicar, analisar, aprender
7. Semana 7 : Gerir uma crise: célula de crise, hibernação, relocalização, evacuação, rapto
8. Semana 8 : Saúde, bem-estar psicossocial, salvaguarda interna e seguros
9. Semana 9 : Segurança digital e proteção da informação
10. Semana 10 : Gerir todos os riscos da organização: registo, apetite, conformidade e reputação
11. Semana 11 : Partilhar o risco com os parceiros e financiar a segurança
12. Semana 12 : Governação, cultura de segurança, continuidade de atividade e projeto final

Semana 1 : Dever de proteção e gestão dos riscos de segurança: o quadro

Objetivos

- Explicar o dever de proteção (duty of care) de uma organização humanitária e as suas consequências jurídicas, éticas e operacionais.
- Descrever o ciclo de gestão dos riscos de segurança e as três estratégias: aceitação, proteção, dissuasão.
- Situar a segurança ao serviço do acesso e dos programas: ficar e agir, em vez de fugir ou de se expor.

Porque é que a segurança é uma função de direção

Todos os anos, centenas de trabalhadores humanitários são mortos, feridos ou raptados; a grande maioria são **pessoal nacional**. As bases de dados públicas sobre a segurança dos humanitários mostram que a violência se concentra num pequeno número de contextos, mas que nenhuma organização que trabalhe em zona de crise está a salvo.

A segurança não é, antes de mais, uma questão de guardas e de muros. É uma **função de direção** que permite chegar às pessoas necessitadas mantendo os riscos para o pessoal a um nível aceitável. Uma organização que gere mal os seus riscos perde o acesso, as equipas, os financiamentos e, por vezes, a reputação.

> Objetivo da gestão dos riscos de segurança: permitir um acesso duradouro às populações, não eliminar todo o risco. A única forma de eliminar todo o risco é não fazer nada.

O dever de proteção

O **dever de proteção** (duty of care) é a obrigação, jurídica e moral, de uma organização tomar todas as medidas razoáveis para proteger o seu pessoal contra danos previsíveis. Estende-se, em graus diversos, aos consultores, aos voluntários, aos visitantes e aos parceiros.

Na prática, exige:

- **avaliar** os riscos antes de expor alguém;
- **informar** claramente o pessoal sobre os riscos (consentimento informado);
- **formar** e equipar;
- pôr em prática **medidas** proporcionadas (procedimentos, comunicações, seguros, apoio psicossocial);
- **responder** aos incidentes e aprender.

Decisões judiciais em vários países reconheceram a responsabilidade de organizações humanitárias que não tinham tomado medidas razoáveis perante um risco conhecido. O dever

de proteção não pode ser inteiramente delegado: uma organização continua responsável mesmo quando recorre a um prestador de serviços ou a um dispositivo comum.

Deve ser **equitativo**: historicamente, o pessoal nacional recebeu menos formação, equipamento e opções de evacuação do que o pessoal internacional para um risco igual ou superior. As boas práticas atuais exigem que esta desigualdade seja tratada de forma explícita.

O ciclo de gestão dos riscos de segurança

O quadro mais utilizado no setor (formalizado nomeadamente pela revisão de boas práticas n.º 8 da Humanitarian Practice Network e pelos guias do Global Interagency Security Forum, GISF) segue um ciclo:

- **1. Análise do contexto**: atores, dinâmicas, tendências da violência.
- **2. Avaliação dos riscos**: ameaças, vulnerabilidades, probabilidade, impacto.
- **3. Escolha das estratégias e das medidas**: aceitação, proteção, dissuasão.
- **4. Planos e procedimentos**: plano de segurança, procedimentos operacionais, planos de contingência.
- **5. Execução**: formação, equipamento, orçamento, responsabilidades.
- **6. Acompanhamento, incidentes e revisão**: comunicação, análise, atualização regular.

O ciclo funciona continuamente: qualquer evolução significativa do contexto (eleições, ofensiva militar, incidente grave) desencadeia uma revisão, sem esperar pela data prevista.

Aceitação, proteção, dissuasão

Três estratégias combinam-se, com uma dosagem própria de cada contexto:

- **Aceitação**: obter o consentimento das comunidades, das autoridades e das partes no conflito à presença e às atividades da organização, através da pertinência dos programas, do respeito pelos princípios, do diálogo e do comportamento do pessoal. É a estratégia de base dos humanitários.
- **Proteção**: reduzir a vulnerabilidade através de medidas e de equipamentos (procedimentos de deslocação, muros, guardas não armados, comunicações, veículos adaptados, abrigos). Protege, mas pode afastar a organização das comunidades («bunkerização»).
- **Dissuasão**: opor uma ameaça para dissuadir uma agressão (guardas armados, escoltas armadas, suspensão condicional das atividades). Está reservada a casos excecionais, porque pode comprometer a neutralidade e a aceitação.

Exemplo. Numa zona onde a organização é bem aceite mas onde a criminalidade urbana é forte, a combinação típica é: aceitação nas comunidades de intervenção, proteção reforçada das residências e das deslocações na cidade (nada de andar a pé à noite, veículos trancados), e suspensão das atividades como alavanca de dissuasão em caso de ataque direcionado.

O limiar de risco aceitável e o programa crítico

Qualquer exposição deve ser **justificada pelo valor do programa**. Quanto mais elevado for o risco, mais a atividade deve ser crítica para as pessoas (salvar vidas) e mais a organização deve ter realmente os meios para o gerir.

As ferramentas de **criticidade dos programas** (por exemplo, o quadro das Nações Unidas) classificam as atividades da mais crítica (atividade vital imediata, ou ordenada pelo Secretário-Geral) à menos crítica. Uma atividade pouco crítica não justifica um risco elevado; uma atividade vital pode justificar um risco elevado, mas não um risco inaceitável.

Exemplo de decisão. Uma formação em gestão de projeto de três dias, numa cidade onde o risco de rapto é considerado elevado, pode ser deslocalizada ou feita em linha. Uma campanha de vacinação contra uma epidemia na mesma cidade pode ser mantida com medidas reforçadas, porque o benefício vital justifica um risco residual mais elevado, dentro do limite fixado pela direção.

> O limiar de risco aceitável é fixado pela direção da organização, por escrito, e não pela equipa mais corajosa no terreno.

Os papéis e as responsabilidades

A segurança é assunto de todos, mas as responsabilidades devem ser claras:

- **Conselho de administração e direção-geral**: política de segurança, limiar de risco aceitável, recursos, supervisão dos incidentes graves.
- **Diretor de país**: responsável pela segurança no país; é um papel de direção que não se delega inteiramente no conselheiro de segurança.
- **Responsável ou conselheiro de segurança**: análise, aconselhamento, procedimentos, formação, acompanhamento dos incidentes.
- **Pontos focais de segurança** nas bases de terreno.
- **Cada membro do pessoal**: respeitar os procedimentos, comunicar, adotar um comportamento que proteja a aceitação, e dizer não a uma missão considerada demasiado perigosa.

O **direito de retirada**: qualquer pessoa pode recusar-se a ir a um local ou pode abandonar um local se considerar o risco demasiado elevado, sem sanção. Inversamente, a direção pode proibir uma deslocação mesmo que a pessoa seja voluntária.

Exercício: um diretor de país perante um pedido de missão

Situação. Um doador pede uma visita de acompanhamento a um projeto de educação num distrito onde três veículos de ONG foram assaltados no mês passado. O pessoal nacional da base pergunta porque é que os internacionais têm um colete de proteção e uma opção de evacuação por avião, ao passo que eles não têm nem seguro adequado nem formação. Um jovem coordenador internacional oferece-se para a visita «porque não tem medo».

Trabalho pedido. 1) O nível de risco é justificado pela criticidade da atividade? 2) Que problemas de dever de proteção identifica? 3) Que decisão e que medidas?

Correção. 1) Uma visita de acompanhamento a um projeto de educação não é uma atividade vital: não justifica um risco elevado. Procuram-se alternativas: acompanhamento à distância (chamadas, fotografias georreferenciadas, parceiro local), verificação por um terceiro mais bem aceite, adiamento, ou encontro num local mais seguro. 2) Desigualdade de tratamento entre pessoal nacional e internacional (seguro, formação, equipamento, opções de relocalização); decisão deixada ao voluntariado individual em vez de uma avaliação dos riscos e de uma decisão da direção. 3) Recusar a missão nestes moldes e explicar ao doador a solução de acompanhamento alternativa; lançar uma revisão das medidas para o pessoal nacional (formação, seguro, plano de relocalização para quem está exposto por causa do seu emprego); lembrar que o limiar de risco é fixado pela direção e não pelo voluntariado.

A reter

- A gestão dos riscos de segurança serve o acesso às populações; não visa o risco zero.
- Dever de proteção: avaliar, informar, formar, equipar, responder e aprender, de forma equitativa entre o pessoal.
- Ciclo: contexto, avaliação, estratégias, planos, execução, acompanhamento e revisão.
- Aceitação primeiro; proteção conforme as necessidades; dissuasão em último recurso.
- O risco aceitável depende da criticidade do programa e é fixado pela direção, por escrito.

Quiz

1. A estratégia de segurança de base das organizações humanitárias é:
   A. A dissuasão
   B. A aceitação
   C. A proteção
   D. O evitamento total

2. O dever de proteção aplica-se:
   A. A todo o pessoal e, em graus diversos, aos consultores, voluntários e visitantes
   B. Apenas ao pessoal internacional
   C. Apenas ao pessoal armado
   D. Unicamente em tempo de guerra

3. Quem fixa o limiar de risco aceitável?
   A. As autoridades locais
   B. O membro do pessoal mais experiente
   C. O doador
   D. A direção da organização, por escrito

4. Guardas armados à volta de um armazém fazem parte de:
   A. A aceitação
   B. A proteção não armada
   C. A dissuasão
   D. O evitamento

5. Um membro do pessoal recusa uma missão que considera demasiado perigosa. Ele:
   A. Deve ser sancionado
   B. Exerce o seu direito de retirada, sem sanção
   C. Deve demitir-se
   D. Deve encontrar um substituto

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

Semana 2 : Analisar o contexto: atores, dinâmicas e tendências da violência

Objetivos

- Conduzir uma análise de contexto estruturada (política, económica, social, de segurança) útil à decisão.
- Mapear os atores segundo a sua influência, os seus interesses e a sua atitude em relação à organização.
- Ler dados de incidentes (frequências, taxas, tendências) sem erros de interpretação, e produzir indicadores de alerta.

Porquê analisar o contexto

Todas as decisões de segurança assentam numa compreensão do contexto. Uma análise fraca produz dois erros simétricos: **subestimar** uma ameaça (e expor o pessoal) ou **sobrestimá-la** (e abandonar populações que poderiam ter sido ajudadas).

Uma boa análise responde a algumas perguntas: quem controla o território e as estradas? Quais são os interesses dos atores, e de que forma a ação humanitária os afeta? Que tipos de violência existem, contra quem, onde, quando e porquê? O que está a mudar?

Fontes: pessoal nacional (a primeira fonte, muitas vezes a mais fina), comunidades, autoridades, outras organizações, fóruns de coordenação da segurança das ONG, Nações Unidas (UNDSS), meios de comunicação locais, redes sociais (com prudência), bases de dados públicas de conflitos. Toda a informação é **cruzada** e classificada segundo a fiabilidade da fonte e a credibilidade da informação.

As grelhas de análise

Duas grelhas simples estruturam a análise:

- **PESTEL adaptado**: político, económico, social, tecnológico, ambiental, legal, a que se acrescenta a segurança (grupos armados, criminalidade, forças de segurança).
- **Análise histórica**: cronologia dos acontecimentos importantes dos últimos anos, para identificar os ciclos (épocas de combates, períodos eleitorais, colheitas, transumância).

A análise conduz a **cenários**: o mais provável, o mais perigoso e, eventualmente, um cenário de melhoria, cada um com **indicadores** observáveis que assinalam que nos estamos a aproximar dele.

Exemplo de indicadores. Cenário «retoma dos combates à volta da cidade»: deslocação de famílias para sul, encerramento dos mercados semanais, subida súbita do preço do combustível, partida dos comerciantes estrangeiros, movimentos de tropas assinalados, discursos hostis nas rádios locais. Três indicadores em seis observados desencadeiam uma reunião de crise e a revisão do nível de segurança.

Mapear os atores

O **mapeamento dos atores** identifica aqueles que podem influenciar a segurança e o acesso: autoridades nacionais e locais, forças armadas e de polícia, grupos armados não estatais, líderes tradicionais e religiosos, milícias, redes criminosas, comerciantes, meios de comunicação, comunidades de acolhimento e deslocadas, outras organizações.

Para cada um: **influência** (fraca a forte), **atitude** em relação à organização (hostil, neutra, favorável), **interesses** e **relação** atual.

Ator	Influência	Atitude	Ação
Chefe da principal milícia	Forte	Neutra, desconfiada	Diálogo regular através de um intermediário aceite; explicar os princípios e os critérios de seleção
Prefeito	Forte	Favorável	Informação regular, respeito pelos procedimentos administrativos
Jovens desempregados da cidade	Média	Hostil (recrutamentos considerados injustos)	Transparência dos recrutamentos, mecanismo de queixas, empregos à jorna equitativos

> Um ator hostil com forte influência é uma prioridade da análise e da estratégia de aceitação, não apenas uma ameaça a evitar.

Ler os dados de incidentes

Os dados de incidentes ajudam a objetivar a ameaça, desde que sejam lidos corretamente:

- **Frequência bruta**: número de incidentes por período.
- **Taxa**: incidentes relativamente à exposição (número de trabalhadores, de deslocações, de dias-pessoa). Sem denominador, um aumento pode simplesmente refletir um aumento da atividade.
- **Enviesamento de comunicação**: um aumento pode resultar de uma melhor comunicação, e não de um agravamento.
- **Tipologia**: um mesmo total pode esconder uma descida dos roubos e uma subida dos raptos, bem mais graves.

Exemplo. Ano 1: 24 incidentes para 300 trabalhadores. Ano 2: 36 incidentes para 600 trabalhadores. Taxa: 8 contra 6 incidentes por 100 trabalhadores por ano. Apesar de uma subida bruta de 50 %, a taxa desceu 25 %. Mas se os incidentes graves (violência contra as pessoas) passarem de 3 para 9, a sua taxa passa de 1 para 1,5 por 100 trabalhadores: a gravidade aumenta. A leitura combina taxa e gravidade.

Compreender a violência contra os humanitários

Os ataques contra os humanitários obedecem a várias lógicas, que é preciso distinguir porque exigem respostas diferentes:

- **Criminosa**: ganho financeiro (roubos, assaltos, raptos para resgate). As medidas de proteção e a discrição sobre os bens de valor são eficazes.
- **Política ou militar**: a organização é vista como aliada de um dos lados, ou a sua ação perturba uma estratégia. A aceitação, a neutralidade percebida e a comunicação são centrais.
- **Ligada ao próprio trabalho**: conflitos de seleção de beneficiários, recrutamentos contestados, despedimentos, queixas não tratadas. A qualidade e a prestação de contas dos programas são medidas de segurança.
- **Incidental**: estar no sítio errado à hora errada (fogo cruzado, bombardeamentos, minas). Análise das zonas e dos horários, procedimentos de movimento.

Muitos incidentes graves que afetam ONG estão ligados a **tensões internas ou de vizinhança** (pessoal despedido, fornecedor afastado, beneficiário excluído): a análise de segurança deve olhar também para a própria organização.

Produzir uma análise útil

Uma análise útil cabe em **duas páginas**, é atualizada regularmente (mensalmente em contexto instável, após qualquer acontecimento importante), e termina com implicações concretas:

- zonas e estradas acessíveis, sob condições, ou interditas;
- horários e modos de deslocação;
- atores a encontrar e mensagens-chave;
- indicadores a vigiar e limiares de revisão;
- consequências para os programas (calendário, modalidades, gestão à distância).

É partilhada com as pessoas que dela precisam, respeitando a **confidencialidade**: uma análise que nomeia atores armados ou informadores pode pôr pessoas em perigo se circular. Também não deve utilizar informações confidenciais provenientes de outras organizações sem o seu acordo explícito.

Exercício: uma cidade que muda

Situação. Uma ONG trabalha há 3 anos numa cidade de guarnição. Dados: ano 1, 18 incidentes para 150 trabalhadores (dos quais 2 contra as pessoas); ano 2, 27 incidentes para 300 trabalhadores (dos quais 6 contra as pessoas). Há um mês: um candidato local não recrutado ameaça publicamente a organização; dois mercados semanais estão fechados; as rendas descem porque famílias abastadas partem; uma rádio local acusa «as ONG» de ajudarem os rebeldes; o fórum de segurança das ONG assinala movimentos de tropas.

Trabalho pedido. 1) Calcule e interprete as taxas de incidentes. 2) Classifique os sinais por lógica de violência. 3) Proponha três implicações práticas.

Correção. 1) Taxa global: 12 e depois 9 incidentes por 100 trabalhadores (descida de 25 %). Taxa de incidentes contra as pessoas: 1,33 e depois 2 por 100 trabalhadores (subida de 50 %). A situação agrava-se em gravidade apesar da descida da taxa global. 2) Ameaça do candidato não recrutado: lógica ligada ao trabalho; acusações radiofónicas: lógica política (perceção de parcialidade); mercados fechados, partidas, movimentos de tropas: indicadores de um cenário de retoma dos combates (risco incidental e político). 3) Tratar a queixa de recrutamento (mecanismo formal, transparência, segurança do pessoal de RH); lançar uma iniciativa de aceitação (encontros com as autoridades e os líderes, programa de rádio sobre os princípios e os critérios de ajuda); rever o cenário e o nível de segurança, preparar a relocalização e a gestão à distância se os indicadores militares se confirmarem.

A reter

- Uma análise fraca subestima ou sobrestima; cruzar e classificar a fiabilidade e a credibilidade das fontes.
- Cenários com indicadores observáveis e limiares que desencadeiam uma revisão.
- Mapear a influência, a atitude e os interesses dos atores; dar prioridade aos atores hostis influentes.
- Sempre um denominador: taxas de incidentes por exposição, lidas em conjunto com a gravidade.
- Muitos incidentes graves têm uma origem ligada ao trabalho: a qualidade dos programas é uma medida de segurança.

Quiz

1. 30 incidentes para 500 trabalhadores. A taxa por 100 trabalhadores é:
   A. 30
   B. 16,7
   C. 6
   D. 0,6

2. Os incidentes passam de 20 para 30 enquanto o pessoal passa de 200 para 400. A taxa:
   A. Aumenta 50 %
   B. Desce 25 %
   C. Mantém-se estável
   D. Duplica

3. Um despedimento mal gerido seguido de ameaças corresponde sobretudo a uma violência:
   A. Ligada ao trabalho da organização
   B. Incidental
   C. Criminosa
   D. Militar

4. Uma análise de segurança que nomeia informadores deve:
   A. Ser publicada por transparência
   B. Ser partilhada com todos os parceiros
   C. Ser enviada aos meios de comunicação
   D. Circular de forma estritamente restrita para não os pôr em perigo

5. Um ator hostil e muito influente deve ser:
   A. Ignorado
   B. Denunciado à imprensa
   C. Uma prioridade da análise e da estratégia de aceitação
   D. Contornado sem nunca ser contactado

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

Semana 3 : Avaliar os riscos: ameaças, vulnerabilidades, probabilidade e impacto

Objetivos

- Identificar as ameaças e avaliar a vulnerabilidade da organização e de cada perfil de pessoal perante elas.
- Classificar os riscos numa matriz probabilidade × impacto, calcular o risco residual após as medidas e compará-lo com o limiar aceitável.
- Redigir uma avaliação dos riscos clara, datada, revisível, que conduza a decisões.

Ameaça, vulnerabilidade, risco

Três noções que não se devem confundir:

- **Ameaça**: aquilo que pode causar um dano (assalto a veículo, rapto, bombardeamento, engenho explosivo, motim, doença, acidente rodoviário).
- **Vulnerabilidade**: o grau de exposição da organização ou de uma pessoa a essa ameaça, consoante a sua localização, as suas deslocações, o seu perfil, os seus bens, os seus procedimentos, a sua aceitação.
- **Risco**: a combinação da probabilidade de uma ameaça se concretizar contra nós e do impacto se ela se concretizar.

Uma mesma ameaça não cria o mesmo risco para todos. **Exemplo:** a ameaça de rapto para resgate pesa mais sobre os perfis vistos como «rentáveis» (pessoal internacional de certas nacionalidades, quadros nacionais de alto nível, pessoas cuja família é vista como abastada). A vulnerabilidade depende também dos procedimentos: deslocações previsíveis, sempre às mesmas horas, aumentam a vulnerabilidade de todos.

A matriz probabilidade × impacto

O método mais difundido classifica cada risco em duas escalas de 1 a 5:

- **Probabilidade**: 1 muito improvável, 2 improvável, 3 possível, 4 provável, 5 muito provável (num período definido, por exemplo 12 meses).
- **Impacto**: 1 negligenciável, 2 menor (danos materiais limitados), 3 moderado (ferimentos ligeiros, interrupção curta), 4 grave (ferimentos graves, perda de bens importantes, suspensão), 5 crítico (morte, rapto, retirada do país).

Pontuação = probabilidade × impacto, de 1 a 25. Níveis habituais: 1 a 4 baixo, 5 a 9 médio, 10 a 16 elevado, 20 a 25 muito elevado (os limiares variam consoante as organizações e devem estar escritos).

Ameaça	Probabilidade	Impacto	Pontuação	Nível
Assalto a veículo no eixo norte	4	4	16	Elevado
Assalto ao escritório	3	2	6	Médio
Rapto de um trabalhador	2	5	10	Elevado
Acidente rodoviário grave	3	5	15	Elevado

Observação: o acidente rodoviário tem muitas vezes uma pontuação tão elevada como as ameaças ligadas à violência, e é mais fácil de reduzir.

Risco residual e limiar aceitável

O **risco inerente** é o risco antes das medidas; o **risco residual** é aquele que resta após as medidas previstas. A decisão toma-se com base no risco residual, comparado com o limiar aceitável fixado pela direção para a atividade em causa.

Exemplo. Assalto no eixo norte: inerente 4 × 4 = 16. Medidas: deslocações em dois veículos, horários variáveis, nada de dinheiro nem de bens de valor visíveis, comunicação com controlo de chamada de hora a hora, atualização diária do estado da estrada pelo fórum das ONG, regra de não resistência. Probabilidade estimada reduzida para 2 (a vulnerabilidade baixa), impacto reduzido para 3 (não resistência, assistência rápida). Residual: 2 × 3 = 6, nível médio.

Se o limiar aceitável para as atividades de distribuição for «médio», a atividade pode prosseguir com estas medidas. Se as medidas não permitirem descer abaixo do limiar, é preciso mudar a atividade (modalidade, local, parceiro) ou suspendê-la.

> Uma medida inscrita mas não aplicada não reduz nenhum risco. A avaliação deve dizer quem aplica o quê, e como se verifica.

Os limites da classificação

A matriz é útil, mas enganadora se for tomada por uma medida exata:

- As notas são **juízos**, não medições. Duas pessoas podem classificar de forma diferente; procura-se um consenso fundamentado, com o pessoal nacional.
- Os **acontecimentos raros e catastróficos** (ataque a um hotel, atentado contra uma base) têm uma probabilidade baixa mas um impacto extremo: uma pontuação de 1 × 5 = 5 classifica-os como «médios», quando exigem planos específicos.
- Os riscos **acumulados**: vários riscos médios combinados podem constituir uma situação inaceitável.
- Os riscos evoluem: uma avaliação não datada ou com oito meses em contexto instável já não tem valor.

Boa prática: manter uma atenção especial a qualquer ameaça de impacto 5, seja qual for a sua probabilidade, e prever para cada uma um plano de contingência (rapto, ataque armado,

evacuação médica).

Perfis e segurança inclusiva

As pessoas não estão expostas da mesma forma consoante o seu **perfil**: nacionalidade, origem étnica ou clã, religião, género, orientação sexual e identidade de género, deficiência, idade, aparência, língua. Um mesmo local pode ser seguro para um e perigoso para outro.

Uma abordagem **inclusiva** da segurança (desenvolvida nomeadamente pelo GISF) consiste em:

- ter em conta os perfis na avaliação dos riscos, sem obrigar ninguém a revelar informações pessoais;
- permitir a cada pessoa comunicar confidencialmente preocupações ligadas ao seu perfil;
- adaptar as medidas (alojamento, deslocações, afetações), sem excluir automaticamente pessoas de certos postos;
- formar os responsáveis nestas questões.

Exemplo. Um trabalhador nacional de um grupo étnico minoritário não pode passar certos postos de controlo sem risco. Em vez de o excluir do projeto, a equipa adapta os itinerários, afeta-o a zonas onde o seu perfil não está exposto, e prevê um alojamento seguro em caso de tensão.

Redigir a avaliação

Uma avaliação dos riscos de segurança útil contém:

- a **zona** e o **período** abrangidos, a data e os autores;
- um resumo do contexto (remissão para a análise);
- o quadro das ameaças com probabilidade, impacto, pontuação inerente;
- para cada risco elevado ou muito elevado: medidas, responsáveis, risco residual;
- a comparação com o limiar aceitável por tipo de atividade;
- as decisões e recomendações (prosseguimento, adaptação, suspensão);
- a data da próxima revisão e os fatores que desencadeiam uma revisão antecipada.

É **validada** pelo diretor de país (e pela sede acima de um certo nível de risco) e **explicada** ao pessoal em causa. Serve também de base ao orçamento de segurança e ao consentimento informado do pessoal.

Exercício: avaliar e decidir

Situação. Uma ONG quer abrir uma base numa cidade a 120 km da capital regional. Ameaças identificadas: assalto a veículo (probabilidade 4, impacto 4); ataque armado contra a base (probabilidade 2, impacto 5); rapto (probabilidade 2, impacto 5); acidente rodoviário (probabilidade 4, impacto 4); doença grave sem acesso a cuidados (probabilidade 3, impacto 4). Limiar aceitável fixado pela direção para atividades de saúde vitais: residual «elevado» no máximo (≤ 16), com plano de contingência para qualquer ameaça de impacto 5. Medidas propostas: comboios de dois veículos e controlo de chamada (assalto reduzido para 2 × 3), instruções rodoviárias e motoristas formados (acidente reduzido para 2 × 4), guardas não armados, muro e abrigo (ataque reduzido para 1 × 5), evacuação médica por um serviço aéreo contratado e kits (doença reduzida para 2 × 3). Nenhuma medida específica para o rapto.

Trabalho pedido. 1) Pontuações inerentes e residuais. 2) A abertura é aceitável? 3) O que falta?

Correção. 1) Inerentes: assalto 16, ataque 10, rapto 10, acidente 16, doença 12. Residuais: assalto 6, ataque 5, rapto 10 (inalterado), acidente 8, doença 6. 2) Todos os residuais são ≤ 16, portanto dentro do limiar, mas duas ameaças de impacto 5 (ataque, rapto) exigem um plano de contingência. 3) Faltam medidas e um plano para o rapto: análise dos perfis expostos, discrição das deslocações, variação dos horários, regras sobre os visitantes, preparação de uma célula de crise e de uma política de gestão dos raptos; e um plano de contingência em caso de ataque (abrigo, comunicações de emergência, procedimento de relocalização). A abertura pode ser decidida assim que estes planos estiverem em vigor, validados pela direção.

A reter

- Risco = probabilidade × impacto de uma ameaça, consoante a vulnerabilidade da organização e das pessoas.
- Decidir com base no risco residual, comparado com o limiar aceitável da atividade.
- Uma medida não aplicada não reduz nada: responsáveis e verificação obrigatórios.
- Qualquer ameaça de impacto 5 exige um plano de contingência, seja qual for a sua probabilidade.
- Segurança inclusiva: integrar os perfis sem excluir nem forçar a divulgação.

Quiz

1. Probabilidade 3, impacto 5. A pontuação é:
   A. 8
   B. 35
   C. 2
   D. 15

2. Após as medidas, um risco passa de 4 × 4 para 2 × 3. O risco residual é:
   A. 16
   B. 10
   C. 6
   D. 8

3. Uma ameaça de probabilidade 1 e impacto 5 (pontuação 5):
   A. Pode ser ignorada
   B. Exige um plano de contingência específico
   C. É automaticamente aceitável
   D. Deve ser classificada com 25

4. A decisão de prosseguir uma atividade toma-se com base:
   A. No risco residual comparado com o limiar aceitável
   B. No risco inerente
   C. Na opinião do doador
   D. No número de incidentes do ano passado

5. Numa abordagem de segurança inclusiva:
   A. Excluem-se automaticamente certos perfis
   B. Obriga-se cada pessoa a declarar a sua orientação sexual
   C. Ignoram-se os perfis
   D. Permitem-se comunicações confidenciais e adaptam-se as medidas

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

Semana 4 : Planos de segurança, procedimentos, deslocações e comunicações

Objetivos

- Redigir um plano de segurança de país ou de zona, com níveis de segurança e medidas associadas.
- Conceber procedimentos operacionais padrão realistas, em particular para as deslocações e os locais.
- Pôr em funcionamento um sistema de comunicações e de acompanhamento dos movimentos que funcione quando tudo o resto falha.

O plano de segurança

O **plano de segurança** traduz a avaliação dos riscos em regras e em responsabilidades. É curto, prático, conhecido de todos e revisto regularmente. Conteúdo tipo:

- resumo do contexto e das principais ameaças;
- estratégia (dosagem de aceitação, proteção, dissuasão);
- níveis de segurança e medidas associadas;
- procedimentos operacionais padrão (deslocações, locais, comunicações, visitantes, dinheiro em numerário, incidentes);
- planos de contingência (evacuação médica, hibernação, relocalização, evacuação, rapto, ataque);
- organograma de segurança e contactos de emergência;
- anexos: mapas, listas de pessoal, inventário dos equipamentos de comunicação.

Cada pessoa recém-chegada recebe um **briefing de segurança** à chegada e assina a declarar que leu o plano. Um plano de 80 páginas que ninguém leu não protege ninguém.

Os níveis de segurança

A maior parte das organizações utiliza 4 ou 5 **níveis de segurança** por zona, cada um associado a medidas automáticas, o que acelera as decisões em período de tensão:

Nível	Situação	Medidas tipo
1. Normal	Riscos baixos e estáveis	Procedimentos padrão
2. Vigilância	Tensões, incidentes isolados	Deslocações limitadas em horários, controlo de chamada reforçado, revisão dos planos
3. Restrição	Violência em alta, possíveis ameaças direcionadas	Apenas deslocações essenciais, mediante autorização; redução do pessoal não essencial; atividades adaptadas
4. Hibernação ou relocalização	Violência generalizada ou direcionada	Reagrupamento num local seguro, ou partida do pessoal mais exposto; atividades suspensas ou à distância
5. Evacuação e suspensão	Risco inaceitável	Saída da zona ou do país segundo o plano; manutenção do contacto com o pessoal que ficou

A passagem de um nível para outro é decidida pelo diretor de país, com base em **indicadores** definidos antecipadamente (ver semana 2), e comunicada imediatamente a todos.

Os procedimentos de deslocação

As deslocações são o momento em que o pessoal está mais exposto. Procedimento tipo:

- **Autorização** prévia segundo o nível de segurança, com base num plano de deslocação: itinerário, horários, passageiros, veículos, contactos.
- **Verificação da estrada** na própria manhã: fórum de segurança, autoridades, transportadores, pessoal local.
- **Veículo** verificado e equipado: combustível, pneu sobresselente, kit, comunicações.
- **Controlo de chamada** (check-in) a intervalos fixados e em cada ponto-chave; procedimento claro se faltar uma chamada.
- **Recolher obrigatório interno**: chegada antes de uma hora fixada, com margem.
- **Comportamento** nos postos de controlo e em caso de assalto (não resistir, não tirar fotografias, calma, cooperação).

Cálculo da partida. Trajeto de 180 km, velocidade média realista de 40 km/h: 4 h 30. Recolher obrigatório interno às 17 h, margem de uma hora: chegada prevista o mais tardar às 16 h. Partida o mais tardar às 11 h 30. Com um controlo de chamada de hora a hora e à chegada: 5 chamadas. Se faltar uma chamada, a base tenta um novo contacto durante 15 minutos e depois desencadeia o procedimento de veículo desaparecido.

Segurança dos locais

Escritórios, residências, armazéns e locais de distribuição são objeto de uma avaliação e de medidas adaptadas:

- **Escolha do local**: bairro, vizinhança (evitar a proximidade de alvos potenciais: edifícios militares, ministérios sensíveis), duas vias de acesso, distância das zonas com risco de

inundação.

- **Perímetro**: muro ou vedação, portão, iluminação, guardas não armados formados, controlo dos visitantes.
- **Edifício**: portas e janelas sólidas, sala segura ou abrigo consoante as ameaças (sala reforçada contra intrusões, abrigo contra tiro indireto).
- **Segurança contra incêndios e elétrica**: extintores, detetores, saídas de emergência.
- **Reservas**: água, alimentos, combustível, medicamentos para a hibernação (muitas vezes 7 a 14 dias).

Cálculo de reservas. 12 pessoas, hibernação de 10 dias: água a 4 litros por pessoa e por dia para beber e para um uso mínimo = 480 litros; com 20 % de margem, cerca de 580 litros. Alimentos: 12 × 10 = 120 rações diárias. Combustível para um gerador a 2 litros por hora, 8 horas por dia: 160 litros.

As comunicações

O sistema de comunicações deve funcionar **quando a rede móvel está cortada**, o que acontece muitas vezes no momento em que mais se precisa dela. Princípio de redundância: pelo menos dois meios independentes.

- **Telemóvel**: prático, mas frágil e suscetível de vigilância.
- **Rádio HF**: longa distância, independente das redes, mas exige operadores formados e licenças.
- **Rádio VHF**: curto alcance, ideal na cidade e em comboio, com repetidores.
- **Telefone satélite** e terminais satélite de dados: independentes, mas caros e por vezes regulamentados ou mal vistos pelas autoridades.
- **Balizas de localização** GPS com botão de alerta.

Regras: indicativos de chamada, linguagem clara mas sem informações sensíveis (nada de nomes, montantes de dinheiro ou itinerários detalhados na rádio), árvore de chamadas (cada responsável liga a um número definido de pessoas), testes regulares, carregadores e baterias de reserva. As comunicações são também uma questão de aceitação: utilizar um rádio ou um telefone satélite onde as autoridades o proíbem pode levantar suspeitas de espionagem.

Procedimentos que são realmente aplicados

Os procedimentos falham muitas vezes por razões simples: demasiado numerosos, mal conhecidos, impossíveis de aplicar, ou contornados por hábito. Boas práticas:

- Escrever **poucos** procedimentos, curtos, adaptados ao contexto real, com o pessoal que os vai aplicar.
- **Explicá-los** (o porquê) e não apenas impô-los.
- **Treiná-los**: simulações de veículo desaparecido, de hibernação, de evacuação médica, pelo menos duas vezes por ano.
- **Verificá-los**: controlos pontuais dos diários de bordo, dos controlos de chamada, dos registos de visitantes.

- Tratar o incumprimento como uma questão de **gestão**: um responsável que contorna os procedimentos dá o exemplo a toda a equipa.

> A complacência é um risco de pleno direito: após meses sem incidentes, os procedimentos afrouxam precisamente no momento em que o contexto pode mudar bruscamente.

Exercício: planear uma missão de terreno

Situação. Uma equipa de 4 pessoas tem de ir da base a um local a 210 km para uma distribuição. Velocidade média realista: 35 km/h. Recolher obrigatório interno: 17 h 30, com uma margem de uma hora. A distribuição dura 3 horas. O local não tem rede móvel nos últimos 80 quilómetros. O nível de segurança da zona é «vigilância». O motorista propõe partir às 9 h «como de costume».

Trabalho pedido. 1) A missão pode fazer-se em ida e volta no mesmo dia? 2) Se não, que organização? 3) Que meios de comunicação e que controlos de chamada?

Correção. 1) Trajeto: 210 / 35 = 6 horas. Ida e volta 12 horas + 3 horas de distribuição = 15 horas; chegada o mais tardar às 16 h 30: partida à 1 h 30 da manhã, impossível (sem circulação noturna). A missão não pode fazer-se no mesmo dia. 2) Pernoita no local ou numa cidade de etapa segura, num alojamento avaliado antecipadamente; ou dividir: dia 1 trajeto (partida às 9 h, chegada por volta das 15 h), dia 2 distribuição e regresso parcial, ou distribuição por um parceiro local com acompanhamento. Variar a hora de partida habitual, que torna os movimentos previsíveis. 3) Telemóvel onde existe rede, telefone satélite ou rádio HF para os 80 km sem rede, baliza de localização; controlo de chamada de hora a hora e em cada ponto-chave (partida, entrada na zona sem rede, chegada, início e fim da distribuição); procedimento de veículo desaparecido conhecido da base.

A reter

- Um plano de segurança curto, conhecido, assinado à chegada, revisto regularmente.
- Níveis de segurança com medidas automáticas e indicadores de passagem definidos antecipadamente.
- Deslocações: autorização, verificação da estrada, controlo de chamada, recolher obrigatório com margem, não resistência.
- Comunicações redundantes, testadas, sem informações sensíveis em claro.
- Poucos procedimentos, explicados, treinados, verificados; a complacência é um risco.

Quiz

1. Trajeto de 160 km a 40 km/h, chegada o mais tardar às 16 h. Partida o mais tardar:
   A. 12 h
   B. 10 h
   C. 14 h
   D. 11 h

2. 10 pessoas, 7 dias de hibernação, 4 litros de água por pessoa e por dia. Água mínima:
   A. 70 litros
   B. 400 litros
   C. 40 litros
   D. 280 litros

3. Porquê exigir dois meios de comunicação independentes?
   A. Para reduzir os custos
   B. Porque os doadores o exigem
   C. Porque a rede móvel falha muitas vezes no momento crítico
   D. Para comunicar com a imprensa

4. Na rádio, evita-se mencionar:
   A. Os indicativos de chamada
   B. Os nomes, montantes de dinheiro e itinerários detalhados
   C. A hora
   D. O nível de segurança

5. Após seis meses sem incidentes, a equipa afrouxa os controlos de chamada. Isto é:
   A. Complacência, um risco a corrigir pela gestão
   B. Normal e sem risco
   C. Uma boa adaptação
   D. Uma decisão do motorista

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

Semana 5 : Construir a aceitação e negociar o acesso

Objetivos

- Construir uma estratégia de aceitação assente nos princípios, na qualidade dos programas e no diálogo com todos os atores.
- Medir a aceitação com indicadores concretos em vez de a presumir.
- Preparar e conduzir uma negociação de acesso humanitário com um ator armado, fixando as suas linhas vermelhas.

A aceitação não é um dado adquirido

A **aceitação** é o consentimento, ativo ou passivo, dos atores que podem prejudicar a organização. Não se decreta: constrói-se e mantém-se, e pode perder-se num só dia.

Assenta em vários pilares:

- **Os princípios**: humanidade, neutralidade, imparcialidade, independência, compreendidos e vistos como reais.
- **A qualidade e a pertinência** dos programas: uma ajuda útil, justa e bem direcionada.
- **A prestação de contas**: as comunidades sabem o que podem esperar e podem queixar-se.
- **O comportamento** do pessoal: respeito, discrição, ausência de arrogância, nenhuma exploração nem abuso.
- **O diálogo** com todos os atores que têm influência, incluindo os grupos armados não estatais.
- **A coerência**: os mesmos critérios em todo o lado, o mesmo discurso para todos.

A aceitação é muitas vezes **local e pessoal**: depende de uma equipa, de um responsável respeitado. Não se transfere automaticamente de uma zona para outra nem de uma pessoa para outra.

O que destrói a aceitação

As perdas de aceitação vêm muitas vezes da própria organização:

- Seleção de beneficiários vista como injusta ou capturada por uma elite ou por um grupo.
- Recrutamentos vistos como favorecendo um clã ou excluindo a população local.
- Promessas não cumpridas, programas interrompidos sem explicação.
- Associação visível a uma parte no conflito (escoltas militares, logótipos de forças armadas, presença em reuniões militares mediatizadas).
- Comportamento pessoal: condução perigosa, consumo ostensivo de álcool num contexto conservador, relações consideradas inapropriadas.

- Comunicação pública imprudente: um comunicado da sede ou uma mensagem nas redes sociais lida localmente como uma tomada de posição.

> Um tweet da sede pode anular meses de trabalho de aceitação no terreno: a comunicação externa faz parte da gestão dos riscos.

Medir a aceitação

A aceitação é presumida com demasiada frequência («as pessoas gostam de nós»). É possível **medi-la** com indicadores:

- As comunidades e os líderes conhecem a organização, as suas atividades e os seus princípios? (inquéritos de perceção, entrevistas)
- A organização recebe **alertas** espontâneos («não passem por ali amanhã»)?
- Os seus pedidos de acesso são concedidos, e em que prazos?
- As queixas recebidas incidem sobre a qualidade da ajuda ou sobre a própria presença da organização?
- Os incidentes visam-na mais ou menos do que outras organizações comparáveis?

Exemplo. Inquérito de perceção junto de 300 pessoas em dois distritos: distrito A, 78 % conhecem a organização e 70 % consideram a ajuda «justa»; distrito B, 41 % conhecem-na e 35 % consideram a ajuda «justa». A aceitação é claramente mais fraca em B, onde a equipa no entanto se sentia «bem aceite». Ações: reuniões comunitárias, divulgação dos critérios de seleção, revisão das listas com os comités, recrutamento local mais equilibrado.

Negociar o acesso: preparação

A **negociação humanitária** visa obter o acesso às populações, a segurança das equipas e o respeito pelos princípios, num diálogo muitas vezes assimétrico. Os métodos estruturados (por exemplo, os do Centro de Competências em Negociação Humanitária, CCHN) insistem na preparação:

- **Análise do interlocutor**: interesses, motivações, normas, constrangimentos, rede, quem ele próprio tem de convencer.
- **Análise do seu próprio mandato**: o que se pode oferecer, o que não se pode.
- **Linhas vermelhas** fixadas e validadas antecipadamente pela hierarquia: nenhum pagamento, nenhum desvio da ajuda, nenhuma lista de beneficiários imposta, nenhuma escolta do grupo armado se comprometer a neutralidade.
- **Zona de negociação**: os pontos abertos a troca (calendário, modalidades, comunicação, escolha dos locais).
- **Equipa**: quem negoceia (pessoa aceite, língua, perfil), quem apoia, quem decide.
- **Plano B**: o que se faz em caso de fracasso? (melhor alternativa a um acordo negociado)

Negociar o acesso: condução e acompanhamento

Princípios de condução:

- Começar por estabelecer a **relação** e a confiança; ouvir antes de pedir.
- Falar das **necessidades das populações** que o interlocutor diz defender: muitos atores armados querem ser vistos como protetores da «sua» população.
- Explicar os princípios em termos concretos: imparcialidade = ajuda segundo as necessidades, para todos; neutralidade = não tomar partido, inclusive contra ele.
- Nunca prometer o que não se pode cumprir; nunca ceder numa linha vermelha sob pressão: pedir tempo e consultar a hierarquia.
- Guardar o **registo** do que foi acordado e informar os outros atores envolvidos se necessário, sem pôr ninguém em perigo.

Acompanhamento. Um acordo de acesso verifica-se na prática: as equipas passam realmente? Os compromissos são cumpridos de ambos os lados? Qualquer violação (taxação, desvio, ameaça) é objeto de uma análise e de uma resposta proporcionada: chamada de atenção, suspensão parcial, suspensão total, coordenação com as outras organizações para evitar que um grupo jogue as ONG umas contra as outras.

Coordenação e posições comuns

Negociar sozinho expõe a organização a exigências que não pode recusar sem risco, ou que outra organização aceitará. A **coordenação** reforça a posição de todos:

- **Regras operacionais comuns** (ground rules) entre organizações de uma zona: nenhum pagamento nos postos de controlo, nenhuma escolta armada salvo exceção, recusa coletiva das listas impostas.
- **Grupos de trabalho sobre o acesso** dinamizados pelo OCHA, que acompanham os constrangimentos de acesso e levam a cabo uma advocacia comum.
- **Fóruns de segurança das ONG** que partilham a informação e as análises.

Limites: a coordenação não deve fazer perder a **independência** de cada organização, nem associá-la a posições políticas. Algumas organizações, como o CICV, conduzem as suas próprias negociações confidenciais. A coordenação faz-se sobre princípios e práticas, não sobre um alinhamento cego.

Exercício: um posto de controlo que «cobra taxas»

Situação. Um grupo armado controla a estrada para 3 campos de deslocados (25 000 pessoas). Há duas semanas que exige 50 USD por camião de ajuda e pede que 10 % dos víveres sejam «entregues aos combatentes que protegem os campos». Duas ONG começaram a pagar «para não abandonar as pessoas». A sua organização distribui víveres e gere um centro de saúde. Um inquérito de perceção recente mostra que 74 % dos habitantes dos campos vos conhecem e consideram a vossa ajuda justa.

Trabalho pedido. 1) Quais são as suas linhas vermelhas? 2) Que alavancas e que interesses do grupo pode mobilizar? 3) Que plano se a negociação fracassar?

Correção. 1) Nenhum pagamento nem parte da ajuda a uma parte no conflito (violação dos princípios, das regras dos doadores e muitas vezes das leis antiterroristas); nenhuma distribuição sob controlo do grupo; lista de beneficiários estabelecida pela organização segundo as necessidades. 2) Alavancas: a forte aceitação nos campos (o grupo quer ser visto como protetor dos deslocados); a importância do centro de saúde, inclusive para as famílias dos combatentes (cuidados imparciais para todos); uma posição comum com as outras organizações através do grupo de trabalho sobre o acesso; a intervenção de líderes religiosos ou tradicionais respeitados pelo grupo. 3) Coordenar com o OCHA e as ONG para que os pagamentos cessem coletivamente; se o acesso continuar condicionado, suspender temporariamente os comboios de víveres explicando porquê às comunidades e ao grupo; considerar modalidades alternativas (transferências monetárias se os mercados o permitirem, compras locais nos campos); manter o centro de saúde se o seu acesso não depender dos comboios; documentar e informar os doadores.

A reter

- A aceitação constrói-se, mantém-se, mede-se, e pode perder-se num dia.
- Seleção de beneficiários, recrutamento, comportamento e comunicação pública: primeiras causas de perda de aceitação.
- Negociar: analisar o interlocutor, fixar as linhas vermelhas, conhecer a sua zona de troca e o seu plano B.
- Nenhum pagamento nem parte da ajuda a uma parte no conflito: linha vermelha comum.
- As regras comuns entre organizações reforçam cada uma delas, sem sacrificar a independência.

Quiz

1. Que sinal indica uma aceitação real?
   A. O pessoal sente-se bem
   B. A comunidade dá alertas espontâneos sobre os perigos
   C. O doador está satisfeito
   D. Os escritórios estão bem protegidos

2. Uma linha vermelha de negociação deve ser:
   A. Fixada e validada antecipadamente pela hierarquia
   B. Improvisada durante a reunião
   C. Negociável se o interlocutor insistir
   D. Secreta mesmo para a equipa

3. Um grupo armado exige 5 % da ajuda. A resposta conforme aos princípios:
   A. Aceitar para manter o acesso
   B. Pagar em numerário em vez de víveres
   C. Aceitar em segredo
   D. Recusar, procurar uma posição comum e outras alavancas, suspender se necessário

4. Porquê coordenar regras comuns entre organizações?
   A. Para partilhar os orçamentos
   B. Para suprimir a independência de cada uma
   C. Para evitar que um ator jogue as organizações umas contra as outras
   D. Para evitar falar com as comunidades

5. Num inquérito, 40 % dos habitantes conhecem a organização num distrito onde a equipa se julga bem aceite. Conclusão:
   A. O inquérito está errado
   B. A aceitação está provavelmente sobrestimada; reforçar a informação e o diálogo
   C. É preciso deixar o distrito
   D. Não há nada a fazer

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

Semana 6 : Incidentes: comunicar, analisar, aprender

Objetivos

- Pôr em funcionamento um sistema de comunicação dos incidentes e dos quase-incidentes que incentive a circulação da informação.
- Analisar um incidente com um método estruturado (cronologia, causas, fatores contributivos) sem cultura da culpa.
- Explorar os dados de incidentes para ajustar as medidas e prestar contas à direção e aos doadores.

Porquê comunicar

Um **incidente de segurança** é qualquer acontecimento que causou ou poderia ter causado um dano ao pessoal, aos bens, à reputação ou aos programas. O **quase-incidente** (near miss) é um acontecimento que poderia ter causado um dano mas não o causou: tiros ouvidos perto de um comboio, falso posto de controlo evitado por pouco, ameaça verbal.

Comunicar serve para:

- **prestar assistência** imediata às pessoas afetadas;
- **alertar** as outras equipas e organizações;
- **compreender** as tendências e adaptar as medidas;
- **prestar contas** à direção, ao conselho, aos doadores e às seguradoras;
- **provar** que a organização exerce o seu dever de proteção.

A pirâmide dos incidentes (observada em numerosos setores) mostra que, antes de um incidente grave, há geralmente muitos quase-incidentes e incidentes menores. Não os comunicar é privar-se dos alertas precoces.

O sistema de comunicação

Um sistema eficaz compreende três níveis:

- **Alerta imediato** (dentro de uma hora): chamada ou mensagem à pessoa designada, com as informações essenciais: quem, o quê, onde, quando, estado das pessoas, necessidade de ajuda.
- **Relatório de incidente** (em 24 a 48 horas): formulário padrão com cronologia, consequências, ações tomadas.
- **Análise** (em 1 a 2 semanas para os incidentes significativos): causas, lições, recomendações.

Para incentivar a comunicação:

- formulário simples, disponível offline e nas línguas do pessoal;

- **nenhuma sanção** pela comunicação de um erro de boa-fé (cultura «justa», que distingue o erro honesto da negligência grave ou da violação deliberada);
- canal **confidencial** para os incidentes sensíveis (violência sexual, assédio, incidentes que envolvam um colega);
- **retorno de informação**: as equipas veem o que muda graças às suas comunicações.

> Se uma equipa nunca comunica nada, quase nunca é porque não se passa nada. É um sinal de alerta sobre a cultura de segurança.

Classificar os incidentes

Uma **tipologia** comum torna os dados comparáveis: violência contra as pessoas (homicídio, ferimento, rapto, agressão sexual, detenção arbitrária), roubo e assalto, intrusão, ameaça, incidente ligado ao conflito (tiros, bombardeamentos, engenhos explosivos), acidente rodoviário, incidente de saúde, incidente de segurança digital, distúrbios civis.

Cada incidente recebe também um **nível de gravidade**, por exemplo de 1 (menor, sem feridos nem perda significativa) a 4 (crítico: morte, rapto, ferimento grave, retirada de uma zona).

Exemplo de quadro trimestral. 42 incidentes comunicados: 15 pequenos roubos, 9 ameaças, 6 acidentes rodoviários (dos quais 2 graves), 5 assaltos a veículos, 4 quase-incidentes ligados aos combates, 2 detenções arbitrárias de curta duração, 1 agressão física. Os incidentes de gravidade 3 e 4 são 8, ou seja, 19 %. Os 5 assaltos ocorreram todos no mesmo eixo, entre as 15 h e as 17 h: a tendência é explorável (mudança de horários, revisão das autorizações neste eixo).

Analisar um incidente

A análise de um incidente significativo procura compreender, não punir. Método em quatro tempos:

- **Cronologia** precisa, reconstituída a partir de várias fontes (pessoas envolvidas, testemunhas, comunicações, GPS).
- **Factos e consequências**: danos, reações, assistência prestada.
- **Causas e fatores contributivos**: contexto (ameaça), vulnerabilidades (procedimentos, comportamento, equipamento), decisões tomadas e as suas razões, o que funcionou bem.
- **Recomendações**: medidas concretas, responsáveis, prazos, e verificação da sua execução.

Perguntas úteis: a ameaça era conhecida? Os procedimentos eram adequados? Eram conhecidos e aplicados? Se não, porquê (impossíveis, desconhecidos, contornados)? A resposta ao incidente foi rápida e adequada? O que deveríamos ter previsto?

As pessoas afetadas devem ser **protegidas** durante a análise: apoio psicológico, respeito pelo seu ritmo, confidencialidade, e nada de interrogatórios repetidos que as traumatizem de novo.

Utilizar os dados

Os dados de incidentes alimentam:

- a **análise de contexto** e a avaliação dos riscos (frequências, locais, horários, autores, modos de atuação);
- as **decisões** sobre as medidas (o que funciona, o que não funciona);
- os **relatórios** à direção (painel de controlo trimestral) e ao conselho;
- a **partilha** com os fóruns de segurança e as bases de dados setoriais, de forma anonimizada e com o acordo da organização.

Indicadores úteis. Número de incidentes por 100 trabalhadores; proporção de incidentes graves; prazo médio de comunicação; proporção de recomendações executadas dentro dos prazos. **Exemplo:** 24 recomendações resultantes das análises do ano; 15 executadas dentro dos prazos, 5 com atraso, 4 não iniciadas. Taxa de execução dentro dos prazos: 62,5 %. As 4 não iniciadas são examinadas prioritariamente pela direção: uma recomendação não aplicada deixa o risco intacto.

Prestar contas e comunicar

Após um incidente grave, vários públicos aguardam informações, com necessidades diferentes:

- **Família** das pessoas afetadas: informação rápida, humana, por uma pessoa designada, antes de qualquer comunicação pública.
- **Pessoal**: informação factual, medidas tomadas, apoio disponível, para evitar os rumores.
- **Doadores**: segundo os contratos, notificação rápida dos incidentes graves e das suas consequências nos programas.
- **Seguradoras**: participação dentro dos prazos para os danos e as despesas médicas.
- **Outras organizações**: alerta através do fórum de segurança.
- **Meios de comunicação**: apenas através do porta-voz designado; no caso de um rapto, a comunicação pública pode pôr a vítima em perigo e é decidida pela célula de crise.

Uma comunicação desastrada pode agravar um incidente: publicar o nome de uma vítima antes de informar a família, acusar publicamente um ator armado, ou revelar informações que comprometam uma negociação.

Exercício: analisar um assalto

Situação. Um veículo da organização foi assaltado às 16 h 40 no eixo sul, a 25 km da base; o motorista e dois trabalhadores não ficaram feridos, mas o veículo, dois computadores e 4 000 USD de ajudas de custo em numerário foram levados. Factos: a autorização de movimento previa uma chegada antes das 16 h; a distribuição tinha sofrido atraso; o controlo de chamada das 16 h não foi feito (sem rede); o responsável da base só desencadeou o procedimento de veículo desaparecido às 17 h 30. No trimestre anterior, tinham sido comunicados 3 quase-incidentes no mesmo eixo ao fim da tarde, sem alteração dos procedimentos. As ajudas de custo em numerário eram transportadas «para simplificar».

Trabalho pedido. 1) Fatores contributivos. 2) O que funcionou bem. 3) Recomendações.

Correção. 1) Partida tardia sem reavaliação (procedimento de recolher obrigatório não aplicado perante o atraso); zona sem rede sem meio de comunicação alternativo; prazo de 90 minutos antes do desencadeamento do procedimento de veículo desaparecido; quase-incidentes anteriores não explorados; transporte de dinheiro em numerário visível e desnecessário. 2) Não resistência do pessoal, sem ferimentos; comunicação imediata após o incidente. 3) Regra clara: em caso de atraso, permanecer no local num sítio seguro avaliado antecipadamente em vez de circular ao fim da tarde neste eixo; telefone satélite ou baliza para as zonas sem rede; procedimento de veículo desaparecido desencadeado o mais tardar 15 minutos após uma chamada falhada; análise sistemática dos quase-incidentes; pagamento das ajudas de custo por dinheiro móvel ou transferência, e limite máximo para o transporte de numerário; apoio psicológico para os três trabalhadores; responsáveis e prazos para cada recomendação, com acompanhamento pelo diretor de país.

A reter

- Comunicar incidentes e quase-incidentes: a base da pirâmide previne o topo.
- Três níveis: alerta imediato, relatório em 48 horas, análise dos incidentes significativos.
- Cultura justa: nenhuma sanção pelo erro honesto comunicado; canais confidenciais.
- Analisar para compreender: cronologia, causas, fatores contributivos, recomendações acompanhadas.
- Após um incidente grave: a família primeiro, um porta-voz único, prudência absoluta em caso de rapto.

Quiz

1. Tiros ouvidos perto de um comboio, sem feridos nem danos, constituem:
   A. Nada a comunicar
   B. Um incidente grave
   C. Um quase-incidente a comunicar
   D. Um incidente de saúde

2. 48 incidentes, dos quais 12 de gravidade 3 ou 4. A proporção de incidentes graves é:
   A. 12 %
   B. 25 %
   C. 36 %
   D. 4 %

3. 30 recomendações, 21 executadas dentro dos prazos. Taxa:
   A. 70 %
   B. 30 %
   C. 21 %
   D. 63 %

4. Numa cultura justa, um trabalhador que comunica um erro honesto:
   A. É sancionado para dar o exemplo
   B. É transferido
   C. Tem de reembolsar os danos
   D. Não é sancionado, e o erro serve para aprender

5. Após o rapto de um trabalhador, quem decide sobre a comunicação pública?
   A. O serviço de comunicação da sede sozinho
   B. Cada colega nas redes sociais
   C. A célula de crise
   D. Os meios de comunicação locais

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

Semana 7 : Gerir uma crise: célula de crise, hibernação, relocalização, evacuação, rapto

Objetivos

- Organizar uma célula de crise e as suas primeiras horas: papéis, informações, decisões, diário.
- Planear e decidir uma hibernação, uma relocalização ou uma evacuação, incluindo para o pessoal nacional.
- Conhecer os princípios de gestão de um rapto ou de uma detenção e o papel de cada um.

O que é uma crise?

Uma **crise** é uma situação que ameaça gravemente as pessoas, a capacidade de funcionamento da organização ou a sua reputação, e que ultrapassa os procedimentos ordinários: rapto, morte violenta, ataque a uma base, evacuação de um país, catástrofe que atinge o pessoal, escândalo grave.

A gestão de crise apoia-se numa estrutura preparada antecipadamente:

- **Célula de gestão de crise** (na sede ou a nível regional): decide a estratégia, mobiliza os recursos, gere as relações com as famílias, as autoridades, os doadores e os meios de comunicação.
- **Equipa de gestão do incidente** (a nível do país): gere a situação no terreno e aplica as decisões.

Esta separação permite ao terreno concentrar-se na ação enquanto a célula gere o ambiente e as decisões estratégicas. Ambas devem ter mandatos escritos, membros designados e suplentes, e ter feito pelo menos um exercício de simulação.

As primeiras horas

As primeiras horas determinam muitas vezes o desfecho de uma crise. Lista de ações tipo:

- **Ativar** a célula segundo os critérios previstos; designar um responsável e um secretário que mantém o **diário de crise** (hora, informação, fonte, decisão, responsável).
- **Apurar os factos**: distinguir o que está confirmado, o que é provável, o que é rumor.
- **Proteger as pessoas**: pôr em segurança o resto do pessoal, assistência médica, reagrupamento.
- **Informar** as famílias (por uma pessoa designada), o pessoal, a direção; controlar a comunicação externa (nenhum comentário público sem decisão da célula).
- **Tomar as decisões** urgentes: nível de segurança, suspensão de atividades, movimentos.
- **Planear** as próximas horas e os turnos: uma crise pode durar semanas, o cansaço é um risco.

> O diário de crise não é uma formalidade: guarda a memória das decisões, protege juridicamente a organização e evita repetir as mesmas discussões a cada mudança de turno.

Hibernação, relocalização, evacuação

Três opções quando a situação se degrada, descritas no plano de segurança:

- **Hibernação**: ficar no local, reagrupados num sítio seguro, à espera de que o perigo imediato passe (combates na cidade, motins). Exige reservas (água, alimentos, combustível, medicamentos), comunicações e uma decisão sobre a duração máxima.
- **Relocalização**: deslocar uma parte do pessoal para uma zona mais segura do mesmo país (capital, outra região), em geral o pessoal mais exposto ou não essencial.
- **Evacuação**: fazer sair o pessoal do país. Para o pessoal internacional, é muitas vezes o regresso ao país de origem; para o pessoal nacional, uma evacuação para fora do país é jurídica e praticamente complexa, e raramente possível.

O **ponto de não retorno**: passado um certo momento (aeroporto fechado, estradas cortadas), a evacuação deixa de ser possível. É preciso, portanto, decidir **cedo**, com base nos indicadores, em vez de esperar pela certeza.

Cálculo de evacuação. 46 pessoas a relocalizar por avião de 12 lugares; 2 lugares reservados ao pessoal da companhia e ao material de comunicação: 10 lugares úteis por rotação. São necessárias 5 rotações. Se cada rotação demorar 3 horas e o aeródromo fechar ao cair da noite, só se podem fazer 3 rotações por dia: 2 dias no mínimo. A lista de prioridade (pessoas mais expostas, doentes, não essenciais) é estabelecida antecipadamente.

O pessoal nacional nas crises

O pessoal nacional é muitas vezes o mais exposto e o menos protegido durante as crises. As boas práticas:

- Discutir antecipadamente com cada trabalhador os seus riscos próprios (perfil, local de origem, família) e as opções realistas.
- Prever opções de **relocalização interna** para quem está ameaçado por causa do seu emprego.
- Garantir a **continuidade dos salários** em caso de suspensão (adiantamentos de salário antes de uma evacuação, meios de pagamento à distância).
- Manter o **contacto** e o apoio após a partida dos internacionais.
- Não transferir a responsabilidade pelos programas para o pessoal nacional ou para os parceiros sem recursos nem acordo, expondo assim quem fica.

Exemplo. Antes de uma evacuação, uma organização paga três meses de adiantamento de salário aos seus 60 trabalhadores nacionais, organiza uma árvore de chamadas diária e acorda com eles um protocolo simples: nenhuma atividade é mantida sem avaliação e acordo de cada um, e nenhum trabalhador guarda bens da organização que o poriam em perigo.

Rapto e detenção

O rapto é uma das crises mais graves e mais longas. Princípios geralmente aceites (a adaptar à política de cada organização e ao direito aplicável):

- **Prevenção**: análise dos perfis expostos, discrição, variação dos itinerários e dos horários, controlo das informações publicadas (incluindo as redes sociais do pessoal).
- **Preparação**: política escrita (incluindo a posição da organização sobre os resgates, que varia consoante as organizações e as leis), formulários de «prova de vida» confidenciais preenchidos antecipadamente pelo pessoal exposto (perguntas cuja resposta só a pessoa conhece), seguro especializado se for caso disso, consultores especializados identificados.
- **Gestão**: célula de crise dedicada, comunicação estritamente controlada, coordenação com a família e, consoante os casos, com as autoridades e os governos envolvidos, apoio de especialistas.
- **Depois**: apoio médico e psicológico de longa duração para a pessoa libertada e a sua família, bem como para os colegas.

A **detenção arbitrária** por autoridades ou grupos armados exige uma reação rápida: localizar a pessoa, contactos com as autoridades, apoio jurídico, visitas se possível, informação da família.

Treinar e tirar lições

Uma célula de crise que nunca treinou perde horas preciosas. Os **exercícios** vão da discussão em torno de um cenário (exercício de mesa de 2 a 3 horas) à simulação completa com injeções de informações em tempo real.

Um bom exercício testa: a ativação (quem liga a quem, em quanto tempo), a repartição dos papéis, a circulação da informação, a manutenção do diário, as decisões difíceis (por exemplo: informar ou não os meios de comunicação, evacuar ou hibernar), e os turnos.

Indicador simples. Prazo de ativação da célula: objetivo inferior a 2 horas. Durante um exercício, o alerta é dado às 22 h; o primeiro membro é contactado às 22 h 20, a célula completa reúne-se às 0 h 45: 2 h 45, acima do objetivo. Causa: a lista de contactos não estava atualizada e dois suplentes não estavam designados. Ação: atualização trimestral da lista, suplentes nomeados, teste de chamada mensal.

Após qualquer crise real, uma **revisão** (passadas pelo menos algumas semanas) examina o que funcionou e o que deve mudar, com a mesma cultura de aprendizagem que para os incidentes.

Exercício: a cidade está cercada

Situação. Os combates aproximam-se de uma cidade onde a organização tem 8 trabalhadores internacionais e 54 trabalhadores nacionais, dos quais 12 originários de outra região e ameaçados devido ao seu grupo étnico. O aeroporto ainda funciona; um avião de 14 lugares (12 lugares úteis) pode fazer 2 rotações por dia para a capital. Estão reunidos 4 dos 6 indicadores do cenário «cerco». A estrada para a capital está cortada. As reservas da residência principal permitem 5 dias de hibernação para 20 pessoas.

Trabalho pedido. 1) Hibernar, relocalizar ou evacuar, e para quem? 2) Quantos dias são necessários para relocalizar as pessoas prioritárias por avião? 3) Que medidas para o pessoal nacional que fica?

Correção. 1) Com 4 indicadores em 6 e uma estrada cortada, o ponto de não retorno aproxima-se: relocalizar já para a capital as pessoas mais expostas (os 12 trabalhadores ameaçados, com o seu acordo) e o pessoal internacional não essencial; manter uma pequena equipa essencial apenas se a hibernação for possível e segura. 2) Pessoas prioritárias: 12 trabalhadores ameaçados + 8 internacionais = 20 pessoas, ou seja, 2 rotações de 12 lugares, possíveis em 1 dia. Se se juntarem familiares a cargo dos trabalhadores ameaçados (por exemplo 16 pessoas), 36 pessoas = 3 rotações, ou seja, 2 dias. 3) Adiantamento de salário de vários meses, contacto diário por árvore de chamadas, nenhuma atividade mantida sem avaliação e acordo, retirada dos bens da organização que os possam expor, informação clara sobre as opções e apoio psicológico; plano de retoma logo que a situação o permita.

A reter

- Célula de crise (estratégia, ambiente) e equipa de terreno (ação): mandatos, suplentes, exercícios.
- Primeiras horas: ativar, apurar os factos, proteger, informar, decidir, planear; manter um diário.
- Hibernar, relocalizar, evacuar: decidir antes do ponto de não retorno, com base em indicadores.
- O pessoal nacional, muitas vezes o mais exposto, tem direito a opções e a um apoio reais.
- Rapto: prevenção, política escrita, provas de vida preparadas, comunicação controlada, especialistas.

Quiz

1. 30 pessoas a relocalizar, avião de 10 lugares úteis. Número de rotações:
   A. 2
   B. 30
   C. 4
   D. 3

2. Hibernação de 15 pessoas durante 8 dias a 4 litros de água por pessoa e por dia:
   A. 120 litros
   B. 32 litros
   C. 480 litros
   D. 600 litros

3. O diário de crise serve sobretudo para:
   A. Informar os meios de comunicação
   B. Guardar o registo das informações e das decisões, e facilitar os turnos
   C. Avaliar o pessoal
   D. Calcular os custos

4. Porquê preparar formulários de «prova de vida» antecipadamente?
   A. Para verificar, em caso de rapto, que a pessoa está viva através de perguntas cuja resposta só ela conhece
   B. Para o seguro de saúde
   C. Para os vistos
   D. Para os recursos humanos

5. Uma célula de crise reúne-se 3 h 10 após o alerta, para um objetivo de 2 horas. Ação prioritária:
   A. Suprimir o objetivo
   B. Não fazer nada, era um exercício
   C. Mudar de diretor
   D. Atualizar os contactos, designar suplentes e testar regularmente

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

Semana 8 : Saúde, bem-estar psicossocial, salvaguarda interna e seguros

Objetivos

- Organizar a proteção da saúde do pessoal: prevenção, cuidados, evacuação médica e primeiros socorros.
- Prevenir e tratar o stress, o esgotamento e o trauma, e medir o bem-estar das equipas.
- Tratar o assédio, a violência sexual contra o pessoal e as necessidades de seguro como riscos de pleno direito.

A saúde, primeiro risco

Em muitos contextos, as **doenças** (paludismo, infeções digestivas, doenças crónicas mal acompanhadas) e os **acidentes** causam mais baixas, repatriamentos e por vezes mortes do que a violência. A proteção da saúde faz, portanto, parte da gestão dos riscos.

Medidas essenciais:

- **Antes da partida ou da afetação**: consulta médica, vacinações, profilaxia antipalúdica adequada, briefing de saúde sobre o contexto.
- **No local**: mapeamento das estruturas de saúde (qualidade, distância, horários, línguas), contratos com clínicas, kits de primeiros socorros, pessoal formado em primeiros socorros (pelo menos uma pessoa por equipa ou por veículo em zona isolada).
- **Evacuação médica**: procedimento escrito, contrato com um prestador ou com uma seguradora, critérios de desencadeamento, prazos realistas.
- **Pessoal nacional**: cobertura de saúde equivalente na prática, incluindo para as famílias segundo a política da organização.

Prazo crítico. A «primeira hora» após um traumatismo grave é decisiva. Se o hospital cirúrgico mais próximo estiver a 6 horas de estrada e nenhuma evacuação aérea for possível antes do dia seguinte, o risco de acidente grave pesa muito mais na avaliação, e a formação em primeiros socorros avançados torna-se prioritária.

Stress, esgotamento e trauma

Os trabalhadores humanitários estão expostos a três tipos de stress:

- **Stress de base e cumulativo**: carga de trabalho, condições de vida, isolamento, conflitos de equipa, insegurança permanente. Não tratado, conduz ao **esgotamento** (burnout).
- **Stress traumático**: exposição a um acontecimento violento ou à morte.
- **Trauma vicariante**: à força de ouvir e de ver o sofrimento dos outros.

Vários inquéritos junto de trabalhadores humanitários evidenciaram taxas elevadas de sintomas de ansiedade, de depressão e de esgotamento, muitas vezes superiores às da população em geral, e mais elevadas ainda no pessoal nacional exposto às mesmas violências que a sua própria família.

Medidas: carga de trabalho razoável, férias e pausas de recuperação respeitadas (descanso e recuperação, R&R, consoante o contexto, por exemplo a cada 6 a 12 semanas em contexto difícil), acesso confidencial a apoio psicológico, formação dos responsáveis para identificar os sinais, primeiros socorros psicológicos após um incidente, cultura que não estigmatiza o pedido de ajuda.

> Um responsável que nunca tira férias envia uma mensagem a toda a sua equipa. O bem-estar é também uma questão de exemplo.

Medir o bem-estar

O bem-estar das equipas mede-se, como qualquer risco:

- **Taxa de utilização das férias** e dos R&R: dias gozados / dias devidos.
- **Horas extraordinárias** médias e número de pessoas acima de um limiar.
- **Baixas por doença** e rotação do pessoal (saídas antecipadas).
- **Inquéritos anónimos** curtos e regulares (escalas validadas de stress ou de esgotamento, perguntas sobre o apoio percebido).
- Recurso ao **apoio psicológico** (em número, nunca em nomes).

Exemplo. Equipa de 40 pessoas: 1 200 dias de férias devidos no ano, 690 gozados, ou seja, 57,5 %. 14 pessoas trabalham regularmente mais de 55 horas por semana. Rotação: 11 saídas no ano, ou seja, 27,5 %. Estes números assinalam um risco de esgotamento elevado: plano de ação (planeamento obrigatório das férias, reforços, redução das reuniões, acompanhamento pela direção).

Assédio e violência sexual contra o pessoal

O **assédio** (moral e sexual), a discriminação e a **violência sexual** contra o pessoal, incluindo por parte de colegas, são riscos subdeclarados. Dizem respeito ao mesmo tempo à segurança, aos recursos humanos e à salvaguarda (safeguarding) interna.

Um dispositivo mínimo compreende:

- um **código de conduta** claro e assinado, que proíbe também a exploração e os abusos sexuais contra as populações;
- **canais de comunicação** múltiplos e confidenciais (incluindo fora da hierarquia e externos);
- uma abordagem **centrada na sobrevivente ou no sobrevivente**: segurança, confidencialidade, respeito pelas suas escolhas, cuidados médicos rápidos (profilaxia pós-exposição ao VIH e contraceção de emergência dentro dos prazos), apoio psicológico;

- **investigações** conduzidas por pessoas formadas, independentes da cadeia hierárquica em causa;
- **sanções** efetivas e a partilha de informações entre organizações para evitar o recrutamento de pessoas sancionadas (dispositivos de verificação de referências interorganizacionais).

Os kits de profilaxia pós-exposição devem estar disponíveis e o pessoal designado formado na sua utilização, porque os prazos de eficácia são curtos (idealmente nas primeiras horas, e o mais tardar em 72 horas).

Os seguros

Os seguros transferem uma parte do risco financeiro. Coberturas habituais:

- **Saúde** (incluindo no estrangeiro) e **evacuação médica**;
- **Acidente, invalidez e morte**, incluindo os riscos de guerra e de terrorismo, muitas vezes excluídos dos contratos padrão;
- **Responsabilidade civil** da organização;
- **Bens**: veículos, equipamentos, stocks, dinheiro em numerário;
- **Rapto e resgate** (kidnap and ransom), que financia sobretudo os consultores especializados e cuja existência deve permanecer confidencial.

Pontos de atenção: exclusões (zonas, atividades, guerra), limites máximos, prazos de participação, cobertura equitativa do pessoal nacional, e coerência com o direito local (seguros obrigatórios).

Cálculo simples. Prémio de 4 % da massa salarial para uma cobertura de acidente e morte que inclui os riscos de guerra, sobre uma massa salarial de 2 400 000 USD: 96 000 USD por ano. Se a organização segurar apenas os 30 internacionais (massa salarial de 1 500 000 USD) e deixar 120 nacionais (900 000 USD) sem cobertura equivalente, a poupança de 36 000 USD cria uma desigualdade grave e um risco jurídico e reputacional.

Os primeiros socorros e a preparação médica

A preparação médica de terreno planeia-se como o resto:

- **Formação**: primeiros socorros básicos para todos, primeiros socorros avançados em zona isolada ou de conflito (controlo de hemorragias, garrote, posição lateral de segurança, queimaduras).
- **Equipamento**: kit individual (nas zonas de conflito, com garrote), kit de veículo, kit da base.
- **Fichas médicas confidenciais** do pessoal (grupo sanguíneo, alergias, tratamentos, contactos de emergência), acessíveis apenas em caso de emergência.
- **Plano de evacuação médica** por zona: estrutura de primeira linha, estrutura de referência, meios de transporte, prazos, números, custo.

Cálculo das necessidades de formação. 85 trabalhadores em zona isolada, objetivo: pelo menos 2 pessoas formadas em primeiros socorros avançados por equipa de 5 em deslocação. Se 17 equipas puderem estar no terreno ao mesmo tempo, são necessárias pelo menos 34 pessoas formadas; com 30 % de margem para as ausências e a rotação, cerca de 45 pessoas.

Exercício: uma equipa no limite

Situação. Uma base de 25 pessoas (5 internacionais, 20 nacionais) em zona de conflito. Em 6 meses: 3 saídas antecipadas de internacionais, 4 baixas por doença prolongadas entre os nacionais; 210 dias de férias gozados de 450 devidos; o chefe da base não gozou nenhumas férias; uma trabalhadora nacional contou a uma colega as investidas repetidas de um supervisor, mas não quer «criar problemas». O hospital cirúrgico mais próximo está a 5 horas de estrada; ninguém está formado em primeiros socorros avançados. O seguro de morte e invalidez cobre apenas os internacionais.

Trabalho pedido. 1) Calcule a taxa de utilização das férias. 2) Identifique os riscos. 3) Proponha medidas prioritárias.

Correção. 1) 210 / 450 = 46,7 %. 2) Esgotamento coletivo (poucas férias gozadas, saídas e baixas, exemplo do chefe da base); assédio sexual comunicado de forma informal, com risco de escalada e de silêncio; risco médico grave (5 horas do hospital, nenhum socorrista avançado); desigualdade de cobertura de seguro. 3) Planeamento obrigatório das férias e dos R&R, começando pelo chefe da base; apoio psicológico acessível e confidencial; informar a trabalhadora, sem a forçar, sobre os canais de comunicação confidenciais e as suas opções, garantir a sua segurança e a ausência de represálias, e fazer intervir a função de salvaguarda segundo a política (um alerta recebido por um responsável não pode ser ignorado); formar rapidamente pelo menos 2 pessoas por equipa em primeiros socorros avançados e rever o plano de evacuação médica; alargar o seguro ao pessoal nacional.

A reter

- Doenças e acidentes pesam muitas vezes mais do que a violência: prevenção, cuidados, evacuação médica planeados.
- Stress cumulativo, traumático e vicariante: férias, R&R, apoio confidencial, exemplo dos responsáveis.
- Medir o bem-estar: férias gozadas, horas, baixas, rotação, inquéritos anónimos.
- Assédio e violência sexual: canais confidenciais, abordagem centrada na sobrevivente ou no sobrevivente, PPE em 72 horas.
- Seguros adaptados aos riscos de guerra, e equitativos entre pessoal nacional e internacional.

Quiz

1. Uma equipa gozou 540 dias de férias de 900 devidos. Taxa de utilização:
   A. 60 %
   B. 40 %
   C. 54 %
   D. 90 %

2. A profilaxia pós-exposição ao VIH deve ser iniciada o mais tardar em:
   A. 7 dias
   B. 2 semanas
   C. 30 dias
   D. 72 horas

3. Massa salarial de 1 800 000 USD, prémio de 3 %. Custo anual:
   A. 5 400 USD
   B. 18 000 USD
   C. 54 000 USD
   D. 540 000 USD

4. O trauma vicariante é causado por:
   A. Um acidente rodoviário
   B. A exposição repetida ao sofrimento dos outros
   C. Um excesso de férias
   D. A diferença horária

5. Um responsável recebe um alerta informal de assédio sexual. Ele:
   A. Informa a vítima sobre as suas opções e os canais confidenciais e ativa o procedimento de salvaguarda
   B. Espera por uma queixa escrita
   C. Confronta publicamente o presumível autor
   D. Ignora se a vítima não quiser criar problemas

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

Semana 9 : Segurança digital e proteção da informação

Objetivos

- Identificar as ameaças digitais próprias das organizações humanitárias: phishing, fraude na transferência bancária, vigilância, fuga de dados.
- Pôr em prática medidas de base proporcionadas: autenticação, cópias de segurança, cifragem, gestão de acessos, dispositivos.
- Proteger os dados das pessoas assistidas e do pessoal, e reagir a um incidente digital.

Porque é que o digital é um risco de segurança

As organizações humanitárias detêm informações muito sensíveis: listas de beneficiários (por vezes com biometria e localização), testemunhos de violações, dados médicos, informações sobre o pessoal, análises de segurança, movimentos. Uma fuga ou um ataque informático pode pôr **vidas** em perigo, não apenas dados.

Vários ciberataques conhecidos visaram organizações humanitárias, incluindo o roubo de dados de centenas de milhares de pessoas vulneráveis. As organizações são também alvo de fraude financeira em linha e de **vigilância** das comunicações por atores estatais ou não estatais.

Principais ameaças:

- **Phishing** (mensagens fraudulentas): falsos e-mails ou mensagens que roubam credenciais ou instalam software malicioso.
- **Fraude na transferência bancária**: falso fornecedor, falso diretor a pedir um pagamento urgente, alteração fraudulenta de dados bancários.
- **Ransomware**: cifragem dos dados em troca de resgate.
- **Roubo ou apreensão de dispositivos** (computadores, telemóveis) nos postos de controlo ou durante assaltos.
- **Vigilância** das comunicações e das redes sociais.
- **Erros internos**: partilha por engano, ficheiro enviado ao destinatário errado, palavra-passe à vista.

As medidas de base

Algumas medidas simples bloqueiam a grande maioria dos ataques comuns:

- **Autenticação multifator** (MFA) no correio eletrónico, no armazenamento em linha, no banco e no software de contabilidade.
- **Gestor de palavras-passe** e palavras-passe longas e únicas.
- **Atualizações** automáticas dos sistemas e das aplicações.

- **Cópias de segurança** regulares, das quais uma cópia offline ou isolada, e testes de restauro (regra 3-2-1: três cópias, dois suportes diferentes, uma cópia fora do local).
- **Cifragem** dos discos dos computadores portáteis e dos telemóveis.
- **Gestão de acessos**: cada pessoa só acede ao que precisa; remoção dos acessos no dia da saída de um trabalhador.
- **Formação** regular, com exercícios de phishing simulados.

Exemplo de exercício. Um falso e-mail de phishing é enviado a 120 trabalhadores: 38 clicam na ligação (31,7 %), 14 introduzem as suas credenciais (11,7 %), 9 comunicam o e-mail ao serviço informático (7,5 %). Após uma formação direcionada, um segundo exercício dá 12 cliques (10 %), 3 introduções de credenciais (2,5 %) e 41 comunicações (34,2 %). O aumento das comunicações é tão importante como a descida dos cliques: transforma o pessoal num sistema de alerta.

Fraude na transferência bancária e procedimentos financeiros

A **fraude do CEO** e a fraude nos dados bancários custam todos os anos somas importantes às organizações, incluindo as humanitárias. Os procedimentos financeiros são a melhor defesa:

- Qualquer **alteração dos dados bancários** de um fornecedor ou de um trabalhador é verificada por uma chamada para um número já conhecido, nunca para o indicado no pedido.
- Nenhum pagamento urgente fora do procedimento, mesmo a pedido aparente de um diretor: a dupla validação continua obrigatória.
- Os acessos ao banco em linha utilizam dispositivos e contas dedicados, com dupla assinatura eletrónica.
- O pessoal sabe que será **apoiado** se recusar um pagamento suspeito, mesmo pedido por um superior.

> A urgência e a confidencialidade são as duas alavancas preferidas dos burlões: «Estou em reunião, faz já esta transferência e não digas nada a ninguém.»

Dispositivos, postos de controlo e vigilância

No terreno, os riscos digitais são também **físicos**:

- Nos postos de controlo, os telemóveis podem ser revistados. Um telemóvel que contenha fotografias de posições militares, mensagens críticas em relação a uma das partes ou listas de beneficiários pode levar a uma detenção. Regra: transportar apenas o necessário, apagar os dados sensíveis dos dispositivos de terreno, utilizar dispositivos dedicados ao trabalho.
- As **redes sociais** do pessoal revelam informações exploráveis: localização em tempo real, opiniões políticas, fotografias de colegas, sinais de riqueza. Uma política sobre a utilização das redes sociais, explicada e não punitiva, reduz estes riscos.

- As **aplicações de mensagens** cifradas de ponta a ponta protegem o conteúdo, mas não o facto de se estar a comunicar, nem o próprio telemóvel se for apreendido desbloqueado.
- A utilização de certas ferramentas (satélites, VPN, drones) pode ser proibida ou suspeita: verificar a legislação e a aceitação.

Proteger os dados das pessoas

A **proteção dos dados** dos beneficiários e do pessoal assenta em princípios reconhecidos (nomeadamente o manual do CICV e do Brussels Privacy Hub sobre a proteção de dados na ação humanitária):

- **Licitude e finalidade**: base legítima e finalidade precisa para cada recolha.
- **Minimização**: recolher apenas o que é necessário.
- **Consentimento informado** quando é essa a base escolhida, tendo em conta as relações de poder (um agregado familiar que precisa de ajuda não é livre de recusar).
- **Segurança**: cifragem, acessos limitados, registo de atividade.
- **Conservação limitada** e eliminação no fim da finalidade.
- **Partilha enquadrada** por acordos de partilha de dados, com uma análise dos riscos (incluindo pedidos de autoridades ou de partes no conflito).
- **Avaliação de impacto** antes de qualquer novo sistema (biometria, pagamento móvel, plataforma partilhada).

Exemplo de minimização. Para uma distribuição de kits, é preciso identificar o agregado familiar e verificar que ainda não recebeu o kit. A pertença étnica ou religiosa não é necessária e não deve ser recolhida; a fotografia e a impressão digital geralmente também não.

Reagir a um incidente digital

Um incidente digital (conta pirateada, computador roubado, ransomware, ficheiro enviado por engano) trata-se como um incidente de segurança:

- **Conter**: mudar as palavras-passe, revogar as sessões, isolar o dispositivo infetado, apagar remotamente um dispositivo roubado.
- **Avaliar**: que dados, que pessoas, que risco para elas?
- **Informar**: direção, encarregado da proteção de dados, pessoas em causa se estiverem expostas a um risco, autoridades de controlo segundo o direito aplicável, doadores segundo os contratos.
- **Restaurar** a partir das cópias de segurança; não pagar um resgate sem decisão da direção e análise jurídica.
- **Aprender**: análise, correções, formação.

Exemplo. Um computador portátil não cifrado com a lista de 3 200 agregados familiares, os seus números de telefone e a sua localização é roubado durante um assalto. O risco para as pessoas depende do contexto: se certos agregados pertencerem a um grupo visado, é elevado. Ações: avaliação imediata, informação das comunidades em causa por canais seguros se

estiverem expostas, alteração das modalidades de contacto, cifragem obrigatória de todos os computadores portáteis.

Exercício: um e-mail urgente do diretor

Situação. Numa sexta-feira às 17 h, a contabilista recebe um e-mail aparentemente do diretor de país, que está em deslocação: «Confidencial. Temos de pagar hoje o adiantamento de 48 000 USD ao novo fornecedor de combustível, senão perdemos o contrato. Dados bancários em anexo. Não estou contactável, reunião com o ministro.» O endereço de envio difere numa letra do endereço habitual. No mesmo dia, um fornecedor habitual pediu por e-mail para alterar os seus dados bancários. O correio eletrónico da organização não tem autenticação de dois fatores.

Trabalho pedido. 1) Sinais de alerta. 2) Conduta imediata. 3) Medidas duradouras.

Correção. 1) Urgência, confidencialidade, indisponibilidade do requerente, novo fornecedor sem processo de compra, endereço de envio ligeiramente diferente, pedido paralelo de alteração de dados bancários. 2) Não pagar; ligar ao diretor para o seu número conhecido (ou ao seu adjunto); não alterar os dados do fornecedor habitual sem chamada de verificação para um número já conhecido; comunicar ao responsável informático e às finanças; conservar os e-mails como provas. 3) Autenticação de dois fatores em todo o correio eletrónico; regra escrita: nenhum pagamento fora do procedimento, dupla validação, verificação telefónica de qualquer alteração bancária; formação e exercícios de phishing; filtragem dos domínios semelhantes; mensagem clara da direção: recusar um pagamento suspeito será sempre apoiado.

A reter

- Os dados humanitários são sensíveis: uma fuga pode pôr vidas em perigo.
- MFA, palavras-passe únicas, atualizações, cópias de segurança 3-2-1, cifragem, acessos mínimos, formação.
- Fraude na transferência: verificação por um número conhecido, dupla validação, apoio a quem recusa.
- Terreno: dispositivos aligeirados nos postos de controlo, política sobre as redes sociais.
- Proteção de dados: finalidade, minimização, segurança, conservação limitada, avaliação de impacto.

Quiz

1. 150 trabalhadores recebem um falso e-mail; 24 clicam. Taxa de cliques:
   A. 24 %
   B. 16 %
   C. 6,25 %
   D. 15 %

2. A regra de cópias de segurança 3-2-1 significa:
   A. 3 cópias, 2 suportes diferentes, 1 cópia fora do local
   B. 3 palavras-passe, 2 fatores, 1 conta
   C. 3 dias, 2 semanas, 1 mês
   D. 3 servidores, 2 países, 1 nuvem

3. Um fornecedor pede por e-mail para alterar os seus dados bancários. O que faz?
   A. Altera imediatamente
   B. Paga em numerário
   C. Responde ao e-mail
   D. Verifica por uma chamada para o número já conhecido

4. Para uma distribuição de kits, recolher a pertença étnica dos agregados familiares é:
   A. Obrigatório
   B. Recomendado
   C. Contrário ao princípio de minimização se não for necessário
   D. Sem risco

5. É roubado um computador não cifrado com listas de beneficiários. Primeiro passo:
   A. Comprar outro computador
   B. Avaliar os dados expostos e o risco para as pessoas, e depois informar
   C. Não dizer nada
   D. Publicar um comunicado

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

Semana 10 : Gerir todos os riscos da organização: registo, apetite, conformidade e reputação

Objetivos

- Construir e manter um registo dos riscos da organização (segurança, fiduciário, operacional, jurídico, reputacional, ético).
- Definir o apetite pelo risco e traduzi-lo em limiares e em decisões, incluindo através da perda esperada.
- Integrar a conformidade (sanções, antiterrorismo, fraude, proteção contra a exploração e o abuso sexual) numa abordagem única.

Dos riscos de segurança aos riscos da organização

A gestão dos riscos da organização (muitas vezes chamada ERM, enterprise risk management) alarga a lógica da segurança a todos os riscos que ameaçam a missão:

- **Segurança**: violência, acidentes, saúde do pessoal.
- **Fiduciários**: fraude, corrupção, desvio, má utilização dos fundos.
- **Operacionais**: rutura de abastecimento, falha de um parceiro, perda de acesso.
- **Jurídicos e de conformidade**: sanções, antiterrorismo, direito do trabalho, fiscalidade, proteção de dados.
- **Éticos e de salvaguarda**: exploração e abuso sexual, assédio, violação dos princípios.
- **Reputacionais**: perda de confiança das comunidades, dos doadores e do público.
- **Financeiros e estratégicos**: dependência de um doador, crise de tesouraria, perda de pertinência.

Estes riscos estão **ligados**: um desvio de ajuda por um grupo armado é ao mesmo tempo fiduciário, jurídico (sanções), operacional (suspensão), reputacional e de segurança (represálias se a organização o denunciar). É por isso que é necessária uma abordagem integrada.

O registo dos riscos

O **registo dos riscos** identifica os principais riscos, com, para cada um: descrição (causa, acontecimento, consequência), categoria, proprietário, probabilidade, impacto, pontuação inerente, medidas existentes, pontuação residual, medidas adicionais previstas, prazo.

Risco	Proprietário	Inerente	Residual	Ação
Desvio de ajuda alimentar por uma autoridade local na província X	Diretor de programas	4 × 5 = 20	3 × 4 = 12	Verificação por terceiros, chamadas aos beneficiários, distribuição direta
Fraude nas compras de combustível	Diretor financeiro	4 × 3 = 12	2 × 3 = 6	Cartões de combustível, reconciliações mensais
Perda do principal doador (55 % das receitas)	Diretor-geral	3 × 5 = 15	3 × 4 = 12	Plano de diversificação, reservas
Exploração sexual por um trabalhador ou um parceiro	Responsável de salvaguarda	3 × 5 = 15	2 × 5 = 10	Formação, verificação de referências, canais de queixa comunitários

O registo é revisto todos os trimestres pela direção e todos os anos pelo conselho ou pelo seu comité de auditoria e riscos. Os **dez principais riscos** são objeto de um acompanhamento especial.

O apetite pelo risco

O **apetite pelo risco** é o nível de risco que a organização aceita correr para cumprir a sua missão. É fixado pelo conselho, por categoria:

- **Segurança**: apetite moderado, elevado apenas para as atividades vitais (ver a criticidade dos programas).
- **Fiduciário**: apetite baixo pela fraude, mas aceitação de um risco residual nos contextos difíceis, desde que seja detetado e comunicado.
- **Exploração e abuso sexual**: tolerância zero para os comportamentos, o que não impede reconhecer que o risco existe e deve ser gerido ativamente.
- **Programático**: apetite mais elevado pela inovação e pelo acesso a zonas difíceis.

O apetite pelo risco não é um slogan: traduz-se em **limiares** (pontuação residual máxima por categoria), em **delegações** (quem pode aceitar que nível de risco) e em **decisões** documentadas. Um apetite demasiado baixo impede de trabalhar onde as necessidades são maiores; um apetite não definido deixa cada responsável decidir sozinho.

A perda esperada

Para certos riscos financeiros, pode completar-se a matriz com a **perda esperada**: probabilidade anual × custo em caso de concretização. Isto ajuda a comparar o custo de uma medida com a perda que ela evita.

Exemplo. Risco de roubo da caixa de um escritório de terreno: probabilidade anual estimada em 20 %, perda média de 15 000 USD (numerário e despesas). Perda esperada: 0,2 × 15 000 = 3 000 USD por ano. Passar para pagamentos por dinheiro móvel custa 1 800 USD por ano e reduz a probabilidade para 5 % e a perda média para 4 000 USD: perda esperada de 200 USD.

Ganho líquido: 3 000 − 200 − 1 800 = 1 000 USD por ano, sem contar a redução do risco para a segurança do caixa.

Limites: a perda esperada não serve para os riscos que afetam vidas ou cujo impacto é catastrófico. Ninguém decide aceitar um rapto porque a sua «perda esperada» seria baixa. Para estes riscos, raciocina-se em termos de limiar aceitável e de planos de contingência.

Conformidade: sanções, antiterrorismo, fraude

As obrigações de conformidade impõem-se através das leis nacionais, dos regimes de sanções e dos contratos dos doadores:

- **Sanções e antiterrorismo**: proibição de pôr fundos ou recursos à disposição de pessoas ou entidades inscritas nas listas. Medidas: verificação dos fornecedores, parceiros e trabalhadores segundo o risco; cláusulas contratuais; vigilância sobre os pagamentos nas zonas controladas por grupos listados; utilização das isenções humanitárias existentes, documentando a sua aplicação.
- **Antifraude e anticorrupção**: política, linha de denúncia, investigações, comunicação aos doadores dentro dos prazos (ver as finanças).
- **Verificação do beneficiário final**: em geral, os doadores não exigem que cada beneficiário da ajuda seja verificado contra as listas, e os princípios humanitários opõem-se a isso; os controlos incidem sobre os parceiros, os fornecedores e o pessoal.

O diálogo com os doadores e os bancos é essencial: a **retirada dos bancos** (de-risking), que se recusam a trabalhar com organizações que atuam em zonas sancionadas, pode bloquear operações inteiras. Documentar a sua diligência ajuda a manter as contas abertas.

Proteção contra a exploração e o abuso sexual

A **proteção contra a exploração e o abuso sexual** (PSEA) das populações assistidas é uma obrigação fundamental. Os seis princípios fundamentais do Comité Permanente Interagências (IASC) proíbem nomeadamente qualquer relação sexual com crianças (menos de 18 anos), qualquer troca de dinheiro, emprego, bens ou serviços por favores sexuais, e impõem a comunicação de qualquer preocupação.

O dispositivo:

- código de conduta e formação de todo o pessoal e dos parceiros;
- verificação de referências no recrutamento (dispositivos interagências);
- **mecanismos de queixa comunitários** acessíveis, seguros, adaptados às mulheres e às crianças;
- assistência às vítimas (médica, psicossocial, jurídica) segundo as suas escolhas;
- investigações rápidas e independentes, sanções, comunicação aos doadores;
- cláusulas PSEA nos acordos com os parceiros.

Indicador enganador: **zero queixas** não significa zero abusos. Na maior parte dos contextos, a ausência de queixas indica antes que os mecanismos não são conhecidos nem considerados seguros pelas comunidades.

Exercício: o comité de riscos do conselho

Situação. Apresenta ao comité de riscos de uma ONG os seguintes elementos. Fraude no combustível: probabilidade anual de 30 %, perda média de 25 000 USD; medida proposta (cartões de combustível e reconciliações) com um custo de 4 000 USD por ano, que reduziria a probabilidade para 10 % e a perda para 10 000 USD. Desvio de ajuda numa província: inerente 4 × 5, residual 3 × 4; limiar de apetite fiduciário do conselho: residual ≤ 9. Mecanismo de queixa PSEA: nenhuma queixa em 2 anos em 5 províncias; um inquérito de conhecimento mostra que 18 % das mulheres inquiridas conhecem o mecanismo. Um parceiro local nunca foi verificado contra as listas de sanções.

Trabalho pedido. 1) A medida para o combustível justifica-se? 2) O risco de desvio está dentro do apetite? O que fazer? 3) Que concluir sobre a PSEA? 4) E o parceiro?

Correção. 1) Perda esperada atual: 0,3 × 25 000 = 7 500 USD; após a medida: 0,1 × 10 000 = 1 000 USD; ganho líquido: 7 500 − 1 000 − 4 000 = 2 500 USD por ano: justifica-se. 2) Residual 12 > 9: fora do apetite. Opções: medidas adicionais (verificação por terceiros, distribuição direta, transferências monetárias), redução do volume na província, ou aceitação explícita e documentada pelo conselho de uma ultrapassagem temporária com plano. 3) Zero queixas com 18 % de conhecimento indica um mecanismo ineficaz, não uma ausência de abusos: campanha de informação, canais adaptados às mulheres, pontos focais femininos, verificação da confiança das comunidades. 4) Verificação imediata contra as listas de sanções, e integração sistemática desta verificação no procedimento de seleção dos parceiros.

A reter

- Os riscos da organização estão ligados: segurança, fiduciário, operacional, jurídico, ético, reputacional, financeiro.
- Registo dos riscos com proprietários, pontuações inerentes e residuais, ações e prazos, revisto pela direção e pelo conselho.
- Apetite pelo risco fixado pelo conselho, por categoria, traduzido em limiares e em delegações.
- Perda esperada = probabilidade × custo: útil para os riscos financeiros, não para as vidas.
- PSEA: zero queixas não é zero abusos; sanções: verificar parceiros, fornecedores e pessoal.

Quiz

1. Probabilidade anual de 25 %, perda de 12 000 USD. Perda esperada:
   A. 12 000 USD
   B. 4 800 USD
   C. 3 000 USD
   D. 300 USD

2. Uma medida custa 2 000 USD por ano e reduz a perda esperada de 5 000 para 1 500 USD. Ganho líquido anual:
   A. 3 500 USD
   B. 1 500 USD
   C. 5 000 USD
   D. −500 USD

3. Quem fixa o apetite pelo risco da organização?
   A. O conselho de administração
   B. Cada chefe de projeto
   C. O principal doador
   D. O auditor externo

4. Um mecanismo de queixa PSEA não recebe nenhuma queixa em dois anos. Conclusão mais provável:
   A. Não há nenhum abuso
   B. É preciso suprimir o mecanismo
   C. O pessoal é exemplar
   D. O mecanismo provavelmente não é conhecido nem considerado seguro

5. As verificações contra as listas de sanções incidem em geral sobre:
   A. Cada beneficiário da ajuda
   B. Os jornalistas
   C. Os parceiros, fornecedores e pessoal segundo o risco
   D. Ninguém

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

Semana 11 : Partilhar o risco com os parceiros e financiar a segurança

Objetivos

- Analisar a transferência de risco para os parceiros nacionais e locais e construir uma partilha equitativa dos riscos.
- Orçamentar a segurança de forma completa e defendê-la junto dos doadores.
- Organizar a segurança nos consórcios, na gestão à distância e na coordenação interorganizacional.

A transferência do risco

Quando o acesso se torna difícil, as organizações internacionais apoiam-se cada vez mais em **parceiros nacionais e locais**, mais bem aceites e muitas vezes os únicos presentes. É uma força para a resposta e para a localização, mas pode tornar-se uma **transferência de risco**: a organização internacional reduz a sua exposição expondo mais o parceiro, sem lhe dar os meios para lhe fazer face.

Sinais de uma transferência injusta:

- o parceiro trabalha em zonas onde a organização internacional proíbe o seu próprio pessoal de ir, sem avaliação conjunta dos riscos;
- o orçamento do parceiro não contém nenhuma rubrica de segurança (comunicações, seguros, formação, veículos adaptados);
- o parceiro suporta sozinho o risco fiduciário (perdas e roubos reembolsados por ele) e o risco jurídico (sanções);
- não está prevista nenhuma assistência em caso de incidente grave que afete o pessoal do parceiro.

Para uma partilha equitativa

A **partilha do risco** (risk sharing) é uma abordagem que reconhece que os riscos devem ser repartidos segundo a capacidade de cada um para os gerir, e financiados. Os trabalhos interorganizacionais sobre este tema (nomeadamente no âmbito do Grand Bargain e das redes de ONG) propõem:

- uma **avaliação conjunta** dos riscos com o parceiro, antes do acordo;
- **custos de segurança elegíveis** no orçamento do parceiro, à medida das necessidades reais;
- um acesso do parceiro à **formação**, às análises de segurança e aos dispositivos de emergência (evacuação médica, seguro);
- uma partilha clara do **risco fiduciário**: que perdas são aceites se os procedimentos tiverem sido seguidos, e quais são reembolsadas;

- **compromissos recíprocos** em caso de incidente grave: assistência, comunicação, apoio às famílias.

> Pergunta de teste: se este incidente acontecesse ao nosso próprio pessoal, o que faríamos? O parceiro merece menos?

Orçamentar a segurança

A segurança custa dinheiro, e os seus custos devem aparecer claramente nos orçamentos; caso contrário, são retirados de outro lado ou ignorados. Rubricas típicas:

- **Pessoal**: conselheiro de segurança, pontos focais, guardas, operadores de rádio.
- **Equipamentos**: comunicações (rádios, telefones satélite, balizas), veículos adaptados, proteções dos locais, equipamentos de proteção individual consoante o contexto.
- **Formação**: segurança básica, formações avançadas, primeiros socorros, exercícios de crise.
- **Serviços**: assinaturas de serviços de análise, fóruns de segurança, evacuação médica, seguros específicos.
- **Reservas de contingência**: hibernação, relocalização, evacuação.

Exemplo de orçamento anual de um país (8 milhões USD de programas, 150 trabalhadores). Conselheiro de segurança e 3 pontos focais: 140 000; guardas (6 locais): 90 000; comunicações: 45 000; formação e exercícios: 35 000; adaptações dos locais: 40 000; seguros específicos e evacuação médica: 60 000; contingência: 30 000. Total: 440 000 USD, ou seja, 5,5 % dos programas e cerca de 2 933 USD por trabalhador. Esta percentagem varia fortemente consoante os contextos, muitas vezes de 2 a 15 %.

Defender o orçamento de segurança

Os doadores aceitam geralmente os custos de segurança se forem **justificados, proporcionados e ligados ao acesso**. Argumentos eficazes:

- ligar cada custo a um risco identificado na avaliação dos riscos e a uma atividade;
- mostrar o que a segurança permite: acesso a zonas precisas, continuidade das atividades, proteção das pessoas assistidas;
- apresentar os custos como custos diretos do projeto (pro rata, segundo chaves justificáveis) em vez de os diluir nos custos indiretos;
- mostrar os dados: incidentes evitados ou mais bem geridos, dias de atividade mantidos.

Exemplo de argumento quantificado. No ano passado, sem telefones satélite, as equipas de duas bases suspenderam as suas deslocações 45 dias no total a cada corte da rede móvel. Equipar estas bases custa 12 000 USD; os 45 dias de suspensão atrasaram atividades no valor de 300 000 USD. O investimento é reduzido face à continuidade que permite.

Consórcios, gestão à distância e coordenação

Num consórcio, cada membro continua responsável pelo seu pessoal, mas o líder deve garantir que os riscos são avaliados e geridos por todos: avaliação comum, partilha de informações, procedimentos de alerta comuns, orçamento de segurança para cada membro.

Na gestão à distância, a segurança das equipas no local (pessoal nacional, parceiros) torna-se prioritária: análise local por quem está exposto, direito de recusar uma atividade, comunicações, meios de relocalização, e contactos regulares.

Coordenação interorganizacional:

- Os **fóruns de segurança das ONG** (plataformas nacionais de partilha de informações e de análises, muitas vezes financiadas por doadores): alertas, relatórios de incidentes, formações, análises.
- O quadro **«Saving Lives Together»**, que organiza a cooperação entre o sistema de gestão da segurança das Nações Unidas e as ONG parceiras.
- O **Global Interagency Security Forum** (GISF) a nível internacional: guias, investigação, intercâmbios entre responsáveis de segurança.

A partilha de informações exige regras: confidencialidade, anonimização, acordo prévio para qualquer dado que não pertença à organização.

Medir a maturidade da gestão dos riscos

Uma organização pode avaliar a sua **maturidade** em gestão dos riscos de segurança em algumas dimensões, classificadas de 1 (inexistente) a 4 (integrado e melhorado continuamente):

- política e governação (limiar de risco, responsabilidades);
- avaliação dos riscos e planos atualizados;
- formação e competências;
- incidentes e aprendizagem;
- gestão de crise;
- dever de proteção equitativo (pessoal nacional, parceiros);
- recursos e orçamento.

Exemplo. Notas de uma organização: 3, 2, 2, 1, 3, 1, 2. Média: 14 / 7 = 2. As duas notas de 1 (incidentes e aprendizagem; dever de proteção equitativo) são as prioridades: dizem respeito à capacidade de aprender e à equidade, em que assentam as outras dimensões. Uma autoavaliação anual, discutida no conselho, permite acompanhar os progressos.

Exercício: um parceiro na linha da frente

Situação. A sua organização financia uma ONG local para atividades de proteção da criança numa província onde o seu pessoal já não está autorizado a ir. O orçamento do parceiro (600 000 USD) não prevê nenhum custo de segurança. O parceiro tem 40 trabalhadores no local; dois deles estiveram detidos durante 3 dias no mês passado; não tem nem seguro de acidentes nem telefone satélite. O acordo prevê que qualquer perda de bens, mesmo devida a uma pilhagem, é reembolsada pelo parceiro.

Trabalho pedido. 1) Identifique os problemas. 2) Proponha um orçamento de segurança realista para o parceiro (comunicações 6 000; formação 8 000; seguro de acidentes 3 % de uma massa salarial de 240 000; reserva de contingência 10 000; ponto focal de segurança a meio tempo 9 000). 3) Que alterações ao acordo?

Correção. 1) Transferência de risco injusta: zona considerada demasiado perigosa para o seu pessoal, sem avaliação conjunta; nenhum custo de segurança; detenção sem apoio previsto; risco fiduciário inteiramente transferido, inclusive em caso de força maior. 2) Comunicações 6 000 + formação 8 000 + seguro 7 200 + contingência 10 000 + ponto focal 9 000 = 40 200 USD, ou seja, 6,7 % do orçamento; a financiar adicionalmente ou por realocação, justificando-o junto do doador. 3) Avaliação conjunta dos riscos e direito do parceiro de suspender uma atividade perigosa; rubrica orçamental de segurança; acesso às formações, às análises e à evacuação médica da sua organização; cláusula de partilha do risco fiduciário (perdas devidas a pilhagem aceites se os procedimentos tiverem sido seguidos e o incidente comunicado); compromisso de assistência em caso de detenção ou de incidente grave.

A reter

- Trabalhar com parceiros não deve tornar-se uma transferência injusta do risco.
- Partilha do risco: avaliação conjunta, orçamento de segurança, acesso às formações e aos dispositivos, perdas partilhadas.
- Orçamentar a segurança em custos diretos, ligados aos riscos e às atividades, muitas vezes 2 a 15 % consoante o contexto.
- Defender a segurança pelo acesso e pela continuidade que permite, com números.
- Fóruns de segurança das ONG, Saving Lives Together, GISF: coordenação com regras de confidencialidade.

Quiz

1. Orçamento de segurança de 360 000 USD para 6 000 000 USD de programas. Proporção:
   A. 3,6 %
   B. 0,6 %
   C. 16,7 %
   D. 6 %

2. Mesmo orçamento para 120 trabalhadores. Custo por trabalhador:
   A. 300 USD
   B. 50 000 USD
   C. 3 000 USD
   D. 30 000 USD

3. Um parceiro reembolsa sozinho qualquer perda devida a uma pilhagem, mesmo que os procedimentos tenham sido seguidos. Isto é:
   A. Uma partilha equitativa
   B. Uma transferência injusta do risco fiduciário
   C. Uma boa prática
   D. Uma exigência de todos os doadores

4. Notas de maturidade 2, 3, 1, 2, 2 em 5 dimensões. Média:
   A. 2
   B. 2,5
   C. 1,8
   D. 10

5. Num consórcio, a segurança do pessoal de cada membro é da responsabilidade:
   A. Apenas do líder
   B. Das autoridades locais
   C. Do doador
   D. De cada membro, com um dispositivo coordenado pelo líder

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

Semana 12 : Governação, cultura de segurança, continuidade de atividade e projeto final

Objetivos

- Organizar a governação dos riscos: política, papéis do conselho e da direção, relatórios, auditorias.
- Desenvolver uma cultura de segurança em que cada pessoa comunica, aprende e protege a aceitação.
- Construir um plano de continuidade de atividade, e realizar o projeto final: um quadro de gestão dos riscos para um país.

A política de segurança e de gestão dos riscos

A **política**, adotada pelo conselho, fixa o quadro que todos os países e serviços aplicam:

- princípios (dever de proteção, aceitação, direito de retirada, igualdade de tratamento, nenhum pagamento às partes no conflito);
- apetite pelo risco e limiares por categoria;
- papéis e responsabilidades, da direção aos pontos focais;
- requisitos mínimos: avaliação dos riscos, plano de segurança, formação, comunicação dos incidentes, gestão de crise;
- posição sobre as questões sensíveis (escoltas armadas, guardas armados, resgates, comunicação em caso de rapto);
- acompanhamento: relatórios, auditorias, revisões.

Normas mínimas por nível de risco tornam a política operacional. **Exemplo:** em qualquer país classificado como de risco elevado, um conselheiro de segurança dedicado, um plano revisto a cada 6 meses, uma formação avançada para todo o pessoal exposto, um exercício de crise anual e comunicações por satélite em cada base.

O papel do conselho e da direção

O **conselho de administração** não gere a segurança no dia a dia, mas tem a responsabilidade última por ela:

- adota a política e o apetite pelo risco;
- recebe um relatório regular (pelo menos anual, trimestral para os riscos principais);
- é informado sem demora dos incidentes graves e das crises;
- verifica que os recursos são suficientes e que as auditorias são acompanhadas.

A **direção** presta contas com um painel de controlo simples: incidentes por categoria e gravidade, taxas por 100 trabalhadores, países acima do limiar, conformidade com as normas mínimas (planos atualizados, formações, exercícios), recomendações em atraso, maturidade.

Exemplo de leitura. 12 países; 10 têm um plano de segurança atualizado (83 %); 7 fizeram um exercício de crise no ano (58 %); 3 países têm riscos residuais acima do apetite. O conselho pede para estes 3 países uma decisão explícita: medidas adicionais, redução de atividades, ou aceitação fundamentada e temporária da ultrapassagem.

Auditar a segurança

As **auditorias de segurança** (internas, por pares ou externas) verificam que o dispositivo existe e funciona:

- documentos: avaliação dos riscos, plano, procedimentos, listas de contactos, registo dos incidentes;
- práticas: controlos de chamada efetivos, registos de movimentos, registos de visitantes, testes de rádio;
- conhecimentos: entrevistas com o pessoal (conhecem o plano, o nível de segurança, o procedimento em caso de incidente?);
- equipamentos: estado dos veículos, comunicações, kits, reservas de hibernação;
- equidade: medidas reais para o pessoal nacional e os parceiros.

Exemplo de amostra. O auditor entrevista 30 trabalhadores: 27 conhecem o nível de segurança atual (90 %), 18 sabem o que fazer se um colega não responder a um controlo de chamada (60 %), 9 participaram num exercício no ano (30 %). Os procedimentos escritos existem, mas a sua apropriação é fraca: a formação e os exercícios tornam-se prioritários.

A cultura de segurança

Os procedimentos mais bem escritos falham sem uma **cultura de segurança**: um conjunto de comportamentos partilhados em que a segurança é vista como um meio de fazer o trabalho, e não como um obstáculo.

Os seus sinais:

- os incidentes e os quase-incidentes são comunicados, e os erros discutidos sem medo;
- os responsáveis aplicam as regras que impõem;
- cada pessoa pode dizer «não» ou «stop» sem ser ridicularizada nem sancionada;
- o pessoal nacional participa nas análises e nas decisões;
- a segurança é discutida nas reuniões de programa, não apenas entre especialistas;
- a qualidade dos programas e o comportamento pessoal são reconhecidos como medidas de segurança.

> A cultura vê-se no que acontece quando um responsável apressado quer contornar uma regra. Se ninguém se atreve a dizer nada, a cultura de segurança é fraca.

A continuidade de atividade

O **plano de continuidade de atividade** prepara a organização para manter as suas funções essenciais apesar de uma perturbação grave: perda de um escritório, corte prolongado da Internet, ciberataque, pandemia, evacuação, saída súbita de pessoas-chave.

Etapas:

- **Identificar as funções críticas**: pagamento dos salários, dos fornecedores e das transferências aos beneficiários, abastecimento dos centros de saúde, comunicações com as equipas, relatórios aos doadores com prazo.
- **Fixar para cada uma um prazo máximo de interrupção**: por exemplo 24 horas para as comunicações de emergência, 7 dias para os salários, 30 dias para os relatórios aos doadores.
- **Prever as soluções de recurso**: escritório alternativo, acesso remoto, cópias de segurança, delegações de assinatura, fornecedores de reserva, stocks.
- **Designar suplentes** para as funções-chave e documentar os acessos essenciais (sem partilhar palavras-passe em claro).
- **Testar** o plano pelo menos uma vez por ano.

Exemplo. O sistema de processamento salarial está alojado num servidor no escritório da capital. Prazo máximo tolerado: 7 dias. Se o escritório ficar inacessível, o restauro a partir da cópia de segurança fora do local demora 3 dias, o que respeita o prazo, desde que a cópia seja recente e testada: a última tem 5 semanas. Ação: cópia de segurança diária automatizada, teste trimestral de restauro.

Projeto final: um quadro de gestão dos riscos para um país

O projeto final do Mini MBA Segurança e gestão de riscos consiste em redigir, para um país ou uma zona reais (apenas com dados públicos, nunca com informações confidenciais de uma organização) ou fictícios mas realistas, um **quadro de gestão dos riscos** de 6 a 10 páginas:

- **1. Análise do contexto**: atores, dinâmicas, cenários, indicadores.
- **2. Avaliação dos riscos**: ameaças, vulnerabilidades por perfil, matriz, riscos inerentes e residuais, comparação com o limiar.
- **3. Estratégia**: dosagem de aceitação, proteção, dissuasão, e estratégia de acesso e de negociação.
- **4. Plano de segurança resumido**: níveis, procedimentos-chave, comunicações, planos de contingência (evacuação médica, hibernação, relocalização, rapto).
- **5. Pessoas**: dever de proteção equitativo, saúde, bem-estar, salvaguarda interna, seguros.
- **6. Riscos da organização**: extrato do registo (fiduciário, conformidade, PSEA, digital, reputação).
- **7. Parceiros, orçamento e governação**: partilha do risco, orçamento de segurança, painel de controlo, continuidade de atividade.

Critérios de avaliação: qualidade da análise, coerência entre riscos e medidas, realismo e proporcionalidade, equidade entre pessoal e parceiros, respeito pelos princípios humanitários,

clareza. O projeto faz parte do exame do terceiro mês.

Exercício: preparar o relatório anual ao conselho

Situação. Dados do ano: 9 países; 210 incidentes para 1 400 trabalhadores (ano anterior: 168 para 1 200); incidentes graves: 21 (ano anterior: 12); planos atualizados em 7 países; exercícios de crise em 4 países; 2 países com um risco residual acima do apetite; 38 recomendações de incidentes, das quais 22 executadas dentro dos prazos; plano de continuidade testado: nenhum. Os parceiros locais comunicaram 35 incidentes, mas não estão incluídos nas estatísticas oficiais.

Trabalho pedido. 1) Calcule as taxas e as percentagens-chave. 2) O que deve o conselho reter? 3) Que decisões lhe pedir?

Correção. 1) Taxa de incidentes: 15 por 100 trabalhadores contra 14 no ano passado (+7 %). Taxa de incidentes graves: 1,5 contra 1,0 por 100 trabalhadores (+50 %). Planos atualizados: 7 / 9 = 78 %; exercícios: 4 / 9 = 44 %; recomendações dentro dos prazos: 22 / 38 = 58 %. 2) A gravidade aumenta claramente mais do que a frequência; a preparação é insuficiente (planos, exercícios, continuidade nunca testada); a aprendizagem é lenta; dois países estão fora do apetite; os riscos dos parceiros são invisíveis nos relatórios. 3) Decisões: para os 2 países fora do apetite, escolher entre medidas adicionais, redução de atividades ou aceitação fundamentada e temporária; exigir planos atualizados e um exercício de crise em todos os países nos próximos 6 meses; testar o plano de continuidade durante o ano; integrar os incidentes dos parceiros nos relatórios e orçamentar a sua segurança; acompanhar trimestralmente as recomendações em atraso.

A reter

- Uma política adotada pelo conselho, declinada em normas mínimas por nível de risco.
- O conselho tem a responsabilidade última: apetite, relatórios, informação imediata sobre as crises, recursos.
- Auditar os documentos, as práticas, os conhecimentos, os equipamentos e a equidade.
- Cultura de segurança: comunicar sem medo, poder dizer stop, exemplaridade dos responsáveis.
- Continuidade de atividade: funções críticas, prazos máximos, soluções de recurso, suplentes, testes regulares.

Quiz

1. 9 países, 6 com um plano atualizado. Percentagem:
   A. 67 %
   B. 60 %
   C. 75 %
   D. 54 %

2. Incidentes graves: 18 para 1 200 trabalhadores. Taxa por 100 trabalhadores:
   A. 18
   B. 15
   C. 0,15
   D. 1,5

3. Numa auditoria, 12 trabalhadores em 40 sabem o que fazer se faltar um controlo de chamada. Isto indica:
   A. Uma boa apropriação
   B. Um problema de rádio
   C. Uma fraca apropriação (30 %): formação e exercícios prioritários
   D. Nada de especial

4. Num plano de continuidade, o prazo máximo de interrupção serve para:
   A. Calcular os salários
   B. Dimensionar as soluções de recurso de cada função crítica
   C. Avaliar o pessoal
   D. Fixar o orçamento de comunicação

5. Um sinal forte de uma boa cultura de segurança é:
   A. Cada pessoa pode dizer «stop» sem ser sancionada
   B. Nenhum incidente comunicado
   C. Procedimentos muito longos
   D. Guardas armados

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