PROTECTION international

Novo Manual de Proteção para Defensores de Direitos Humanos

Pesquisado e escrito por Enrique Eguren e Marie Caraj

Novo Manual de Proteção

para

Defensores de Direitos Humanos

Pesquisado e escrito por Enrique Eguren,
e Marie Caraj, Protection International (PI)

Publicado por Protection International

Publicado por Protection International 2009
Rue de la Linière, 11
B-1060 Bruxelas, Bélgica.

Primeira edição (baseada na terceira edição do *New Proteccion Manual for Human Rights Defenders*).

Traduzido do inglês por: Rui Correia

Protection International

Rue de la Linière, 11.

B-1060 Bruxelas, Bélgica

Tel: +32(0)2 609 44 05 / +32(0)2 609 44 07 /
Fax: +32(0)2 609 44 07
pi@protectioninternational.org

O Manual pode ser baixado gratuitamente a partir do site:
www.protectionline.org

O *Novo* Manual está disponível em inglês, francês, espanhol e português (o documento está sendo traduzido para outras línguas por Protection International)

ISBN: 78-2-930539-14-0

Prefácio à primeira edição, por Hina Jilani

Em meu trabalho como Representante Especial do Secretário-Geral para Defensores de Direitos Humanos tomei nota com grave preocupação do aumento no número de relatos sobre sérios abusos de direitos humanos contra os defensores, e uma notável mudança nestes abusos, passando de ações de nível baixo, como intimidação e perseguição, a violações mais sérias, como ameaças e ataques contra a integridade física dos defensores. Em 2004 trabalhamos sobre comunicações de ao menos 47 defensores que foram assassinados devido ao seu trabalho.

Está claro que a responsabilidade principal de proteção dos defensores de direitos humanos recai nos governos, tal e como está estabelecido na Declaração sobre Defensores[1] *das Nações Unidas. Devemos continuar trabalhando para que todos os governos tomem seriamente em consideração suas obrigações com respeito a isso e tomem medidas efetivas para assegurar a proteção dos defensores de direitos humanos.*

No entanto, a gravidade dos riscos que os defensores assumem diariamente é tal que é também importante buscar outros meios para reforçar sua proteção. Neste sentido, espero que este Manual de Proteção apóie aos defensores no desenvolvimento de seus próprios planos de segurança e mecanismos de proteção. Muitos defensores estão tão comprometidos em seu trabalho para proteger a outros que às vezes não prestam suficiente atenção a sua própria segurança. É importante que todos os que estamos envolvidos no trabalho em direitos humanos entendamos que também devemos preocupar-nos com nossa segurança, não apenas por nós mesmos mas também pelas pessoas com as quais e para quem trabalhamos.

Hina Jilani
Antiga Representante Especial do Secretário-Geral das Nações Unidas para os Defensores de Direitos Humanos

1 Declaração sobre o direito e o dever dos indivíduos, grupos e instituições de promover e proteger os direitos humanos e as liberdades fundamentais universalmente reconhecidos, 1998.

Protection international -PI-

Os integrantes da PI têm mais de 25 anos de experiência combinada na proteção de defensores de direitos humanos e outros grupos vulneráveis.[1]

A PI tem como objetivo o cumprimento das obrigações nacionais e internacionais de proteção aos defensores. Muitas ONGs e outras instituições trabalham na área de direitos humanos e sobre temas de defensores. A PI pretende complementar este trabalho.

A estratégia global da PI para a proteção de defensores de direitos humanos inclu:

Proteção, capacitação em segurança e treinamentos

- Avaliação de risco, administração da segurança e proteção.
- Transferência de conhecimento e ferramentas.
- Publicação de manuais, entre os quais está este *Novo* Manual (e sua edição prévia[2]).
- Capacitação: entre 2004 e 2008, mais de 1700 defensores participaram em oficinas de segurança e capacitação da PI, melhorando assim suas capacidades de administração de sua própria segurança e a proteção de outros.

Pesquisa sobre proteção

- Estudos e elaboração de ferramentas operacionais de proteção e segurança.
- Publicação de informação sobre as lições aprendidas e melhores práticas.

Promoção da proteção

- Distribuição de informação sobre proteção entre defensores de direitos humanos, pessoas deslocadas, instituições da União Européia (UE) e Estados membros da UE na forma de recomendações, relatórios e comunicados de imprensa e documentários.
- Relembrar autoridades nacionais e internacionais sobre suas obrigações internacionais em relação à proteção dos defensores de direitos humanos, deslocados internos, refugiados e outros atores sociais.
- Promoção de debates e ação para proteger defensores de direitos humanos; envolvimento dos parlamentos, sindicatos e dosmídia.
- Luta contra a impunidade e abusos de poder contra defensores de direitos humanos através de acompanhamento de procedimentos judiciais.

Vídeos de proteção (vídeo de defesa)

- Perfis de defensores de direitos humanos.

1 A partir de 25 de outubro de 2007, por meio de um Decreto Real do Serviço de Justiça Pública Federal , o Escritório Europeu das Brigadas da Paz Internacional transformou-se em "Protection International" através de uma mudança de seus estatutos publicada no Diário Oficial Belga. A PI é uma organização sem fins lucrativos.

2 Publicado em 2005 com o apoio financeiro de Front Line e do Departamento de Cooperação e Desenvolvimento Irlandês (Development Cooperation Ireland).

Escritório de Proteção

- Em parceria com redes locais de defensores de direitos humanos, escritórios de proteção são criados como centros nacionais ou regionais para proteção e administração de segurança.
- Progressiva transferência de todo o processo de segurança e administração de proteção para os parceiros locais (controle e apropriação por parte dos parceiros locais é parte deste processo).

Protectionline

- www.protectionline.org é um sitio web feito por, para e com defensores de direitos humanos. Ele contém depoimentos, ações urgentes e ações desenhadas para promover a proteção dos defensores de direitos humanos.
- Atualização diária de informação, documentos, publicações, testemunhos, acções urgentes e instrumentos concebidos para promover a protecção dos defensores.

Estrutura normativa:

A PI respeitatodos os padrões internacionais de direitos humanos e direito humanitário. Especificamente, a PI utiliza as diretrizes da Declaração sobre Defensores de Direitos Humanos das Nações Unidas (1998), as Diretrizes da UE sobre Defensores de Direitos Humanos (2004), assim como as resoluções sobre defensores promovidas pela PI e adotadas pelos Estados-membros da UE como Espanha, Bélgica e Alemanha.

PI: Capacitação e Oficinas de Segurança

Entre 2004 e 2007, um total de 1747 defensores de direitos humanos participaram em oficinas de segurança e capacitações da PIs.

- Na América do Sul e América Central: 558 defensores
  (Bolívia, Brasil, Colômbia, Guatemala, Honduras, México, Peru)
- Na Ásia: 650 defensores
  (Birmânia, Indonésia, Nepal, Tailândia)
- Na África: 441 defensores
  (Quênia, Uganda, Republica Democrática do Congo)
- Na Europa: 98 defensores
  (Alemanha, Bélgica, Irlanda, Sérvia, República da Ingushetia)

Defensores de direitos humanos frequentemente protegem outros e acabam negligenciando sua própria segurança. Há várias razões para isso. O treinamento da PI em segurança e proteção trabalha com estas razões e permite tempo para reflexão sobre os riscos e ameaças aos defensores. O treinamento da PI facilita um detalhamento dos riscos e também do know-how e lógica necessários para incorporar segurança aos planos de trabalho dos defensores. Durante o treinamento, a questão de segurança é dividida em diferentes elementos para permitir sua análise, reflexão sobre possíveis teorias, cenários e conseqüências de escolhas específicas, para então escolher a opção cujas conseqüências o defensor acredita poder administrar. Isto tudo sabendo que é impossível ter completa certeza sobre um resultado específico.

Em nenhum caso existe resposta mágica que funcione todas as vezes; o treinamento tem como objetivo garantir que os defensores adquiram as habilidades necessárias para sua segurança: análise, resultados, administração e atualização do processo. Eles devem fazer isso individualmente, dentro da organização e entre organizações, levando sempre em consideração aspectos políticos, psicossociais e físicos.

Prefácio

Após mais de uma década de treinamentos, pesquisa e encontros com defensores de direitos humanos e outros atores responsáveis pela proteção dos defensores, nós da Protection International decidimos renovar nosso tributo aos defensores e uma vez mais incluir suas contribuições neste novo manual de proteção escrito com, por e para todos os defensores de direitos humanos.

Nos últimos três anos, a Protection International desenvolveu ainda mais seus treinamentos e pesquisas, beneficiando-se da experiência de campo e dos aportes de defensores de direitos humanos.

Neste novo manual, a Protection International avança a lógica de administração que pode ser adotada em diferentes ambientes organizacionais e estruturas. Chegarão sempre ao mesmo resultado: a incorporação de planos de segurança ao plano de trabalho. Não existe resposta mágica, meramente escolhas e conseqüências para administrar. Isto pode ser alcançado através de brainstorming, fazendo as perguntas corretas, realizando análises de risco e segurança organizacional, elaborando planos e processos inclusivos...

Este novo manual, portanto, objetiva ser apropriado por defensores de direitos humanos como um processo de lógica de segurança e proteção em sua totalidade. Apropriação do tema é um componente da segurança em si mesmo. O novo manual contribui para a independência e sustentabilidade da segurança-proteção dos defensores de direitos humanos.

Apesar de não existir um plano de segurança que funcione para todos os casos, o novo manual transcende diferenças entre contextos e estruturas culturais, sociais, religiosas e organizacionais. O manual pode ser facilmente usado por defensores de direitos humanos para adequar sua proteção e segurança. Estamos conscientes de que eles têm essencialmente a mesma base: conhecimento e experiência de seu próprio contexto.

A Protection International diferencia entre a segurança dos próprios defensores de direitos humanos e a proteção do defensor de direitos humanos em relação a outros atores.

Agradecimentos:

♦ A nova versão revista e aumentada deste manual e a nova edição são o resultado da contribuição das seguintes pessoas:

- todos os defensores de direitos humanos que participaram nas oficinas de capacitação em segurança e proteção da PI. Seria impossível listá-los todos aqui. Eles estão localizados nos seguintes países: Bolívia, Brasil, Birmânia, República Democrática do Congo, Guatemala, Honduras, Indonésia, Ingushetia, Quênia, México, Nepal, Peru, Sérvia, Sri Lanka, Tailândia e Uganda.

- Atuais e antigos membros da PI: Pascale Boosten, Soledadd Briones, Shaun Kirven, Christoph Klotz, Rainer Mueller, Michael Schools.

- Os colaboradores da PI são Ana Cornida, Eric Juzen, Maria Martin, Thomas Noirfalisse, Sheila Pais, Flora Petrucci, Sophie Roudil, Catherine Wielant, Jabier Zabala...

• Carmen Díez e Montserrat Muñoz tomaram extremo cuidado no design e diagramação das edições anteriores e atual do Manual. Thomas Noirfalisse contribuiu com seu design para o logo da PI e apresentou idéias para o design da capa.

Lembrança calorosa de Brigitte Scherer.

Nós somos gratos ao apoio do *Bundeministerium für Wirtschaftliche Zusammenarbeit und Entwicklung* (Ministério alemão de Cooperação e Desenvolvimento) e do *Service public fédéral Affaires Etrangères Belgique* (Serviço Belga de Relações Exteriores).

O *Novo* Manual de Proteção para Defensores de Direitos Humanos atualiza e amplia o primeiro Manual de Proteção para Defensores de Direitos Humanos (autoria de Luis Enrique Eguren © 2005 PI), o qual foi publicado com o apoio financeiro de Front Line e do Departamento de Cooperação e Desenvolvimento Irlandês (Development Cooperation Ireland).

O rascunho do primeiro Manual foi comentado por Arnold Tsunga (Zimbabué, Lawyers for Human Rights), Sihem Bensedrine (Tunis, Conseil National pour les Libertés en Tunisie), Padre Brendan Forde (Franciscanos Itinerantes, Colômbia), Indai Sajor (Filipinas, ex-Diretora do Asian Centre for Women's Human Rights, Filipinas), James Cavallaro (Brasil, Diretor Associado do Programa de Direitos Humanos da Harvard Law School), Nadejda Marques (pesquisadora e consultora, Justiça Global, Rio de Janeiro, Brasil) e Marie Caraj (Escritório Europeu de PBI, Bélgica).

Outros colegas também contribuíram com seu próprio trabalho. Temos que mencionar a José Cruz e Iduvina Hernández, do SEDEM (Guatemala), Jaime Prieto (Colômbia), Emma Eastwood (RU) e Cintia Lavandera (Programa de Defensores de Direitos Humanos da Anistia Internacional em Londres).

O Programa de Defensores de Direitos Humanos da Anistia Internacional em Londres e o Projeto Indonésia da PBI providenciaram os fundos para traduções da primeira edição do Manual para o português e indonésio, respectivamente. A Comissão Internacional de Juristas traduziu-o para o idioma tailandês, e a PBI para o nepalês.

O Capítulo 2.11 é baseado no trabalho de Robert Guerra, Katitza Rodriguez e Caryn Madden, da Privaterra (Canada).

Agradecimentos do autor: Luis Enrique Eguren

Muitas outras pessoas contribuíram para a coleta de informação e conhecimento necessários para escrever este Manual. Seria impossível listá-los todos aqui. Eu gostaria apenas de mencionar alguns nomes como:

Para todas as pessoas da PBI, e especialmente para meus ex-colegas no projeto PBI Colômbia como Marga, Elena, Francesc, Emma, Tomás, Juan, Mikel, Solveig, Mirjam, Jacobo e tantos outros...

A Danilo, Clemencia e Abilio e seus colegas da Comisión Intereclesial de Justicia y Paz, na Colômbia. Eles me ensinaram como viver dentro do coração das pessoas.

Ao povo de Santa Marta, em El Salvador, e de Cacarica, Jiguamiandó e San José de Apartado, na Colômbia. Eles, entre outros, me ensinaram como as pessoas do campo vivem com dignidade.

Para Irma Ortiz, co-treinadora em muitas oficinas, e todos os outros colegas da organização Pensamiento y Acción Social (PAS) na Colômbia.

Pelo conselho e aprendizagem inicial com REDR (Londres) e Koenraad van Brabant (Bélgica).

E a tantos defensores com os quais trabalhei em El Salvador, Guatemala, Colômbia, México, Sri Lanka, Birmânia, Croácia, Sérvia, Kosovo, Ruanda, República Democrática do Congo, Ingushetia, etc... um mar de conversas, lágrimas, sorrisos, aprendizagem e compromisso...

Finalmente, não poderia nada fazer sem o amor e dedicação e apoio de Grisela e Iker e de meus pais. Com todo meu carinho para eles.

Agradecimentos da co-autora: Marie Caraj

Eu sinto admiração, respeito, solidariedade, empatia e gratidão por cada defensor humano que eu encontrei, encontrarei e nunca encontrarei. Eles mudaram minha vida. Os dias passados juntos foram, imperceptivelmente, criando um laço entre nós.

Estou dividida entre a raiva contra violadores de direitos humanos e a esperança de que um dia eles verão que não estão sendo discriminados por defensores de direitos humanos e poderão, seguramente, unir-se ao movimento no momento em que todos os direitos humanos sejam respeitados e os defensores possam gozar de uma vida normal.

Para Leze Gegaj, minha mãe, a primeira defensora de direitos humanos que eu conheci.

Para todos os meus amigos e colegas por seu apoio tácito ou explícito. Muitos deles compartilharam as histórias que eu trouxe de volta e me ajudaram a recarregar as baterias.

Nós agradecemos a contribuição de todas as pessoas mencionadas, e aos muitos defensores com quem trabalhamos e de quem tanto temos aprendido. Quaisquer erros contido neste *Novo* Manual (apesar de termos feito o máximo para que não haja restado nenhum!) são inteiramente devidos a nossas falhas em verificar o texto.

Esperamos que este novo manual seja uma ferramenta útil para melhorar a proteção e a segurança dos defensores de direitos humanos, ainda que saibamos que o manual não pode oferecer garantias, e que ao final estes são temas sobre os quais as pessoas, elas mesmas, devem assumir sua responsabilidade. Aguardamos seus comentários e opiniões.

Protection International
April 2009

Isenção de responsabilidade com respeito ao texto

O conteúdo deste manual não representa necessariamente a posição da Protection International.

Os autores e os editores não garantem que a informação contida nesta publicação seja completa e correta e não serão legalmente responsáveis por danos que possam surgir a partir de seu uso. Nada deste manual pode ser tomado como uma norma ou como garantia, ou ainda usado sem o critério necessário para valorar os riscos e os problemas de segurança que um defensor pode enfrentar.

Novo Manual de Segurança e Proteção para Defensores de direitos humanos

Defensores de direitos humanos em risco

Os Direitos Humanos estão amparados pelo direito internacional, mas o trabalho para assegurar seu cumprimento e assumir os casos daqueles cujos direitos foram violados pode resultar num exercício perigoso em muitos países do mundo. Os defensores de direitos humanos são muitas vezes a única força posicionada entre o cidadão comum e o desproporcional poder do Estado. Por isto, são atores fundamentais no desenvolvimento dos processos e instituições democráticas, para por fim à impunidade e para a promoção e proteção dos direitos humanos.

Os defensores de direitos humanos são vítimas de perseguições, detenções, torturas, difamações, suspensões trabalhistas, privações de liberdade de movimento e de obstáculos na obtenção do reconhecimento legal de suas associações. Em alguns países são assassinados ou "desaparecidos."

Nos últimos anos, aumentou a consciência geral acerca do enorme risco que correm os defensores de direitos humanos em seu trabalho. O risco é de fácil identificação quando os defensores trabalham em situações hostis como, por exemplo, quando a lei de um país penaliza as pessoas que realizam certos tipos de trabalho relacionados com os direitos humanos. Os defensores também correm risco quando as leis autorizam plenamente o trabalho em direitos humanos por um lado, mas por outro, não punem aqueles que ameaçam ou atacam os defensores. Em situações de conflito armado, o risco é ainda maior.

Excetuando algumas situações caóticas nas quais a vida de um defensor pode estar nas mãos de soldados durante um controle nas estradas, a violência perpetrada contra os defensores não deve ser considerada indiscriminada. Na maioria dos casos os ataques violentos representam uma resposta deliberada e organizada contra o trabalho dos defensores, vinculada a uma clara agenda política ou militar.

Estes desafios fazem com que os defensores de direitos humanos precisem implementar estratégias amplas e dinâmicas de segurança no dia-a-dia de seu trabalho. Oferecer aos defensores conselhos bem-intencionados ou recomendar-lhes que "andem com cuidado" não é suficiente: é imprescindível uma melhora no manejo de sua segurança. Este Manual não oferece soluções "feitas sob medida", prontas para serem aplicadas em qualquer situação. No entanto, busca proporcionar uma série de ferramentas dirigidas a melhorar a gestão da segurança dos defensores.

As lições de segurança mais efetivas vêm dos próprios defensores - de suas experiências diárias e das táticas e estratégias que vão desenvolvendo com o tempo para proteger seu próprio entorno de trabalho e dos demais. Este Manual deve, portanto, ser considerado como um trabalho em processo de elaboração que deverá ser atualizado e adequado à medida que compilamos mais informação dos defensores de direitos humanos.

Também há lições a aprender das ONGs humanitárias internacionais, que começaram recentemente a desenvolver suas próprias normas e procedimentos para salvaguardar a segurança de seu pessoal.

É importante ter em conta que o principal risco dos defensores é que, muitas vezes, as ameaças se convertem de fato em ataques. Os agressores possuem a vontade, os meios e se valem da impunidade para levar a cabo as ameaças. Portanto, o melhor instrumento para proteger os defensores é a ação política dirigida à necessidade, tanto por parte de governos quanto da sociedade civil, de pressionar e atuar contra aqueles que dia após dia ameaçam, perseguem e matam defensores. Por isso, os conselhos apresentados neste Manual não pretendem de nenhuma maneira substituir a devida obrigação de todos e cada um dos governos de proteger os defensores de direitos humanos.

Dito isto, os defensores podem melhorar consideravelmente sua segurança observando algumas normas e procedimentos propostos e já comprovados.

Este Manual representa una modesta contribuição para um objetivo compartilhado por muitas e diversas organizações: preservar o inestimável trabalho realizado pelos defensores defensores de direitos humanos. São eles quem estão na linha de frente, e são também eles os protagonistas deste Manual.

O Manual

O objetivo deste Manual é proporcionar aos defensores de direitos humanos um conhecimento adicional e alguns instrumentos que possam ser de utilidade imediata para melhorar sua segurança e proteção. Esperamos que este manual possa contribuir para a formação em questões de proteção e segurança e osajude a realizar sua própria valoração dos riscos e a desenvolver as normas de segurança e procedimentos que sejam mais convenientes para cada situação em particular.

Este Manual é o resultado de mais de 25 anos de experiência combinada dos membros da Protection International (PI) trabalhando com direitos humanos e direito humanitário e na proteção de defensores de direitos humanos e outros grupos vulneráveis. A experiência dos membros da PI vem de seu prévio envolvimento e participação em missões de campo e na estrutura das Brigadas da Paz Internacional (Peace Brigades International, PBI).

Nós tivemos a oportunidade de aprender e compartilhar experiências e conhecimento com centenas de defensores no terreno, e também em oficinas, reuniões e discussões sobre segurança. A maior parte do conteúdo do Manual já foi colocada em prática, seja diretamente na proteção do trabalho dos defensores ou ainda em oficinas de formação já realizadas. Este Manual é, assim, resultado de todos estes intercâmbios, e estamos enormemente agradecidos pelo apoio dos defensores que nele participaram.

A segurança e a proteção são duas questões complexas. Ambas se baseiam num conhecimento estruturado, mas também estão influenciadas por atitudes individuais e pelo funcionamento da organização. Uma das mensagens-chave deste Manual é a de que é preciso dar à questão da segurança o tempo, o espaço e a energia necessários, apesar das agendas de trabalho sobrecarregadas, do acentuado estresse e, inclusive, do medo que sofrem muitos dos defensores e suas organizações. Isto implica ir além dos conhecimentos individuais sobre a segurança e encaminhar-se para uma cultura organizativa onde a segurança seja parte integral do trabalho.

O adequado conhecimento do cenário de trabalho é também um aspecto crucial para uma correta gestão da segurança dos defensores. Este Manual contém uma estrutura geral, assim como instruções passo a passo sobre como elaborar um plano de segurança (o produto) e como gerir a segurança (processo). O Manual inclui reflexões sobre conceitos básicos como o risco, a vulnerabilidade e a ameaça; e algumas sugestões de como melhorar e desenvolver a segurança dos defensores no dia-a-dia do trabalho. Esperamos que os temas aqui tratados ajudem a ONGs e aos defensores a atuar melhor frente aos crescentes desafios inerentes ao trabalho em direitos humanos.

Assim, devemos ter em mente que os defensores arriscam seu bem-estar e inclusive suas vidas, e isto é algo realmente sério. Algumas vezes a única maneira de salvar uma vida é esconder-se ou fugir. Queremos que fique muito claro que todas as técnicas e sugestões deste Manual não são, em absoluto, o único enfoque de segurança dos defensores: o Manual foi escrito com toda a boa vontade, mas lamentavelmente não pode oferecer garantias de êxito.

Vamos melhorar este Manual...

O Manual está em contínuo processo de elaboração e será necessário desenvolvê-lo, melhorá-lo e aperfeiçoá-lo. Sua informação como defensor sobre qualquer aspecto deste Manual nos será de grande valor.

Pedimos que nos envie qualquer comentário e opinião – sobretudo quanto a sua experiência no uso do Manual em seu trabalho. Com sua ajuda, podemos transformá-lo num instrumento prático para os defensores do mundo inteiro.

Contate-nos via e-mail: pi@protectioninternational.org

Ou por correio, escrevendo para a PI

Protection International. Rue de la Linière, 11 - 1060 Bruxelles (Belgium)
Tel : + 32 (0)2 609 44 05, +32 (0)2 609 44 07
Fax: +32 (0)2 609 44 06

www.protectioninternational.org, www.protectionline.org

Uma pequena introdução aos defensores de direitos humanos

"Defensor de direitos humanos" é uma expressão utilizada para descrever as pessoas que, individualmente ou com a ajuda de outros, se esforçam em promover ou proteger os direitos humanos. Os defensores de direitos humanos são conhecidos, sobretudo, pelo que fazem, e a expressão pode, portanto, ser melhor definida ao descrever-se suas ações e alguns dos contextos nos quais trabalham.

O trabalho de um defensor de direitos humanos é legal e legitimado pela sociedade civil que ele/a representa.

Todos os dias ao redor do mundo centenas de defensores de direitos humanos são expostos a violência política em função de sua defesa do direito de outros. Arriscando sua própria integridade física e mental, eles lutam para acabar com a impunidade de violações de direitos humanos e para promover justiça social e paz.

Em 1998 a Assembléia Geral das Nações Unidas aprovou a " Declaração sobre o Direito e a Responsabilidade dos Indivíduos, Grupos ou Órgãos da Sociedade de Promover e Proteger os Direitos Humanos e Liberdades Fundamentais Universalmente Reconhecidos " (daqui por diante a "Declaração da ONU sobre os Defensores de Direitos Humanos"). Em outras palavras, cinqüenta anos depois da Declaração Universal dos Direitos Humanos, e depois de vinte anos de negociações sobre um anteprojeto da declaração sobre os defensores de direitos humanos, as Nações Unidas finalmente reconheceram uma realidade: que milhares de pessoas estavam promovendo e contribuindo com a proteção dos direitos humanos no mundo inteiro. Esta é uma Declaração abrangente que honra a quantidade e variedade de pessoas comprometidas com a promoção e proteção dos direitos humanos.

Originalmente, a posição de Representante Especial do Secretário-Geral da ONU para os defensores de direitos humanos foi criada para "buscar, receber, revisar e responder a toda informação sobre a situação e os direitos de todo indivíduo, que atue individual o coletivamente, a promover e proteger os direitos humanos e liberdades fundamentais." Em 2008 ela foi substituída pela posição de Relator Especial da ONU sobre Defensores de Direitos Humanos.

As Diretrizes da União Européia (UE) sobre Defensores de Direitos Humanos (2004) não apenas integraram a Declaração sobre Defensores de Direitos Humanos da ONU por inteiro, mas também contém recomendações específicas para os Estados-membros da UE.

Os defensores de direitos humanos estão dentro da lei e são legitimados pelas comunidades internacional e nacional. A PI se subscreve à definição de quem é um defensor de direitos humanos prevista na Declaração da ONU sobre Defensores de Direitos Humanos e reiterada nas Diretrizes da UE sobre Defensores de Direitos Humanos:

> "Utiliza-se a expressão 'defensor de direitos humanos' para descrever a pessoa que, individualmente ou juntamente com outras, esforça-se em promover ou proteger os direitos humanos. Os defensores

de direitos humanos são identificados acima de tudo pelo que eles fazem e é através de uma descrição de suas ações e de alguns contextos onde trabalham que o termo pode ser explicado."[1]

(Veja no Apêndice ao fim do Manual mais informações sobre a Declaração da ONU sobre Defensores de Direitos Humanos e sobre as Diretrizes da União Européia).

Quem é responsável por proteger os defensores de direitos humanos?

A Declaração sobre os Defensores de Direitos Humanos sublinha que o Estado é o principal responsável por proteger os defensores de direitos humanos. Neste sentido, reconhece "*o valioso trabalho de indivíduos, grupos e associações ao contribuir na efetiva eliminação de toda violação dos direitos humanos e liberdades fundamentais*" e "*a relação entre a paz internacional e a segurança e desfrute dos direitos humanos e liberdades fundamentais*".

Contudo, segundo Hina Jilan[2], Representante Especial do Secretário-Geral da ONU para os defensores de direitos humanos, "a manifestação das violações dos direitos humanos e a busca de compensação por elas depende em grande medida do grau de segurança de que desfrutem os defensores de direitos humanos"[3]. Todos os relatórios sobre os defensores de direitos humanos do mundo inteiro revelam histórias de tortura, desaparições, assassinatos, ameaças, roubos, entrada ilegal em escritórios, coação, detenções ilegais, estar submetido a atividades de inteligência e de vigilância, etc. Lamentavelmente, esta é a rega e não a exceção para os defensores.

Leitura sugerida

Para mais informação sobre os defensores de direitos humanos, visite:

- www.unhchr.ch/defender/about1.htm (Alto Comissariado da ONU para os Direitos Humanos).
- www.protectionline.org (Protection International).
- Observatório para a Proteção dos Defensores de Direitos Humanos, criado pela Federação Internacional dos Direitos Humanos (FIDH; www.fidh.org) e a Organização Mundial Contra a Tortura (OMCT; www.omct.org).
- www.amnesty.org e http://web.amnesty.org/pages/hrd-index-eng (Anistia Internacional).
- www.ishr.ch, veja abaixo "HRDO" (Escritório para os Defensores de Direitos Humanos do Serviço Internacional para os Direitos Humanos em Genebra).
- www.frontlinedefenders.org (Front Line, Fundação Internacional para os Defensores de Direitos Humanos).

1 Defensores de Direitos Humanos: Protegendo o Direitoa a Defender os Direitos Humanos. Folheto No. 29. www.ohchr.org

2 Margaret Sekaggya (Uganda) sucedeu à Hina Jilani em 2008, como Relatora Especial sobre a situação dos defensores de direitos humanos, nomeada pelo Conselho de Direitos Humanos da ONU.

3 Relatório sobre os defensores deos direitos humanos, 10 de Ssetembro de 2001 (A/56/341).

Para mais informação sobre os instrumentos legais internacionais existentes e a Declaração da ONU sobre os defensores de direitos humanos, visite:

- www.unhchr.ch: esta é a página eletrônica do Alto Comissariado da ONU para os Direitos Humanos.
- www.protectionline.org (Protection International).
- www.ishr.ch/index.htm (Serviço Internacional dos Direitos Humanos, Genebra) para uma compilação de instrumentos internacionais e regionais para a proteção dos defensores de direitos humanos.

PARTE I

RISCO, AVALIAÇÃO DE AMEAÇAS E OUTRAS FERRAMENTAS

Nesta primeira parte do Manual trataremos de conceitos básicos de segurança, algumas ferramentas práticas e abordagens de segurança para alguns casos específicos.

Todos estes temas serão integrados ao plano de segurança e ao manual de segurança da organização.

ÍNDICE DA PRIMEIRA PARTE:

CAPÍTULO 1.1

Tomando decisões fundamentadas sobre segurança e proteção

Objetivo:

Tomar consciência da importância de analisarmos nossos cenários de trabalho por razões de segurança.

Aprender diferentes métodos para realizar análises de contexto e sobre os atores relevantes.

O ambiente de trabalho dos defensores dos direitos humanos

Os defensores dos direitos humanos trabalham geralmente em cenários complexos, com uma grande variedade de atores, que se vêem afetados por processos de tomada de decisões sumamente políticas. Nestes cenários ocorrem muitas coisas simultaneamente, e cada uma delas exercerá sua influência sobre as outras. As dinâmicas de cada ator chave neste cenário terão um papel significativo na relação daquele ator com outros. Os defensores de direitos humanos necessitam, portanto, possuir informação não somente sobre as questões diretamente relacionadas a seu trabalho, mas também sobre as posições dos atores chaves.

Um exercício inicial seria o de organizar uma sessão de reflexão em grupo para tentar identificar e enumerar todos os atores sociais, políticos e econômicos que possam exercer influência sobre a atual situação de segurança.

Análise do cenário de trabalho

É muito importante conhecer e compreender da melhor forma possível o contexto em que se trabalha. Uma boa análise deste contexto permite tomar decisões contextualizadas sobre quais medidas e procedimentos de segurança colocar em prática. É também importante prever possíveis situações futuras para, na medida do possível, poder adotar medidas preventivas.

Entretanto, a simples análise do ambiente de trabalho não é suficiente. Também é necessário observar como cada intervenção poderia afetar a situação e como poderiam reagir outros atores ante a ela. É também importante considerar as dimensões de um ambiente de trabalho: pode-se fazer uma **macro** análise sobre o país ou a região, mas também se deve averiguar como funcionam estas macro

dinâmicas na área concreta em que estejam trabalhando, isto é, sua **micro** dinâmica.

Por exemplo, os paramilitares de uma zona local poderiam atuar de forma diferente do previsto, segundo uma análise regional ou nacional. Por isso, é necessário estar consciente destas características locais. Também é crucial evitar uma visão estática de um cenário de trabalho, porque as situações evoluem e mudam. Estes cenários devem, portanto, ser revisados com regularidade.

Há, entre outros, três métodos práticos na hora de analisar o ambiente de trabalho: "**formular perguntas**", "**análise de forças externas**" e a "**análise de atores envolvidos**".

Formular perguntas

O simples fato de formular as perguntas adequadas pode ajudar a compreender melhor seu ambiente de trabalho. Resulta num instrumento útil para gerar debates num pequeno grupo, mas apenas funcionará se as questões são formuladas de forma que facilitem a busca de uma solução.

Suponhamos, por exemplo, que a perseguição por parte das autoridades locais se converteu num problema. Se formulamos a pergunta: "O que se deveria fazer para reduzir a perseguição?", talvez encontremos simplesmente um remédio para o sintoma, isto é, a perseguição.

Mas se a pergunta é formulada orientando-a para uma solução, fica mais fácil encontrar uma solução real. Por exemplo, se perguntamos: "É nosso ambiente sociopolítico suficientemente seguro para que possamos dar conta do nosso trabalho?", obter-se-iam somente duas possíveis respostas: "sim" ou "não".

Se a resposta for "sim", é necessário formular outra pergunta que possa ajudar a determinar com exatidão e compreender devidamente quais são os pontos-chave em jogo para preservar a segurança. Se, após uma deliberação apropriada sobre todas as atuações, planos e recursos disponíveis, e ainda sobre a legislação, negociações em curso, as comparações com outros defensores da região, etc., a resposta for "não", esta já seria uma solução para o problema de segurança.

Uso do método de Formular Perguntas:

- Busque perguntas que lhe ajudem a delimitar e compreender devidamente os pontos-chave em jogo para preservar sua segurança;
- Formule as perguntas orientando-as para a obtenção de uma solução;
- Repita o processo tantas vezes quanto necessário (em forma de debate).

Algumas perguntas práticas:

- Quais são as questões-chave em jogo nos cenários sociopolítico e econômico?

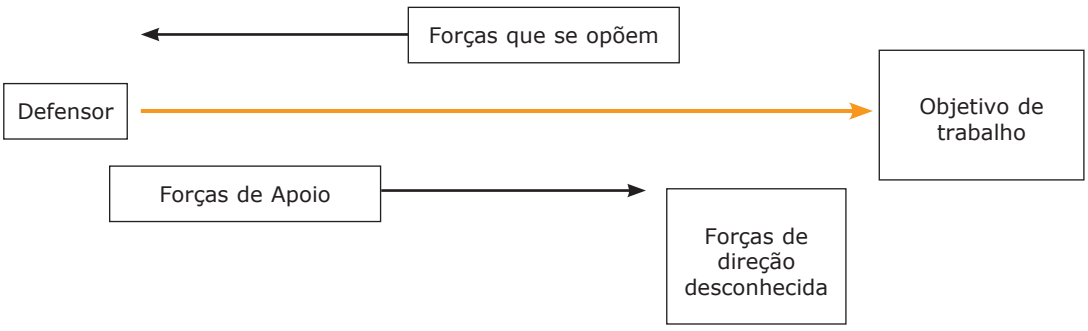
- Quem são os atores mais importantes relacionados com estas questões-chave?
- Em que medida poderia nosso trabalho afetar de forma negativa ou positiva os interesses destes atores-chave?
- Como poderíamos reagir na hipótese de nos convertermos em alvo destes atores por conta do nosso trabalho?
- É nosso entorno sociopolítico suficientemente seguro para executarmos nosso trabalho?
- Como responderam as autoridades locais/nacionais ao trabalho anterior dos defensores de direitos em relação a esta questão?
- Como responderam os atores-chave a atuações similares de defensores de direitos, ou outros, em relação a estas questões?
- Como responderam os meios de comunicação e a comunidade em circunstâncias similares?
- Etc.

Análise das forças externas

A análise das forças externas é uma técnica que ajuda a identificar visualmente como diferentes forças apóiam ou enfraquecem o alcance dos objetivos de trabalho. Mostra tanto as forças que apóiam como as que se opõem, e se baseia na premissa de que os problemas de segurança podem se originar das forças que se opõem, ao passo que se pode tirar proveito de algumas forças de apoio. Esta técnica pode ser realizada por uma pessoa sozinha, mas é mais efetiva quando usada por um grupo diverso, com um objetivo de trabalho claramente definido e um método para alcançá-lo.

Comece desenhando uma flecha horizontal num quadro. Escreva um pequeno resumo de seu objetivo de trabalho nesse quadro. Isto proporcionará um foco para identificar as forças favoráveis e contrárias. Desenhe outro quadro sobre a flecha central: enumere aqui todas as possíveis forças que poderiam se opor ao alcance de seu objetivo. Abaixo da flecha, desenhe um quadro parecido que contenha todas as forças de apoio potencial. Desenhe um último quadro para as forças cuja direção é desconhecida ou incerta.

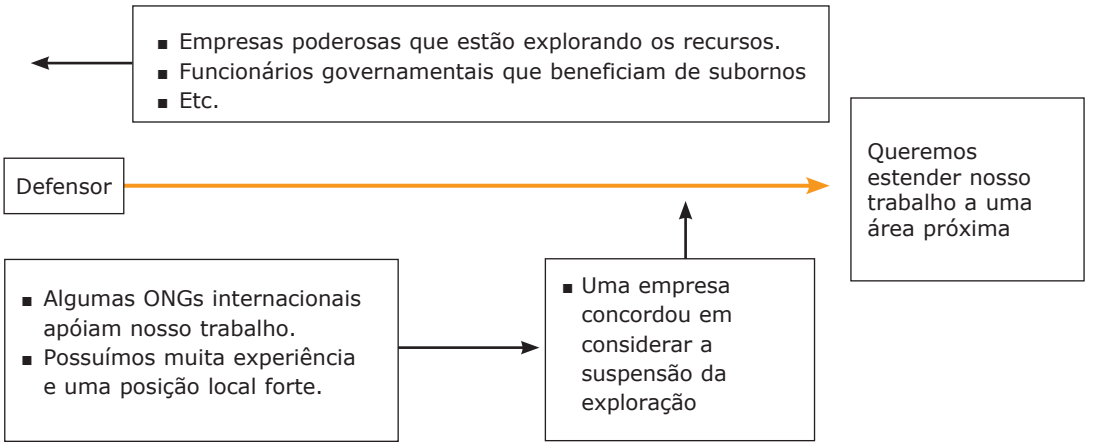
Tabela 1: Análise das forças externas para avaliar os cenários de trabalho



Depois de completar o gráfico, é o momento dos resultados. A análise das forças externas lhe ajuda a visualizar claramente as forças com as quais trabalhamos. O objetivo é encontrar formas de reduzir ou eliminar o risco gerado pelas forças contrárias, em parte através da ajuda potencial das forças de apoio. Quanto às forças de direção desconhecida, é necessário decidir se elas serão consideradas de apoio, ou analisá-las continuamente para poder, assim, detectar os sinais de sua conversão para uma posição de apoio ou de oposição.

Por exemplo:

Imaginemos que você pertence a uma organização que trabalha sobre os direitos da população indígena ao uso dos recursos naturais de seu território, e que há vários conflitos com diversos atores interessados na exploração destes recursos. Agora você quer ampliar seu trabalho a uma área próxima com problemas similares.



A análise de atores

A análise de atores é uma boa forma de aumentar a informação que se tem para tomar decisões sobre proteção. Ela requer a identificação e descrição dos diferentes atores envolvidos e de suas relações, com base em suas características e interesses - e tudo isto em relação a um tema concreto de proteção.

Um ator de proteção é toda pessoa, grupo ou instituição que esteja envolvido ou tenha um interesse no resultado de uma política em área da proteção.[1]

1 Adaptado de *Sustainable Livelihoods Guidance Sheets* No. 5.4 (2000).

Os atores que estão envolvidos na proteção podem ser classificados da seguinte maneira:

Os atores principais. No contexto de proteção, estes são os **próprios defensores**, e **aqueles para e com quem trabalham**, porque todos têm um interesse direto em sua própria proteção.

Os atores com responsabilidades têm obrigação de proteger os defensores, isto é:

- Instituições governamentais e estatais (incluindo as forças de segurança, os juízes, os legisladores, etc.);
- Organismos internacionais com um mandato que inclua a proteção, como alguns organismos da ONU, organizações regionais, forças de manutenção da paz, etc;
- No caso de atores armados de oposição, é possível definir-lhes a obrigação de não atacar os defensores (como população civil que são), especialmente quando estes atores armados controlam o território.

Os atores-chave podem influenciar em grande medida a devida proteção dos defensores. Eles podem ter uma influência política ou a capacidade de pressionar os atores com responsabilidades se não as cumprem (outros governos, organismos da ONU, etc.), e também podem exercer pressão sobre outros atores que podem estar envolvidos direta ou indiretamente em atacar e pressionar os defensores (tais como, empresas privadas, ou meios de comunicação ou também outros governos). Tudo depende do contexto, dos interesses e estratégias de cada um destes interessados. Uma lista não exaustiva de atores-chave em proteção incluiria:

- Organismos da ONU (ademais dos que têm mandato em proteção);
- O Comitê Internacional da Cruz Vermelha (CICR);
- Outros governos e instituições multilaterais (tanto doadores como decisores políticos);
- Outros atores armados;
- ONGs (tanto nacionais como internacionais);
- Igrejas e instituições religiosas;
- Empresas privadas;
- Os meios de comunicação.

Um obstáculo importante na hora de analisar as estratégias e ações dos atores envolvidos é a possibilidade de que eles não tenham relação entre si, ou ainda que as relações entre eles não sejam claras e definidas. Muitos atores com responsabilidade de proteção, especialmente os governos, as forças de segurança e as forças armadas de oposição causam (ou favorecem) as violações de direitos humanos e a falta de proteção dos defensores. Outros atores, que em tese compartilhariam as mesmas preocupações de proteção, poderiam ter também interesses opostos como, por exemplo, pessoas dentro dos governos, organismos da ONU e de ONGs. Todos estes fatores, junto àqueles inerentes às situações de conflito, projetam uma visão complexa do cenário em seu conjunto.

Análise de atores, estruturas e processos variáveis

Os atores chave **não são estáticos**, mas interagem entre si em múltiplos níveis, criando uma densa rede de relações. Em termos de proteção, é importante destacar e prestar atenção às interações que moldam e transformam as necessidades de proteção das pessoas.

As estruturas são as partes do setor público, a sociedade civil ou as entidades privadas que se relacionam entre si. Se as observamos desde o ponto de vista da proteção, dentro do setor público, poderíamos considerar o governo como um grupo de atores com uma estratégia unificada ou ainda com estratégias internas conflitantes. Por exemplo, poderíamos encontrar fortes discrepâncias entre o Ministério de Defesa e o Ministério de Relações Exteriores durante um debate sobre políticas referentes aos defensores de direitos humanos, ou entre o Ministério Público e o Exército. As estruturas podem ter uma composição variada; por exemplo, poderia ser criada uma comissão intersetorial (membros do governo, ONGs, a ONU e corpo diplomáticos) para fazer um seguimento da situação de proteção de uma organização específica de defensores dos direitos humanos.

Os processos são as cadeias de decisões e ações executadas por uma ou várias estruturas, com o objetivo de melhorar a situação de proteção de um grupo específico. Os processos podem ser legislativos, culturais e sobre políticas de proteção. Nem todos estes processos conseguem obter melhoras na proteção: em alguns casos os processos de proteção entram em conflito ou reduzem mutuamente sua eficácia. Por exemplo, as pessoas supostamente sob proteção poderiam não aceitar uma política de proteção dirigida pelo governo por considerar que tal política pretende expulsar a população de uma região. A ONU e as ONGs poderiam apoiar as pessoas neste processo.

A análise de atores chave é fundamental para compreender:

- Quem é um ator chave e em que circunstâncias seu "interesse" deverá ser levado em conta;
- A relação entre os atores de proteção, suas características e interesses;
- Como eles seriam afetados por atividades de proteção;
- A vontade de cada ator para envolver-se nessas ações de proteção.

Existem muitos métodos para realizar uma análise de atores. Os que utilizamos aqui seguem uma metodologia simples e imediata, essencial para obter bons resultados.

Ao analisar os processos de proteção é importante observá-los sob uma perspectiva temporal adequada e ter sempre em conta os interesses e os objetivos de todos os atores envolvidos.

Uma análise de atores em quatro passos:

1. Examine a situação de proteção de forma ampla (isto é, a situação de segurança dos defensores dos direitos humanos numa região específica dentro de um país).
2. Quem são os atores envolvidos? (Principalmente quais as instituições e grupos e indivíduos com responsabilidade ou interesse em proteção?) Identifique e enumere todos os atores relevantes para este tema de proteção (através de sessões de reflexão e debates).
3. Investigue e analise as características e os aspectos próprios dos atores, tais como seu poder de influência sobre a situação de proteção, seus fins, suas estratégias, sua legitimidade e seus interesses (incluindo sua vontade de contribuir na proteção).
4. Investigue e analise as relações entre os atores.

Depois ter feito esta análise, seus resultados podem ser visualizados numa matriz como a seguinte (ver Gráfico 1.2). Copie a mesma lista de atores na primeira coluna e ao longo da primeira linha. Depois:

- Analise as características de cada ator (objetivos e interesses, estratégias, legitimidade e poder), preencha os quadros seguindo a diagonal onde cada ator se encontra consigo mesmo:

Por exemplo:

Coloque os objetivos e interesses e estratégias dos grupos de oposição armada no quadro "A.

- Para analisar as relações entre todos os atores, preencha os quadros que definem as relações mais importantes relativas à questão de proteção, por exemplo, o quadro de intersecção entre o exército e o Alto Comissariado das Nações Unidas para os Refugiados (ACNUR), no quadro "B", etc.

Depois de preencher os quadros mais relevantes, você obtém uma visão geral e uma perspectiva dos objetivos e estratégias de interação entre os principais atores com relação à questão específica de proteção.

Gráfico 2: Sistema matriz para a análise de atores

	Governo	Exército	Polícia	Grupo de oposição armada	ONGs nacionais de direitos humanos	Igrejas	Outros governos	Agências de ONU	ONGs Internacionais
Governo	(ator)								
Exército		(ator)						B	
Polícia			(ator)						
Grupos de oposição armados				A					
ONGs nacionais de direitos humanos					(ator)				
Igrejas						(ator)			
Outros governos							(ator)		
Agências da ONU								(ator)	
ONGs Internacionais									(ator)

Quadro "**A**":

Para cada ator:

- objetivos e interesses
- estratégias,
- legitimidade
- poder

Quadro "**B**":

Inter-relação entre atores:

(Inter-relação relativa à questão de proteção e às questões estratégicas de ambos atores)

Resumo

- Todos os defensores de direitos humanos enfrentam riscos.
- Nem todos os defensores de direitos humanos são iguais diante de riscos.
- Riscos dependem do contexto político.
- O contexto político muda, ele é dinâmico.
- Portanto, o risco é dinâmico.

Esta é a hipótese sobre a qual baseamos a importância de descobrir. Informação chave ao perguntar as perguntas corretas.

Então, mapeie e analise os atores chave com todos os seus componentes até o substrato mais detalhado.

Estabeleça como eles interagem em relação a questões de proteção e como estas questões se relacionam com questões estratégicas para o ator chave em questão.

Descubra interesses convergentes e divergentes, alianças, métodos operacionais, etc.

Veja quais são as estruturas subjacentes e seus processos.

Você será capaz de indicar as diferentes forças (resistência, apoio e não identificadas).

Na primeira vez os passos descritos acima podem ser difíceis. Mas se a análise é atualizada regularmente, o processo fica mais fácil.

Isto lhe ajudará a tomar decisões mais bem informadas sobre segurança e proteção.

Valoraçao do risco: ameaças, vulnerabilidades e capacidades

Objetivo:

Compreender os conceitos de ameaça, vulnerabilidade e capacidade de segurança.

Aprender a realizar uma valoração do risco.

Análise de risco e necessidades de proteção

O trabalho dos defensores de direitos humanos pode causar um impacto negativo sobre os interesses de certos atores, e isto pode, por sua vez, por em risco os próprios defensores. Portanto, é muito importante enfatizar que o **risco é parte inerente das vidas dos defensores em certos países**.

A análise do risco pode ser dividida da seguinte maneira:

> Analisar os interesses e estratégias dos principais atores envolvidos ⇨ avaliar o impacto do trabalho do defensor sobre estes interesses e estratégias ⇨ avaliar a ameaça contra os defensores ⇨ avaliar as vulnerabilidades e as capacidades dos defensores ⇨ estabelecer o risco.

Em outras palavras, a trabalho que os defensores realizam pode incrementar o risco que enfrentam.

- O **que** fazem pode provocar ameaças.
- **Como**, **onde**, e **quando** trabalham, fazendo perguntas sobre suas vulnerabilidades e suas capacidades.

Não existe uma definição amplamente aceita de risco, mas podemos dizer que risco se refere às possíveis situações, por mais incertas que sejam, que poderiam causar um dano.

Em qualquer situação, todos aqueles que trabalham com direitos humanos podem compartilhar um nível comum de perigo, mas o simples fato de se encontrar no mesmo lugar não significa que todos sejam igualmente vulneráveis a este risco geral. A vulnerabilidade – a possibilidade de que um defensor ou um grupo sofra um ataque ou dano – varia de acordo com diferentes fatores, como estudaremos a seguir.

Um exemplo:

> *Suponhamos que o Governo de um país representa uma ameaça geral para todo tipo de trabalho sobre direitos humanos. Isto significa que todos os defensores correm um certo risco. Mas também sabemos que alguns defensores correm maior risco do que outros; por exemplo, uma grande ONG já bem estabelecida, com base na capital, seguramente não será igualmente vulnerável como uma pequena ONG local. Poderíamos dizer que isto é de senso comum, mas seria interessante analisar o porquê desta situação para compreender e responder melhor aos problemas de segurança dos defensores.*

O nível de risco enfrentado por um grupo de defensores aumenta de acordo com as ameaças recebidas e a sua vulnerabilidade frente a estas ameaças, como indicamos na seguinte equação:[1]

$$\textbf{RISCO} = \frac{\textbf{TAMEAÇAS X VULNERABILIDADES}}{\textbf{CAPACIDADES}}$$

As **ameaças** representam a possibilidade de que alguém viole a integridade física ou moral ou a propriedade de outra pessoa por meio de uma ação intencionada e em geral violenta.[2] Avaliar uma ameaça significa analisar a possibilidade de que esta ameaça se concretize na forma de ataque.

Numa situação de conflito, os defensores podem enfrentar muitas ameaças diferentes, como o "targeting" (ameaças diretas com um alvo concreto), a delinqüência comum e as ameaças indiretas.

A forma mais comum de ameaça – o targeting – busca enfraquecer ou mudar o trabalho de um grupo, ou influenciar na atividade das pessoas envolvidas. O targeting geralmente está muito vinculado ao trabalho realizado pelos defensores em questão, assim como aos interesses e às necessidades das pessoas que se opõem ao trabalho de tais defensores.

As **ameaças indiretas** surgem do possível dano causado por:

- **combates em conflitos armados**, tais como "estar no lugar errado na hora errada", de modo que essas ameaças concernem especialmente aos defensores que trabalham em zonas de conflito armado.

1 Adaptado de Van Brabant (2000) e REDR.
2 Dworken (1999).

- Os defensores podem enfrentar ameaças de **ataques por delinqüência comum**, sobretudo se seu trabalho os leva a zonas de risco. Em outros casos, o targeting ocorre sob a aparência de incidentes de "delinqüência comum", ou de "crimes comuns".

As **ameaças tipo targeting (ameaças focalizadas)** podem também ser consideradas de forma complementar: os defensores de direitos humanos poderiam sofrer **ameaças diretas (declaradas)** ao receber, por exemplo, uma ameaça de morte (veja o Capítulo 1.3, sobre como avaliar as ameaças declaradas). Há também casos de ameaças **indiretas**, quando um defensor vinculado ao seu trabalho é ameaçado e existem razões para suspeitar que você poderia ser o seguinte.

Resumo dos tipos de ameaças

- Targeting (ameaças declaradas, ameaças potenciais): ameaças vinculadas a seu trabalho.
- Ameaças por delinqüência comum (crimes comuns).
- Ameaças indiretas: Ameaças decorrentes de combates no caso de conflitos armados.

Vulnerabilidades

A vulnerabilidade é o grau em que as pessoas estão suscetíveis a perdas, danos, sofrimento ou a morte em caso de um ataque. A vulnerabilidade varia de acordo com o defensor ou grupo, e muda com o tempo. As vulnerabilidades são sempre relativas, porque todas as pessoas e grupos são vulneráveis em certo grau. Entretanto, toda pessoa possui seu próprio nível e tipo de vulnerabilidade, de acordo com as circunstâncias. Vejamos alguns exemplos:

- A vulnerabilidade pode estar vinculada à localização. Por exemplo, um defensor poderá estar mais vulnerável quando viajar para realizar uma visita de campo do que quando se encontra num importante escritório, onde um ataque seria visto por alguma testemunha.
- Vulnerabilidade pode incluir a falta de acesso a um telefone, a um transporte local seguro ou a inexistência de fechaduras apropriadas nas portas de uma casa. Mas as vulnerabilidades também estão relacionadas com a falta de redes de colaboração e de soluções compartilhadas entre os defensores.
- Vulnerabilidade pode também estar relacionada com o trabalho em equipe e com o medo: um defensor que recebe uma ameaça pode sentir medo, e seu trabalho poderia ser afetado por este medo. Se o defensor não dispõe de um sistema efetivo para enfrentar o medo (alguém com quem falar, uma boa equipe de colegas, etc.) há grandes possibilidades de que ele/ela cometa erros ou tome decisões inadequadas que poderiam criar ainda mais problemas de segurança.

(Ao final do capítulo há uma lista de possíveis vulnerabilidades e capacidades).

Capacidades

As capacidades são os pontos fortes e os recursos aos quais pode acessar um grupo ou um defensor individual para conseguir um nível razoável de segurança. Exemplos de capacidades seriam: a formação em segurança ou em questões jurídicas; o trabalho em equipe de um grupo; o acesso a um telefone e a um transporte seguro, acesso a boas redes de defensores, e um sistema efetivo para enfrentar o medo, etc.

Na maioria dos casos, a vulnerabilidade e as capacidades representam dois lados da mesma moeda.

Por exemplo:

Não conhecer suficientemente seu ambiente de trabalho é uma vulnerabilidade, enquanto possuir este conhecimento é uma capacidade. Poderíamos dizer o mesmo da falta de acesso a um transporte seguro ou a boas redes de colaboração de defensores.

Entretanto, na maioria dos casos o comportamento é um fator determinante.

Por exemplo:

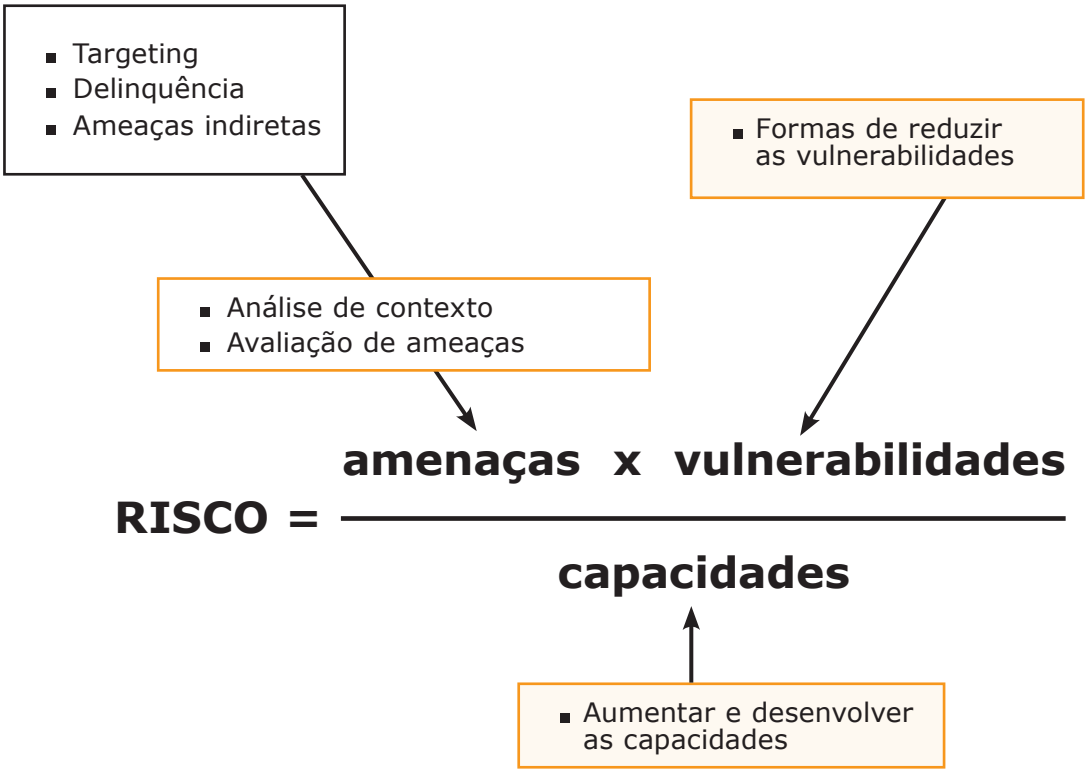
Possuir um telefone pode potencialmente ser uma vulnerabilidade e uma capacidade, dependendo de como ele é usado. Se ele é usado com volume alto e informação confidencial é comunicada, trata-se de uma vulnerabilidade. Mas se usado discretamente e a informação confidencial repassada através de códigos, estamos diante de uma capacidade.

(Ao final do capítulo há uma lista de possíveis vulnerabilidades e capacidades).

Em resumo

Para reduzir o risco a níveis toleráveis – isto é, para proteger – é necessário:

- Reduzir as ameaças;
- Reduzir os fatores de vulnerabilidade;
- Aumentar as capacidades de proteção.



O risco é um conceito dinâmico que varia com o tempo e com as mudanças na natureza das ameaças, das vulnerabilidades e das capacidades. Por isto, o risco deve ser avaliado periodicamente, sobretudo quando se altera o ambiente de trabalho, as ameaças ou as vulnerabilidades. Por exemplo, as vulnerabilidades também podem aumentar se uma mudança dos líderes coloca um grupo de defensores numa situação mais fraca que a anterior. O risco aumenta drasticamente no caso de uma ameaça presente e clara. Neste caso, não é adequado tentar reduzir o risco aumentando as capacidades, porque isso leva tempo.

Certas medidas de segurança tais como a formação jurídica ou barreiras de proteção, poderiam reduzir o risco ao diminuir os fatores de vulnerabilidade. No entanto, estas medidas não fazem frente à principal fonte do risco, ou seja, as ameaças, nem tampouco à vontade de perpetrá-las, sobretudo em situações em que os perpetradores sabem que provavelmente não serão punidos. Todas as intervenções importantes em termos de proteção deveriam, portanto, concentrar-se em reduzir as ameaças, além de reduzir as vulnerabilidades e aumentar as capacidades.

Por exemplo:

Um pequeno grupo de defensores trabalha numa cidade com temas relacionados à propriedade da terra. Quando seu trabalho começa a afetar os interesses de um proprietário de terras local, recebem uma clara ameaça de morte. Se aplicarmos a equação de risco à situação de segurança, comprovar-se-á que o risco que correm estes defensores é

muito elevado, sobretudo devido à ameaça de morte. Se pretendermos então reduzir este risco, seguramente este não é o momento adequado para começar a mudar as fechaduras da porta do escritório (porque o risco não está relacionado com um roubo no escritório), nem tampouco para comprar um telefone celular para cada defensor (ainda que a comunicação seja um fator importante para a segurança, seguramente não resultaria suficientemente efetiva se alguém tentar assassinar um defensor). Neste caso, a estratégia mais relevante seria a de trabalhar em rede e gerar respostas políticas para confrontar diretamente a ameaça (e se isto parece pouco efetivo no curto prazo, talvez a única forma de reduzir o risco de forma significativa seja diminuir a exposição dos defensores, afastando-se por um tempo - a capacidade de viajar para um lugar seguro também é uma capacidade). Tomar uma decisão como esta e levá-la a efeito também envolve capacidade psicossocial para que o defensor veja que a saída temporária não é sinônimo de covardia ou derrota. Retirar-se pode permitir reflexão e o recomeço do trabalho quando estiver mais bem equipado.

As vulnerabilidades e as capacidades, assim como algumas ameaças, podem variar de acordo com o sexo e a idade. Desta forma, é importante ajustar a informação das valorações de risco também a estas variáveis.

Valoração de vulnerabilidades e capacidades

Para poder desenhar a avaliação das vulnerabilidades e capacidades de um grupo (ou pessoa) em concreto, é necessário definir o grupo em questão (uma comunidade, um coletivo, uma ONG, indivíduos, etc.), a zona geográfica onde está localizada e o espaço de tempo (o perfil de vulnerabilidade muda e evolui com o tempo). Uma vez feito isso, proceda à avaliação das vulnerabilidades e capacidades, utilizando como guia a **tabela 1.3**, localizada ao final deste capítulo.

Tome nota: A avaliação das vulnerabilidades e capacidades deve ser considerada como uma atividade sempre em curso, baseada na análise da informação obtida para se manter uma visão clara de uma situação que está em constante evolução. Ao avaliar as capacidades, é ainda importante estabelecer quais são as capacidades reais naquele momento e só então enumerar aquelas potenciais ou desejáveis. Mais tarde, você precisará criar um processo para atingir as capacidades desejáveis.

Tabela 3: Informação necessária para avaliar as vulnerabilidades e as capacidades de um grupo

"Nota: De maneira geral, a informação situada na coluna da direita indica as vulnerabilidades e capacidades de cada componente".

Vulnerabilidades e capacidades	Informação necessária para avaliar as vulnerabilidades ou capacidades dos defensores em relação aos componentes
Componentes geográficos, físicos e técnicos	
Exposição	A necessidade de cruzar ou permanecer em zonas perigosas para realizar atividades rotineiras ou ocasionais, com atores ameaçadores nessas zonas.
Estruturas físicas	As características da habitação (escritórios, casas, refúgios); materiais de construção, portas, janelas, armários. Barreiras protetoras. Iluminação noturna.
Escritórios e lugares abertos ao público	Seus escritórios são abertos ao público? Há áreas reservadas unicamente ao pessoal? Você trata com desconhecidos que vêm a seus escritórios?.
Lugares de esconderijo, rotas de fuga	Existe algum lugar para se esconder? São acessíveis (distância física) e para quem? (para pessoas específicas ou para o grupo inteiro)? Você poderia sair momentaneamente do lugar se fosse necessário?
Acesso à zona	Que dificuldades podem encontrar os visitantes de fora (funcionários do governo, ONGs, etc.) para chegar à zona? (no caso de uma vizinhança perigosa, por exemplo) Que dificuldades de acesso têm os atores que geram ameaças?
Transporte e alojamento	Existe algum acesso a transporte seguro (público ou privado) para os defensores? Estes transportes representam alguma vantagem ou desvantagem particular? Dispõem os defensores de um alojamento seguro durante seus deslocamentos?
Comunicação	Existem sistemas de telecomunicações (rádio, telefone)? Dispõem os defensores de um bom acesso a estes meios? Funcionam corretamente o tempo todo? Poderiam os atores ameaçadores cortá-los antes de um possível ataque?
Componentes relacionados com conflito	
Vínculos com as partes em conflito	Existe algum vínculo entre os defensores e as partes em conflito (parentes, vêm da mesma zona, interesses comuns) que possa ser utilizado injustamente contra os defensores?
Atividades dos defensores que afetam a uma parte no conflito	O trabalho dos defensores afeta de forma direta aos interesses de algum ator? (Como por exemplo no caso da proteção de recursos naturais valiosos, o direito à propriedade) Você trabalha em algum assunto delicado para os atores com poder? (como por exemplo de novo, o direito à propriedade da terra).

Transporte de objetos e mercadorias e informação escrita	Possuem os defensores objetos ou mercadorias que possam ser valiosos para os grupos armados, e que portanto aumentem o risco de *targeting* ou de roubo? (Gasolina, ajuda humanitária, pilhas, manuais de saúde, etc.) Têm os defensores que levar consigo informação escrita sensível ou comprometedora?
Conhecimento sobre zonas de combate e zonas minadas	Possuem algum tipo de informação sobre o que se passa em zonas de combate que possa causar algum risco? E sobre possíveis zonas seguras para contribuir com sua segurança? Você tem informação confiável sobre as zonas minadas?
Componentes relacionados ao sistema jurídico e político	
Acesso às autoridades e a um sistema jurídico para reclamar seus direitos	Podem os defensores iniciar um procedimento legal para reclamar seus direitos? (Acesso a uma representação legal, presença física em julgamentos ou reuniões, etc.) Podem os defensores obter uma assistência apropriada das autoridades frente a seu trabalho e suas necessidades de proteção?
Capacidade para obter resultados do sistema jurídico e das autoridades	Têm os defensores o direito a reclamar seus direitos? Ou estão sujeitos a leis internas repressivas? Podem adquirir suficiente poder/influência para fazer com que as autoridades registrem suas reclamações?
Registro, capacidade de manter a contabilidade e os critérios legais	São os defensores negados um registro legal, ou estão estes sujeitos a longos atrasos? Sua organização é capaz de manter a contabilidade em ordem, de acordo com os requerimentos legais nacionais? Você utiliza programas informáticos piratas?
Componentes relacionados à gestão de informação	
Fontes e precisão da informação	Possuem os defensores fontes de informação fidedignas nas quais basear suas acusações? Publicam os defensores informação precisa e seguindo métodos adequados?
Manter, enviar e receber informação	Podem os defensores guardar informação em um lugar seguro e de confiança? Poderia esta informação ser roubada? Está protegida de vírus e de *hackers*? Você pode enviar e receber informação de forma segura? Os defensores sabem fazer a diferença entre informação confidencial e secreta? Os defensores guardam com eles informação mesmo fora do horário de trabalho?
Ser testemunha ou possuir informação-chave	São os defensores testemunhas-chaves para apresentar queixa ou representações contra um ator com poder? Possuem os defensores informação única e relevante sobre um caso ou processo específicos?
Ter uma explicação coerente e aceitável sobre o trabalho e seus objetivos	Têm os defensores uma explicação clara, sustentável e coerente sobre seu trabalho e objetivos? Esta explicação é aceitável, ou pelo menos tolerável, por parte da maioria, ou de todos os atores? (em especial os atores armados) Estão todos os membros do grupo capacitados para proporcionar esta explicação quando alguém lhes solicite? (por exemplo num posto de controle).

Componentes sociais e organizativos	
Existência de uma estrutura de grupo	Está o grupo organizado ou estruturado de alguma forma? Proporciona esta estrutura um grau aceitável de coesão do grupo?
Habilidade de tomar decisões conjuntas	A estrutura do grupo é um reflexo de interesses particulares ou representa ao grupo inteiro (incluindo afiliados)? Quem assume as principais decisões e responsabilidades, uma única pessoa ou várias? Foram criados sistemas de emergência para a tomada de decisões e assunção de responsabilidades? Quão participativa é a tomada de decisões? A estrutura do grupo permite: a) tomada de decisões conjuntas e sua implementação, b) debater os temas em grupo, c) reuniões esporádicas e ineficientes, d) nenhuma das mencionadas acima?
Planos de segurança e procedimentos	Foram colocadas em funcionamento normas e procedimentos de segurança? Existe um bom conhecimento e apropriação dos procedimentos de segurança? As normas de segurança são cumpridas? (Para mais detalhes veja o Capítulo 1.8).
Gestão da segurança fora do âmbito laboral (família e tempo livre)	Como os defensores manejam seu tempo fora do trabalho (família e tempo livre)? O consumo de álcool e drogas representa grandes vulnerabilidades. As relações pessoais também podem converter-se em vulnerabilidades (ao mesmo tempo que podem ser vantagens). As famílias e os amigos estão envolvidos nas atividades do defensor, de que forma?
Condições trabalhistas	Todas as pessoas têm um contrato de trabalho adequado? Existe um fundo de emergência? E seguros?
Contratação de pessoal	Algum procedimento é seguido para a contratação de pessoal ou de membros? Existe algum plano de segurança apropriado para voluntários ocasionais (como os estudantes, por exemplo) ou os visitantes da organização?
Trabalhar com as pessoas ou com organizações conjuntas	O trabalho é direto com o público? Conhecem bem as pessoas? Trabalham conjuntamente com alguma organização como intermediária entre as pessoas?
Cuidar de testemunhas ou vítimas com as que trabalhamos	Avaliam os riscos das vítimas e testemunhas, etc., quando trabalham em casos concretos? Tomam medidas de segurança específicas quando os encontramos ou quando vêm ao escritório? Como reagem se recebem ameaças?
Vizinhos e ambiente social	Estão os defensores bem integrados socialmente na área local? Alguns grupos sociais consideram o trabalho dos defensores como algo bom ou nocivo? Estão os defensores rodeados de gente supostamente hostil (vizinhos que atuam como informantes, por exemplo)? Os vizinhos que apóiam o trabalho fazem parte do sistema de alerta do defensor?
Capacidade de mobilização	Podem os defensores mobilizar a população em atividades públicas?

Componentes relacionados ao impacto psicológico (grupo/indivíduos)	
Capacidade para administrar o estresse e o medo	As pessoas-chaves ou o grupo em conjunto confiam em seu próprio trabalho? Expressam os indivíduos sentimentos de unidade e de tarefa comum (tanto em palavras como em atos)? O nível de estresse afeta na comunicação e nas relações interpessoais? As pessoas têm acesso a apoio psicológico externo e/ou desenvolveram habilidades psicossociais internas?
Sentimentos de frustração ou de "sentir-se perseguido"	Os sentimentos de frustração ou perda de esperança são expressados claramente (tanto em palavras como em atos)?
Componentes relacionados a sociedade, cultura e religião	
Discriminação	São os defensores discriminados (tanto dentro quanto fora da organização) com base ao seu gênero, etnia, religião ou orientação sexual? Existe alguma confusão entre direitos humanos, sociais, econômicos, identidade, cultura e religião?
Componentes relacionados a recursos para o trabalho	
Habilidade de compreender o contexto e o risco do trabalho	Têm os defensores acesso a uma informação precisa de seu contexto de trabalho, dos atores envolvidos e de seus interesses? São os defensores capazes de processar esta informação e valorar as ameaças, as vulnerabilidades e as capacidades?
Capacidade para definir planos de atuação	Podem os defensores definir e, em particular, implementar planos de ação? Há exemplos anteriores disto?
Capacidade para obter conselho de fontes bem informadas	Pode o grupo obter conselho confiável? De fontes apropriadas? Pode o grupo decidir independentemente quais fontes utilizar?
Pessoal e carga de trabalho	O número de pessoas ou trabalhadores é proporcional à quantidade de trabalho existente? É possível organizar as visitas ao campo em equipes (de um mínimo de duas pessoas)?
Recursos financeiros	A organização dispõe de recursos financeiros suficientes para a segurança? Administram o dinheiro de uma forma segura?
Conhecimento de idiomas e regiões	Os defensores têm conhecimento dos idiomas necessários para trabalhar nesta zona? Conhecem bem a zona? (estradas, povoados, telefones públicos, centros de saúde, etc.)
Componentes relacionados a contatos nacionais e internacionais e aos meios de comunicação	
Acesso a redes nacionais e internacionais	Têm os defensores contatos nacionais e internacionais? Com delegações visitantes, embaixadas, outros governos, etc? Com líderes da comunidade, líderes religiosos, ou outros personagens influentes? Podem realizar ações urgentes através de outros grupos? Você tem acesso a determinadas organizações ou qualidade de membro que poderiam melhorar sua capacidade de proteção?
Acesso aos meios de comunicação e capacidade para obter resultados com eles	Têm os defensores acesso aos meios de comunicação (nacional, internacional)? E a outros meios de comunicação (meios de comunicação independentes)? Sabem os defensores como se relacionar com os meios de comunicação corretamente?

Uma balança de risco: outra maneira de compreender o risco

Uma balança é também útil para entender o conceito de risco: é algo que poderíamos chamar... um "riscômetro". Se colocarmos dois pesos com nossas ameaças e vulnerabilidades num dos pratos da balança, e outro peso com nossas capa-cidades no outro prato, veremos como nosso risco aumenta ou se reduz:

Fig. 1

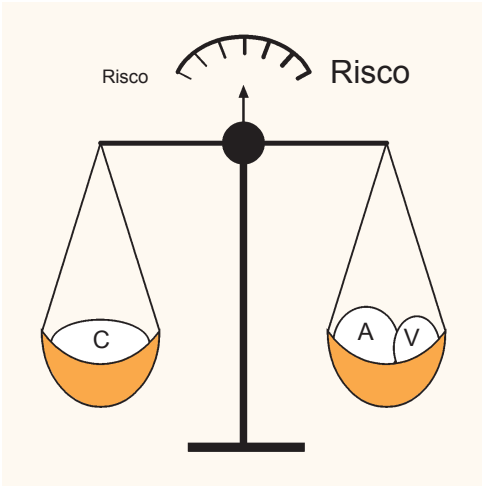
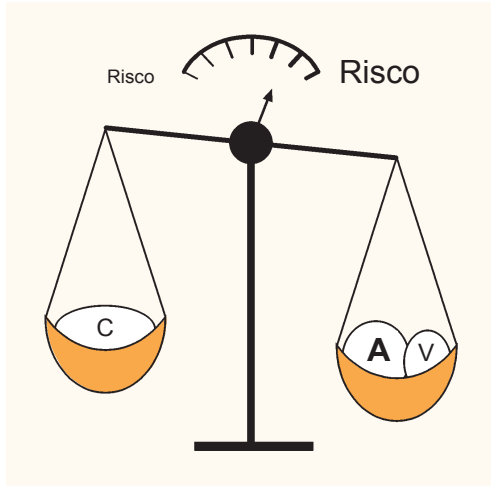
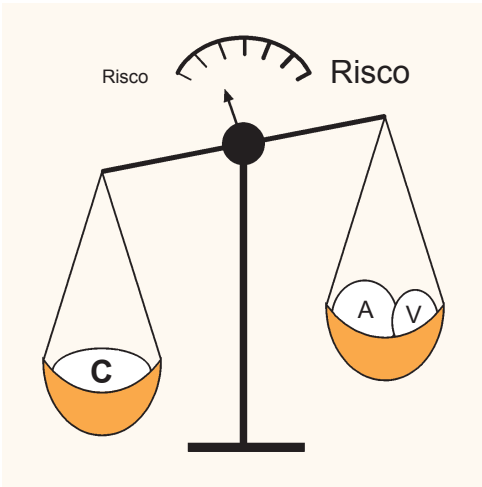


Fig. 2



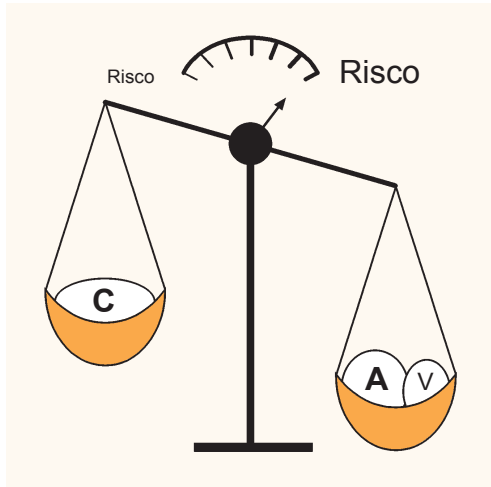
Quanto mais vulnerabilidades e ameaças temos, mais risco enfren-tamos.

Fig. 3



Quanto mais capacidades temos, menos risco enfrentaremos. E para reduzir o risco, também podemos reduzir nossas ameaças e vulnerabi-lidades, assim como aumentar nos-sas capacidades.

Fig. 4



Mas, vejamos o que acontece se enfrentamos ameaças grandes: não importa que tentemos aumentar nossas capacidades neste momento específico; a balança mostrará um alto nível de risco de qualquer forma!

Resumo

$$\text{RISCO} = \frac{\text{ameaças x vulnerabilidades}}{\text{capacidades}}$$

Vulnerabilidade e capacidades são variáveis internas (o defensor pode trabalhá-las).

Ameaças são variáveis externas (as ameaças podem ser feitas mesmo que não sejam factíveis).

1 • Trabalhar a respeito de vulnerabilidades e capacidades poderá resultar em menor possibilidade de que as ameaças se realizem. Faça uma lista de suas vulnerabilidades e capacidades. Discutir pode ajudar.

2 • Separe-as em componentes globais e, outra vez em componentes específicos.

3 • Defina suas capacidades ideais: trabalhe para alcançá-las e considere o processo necessário para tal. Na maioria das vezes o mesmo tipo de ações pode resolver vários itens de um mesmo componente.

3 • O resultado dos passos acima terá como impacto reduzir a possibilidade de uma ameaça e portanto reduzir risco.

Apesar de alguns componentes estarem ligados ao ambiente, componentes podem ser considerados variáveis internas sobre as quais o defensor pode trabalhar. Por exemplo, uma área perigosa é, obviamente, uma variável "externa" mas mesmo assim o defensor pode desenvolver habilidades ("internas") para lidar com isso.

Uma ameaça é externa e apesar de medidas dissuasivas o ameaçador pode ainda levá-la a cabo. O defensor pode "apenas" trabalhar para reduzir a probabilidade de que a ameaça seja efetivada e não necessariamente eliminá-la, a menos que o contexto político mude.

Conhecendo e avaliando ameaças

Objetivo:

Obter um conhecimento detalhado das ameaças e de como responder a elas.

Avaliação das ameaças: como entendê-las em profundidade

A repressão contra os defensores dos direitos humanos se baseia sobretudo na psicologia. As ameaças são uma moeda comum para fazer com que os defensores se sintam vulneráveis, ansiosos, confusos e impotentes. Em última instância, a repressão também pretende fragmentar as organizações e fazer com que os defensores percam a confiança em seus dirigentes e companheiros. Por isto os defensores devem ter muito cuidado para conseguir lidar com as ameaças ao mesmo tempo em que tentam manter uma adequada sensação de segurança no trabalho diário. Este é também o principal objetivo deste capítulo.

No Capítulo 1.2, definimos as ameaças como "a possibilidade de que alguém cause dano à integridade física ou moral ou à propriedade de outra pessoa através de uma ação intencionada e geralmente violenta". Também falamos sobre **possíveis** ameaças (**indiretas**) (quando um defensor próximo a seu trabalho é ameaçado e existem suspeitas críveis de que você poderia ser o próximo), e ameaças **declaradas** (**diretas**) (receber uma ameaça de morte, por exemplo). Agora veremos como lidar com as **ameaças declaradas**.

Uma ameaça declarada é uma **declaração ou o indício de uma intenção de infligir dano, castigar ou ferir, normalmente com a intenção de alcançar um objetivo**. Os defensores dos direitos humanos recebem ameaças devido ao impacto de seu trabalho, e a maioria das ameaças têm como objetivo paralisar o que o defensor esteja fazendo, ou forçá-lo/a a que faça algo (ou outra coisa).

Uma ameaça sempre tem uma **origem**, quer dizer, a pessoa ou grupo que foi afetado pelo trabalho do defensor e que articula a ameaça. A ameaça também tem um **objetivo** que está vinculado ao impacto do trabalho do defensor, e uma **forma de expressão**, isto é, como ela chega ao conhecimento do defensor.

As ameaças são complicadas. Poderíamos afirmar com certa ironia que as ameaças são "ecológicas", porque pretendem obter o maior resultado com a menor energia. Uma pessoa que ameaça decide ameaçar antes de entrar em ação – um maior uso de energia. Por quê? Existem várias razões, e vale à pena enumerá-las:

- A pessoa que ameaça tem a capacidade de atuar, mas o preocupa em certo modo o custo político de atuar abertamente contra um defensor dos direitos humanos. As ameaças anônimas podem ser feitas pela mesma razão.
- A pessoa que ameaça tem uma capacidade limitada de atuação e pretende lograr o mesmo objetivo, escondendo sua falta de capacidade atrás de uma ameaça. Esta capacidade limitada poderia ser somente temporal devido a outras prioridades, ou permanente, mas em ambos os casos, a situação poderia mudar e levar mais adiante a pessoa a realizar uma ação direta contra o defensor.

Uma ameaça é uma experiência pessoal, e sempre produz um efeito. Em outras palavras, as ameaças sempre afetam as pessoas de uma maneira ou outra. Numa ocasião, um defensor afirmou que "as ameaças conseguem exercer algum efeito, inclusive o simples fato de que estamos falando sobre elas". De fato, qualquer ameaça pode causar um impacto duplo: emocionalmente e em termos de segurança. Aqui nos concentraremos na segurança, mas não devemos esquecer o aspecto emocional de toda ameaça nem o impacto das emoções na segurança.

Sabemos que a ameaça está geralmente relacionada com o impacto de nosso trabalho. Portanto, a ameaça representa um indicador de como o trabalho do defensor está afetando a outra pessoa. Vista sob esta perspectiva, uma ameaça representa uma fonte de informação muito valiosa, e deveria ser analisada cuidadosamente.

"Fazer" uma ameaça ou "representar de fato" uma ameaça

São muitas as razões porque alguns indivíduos ameaçam os defensores de direitos humanos, e somente alguns têm a intenção ou capacidade de levar a termo uma ação violenta. Entretanto, alguns indivíduos podem supor uma séria ameaça sem nem sequer chegar a articulá-la de maneira concreta. Esta distinção entre *fazer* e *representar de fato* uma ameaça é importante:

- Algumas das pessoas que **fazem** uma ameaça **representam de fato**, ao final, uma ameaça;
- Muitas das pessoas que **fazem** ameaças **não representam** uma ameaça;
- Algumas pessoas que **nunca fazem** ameaças, estas sim, r**epresentam de fato** uma ameaça.

Uma ameaça apenas será crível se a pessoa que a faz tem a capacidade de atuar contra você: a ameaça deve mostrar um nível mínimo de força ou possuir um elemento ameaçador pensado para provocar o medo.

A pessoa que se esconde atrás de uma ameaça pode demonstrar sua capacidade de atuação muito facilmente, colocando, por exemplo, uma ameaça escrita no interior de um carro trancado, ainda que você o tenha deixado estacionado

apenas por alguns minutos; chamando-o justamente no momento em que acaba de chegar em casa, fazendo que você saiba que está sendo vigiado.

Podem também tentar assustá-lo, usando elementos simbólicos nas ameaças, enviando-lhe, por exemplo, um convite para seu próprio funeral ou colocando um animal morto na entrada de sua casa ou em sua cama.

Muitas ameaças representam uma combinação das características mencionadas. É importante poder distingui-las, porque algumas das pessoas que enviam ameaças fingem dispor da capacidade de agir utilizando elementos simbólicos que causam medo.

Qualquer pessoa pode fazer uma ameaça, mas nem todas supõem uma ameaça.

No fim das contas, o que é necessário saber é se a ameaça pode se concretizar. O enfoque será completamente diferente se você chegar à conclusão razoável de que a ameaça não é tão provável quanto você suspeita.

Por isto, os três objetivos principais na hora de avaliar uma ameaça são:

- Obter toda a informação possível da razão e origem da ameaça (ambos estarão relacionados com o impacto de seu trabalho);
- Alcançar uma conclusão racional sobre se a ameaça pode se concretizar ou não;
- Decidir o que fazer.

Cinco passos para avaliar uma ameaça

1 • **Determinar os fatos que rodeiam a (s) ameaça (s).** É importante saber o que ocorreu exatamente. Isto se pode saber mediante entrevistas ou interrogando pessoas-chaves, e até mesmo por meio de relatórios relevantes.

2 • **Determinar se existe um padrão de ameaças ao longo do tempo.** Se foram recebidas várias ameaças sucessivas (como é o caso habitual), é importante examinar os padrões, tais como os meios utilizados para ameaçar, o momento no qual as ameaças aparecem, os símbolos, a informação passada por escrito ou verbalmente, etc. Nem sempre é possível estabelecer tais padrões, mas são importantes na hora de realizar uma boa avaliação da ameaça.

3 • **Determinar o propósito da ameaça.** Tendo em vista que a ameaça freqüentemente tem um claro propósito relacionado com o impacto do trabalho, é possível que seguindo o fio condutor deste impacto seja possível estabelecer o que se pretende conseguir com a ameaça.

4 • **Determinar quem está por trás da ameaça.** (Para isto é necessário ter seguido previamente os três primeiros passos.) É preciso tentar ser o mais específico possível e distinguir entre o autor moral e o agente. Por exemplo, pode-se dizer que é "o governo" quem está ameaçando. Mas, tendo em conta que todos os governos são atores complexos, seria conveniente descobrir que parte do governo está por trás das ameaças. As "forças de segurança" ou os "grupos guerrilheiros" são também atores complexos. É preciso recordar que também uma ameaça assinada pode ser falsa: esta poderia ser uma boa tática por parte de quem ameaça para evitar os custos políticos e ainda conseguir, de toda maneira, o objetivo de provocar medo num defensor e tentar impedir que ele/ela continue seu trabalho.

5 • **Chegar a uma conclusão racional sobre se a ameaça pode ou não se concretizar.** A violência é condicionante. Nunca se pode estar completamente seguro se uma ameaça se concretizará ou não. Fazer previsões sobre violência é o mesmo que dizer que numa determinada circunstância existe um risco específico de que uma certa pessoa ou grupo agirá/rão de forma violenta contra um alvo pré-selecionado.

Os defensores não são "adivinhadores" e não podem pretender saber o que vai acontecer. Todavia, é possível poder chegar a uma conclusão racional, se uma ameaça em concreto poderia ser levada a termo. Pode ser que não haja informação suficiente sobre a ameaça por meio dos quatro passos prévios e, assim, não seja possível chegar a uma conclusão. Também é possível chegar a diferentes conclusões sobre a definição de uma ameaça "real". Em todo caso, é preciso agir, tendo como referência o pior cenário.

Por exemplo:

Um defensor de direitos humanos recebeu várias ameaças de morte. O grupo analisa as ameaças e chega a duas conclusões opostas, ambas baseadas em boas informações. Alguns opinam que a ameaça é completamente falsa, enquanto outros vêem alguns sinais preocupantes sobre sua gravidade. Ao final da reunião, o grupo decide pautar-se pelo pior dos casos, isto é, considerar que a ameaça é possível, e tomar as medidas de segurança necessárias.

Esta avaliação de ameaça passa de fatos sólidos (passo número 1) a um raciocínio cada vez mais especulativo; o segundo passo (passo 2) requer uma interpretação dos fatos, o que nos leva aos passos 3, 4 e 5. Existem bons motivos para seguir a ordem dos passos. Se passássemos diretamente do segundo ao quarto passo, por exemplo, perderíamos a informação mais sólida proveniente dos passos anteriores.

Acompanhamento e encerramento de um caso de ameaça

Uma ameaça ou incidente de segurança podem gerar alarme no grupo de defensores, mas geralmente é difícil manter esta percepção de alarme até que a ameaça ceda realmente. Tendo em conta a constante pressão externa a que estão submetidos os defensores por seu trabalho, se a organização fizesse soar o alarme com muita freqüência, o grupo perderia o interesse e baixaria a guarda.

Apenas se deve acionar o alarme de um grupo quando existirem evidências inequívocas e isso deveria se destinar a prevenir um possível ataque. O alarme serve, portanto, para motivar os membros do grupo a atuar, e exigir que se realize uma serie de ações específicas. Para ser efetivo, um alarme deveria somente estimular a motivação a um nível moderado: um nível muito baixo não ativa a reação das pessoas e um nível muito alto cria uma sobrecarga emocional. Caso a ameaça se prolongue ao longo do tempo, é primordial, uma vez ativado o alarme inicial, fazer um debriefing com as pessoas e o seguimento necessário da ameaça para corrigir informações erradas, alterar recomendações mal orientadas, e reforçar a confiança do grupo quando for necessário.

Para finalizar, caso a ameaça não se materialize, é necessário proporcionar algum tipo de explicação da razão, e o grupo deve ser informado quando a ameaça diminuir ou desaparecer por completo.

Um caso de ameaça pode encerrar-se quando se avalie que o atacante potencial já não se supõe uma ameaça. Antes de fechar um caso, e para assegurar-se de estarem certos, é preciso comprovar primeiro se é possível explicar o porquê de se encerrar de fato o caso. Também é preciso se perguntar quais possíveis circunstâncias poderiam levar o indivíduo ou ator responsável pelas ameaças a repeti-las ou concretizá-las com um ataque direto.

Reação das ameaças em relação à segurança

- Uma ameaça pode ser considerada como um incidente de segurança. Para maior informação sobre como responder aos incidentes de segurança, veja o Capítulo 1.4.
- Após a avaliação de ameaças declaradas, se você avalia que ainda corre o risco de ser atacado, veja o Capítulo 1.5, sobre a prevenção de ataques.

Resumo

As ameaças podem ser incidentais, diretas (declaradas) e indiretas (não declaradas).

Uma ameaça declarada é uma declaração ou indicação de intenção de fazer algo contra alguém.

Cinco passos ajudarão a determinar a viabilidade de uma ameaça para decidir o que fazer:

1. Determine os fatos
2. Determine o padrão ao longo do tempo
3. Determine o objetivo
4. Determine a fonte
5. Tire uma conclusão pensada e sensata sobre a viabilidade da ameaça.

Evite conclusões instantâneas "óbvias" e tente ser tão específico quanto possível, abrindo cenários conforme os fatos e padrões indicam e também para desenvolvê-los tanto quanto possa substanciá-los.

Incidentes de segurança: definição e análise

Objetivo:

Learning how to recognise and respond to security incidents.

O que é um incidente de segurança?

Para simplificar, um incidente de segurança poderia ser definido como **qualquer fato ou evento que você acredite que poderia afetar sua segurança pessoal ou a segurança de sua organização**.

Os incidentes de segurança podem ser incidentais ou provocados intencionalmente ou de maneira involuntária.

Os incidentes de segurança podem consistir, por exemplo, em ver o mesmo veículo suspeito estacionado em frente a seu escritório ou sua casa durante vários dias; que o telefone toque à noite e ninguém responda, que alguém esteja fazendo perguntas sobre você numa cidade ou povoado vizinho, um furto em sua casa, etc.

Mas, nem tudo representa um incidente de segurança. Por isto, é preciso **registrá-lo**, tomando nota do fato, para logo **analisá-lo**, se possível, com companheiros, e poder estabelecer se realmente poderia afetar a sua segurança. Ao chegar a este ponto, você poderá **reagir** ao incidente. A seqüência de eventos é a seguinte:

> Você detecta algo ⇨ se dá conta de que poderia se tratar de um incidente de segurança ⇨ registra-o / compartilha-o ⇨ analisa-o ⇨ estabelece que se trata de um incidente de segurança ⇨ reage de maneira apropriada.

If the matter is pressing, this sequence should still take place, just much more quickly than usual to avoid delay (see below).

Como distinguir os incidentes de segurança das ameaças:

Se você está esperando um ônibus e a pessoa ao lado o ameaça por causa de seu trabalho, isto – à parte de ser uma ameaça – constitui um incidente de

segurança. Mas se você descobre que um carro de polícia está vigiando seu escritório desde o outro lado da rua, ou roubam seu celular, estes são incidentes de segurança, mas não necessariamente ameaças. Mesmo que incidentes de segurança possam ser claramente diferenciados de ameaças (por exemplo, estar em uma multidão ou perder a chave), lembre que incidentes de segurança provocados intencionalmente tem um objetivo que pode ser distinto de uma ameaça (veja o capítulo 1.1). O objetivo mínimo de um incidente de segurança provocado intencionalmente é recolher informação sobre o defensor mesmo se isso poderá ser usado contra ele posteriormente.

Fazer uma clara distinção é importante pelo menos para a saúde mental do defensor.

Todas as ameaças são incidentes de segurança mas nem todos os incidentes de segurança são ameaça.

Por que os incidentes de segurança são tão importantes?

Os incidentes de segurança são cruciais na hora de lidar com sua segurança porque **proporcionam uma informação vital sobre o impacto que seu trabalho está gerando, e sobre a possível ação que poderia ser planejada ou realizada contra você**. Ao mesmo tempo, este tipo de incidentes lhes permitem mudar sua conduta ou atividades e evitar lugares que poderiam ser perigosos, ou mais perigosos do que o normal. Os incidentes de segurança podem, assim, ser considerados como indicadores da situação de segurança de um local. Se você não detecta estas mudanças, seria difícil reagir apropriadamente e a tempo para manter-se seguro.

Por exemplo: após detectar certos incidentes de segurança você poderia deduzir que está sob vigilância; então já pode atuar a respeito da vigilância.

Os incidentes de segurança representam "a unidade mínima" das medidas de segurança e indicam a resistência/pressão contra seu trabalho. Não permita que passem despercebidos!

Quando e como se detectam os incidentes de segurança?

Dependerá de quão óbvios sejam os incidentes. Se eles passam facilmente despercebidos, a capacidade para detectá-los dependerá da formação e experiência em segurança e do nível de conscientização sobre eles.

Quanto maior conscientização e formação, menor será o número de incidentes que escaparão de sua atenção.

Às vezes, os incidentes de segurança passam inadvertidos ou reparamos neles brevemente, para logo os deixarmos de lado, ou às vezes, reagimos exageradamente ante algo que percebemos como um incidente de segurança.

Por que um incidente de segurança poderia passar despercebido?

Um exemplo:

Um defensor percebe um incidente de segurança, mas a organização onde trabalha não reage em absoluto. Isto poderia ser devido a que…

- o defensor não está consciente de que ocorreu um incidente de segurança;
- o defensor está consciente deste fato, mas o descarta por sua pouca importância;
- o defensor não informou a organização (ou se esqueceu, ou não acreditou, ou achou que não fosse necessário, ou decidiu não comentar porque teria ocorrido por causa de um erro de sua parte);
- o defensor anotou e registrou os incidentes, mas a organização, após fazer uma avaliação em conjunto do incidente, não considera necessário reagir.

Por que, às vezes, reagimos exageradamente aos incidentes de segurança?

Por exemplo:

Um/uma colega poderia constantemente contar histórias sobre incidentes de segurança, mas ao examiná-los detalhadamente, não parecem ter nenhum fundamento nem serem merecedores de consideração. Neste caso, na realidade, o incidente de segurança é o fato de que seu colega tenha um problema que faz com que veja incidentes de segurança inexistentes. Pode ser que tenha muito medo, ou que esteja estressado/a, e neste caso, deveriam oferecer-lhe ajuda para resolver o problema.

Não nos esqueçamos que é freqüente que os incidentes de segurança passem despercebidos ou sejam descartados: tenhamos cuidado com isto!

Como fazer frente aos incidentes de segurança

Existem várias formas de lidar rapidamente com um incidente de segurança. Os passos seguintes têm em consideração o momento e o tipo de incidente a partir do momento em que se anuncia um incidente de segurança, enquanto está ocorrendo, e uma vez concluído.

Para lidar com um possível incidente de segurança, podemos seguir três passos básicos:

1 • **Registrá-lo.** Todo incidente de segurança detectado por um defensor deve ser registrado, mesmo que numa simples caderneta pessoal, ou num caderno disponível para todo o grupo.

2 • **Analisá-lo.** Todos os incidentes de segurança registrados devem ser devidamente analisados, imediatamente ou regularmente. É preferível

analisá-los em equipe do que individualmente, porque assim se minimiza o risco de passar por cima de algo. Deve ser designado, ainda, alguém com a responsabilidade para garantir que estas análises sejam efetivamente realizadas.

Devem ser tomadas decisões sobre manter ou não a confidencialidade de certos incidentes (tais como ameaças, por exemplo). É ético e razoável esconder informação sobre uma ameaça de colegas e outras pessoas com quem trabalho? Não existe uma regra única aplicável a todas as situações, mas em geral, é preferível ser o mais transparente possível na hora de compartilhar informação e de lidar com as preocupações, assim como os medos.

3 • **Reagir.** Os incidentes de segurança oferecem informação sobre o impacto do trabalho, por isso deveriam gerar:

- uma reação ao próprio incidente;
- **retro-alimentação**, em termos de segurança, ao menos em três níveis (do concreto para o mais geral): sobre nossos **planos** de trabalho, e sobre nossas **estratégiase**:

EXEMPLO

de um incidente que proporciona **retro-alimentação** sobre como trabalhar com mais segurança:

É a terceira vez que alguém de sua organização tem problemas ao passar por um controle policial, porque, com freqüência, esquece os documentos necessários. Portanto, decidem criar uma lista que deverá ser consultada por todos os trabalhadores antes de sair da cidade. Também poderiam decidir mudar o trajeto neste tipo de viagem.

EXEMPLO

de um incidente que proporciona retro-alimentação no âmbito do **planejamento** de segurança:

No mesmo controle policial, você é detido durante meia hora e é informado que seu trabalho é mal visto. Dissimuladamente, deixam escapar algumas ameaças. Quando você se dirige à sala da polícia, exigindo uma explicação, repete-se a mesma cena. Você organiza uma reunião do grupo para revisar seus planos de trabalho, porque parece evidente que é necessário realizar algumas mudanças para poder prosseguir com o trabalho. Na seqüência, você organiza uma série de reuniões com funcionários do Ministério da Justiça (ou Ministério do Interior), muda alguns aspectos de seus planos e organiza reuniões semanais para ir supervisionando a situação.

EXEMPLO

de um incidente que proporciona retro-alimentação sobre as **estratégias** de segurança:

Pouco tempo depois de começar a trabalhar como defensor numa nova área, você recebe ameaças de morte e um de seus colegas é agredido fisicamente. Não estava previsto este tipo de oposição a seu trabalho, nem mesmo você havia diagnosticado em sua estratégia global. Portanto, você deverá mudar sua estratégia para tentar gerar um consentimento local para com seu trabalho e impedir mais ataques e ameaças. Para isto, talvez você deva suspender seu trabalho por um tempo, retirar-se da área e reconsiderar todo o projeto.

Reagir *urgentemente* a um incidente de segurança

Existem muitos modos de responder imediatamente a um incidente de segurança. Os seguintes passos foram formulados em função de quando e como reagir desde o momento em que se anuncia um incidente de segurança, enquanto está ocorrendo, e uma vez concluídor.

Passo 1: Informar sobre o incidente:

- O que ocorre/ocorreu? (tente focar nos fatos registrados).
- Onde e quando ocorreu?
- Quem está envolvido? (no caso de que você tenha provas e possa determiná-las).
- A pessoa ou propriedade sofreu algum tipo de dano ou prejuízo?

Passo 2. Decidir quando reagir. Há três possibilidades:

- Uma **reação imediata** é necessária quando é preciso atender a pessoas feridas ou interromper um ataque em curso.
- Uma **reação rápida** (nas horas e dias seguintes) é necessária quando é preciso prevenir que surjam novos possíveis incidentes (o incidente em si já passou).
- Uma **ação de seguimento** (em vários dias, semanas ou inclusive meses): se a situação se estabilizou, talvez não seja necessária uma reação nem imediata nem rápida, mas de seguimento. Da mesma forma, também qualquer incidente de segurança que tenha requerido uma reação imediata ou rápida deverá ser observado por meio de uma ação de seguimento para conservar nosso espaço de trabalho ou revisar nosso contexto de atuação.

Passo 3. Decidir como reagir e quais são seus objetivos.

- Se a reação deve ser imediata, os objetivos são claros: atender aos feridos ou interromper o ataque.

- Se a reação deve ser rápida, os objetivos deverão ser estabelecidos pela pessoa encarregada ou a equipe de crise (ou algo similar) e deverá **centrar-se em restaurar a segurança necessária para os afetados pelo incidente.**

As ações/reações posteriores se realizarão seguindo os canais habituais da organização para a tomada de decisões, com o objetivo de restaurar um ambiente de trabalho seguro, assim como de restabelecer os procedimentos organizativos internos e melhorar as reações posteriores em relação aos incidentes de seguranças.

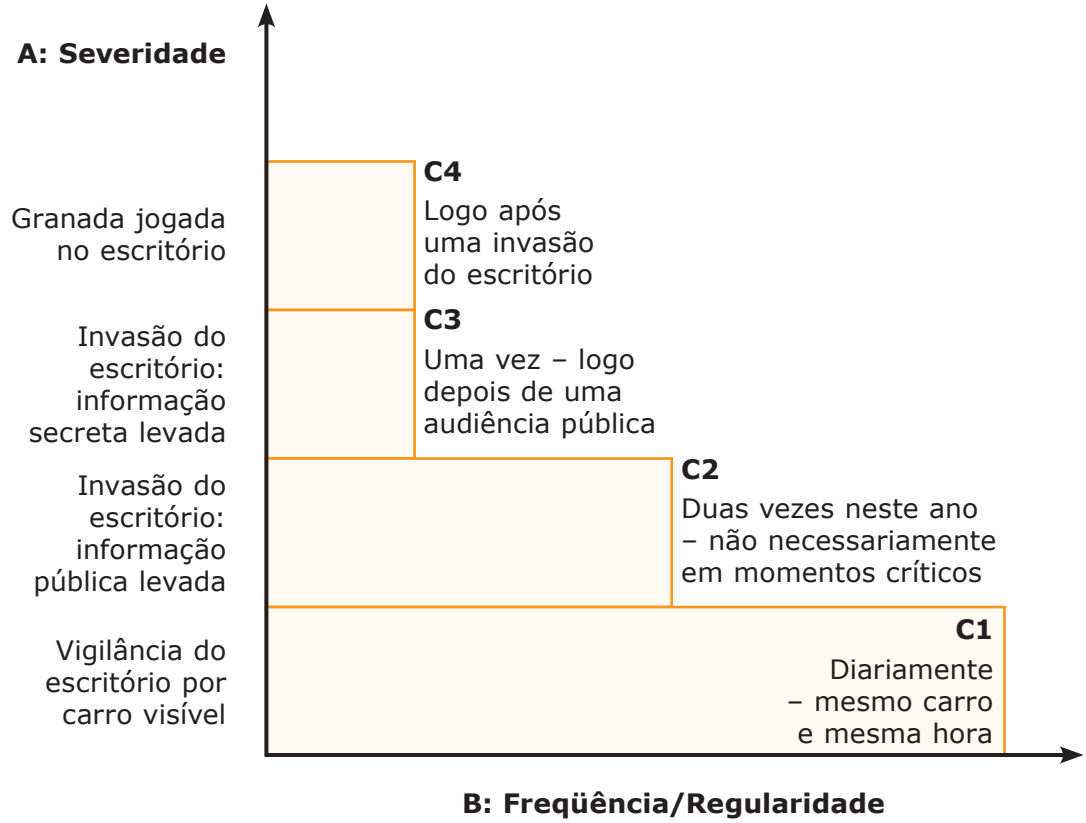
Toda reação deve também ter presente a segurança e proteção de outras pessoas, organizações ou instituições com as quais mantenhamos uma relação de trabalho (e possam se ver afetados.

Estabeleça seus objetivos antes de começar a atuar. A rapidez da ação é importante, mas saber porque relizar esta ação é mais importante ainda. Ao estabelecer de de antemão o que você pretende atingir (objetivo), você poderá decidir como quer atingi-lo (tática a seguir).

Por exemplo:

Se um grupo de defensores descobre que um de seus colegas não chegou ao seu destino numa cidade segundo o planejado, poderiam iniciar uma reação ligando para o hospital, para seus contatos com outras ONGs, a um Escritório da ONU mais próximo e para a polícia. Mas antes de iniciar estas chamadas, é muito importante determinar o que se pretende conseguir e o que se decidirá. Caso contrário, poderiam gerar um alarme desnecessário (imaginemos que o defensor se atrasou porque perdeu o ônibus ou se esqueceu de ligar para o escritório) ou uma reação oposta à pretendida.

Registrar incidentes de segurança (e ameaças) ajuda a analisá-los da perspectiva de anteciparmos a eles em momentos específicos. Por exemplo, se o livro indica incidentes de segurança em momentos pré-eleitorais, é possível que no próximo período pré-eleitoral ocorra outro incidente. O registro também nos ajuda a avaliar a probabilidade de uma ação contra o defensor por parte do agressor em potencial, ou no caso de incidentes de segurança devido ao descaso do defensor, isso contribuirá par avaliar como a segurança é gerida pelos defensores.



C: Probabilidade iminente de ações mais severas contra os defensores por parte do potencial agressor.

C1: MUITO BAIXO: (A1: vigilância do escritório por carro visível + B1: mesmo carro à mesma hora diariamente).

C2: BAIXO: (A2: Invasão do escritório: informação pública levada + B2: duas vezes neste ano, não em momentos críticost).

C3: ALTO: (A3: Invasão do escritório: informação secreta levada (nomes de test-emunhas secretas levado) + B3: uma vez antes de uma audiência pública).

C4: MUITO ALTO: (A4: Granada jogada no escritório + B4: Logo após uma invasão C3).

(...)

Resumo

Um incidente de segurança é qualquer fato ou evento que você pense possa afetar sua segurança pessoal ou a de sua organização.

Incidentes de segurança podem ser incidentais ou provocados intencionalmente ou não.

Incidentes de segurança medem a segurança e o impacto do trabalho do defensor de direitos humanos em relação a outros interesses.

Todos os defensores têm incidentes de segurança. O contrário implicaria que:

- O impacto do trabalho do defensor é insignificante porque não é feito corretamente ou porque o interesse de ninguém é afetado. Em outras palavras: ninguém está interessado.

- O potencial agressor já possui toda a informação que necessita sobre o defensor e não se incomoda: o defensor não foi capaz de perceber os incidentes de segurança (vigilância, informação recolhida de outra forma...).

Um incidente de segurança não é uma ameaça, mas requer atenção.

Três passos para lidar com incidentes de segurança:

1 • Registre-os

2 • Analise-os

3 • Reaja a eles

CAPÍTULO 1.5

Prevenir e reagir a ataques

Objetivo:

Avaliar a possibilidade de que diferentes tipos de ataque se tornem realidade.

Prevenir os possíveis ataques diretos contra defensores.

Realizar contra vigilância.

Ataques contra os defensores dos direitos humanos

Violência é um processo assim como um ato. Uma agressão violenta contra um defensor não ocorre no vácuo. Uma análise cuidadosa de agressões geralmente mostra que elas são a culminação de conflitos, disputas, ameaças, incidentes de segurança e erros que podem ser identificados ao longo do tempo.

Os ataques contra defensores são produto de, ao menos, três fatores que interagem entre si:

1 • **O indivíduo que leva a termo uma ação violenta e os meios**. Os ataques contra os defensores geralmente são produto de processos de pensamento e de condutas que podemos decifrar para aprender com eles, ainda que sejam ilegítimos. O agressor terá de utilizar-se de meios ao menos para recolher informação (incidentes de segurança) sobre o defensor alvo.

2 • **Antecedentes e fatores desencadeadores que levam o atacante a considerar a violência como uma opção**. A maioria dos indivíduos que atacam os defensores considera a ação de atacar como uma forma de "conseguir um objetivo" ou de "resolver um problema". A impunidade e/ou vontade de pagar o custo político como "valendo a pena".

3 • **O contexto e circunstâncias** that facilitates violence, allows it to take place or does not stop it. A quick way to and away the HRD.

Quem representa, então, um perigo para os defensores?

No geral, qualquer indivíduo (ou grupo) que pense que atacar um defensor é uma forma tentadora, aceitável, ou potencialmente efetiva de conseguir um objetivo pode ser considerado um agressor em potencial. A ameaça aumenta se quem considera o ataque também possui, ou ainda pode desenvolver, a capacidade de atacar um defensor.

A ameaça de um ataque pode diminuir se...
Surgem mudanças na capacidade potencial do agressor para organizar um ataque, muda sua atitude em relação a quão aceitável é um ataque, ou aumentam as probabilidades de ser capturado/a e punido/a.

Alguns ataques vêm precedidos por ameaças. Outros não. Entretanto, geralmente os indivíduos que planejam um ataque violento demonstram suas intenções em sua conduta, posto que necessitam averiguar o melhor momento para atacar, planejar como alcançar o alvo, e como escapar.

Portanto, é fundamental detectar e analisar qualquer sinal que indique um possível ataque. Isto requer:

- Determinar a possibilidade de que se leve a termo uma ameaça (veja o capítulo 1.3);
- Identificar e analisar os incidentes de segurança.

Os incidentes de segurança que demonstram a vigilância dos defensores ou de seu lugar de trabalho são destinados a obter informação. Esta informação nem sempre é recolhida com a intenção de ser utilizada num ataque, mas é importante determinar isso. (veja o Capítulo 1.4) Vigilância pode ser usada para vários fins:

- Estabelecer que atividades estão sendo realizadas, quando e com/por quem;
- Utilizar esta informação mais adiante para atacar a pessoas ou organizações;
- Obter a informação necessária para levar a termo um ataque;
- Recolher informação para fazer uma acusação na Justiça ou outro tipo de medida coativa (sem violência direta);
- Intimidar-nos ou intimidar os colaboradores ou outras pessoas com as que trabalhamos.

É importante recordar que a vigilância costuma ser necessária para levar a cabo um ataque, mas que não constitui por si mesma um ataque. Além disso, nem toda a vigilância implica num ataque posterior. Entretanto, por outro lado, em algumas ocasiões, um indivíduo pode improvisar um ataque quando, de repente, vê uma oportunidade para isto, ainda que inclusive nestes casos costuma haver um mínimo de preparação prévia.

Não há muita informação disponível que possa ajudá-lo a reconhecer a fase de preparação de um ataque. A ausência de estudos sobre este tema contrasta enormemente com o grande número de ataques contra defensores. No entanto, os estudos existentes trazem interessantes revelações.[1]

♦ **Atacar um defensor não é fácil e requer recursos.** A vigilância é necessária na hora de estabelecer os movimentos de um indivíduo e o melhor momento para atacar. Acertar o alvo e escapar de forma efetiva e rápida é também primordial (mas se o ambiente é altamente favorável para o agressor, isto lhe resultará mais simples realizar os ataques).

♦ **Quem ataca os defensores geralmente demonstra certo grau de consistência.** A maioria dos ataques é dirigida a defensores muito envolvidos em temas que afetam os agressores. Isto quer dizer que os ataques freqüentemente não são casuais ou sem objetivo, mas respondem aos interesses dos agressores.

♦ **Os fatores geográficos são importantes.** No geral, os ataques a defensores em zonas rurais não se divulgam tanto e, em conseqüência, provocam menos reações na aplicação da lei e em nível político do que os ataques a defensores de zonas urbanas. Os ataques em zonas urbanas contra escritórios de ONGs ou contra organizações destacadas geram uma reação muito maior.

♦ **Escolhas e decisões são tomadas antes de uma agressão.** Os indivíduos que pretendem atacar uma organização de defensores devem decidir se vão atacar os líderes ou os membros da base, ou escolher entre um único ataque (contra uma pessoa chave importante o que, por sua vez, gera um maior custo político) ou uma série de ataques (que afetem os membros da organização). Os poucos estudos realizados a respeito sugerem que em geral são utilizadas ambas as estratégias.

Estabelecer a viabilidade de um ataque

Para poder averiguar a viabilidade de que um ataque seja realizado, devemos analisar os fatores relevantes. Para poder determinar quais são estes fatores, devemos distinguir os diferentes tipos de ataques, isto é, os ataques diretos (targeting), a delinqüência comum e os ataques indiretos (estar no lugar errado na hora errada), fazendo uso dos três quadros das páginas seguintes.[2]

1 Claudia Samayoa e Jose Cruz (Guatemala) e Jaime Prieto (Colômbia) realizaram estudos interessantes sobre ataques contra defensores dos direitos humanos. Mahony e Eguren (1997) também realizaram uma análise destes ataques.

2 Esta classificação de ataques inclui as mesmas categorias de ameaças: veja o capítulo sobre ameaças para mais informação.

Quadro 1: Determinar a probabilidade de um ataque direto (targeting)

(**AP** = Agressores Potenciais)

Probabilidade de ataques diretos (Targeting)			
Fatores	Probabilidade baixa	Probabilidade média	Probabilidade alta
Capacidade de ataque	Os AP possuem uma capacidade limitada para atuar nas áreas onde trabalhamos	Os AP possuem capacidade operacional próxima das áreas onde trabalhamos	As zonas onde trabalhamos estão sob controle dos AP
Meio financeiro	Os AP não necessitam de nosso material ou dinheiro para suas atividades	Interesse em nosso material, dinheiro ou outras práticas de ganância econômica (o seqüestro, por exemplo)	Os AP têm uma necessidade manifesta de material ou dinheiro
Meio político ou militar	Nenhum – nosso trabalho não tem nada a ver com seus objetivos	Interesse parcial – nosso trabalho limita seus objetivos políticos ou militares	Nosso trabalho obstaculiza claramente seus objetivos, beneficia os seus oponentes, etc
Antecedentes de ataques prévios	Nenhum ou excepcional	Casos ocasionais	Muitos casos prévios
Atitudes ou intenções	Atitude favorável ou indiferente	Indiferente. Ameaças ocasionais. Avisos freqüentes.	Agressiva, com ameaças claras e vigentes
Capacidade das forças de segurança de impedir ataques	Existente	Baixa	Nenhuma, ou as forças de segurança colaboram com os AP (ou são os AP)
Nosso grau de influência política contra os AP	Bom	Médio ou baixo	Limitado (de acordo com circunstâncias) ou nenhum

Exemplo

de uma avaliação do grau de probabilidade de um ataque direto (targeting):

Os AP controlam as zonas onde trabalhamos, mas não têm nenhum motivo econômico para nos atacar. Nosso trabalho apenas limita seus objetivos políticos e militares parcialmente, e não existem precedentes de ataques similares na cidade. Sua atitude é indiferente, e é evidente que não querem atrair nenhuma atenção nacional ou internacional, nem pressão alguma atacando-nos.

Neste caso consideraríamos o grau de probabilidade de ataque direto como baixo ou médio.

Quadro 2: Determinar a probabilidade de um crime de agressão

(**C** = Criminosos)

Probabilidade de crime de agressão			
Fatores	Probabilidade baixa	Probabilidade média	Probabilidade alta
Mobilidade e localização dos C	Os C geralmente permanecem em suas próprias áreas, fora das nossas áreas de trabalho	Os C freqüentemente transitam em outras áreas à noite (ou operam próximo de onde trabalhamos)	Os C atuam em qualquer parte, tanto de dia como de noite
Agressividade dos C	Os C evitam enfrentamentos (cometem crimes majoritariamente onde não há a presença de defensores ou testemunhas)	Os C cometem crimes na rua (mas não em escritórios com pessoal)	Os C roubam abertamente na rua e entram em lugares fechados
Acesso a/uso de armas	Desarmados, ou uso de armas não letais	Armas rudimentares, inclusive facões	Armas de fogo, às vezes de grande porte
Tamanho e organização	Operam individualmente ou em pares	2-4 pessoas operam juntas	Operam em grupos
Resposta e contenção policial	Resposta rápida, com capacidade de dissuasão	Resposta lenta, pouco êxito capturando criminosos em ação	A polícia não responde nem com a menor efetividade
Formação e profissionalismo das forças de segurança	Bem formadas e profissionais (podem faltar recursos)	Formação regular, salário baixo, recursos limitados	A polícia é inexistente ou corrupta (colabora com os delinqüentes)
Situação geral de segurança	A situação é segura ou relativamente segura	Falta de segurança	Não se observam os direitos, impunidade absoluta

Exemplo

de uma avaliação da probabilidade de um crime:

Nesta cidade, os criminosos operam em várias regiões, em pares ou em pequenos grupos, às vezes durante o dia. Geralmente são agressivos e com freqüência portam armas. A polícia responde, mas é lenta e ineficaz, com formação pouco profissional e com falta de recursos. Entretanto, o delegado de polícia é muito disciplinado. Existe uma falta geral de segurança, e se aplicarmos esta análise aos bairros mais longínquos da cidade, a probabilidade da ocorrência de um crime encontra seu ponto mais alto, já que **todos** *os indicadores demonstram um nível elevado de criminalidade.*

A probabilidade de um ataque criminoso no centro de uma cidade como esta é de média a alta.

Quadro 3: Determinar a possibilidade de um ataque incidental (indireto)

(**AP** = Agressores Potenciais)

Probabilidade de um ataque incidental			
Fatores	Probabilidade baixa	Probabilidade média	Probabilidade alta
Nosso conhecimento das áreas de combate	Bom	Médio	Temos muito pouco conhecimento sobre a localização das áreas de combate
Proximidade das áreas de combate	Nosso trabalho está longe destas áreas	Nosso trabalho está próximo destas áreas e ocasionalmente se entra nelas	Nosso trabalho se realiza nas áreas de combate
Mobilidade das áreas de combate	As áreas de conflito são estáticas ou variam de forma lenta e verificável	Variam bastante	Variam continuamente, o que as torna imprevisíveis
Nosso conhecimento da localização de zonas minadas	Possuímos um bom conhecimento ou não existem zonas minadas	Conhecimento aproximado	Desconhecidas
Proximidade de nosso lugar de trabalho das zonas minadas	O trabalho se realiza longe destas zonas ou são inexistentes	Trabalhamos próximos destas zonas	Nosso trabalho se realiza em áreas em que há campos minados
Táticas de combate e armas utilizadas	Discriminadas	Discriminadas, com uso ocasional de artilharia, emboscadas e franco-atiradores	Indiscriminadas: bombardeio, artilharia pesada, ataques terroristas ou ataques com bombas

Exemplo

de uma avaliação da probabilidade ataques indiretos:

Nesta região, você está familiarizado com as áreas de combate, que variam de forma lenta e previsível. Você trabalha próximo das áreas onde ocorrem enfrentamentos e, ocasionalmente, visita ou fica nas áreas de combate. Você não está próximo de zonas minadas. As táticas de combate usadas são discriminadas e portanto geralmente não afetam os civis.

Trabalhar nesta zona representa uma probabilidade baixa de uma agressão indireta.

Prevenir uma possível agressão direta ou indireta

Apesar de o defensor ser um alvo em ambos os casos, vamos distinguir entre:

- agressão (ataque) direto contra o defensor.
- agressão indireta contra o defensor quando a situação envolve alguém próximo ao defensor.

Em ambos os casos prevenir um ataque requer uma lógica própria.

Agora já sabemos que uma ameaça pode diminuir se surgem mudanças na capacidade potencial do atacante para organizar um ataque, em sua atitude em relação ao que considera aceitável para uma agressão ou nas probabilidades de ser capturado e punido.

Em ambos os casos prevenir um ataque requer uma lógica própria:

- Persuadir um atacante potencial de que uma agressão implica em custos e conseqüências inaceitáveis.
- Fazê-lo entender que uma agressão é menos factível na realidade.

Este raciocínio para prevenir ataques é paralelo à análise do Capítulo 1.2, que demonstrava que o risco depende das vulnerabilidades e capacidades do defensor. Este raciocínio também argumenta que, para poder se proteger e poder reduzir o risco, é necessário atuar contra a ameaça, reduzir vulnerabilidades e aumentar capacidades.

Quando alguém é objeto de uma ameaça e quer reduzir o risco associado a ela, é importante atuar, não somente contra a própria ameaça, mas também sobre as **vulnerabilidades** e **capacidades** mais proximamente vinculadas à ameaça. Quando estamos submetidos a grandes pressões e queremos atuar com maior rapidez, em geral atuamos em relação às vulnerabilidades de fácil solução ou as mais acessíveis, em vez de atuarmos sobre as mais relevantes para a ameaça em questão.

Tenha Cuidado: se o risco de ataque é elevado (quer dizer, se a ameaça é iminente, e você tem várias vulnerabilidades e poucas capacidades), não há sentido em se concentrar nas vulnerabilidades ou capacidades para reduzir o risco, porque alterá-las e efetivá-las requer tempo. Se o risco é muito elevado (quando um ataque direto e severo é iminente) apenas é possível evitá-lo de três modos:

a • Confrontando a ameaça com rapidez e efetividade, se se sabe que pode conseguir um resultado imediato e específico que prevenirá o ataque. (Normalmente é muito difícil estar certo de que se obterá um resultado imediato e efetivo, porque as reações requerem seu tempo, e o tempo é muito valioso nestes casos).

b • Procurar não se expor em absoluto (por exemplo, se escondendo ou abandonando a região temporariamente[3]).

3 Há também situações nas quais viajar representa uma situação de risco maior.

c • Solicitar proteção! Veja dois exemplos que podem ser efetivos, dependendo do contexto: :

- Proteção da comunidade: se você se esconde ou recebe refúgio em uma comunidade, a visibilidade e testemunhas presentes podem conter o agressor potencial.

- Proteção armada: pode ser útil de alguma forma em alguns poucos casos, mas presumindo-se, para tanto, que seja disponível (imediata), e que isto poderia dissuadir o suposto agressor e não aumentar o perigo da situação do defensor em médio e longo prazo. Na prática, é muito difícil que se cumpram estes três requisitos para proteção armada. Em alguns casos, após uma pressão nacional ou internacional, o Governo decide oferecer escoltas armadas ao defensor: nestes casos, aceitar ou recusar a escolta poderia determinar o grau de responsabilidade estatal na segurança dos defensores, mas ainda que o defensor não aceite as escoltas armadas, um Governo não pode sob nenhuma hipótese declarar-se isento de suas obrigações. As empresas privadas de segurança podem representar um risco maior se estiverem vinculadas aos agressores.[4] No que se refere à posse de armas por parte dos defensores, devemos mencionar que elas geralmente são ineficientes na hipótese de ataque organizado, e além disso podem colocar os defensores numa situação de vulnerabilidade visto que o Governo poderia utilizar este fato como justificativa para atacá-los sob o pretexto de luta antiterrorista ou insurgência. Além disso, o fato de o defensor carregar armas poderia ser distorcido contra ele/a como uma contradição à Declaração sobre Defensores de Direitos Humanos da ONU.

É muito mais fácil lidar com as situações de ameaça que podem levar a um ataque quando outros atores relevantes se envolvem e trabalham conjuntamente, por exemplo, com um sistema judicial operativo; redes de apoio (nacionais e internacionais) que possam pressionar as autoridades responsáveis; redes sociais (dentro das organizações ou entre elas), redes pessoais e de familiares, ONU/forças internacionais de paz, etc.

Vigilância e contra-vigilância

A **contra-vigilância** pode ajudá-lo a determinar se você está sendo vigiado. É difícil descobrir se seus sistemas de comunicação foram grampeados, e por esta razão você deve presumir que sempre o são[5]. Entretanto, é possível determinar se alguém vigia seus escritórios e seus movimentos.

Quem poderia estar vigiando?

Pessoas que freqüentemente podem estar localizadas na sua região, como porteiros de edifícios, vendedores que trabalham perto da entrada do edifício, pessoas em veículos próximos, visitas, etc., poderiam potencialmente estar vigiando

4 Para mais informação, veja o Capítulo "Melhorando a segurança em casa e no trabalho".
5 Para mais informação, veja o Capítulo sobre segurança nas comunicações.

seus movimentos. Há pessoas que espiam por dinheiro, ou porque são pressionadas para fazê-lo; por suas inclinações, ou devido a uma combinação destes fatores. Os responsáveis pela vigilância podem também colocar colaboradores ou membros de sua organização para fazer este serviço.

Você também pode ser vigiado de longe. Normalmente, são membros de uma organização que praticam a tática de tentar vigiar sem serem vistos. Isto requer manter uma certa distância, alternar-se com outras pessoas por turnos e observar a partir de diferentes lugares, utilizando diferentes veículos, etc.

Como certificar-se de que você está sob vigilância

Você pode averiguar se está sob vigilância, observando aqueles que poderiam estar vigiando-o, e adotando as seguintes regras (sem, evidentemente, cair em paranóia):

- Se você suspeita que alguém poderia estar vigiando-o, você deveria prestar atenção na atividade de pessoas de sua área e em mudanças em suas condutas como, por exemplo, alguém que começa a fazer perguntas sobre suas atividades. Lembre que podem ser tanto homens como mulheres, ou ainda idosos e jovens.

- Se você suspeita que estão seguindo-o, você poderia iniciar uma medida de contra-vigilância que envolva uma terceira pessoa de confiança, desconhecida para aqueles que poderiam estar vigiando. A terceira pessoa poderia observar, à frente e a partir de uma boa distância, os movimentos que se produzem quando você chega, sai ou se dirige a algum lugar. A pessoa que está vigiando provavelmente o faz a partir de um lugar onde possa localizá-lo facilmente, incluindo sua casa, o escritório e os lugares onde você costuma trabalhar.

Por exemplo

Antes de chegar em casa, você poderia pedir a um membro da família ou a um vizinho de confiança que tome uma posição próxima (por exemplo, trocando o pneu do carro), para comprovar se alguém está à espera de sua chegada. Você poderia fazer o mesmo quando sai do escritório a pé. Se você usa um veículo particular, deverá deixar que saia outro carro depois do seu, para dar tempo ao suposto observador para que se aproxime.

A vantagem da contra-vigilância é que, ao menos inicialmente, a pessoa que observa não perceberá que está sendo vigiada. Portanto, você deve deixar claro a toda pessoa envolvida na contra-vigilância que não é recomendável enfrentar a pessoa que o observa. Desta forma, saberiam que você está sabendo de suas atividades, e isto poderia desencadear uma reação violenta. É importante ser extremamente cuidadoso e manter uma distância quando suspeitar que alguém o está vigiando. Uma vez detectada a vigilância, pode ser colocada em funcionamento a ação recomendada neste manual.[6]

6 Veja o Capítulo "Melhorando a segurança em casa e no trabalho".

A maioria de nossos conselhos sobre a contra-vigilância faz referência, de forma quase exclusiva, a zonas urbanas e semi-urbanas. Nas zonas rurais, a situação é muito diferente, porque os defensores e as comunidades que vivem nestas zonas estão mais acostumados a detectar a presença de estranhos. Portanto, a pessoa que queira vigiá-lo numa zona rural, terá mais dificuldades para aproximar-se dos habitantes - a não ser que a população local seja muito hostil a seu trabalho.

Nota: há situações nas quais pode ser vantajoso estabelecer uma relação com as forças de segurança que o monitoram. Às vezes a vigilância não é tão secreta, e se exterioriza com o objetivo de intimidar. Em algumas ocasiões, os defensores estabelecem relações com pessoas das forças de segurança para que os avisem quando se planeja vigiá-los ou inclusive levar a cabo uma ação contra eles.

Quando verificar se você está sendo vigiado

É recomendável verificar se você está sendo vigiado quando tenha alguma razão para suspeitar – por exemplo, por incidentes de segurança que poderiam estar relacionados com a vigilância. Se seu trabalho de direitos humanos traz um certo risco, é aconselhável organizar, de vez em quando, uma simples ação de contra-vigilância, apenas por via das dúvidas.

Você também deve pensar no risco que representa para os demais quando está sendo vigiado – você pode supor um maior risco para uma testemunha ou um familiar de uma vítima que você visite, do que para si mesmo. Pense sobre onde seria mais seguro vê-los. Talvez você precise avisá-los que seus movimentos estão sendo vigiados.

Reagir aos ataques

Não existe uma regra única aplicável a todos os ataques contra defensores. Os ataques também são incidentes de segurança, e você encontrará as opções de como reagir aos incidentes de segurança no Capítulo 1.4.

In any kind of aggression there are two essential things to remember:

- Pense sempre na segurança – tanto durante o ataque como **depois**. (se você está sendo atacado e tem duas possíveis alternativas, opte pela mais segura!).

- Após um ataque, você deverá se recuperar física e psicologicamente, atuar para resolver a situação, e tentar restaurar um ambiente de trabalho seguro para você e sua organização. É importante que você mantenha a maior quantidade de informação possível sobre o ataque: o que ocorreu, quem/quantas pessoas estavam envolvidas, placas dos veículos, descrições, etc. Tudo isso pode ser útil para documentar o caso, e deve ser anotado o quanto antes. Conserve cópias de todos os documentos que você apresente às autoridades para documentar o caso.

Resumo

Ataques são o fim de processos que incluem incidentes de segurança e talvez ameaças.

Ataques não são eventos "inesperados".

Ataques podem ser incidentais (indiretos) ou diretos (targeting).

Não é fácil atacar defensores de direitos humanos pois eles são figuras públicas e possuem algum tipo de apoio.

Ataques são o produto de três fatores que interagem entre si:

- O ator que realiza a ação violenta e possui os meios para tal.
- Antecedentes e fatores desencadeadores que levam o atacante a considerar a violência como uma opção.
- O contexto e as circunstâncias.

Uma agressão requer recursos adequados e capacidades, acesso ao indivíduo, uma fuga rápida e um certo nível de impunidade, ou a decisão por parte do agressor de pagar o custo político do ataque.

Assim, prevenir ataques requer ações tanto para manter o custo político tão alto quanto possível (reduzir o nível de impunidade) e reduzir a exposição física do defensor ao risco de ataque próximo a zero.

Elaborando uma estratégia global de segurança

Objetivos:

Reconhecer estratégias e táticas já em funcionamento.

Analisar estratégias e táticas em funcionamento.

Definir uma estratégia global para ocupar o espaço de trabalho.

Estratégia e táticas de dissuasão ad hoc

Defensores e grupos sob ameaça usam diferentes estratégias de dissuasão para lidar com os riscos. Estas estratégias variam muito dependendo do ambiente (rural, urbano), do tipo de ameaça, dos recursos sociais, financeiros e legais disponíveis, etc.

A maior parte das estratégias ad hoc, ou aleatórias, podem ser implementadas imediatamente e em resposta a objetivos de curto prazo. Elas funcionarão, portanto, mais como táticas do que como estratégias globais de resposta. Muitas estratégias também respondem a percepções subjetivas de risco, e podem às vezes causar algum tipo de dano ao grupo, especialmente se a estratégia não pode ser revertida.

Estratégias ad hoc são relacionadas com o tipo e gravidade da ameaça e às capacidades e vulnerabilidades do grupo.

Quando pensamos sobre segurança e proteção devemos levar em consideração tanto nossa estratégia quanto a de outras pessoas. Reitere as estratégias efetivas, tente limitar as danosas e respeite as remanescentes (sobretudo estratégias ad hoc ligadas a crenças culturais ou religiosas).

Algumas estratégias ad hoc adotadas por defensores de direitos humanos:

- Reforçar barreiras protetoras, esconder objetos de valor.
- Evitar comportamentos que podem ser questionados por outro ator, especialmente se o território onde você trabalha faz parte de uma disputa militar.
- Esconder-se durante situações de alto risco, incluindo em lugares de difícil acesso, como montanhas ou a selva, mudar de casas, etc. Algumas vezes famílias inteiras se escondem, e algumas vezes apenas o/a defensor/a. Esconder-se pode ocorrer à noite ou durar várias semanas, e pode envolver nenhum contato com o exterior.
- Buscar proteção armada ou política de um dos atores do conflito armado.
- Suspender atividades, fechar o escritório, evacuar. Migrações forçadas (deslocados internos ou refugiados) ou ir para o exílio.
- Confiar na "boa sorte" ou recorrer a crenças religiosas ou "mágicas".
- Tornar-se mais reservado, incluindo com os colegas; negar a existência de ameaças ao não discuti-las, consumo excessivo de álcool, trabalho excessivo, comportamento errático.

Defensores também têm acesso a estratégias de resposta. Estas incluem a publicação de relatórios tornando públicas questões específicas, fazendo alegações, realizando demonstrações, etc. Em muitos casos, estas estratégias não representam um plano de longo prazo, mas respondem a necessidades de curto prazo. Em alguns casos as estratégias de resposta podem até mesmo criar mais problemas de segurança do que aqueles que a resposta tentava resolver.

Analisando estratégias de dissuasão

Tanto para estratégias globais quanto para medidas ad hoc de dissuasão, leve os seguintes elementos em consideração:

- **Responsividade**: Sua estratégia responderá rapidamente a necessidades de segurança individuais ou de grupo?
- **Adaptabilidade**: Suas estratégias serão rapidamente adaptáveis a novas circunstâncias quando o risco de ataque diminuir? Um defensor pode ter várias opções disponíveis, por exemplo tanto esconder-se ou morar na casa de outras pessoas por algum tempo. Tais estratégias podem parecer fracas ou instáveis, mas oferecem grande duração.
- **Sustentabilidade**: Pode a sua estratégia durar ao longo do tempo, apesar de ameaças ou ataques não letais?
- **Efetividade**: Suas estratégias protegerão adequadamente as pessoas ou grupos afetados?

♦ **Reversibilidade**: Se suas estratégias não funcionarem ou se a situação mudar, elas podem ser revertidas e/ou modificadas?

Administrando o risco após uma análise de risco

Uma vez que sua análise de risco foi feita, você precisará olhar para os resultados. Assim como é possível medir a quantidade de risco que você está enfrentando, você pode compreender também qual é o **nível** do risco.

Diferentes defensores e organizações podem perceber diferentes níveis de risco. O que é inaceitável por alguns defensores pode ser aceitável para outros, mesmo dentro da mesma organização. Melhor do que discutir o que "deve" ser feito ou se você está preparado para seguir adiante, os limites das pessoas ao risco devem ser debatidos: você deve encontrar um limite aceitável entre todos os membros do grupo.

Dito isto, há diferentes maneiras de lidar com risco:

- Você pode **aceitar** o risco como ele se encontra, porque você sente que pode viver assim.
- Você pode **reduzir** o risco ao trabalhar sobre as ameaças, vulnerabilidades e capacidades.
- Você pode **compartilhar** o risco, ao realizar ações conjuntas com outros defensores para fazer ameaças potenciais a um defensor ou organização menos efetivos.
- Você pode **protelar** o risco, ao mudar suas atividades ou mudar as abordagens para reduzir ameaças potenciais.
- Você pode **escapar** do risco ao reduzir ou parar suas atividades (em alguns casos isso representaria sua saída do país).
- Você pode **ignorar** o risco, fechando os olhos. Não é preciso dizer que está não é a melhor opção.

Lembre-se de que o nível de risco é geralmente diferente para cada organização ou indivíduo trabalhando num caso direitos humanos, e mesmo os agressores geralmente tendem a atacar a parte mais fraca.

Por exemplo:

Vejamos o caso de um agricultor morto pela milícia privada de um proprietário rural. Talvez várias organizações e indivíduos estejam envolvidos, tal como um grupo de advogados da capital mais próxima, um sindicato rural e três testemunhas (camponeses que moram numa vila próxima). É crucial avaliar os diferentes níveis de risco de cada um destes atores de modo a planejar corretamente a segurança de cada um.

Resumo

Quando a questão é segurança, os defensores não começam do zero. Eles desenvolveram modos de lidar com riscos e ameaças. O contrário poderia implicar que eles já não estão vivos ou que deixaram seu trabalho.

Os defensores ao menos desenvolveram estratégias e táticas aleatórias, ou ad hoc. Alguns podem também ter elaborado estratégias globais de dissuasão.

Qualquer que seja a estratégia, elas precisam responder ao menos aos seguintes critérios: responsividade, adaptabilidade, sustentabilidade, efetividade e reversibilidade.

Uma avaliação de risco deve ser realizada para determinar se este é "aceitável". Caso contrário, o defensor poderá ter de reduzir, compartilhar, protelar ou escapar do risco.

Os defensores dos direitos humanos que trabalham em ambientes hostis

Com freqüência defensores de direitos humanos trabalham em ambientes hostis. São muitos os motivos. A maioria dos casos é devida ao possível enfrentamento que suscita seu trabalho contra atores poderosos que violam as normas internacionais de direitos humanos, tanto autoridades governamentais ou estatais, forças de segurança, grupos armados de oposição ou milícias armadas privadas. Esses atores podem realizar todo tipo de represálias para tentar fazer com que os defensores parem com seu trabalho, desde uma repressão sutil com ataques contra a liberdade de expressão, até ameaças declaradas e ataques diretos. O grau de tolerância do ator dependerá do trabalho do defensor - algumas atividades podem ser consideradas aceitáveis, outras não. Esta incerteza é, com freqüência, também proposital.

Ao chegarmos neste ponto, devemos fazer duas reflexões importantes: em muitos casos, somente são hostis ao defensor certos componentes **integrantes** dos atores complexos. Por exemplo, alguns dos componentes integrantes de um governo podem estar relativamente preocupados com a proteção dos defensores, ao passo que outros componentes querem atacá-los. Os defensores podem também experimentar uma maior hostilidade durante momentos de agitação política, tais como eleições ou outros eventos políticos.

O espaço sócio-político de atuação dos defensores

O presente manual está dirigido à proteção e segurança dos defensores dos direitos humanos que trabalham em ambientes hostis e as medidas para melhorar esta segurança. Existem também outras ações sócio-políticas que podem ser aplicadas para melhorar o respeito aos direitos humanos: as campanhas e atividades de promoção dos defensores com freqüência estão destinadas a assegurar uma aceitação mais ampla dos direitos humanos na sociedade e obter

ações mais efetivas por parte das autoridades para assegurar a proteção dos direitos humanos. Apesar de não podermos relacionar este tipo de atividades com a segurança, quando elas são efetivas podem causar um impacto positivo na proteção do **espaço sócio-político de atuação** dos defensores.

Este espaço sócio-político de atuação pode ser definido como a **variedade de possíveis ações que pode realizar o defensor expondo-se a um risco pessoal aceitável**. Em outras palavras, o defensor contempla "una ampla variedade de possíveis ações políticas e associa cada ação a um custo específico ou a um conjunto de conseqüências". O defensor considera alguma destas conseqüências "aceitáveis e outras inaceitáveis, definindo assim os limites de um espaço político específico"[1].

Por exemplo:

> *Um grupo de defensores poderia estar defendendo um caso sobre direitos humanos, quando um dos membros recebe uma ameaça de morte. Se consideram que têm suficiente espaço sócio-político, talvez optem por fazer pública a ameaça, e continuar mais tarde com o caso. Mas se consideram que seu espaço político é limitado, talvez decidam que a divulgação da ameaça representa custos inaceitáveis. Talvez, inclusive, optem por deixar o caso por um tempo e melhorar, neste período, suas capacidades de segurança.*

A noção do risco "aceitável" pode mudar com o tempo e varia enormemente entre diferentes indivíduos ou organizações. Para alguns, o risco mais insuportável seria o de tortura ou morte de um familiar. Alguns defensores opinam que a prisão é um risco aceitável, sempre e quando contribui para alcançar os objetivos. Outros alcançam seu limite quando recebem a primeira ameaça.

Este espaço político de atuação não somente vem definido de forma subjetiva pelos defensores, mas também é muito sensível a mudanças do ambiente político nacional que os rodeia. Portanto, devemos considerá-lo como um espaço relativo e mutante.

A segurança e o espaço de atuação do defensor

Podemos resumir todas as estratégias de segurança em poucas palavras: expandir o espaço de atuação e mantê-lo assim. Se falamos em termos estritos de segurança, o espaço de trabalho do defensor requer pelo menos um grau mínimo de tolerância por parte dos principais atores da região – especialmente por parte das autoridades políticas e militares e dos grupos armados que podem ser afetados pelo trabalho dos defensores e que poderiam, portanto, atuar contra eles.

Esta tolerância pode ser **explícita**, como uma permissão formal das autoridades, ou **implícita**, como por exemplo, no caso dos grupos armados. A tolerância será

1 Esta definição, assim como outras partes fundamentais deste conceito, foram tomadas de Mahony e Eguren (1997), p. 93. Eles também desenvolveram um modelo de espaço político que integra o espaço laboral dos defensores com seu acompanhamento protetor.

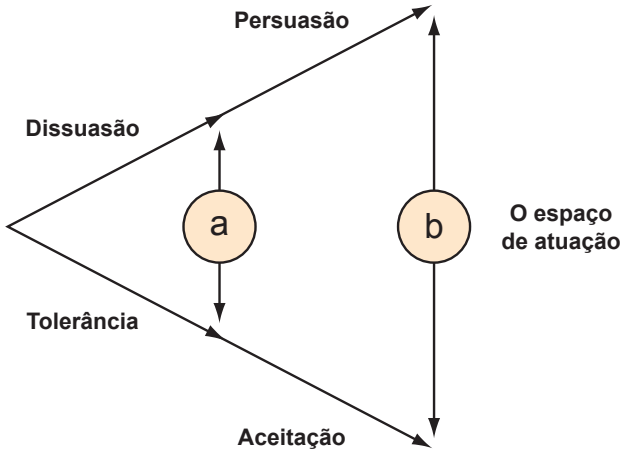
mais alta se o ator vê que o trabalho do defensor pode trazer algum benefício, e será mais baixa se o ator detecta custos relacionados com o trabalho do defensor. Neste caso, seu grau de tolerância dependerá dos custos políticos que representará atacar os defensores.

Tudo isso é relevante sobretudo em conflitos armados onde os defensores enfrentam a mais de um ator armado: um ator parte no conflito poderia considerar o trabalho dos defensores vantajoso para seu oponente. A aceitação manifesta de um ator poderia, portanto, motivar a hostilidade de seu oponente.

O espaço de atuação dos defensores pode ser representado em dos eixos:

- um eixo representa o grau de tolerância ou aceitação do ator frente ao trabalho do defensor, baseando-se no impacto que possa causar tal trabalho aos objetivos ou interesses estratégicos do ator (o contínuo "tolerância-aceitação").

- outro eixo representa em que medida se pode dissuadir os ataques, baseando-se nos custos políticos de um ataque, os quais aumentam de acordo com a probabilidade de dissuadir o ator com argumentos racionais/morais ou, inclusive, com as vantagens políticas que obtém ao não atacar nem violar os direitos humanos (o contínuo "dissuasão-persuasão").



Com o tempo, pode-se conseguir uma expansão do espaço de atuação. Para se conseguir a aceitação do trabalho do defensor, por meio de uma estratégia de persuasão, é necessário ter em conta as necessidades da população, a imagem, procedimentos e a integração do defensor, etc., representados no espaço "b". Mas, nas regiões de conflito armado, o espaço geralmente se limita unicamente à tolerância dos atores armados, que será parcialmente determinada pelos custos que eles supõem existir ao atacarem os defensores (dissuasão), reduzindo assim o espaço a "a".

Geralmente, o espaço "b" é mais habitado por defensores não contenciosos do que pode defensores que denunciam abusos abertamente. A menos que o agressor seja convencido e persuadido sobre quão benéfico é o trabalho do defensor e acabe aceitando-o.

Estratégia global de segurança

- Expandir sua área de trabalho aumentando a tolerância e aceitação.
- Expandir sua área de trabalho aumentando a dissuasão e persuasão.

Definir e implementar uma estratégia global de segurança contribuirá para aumentar o custo político das ações contra defensores de direitos humanos e reduzirá o nível de impunidade de um potencial agressor ao ampliar a área de atuação dos defensores. Conseqüentemente, a estratégia global de segurança se baseia em grande medida em ações de incidência (lobby).

Expandir o espaço de atuação mediante o aumento da tolerância e aceitação

O trabalho dos defensores poderia afetar os objetivos ou interesses estratégicos de alguém que não está muito interessado em direitos humanos, o que causaria um ambiente hostil para os defensores. Para ganhar a aceitação, ou pelo menos mais tolerância com relação ao trabalho dos defensores, é importante, em seu trabalho, reduzir a confrontação na medida do possível. Algumas sugestões sobre como fazê-lo:

■ **Fornecer informação e formação sobre a natureza e legitimidade do trabalho dos defensores.** Os funcionários governamentais e outros atores poderiam estar mais inclinados a cooperar se conhecessem e compreendessem o trabalho e as razões pelas quais os defensores o realizam. Não basta manter informados aos altos cargos, porque o trabalho diário dos defensores geralmente abarca uma grande variedade de funcionários pertencentes a diversos órgãos governamentais. É preciso realizar um esforço contínuo para informar e formar os funcionários de todos os níveis.

■ **Esclarecer os objetivos do trabalho dos defensores.** Em todos os conflitos, é recomendável esclarecer e limitar o alcance e os objetivos do trabalho. Desta forma, reduzir-se-ão os mal-entendidos ou enfrentamentos desnecessários que impedem, muitas vezes, que os defensores alcancem seus objetivos.

■ **Limitar os objetivos de trabalho para ajustar-se ao espaço sócio-político.** Se o trabalho dos defensores afeta os interesses estratégicos de um ator armado em concreto, este poderia reagir com uma maior violência e uma menor consideração por sua imagem. Certos tipos de trabalho tornam os defensores mais vulneráveis que outros, assim, é preciso assegurar-se de que os objetivos se ajustam da melhor maneira possível à valoração de risco e às capacidades de proteção.

■ **Conceder um espaço nas estratégias para "salvar a cara".** Se é preciso enfrentar um ator poderoso, pode ser útil buscar a maneira pela qual o ator possa "resguardar sua imagem", quando finalmente ele venha a tomar medidas sobre a situação de direitos humanos.

■ **Estabelecer alianças** de forma ampla, com tantos setores sociais quanto seja possível.

■ **Buscar um ponto médio** entre a transparência no trabalho, que demonstre que os defensores não têm nada a esconder, e a proteção da informação que possa comprometer o trabalho ou a segurança.

■ **Finalmente,** recordemos que a legitimidade e a qualidade do trabalho são condições imprescindíveis para manter o espaço de atuação aberto, mas podem ser insuficientes, e talvez também seja necessário dissuadir os agressores potenciais (veja mais informação abaixo).

Expandir o espaço de atuação mediante dissuasão e persuasão

Os defensores dos direitos humanos que trabalham em ambientes hostis devem ser capazes de gerar custos políticos suficientes para dissuadir um agressor de tentar um ataque: isto é o que denominamos **dissuasão**.

Resulta prático saber distinguir entre a dissuasão "geral" e a dissuasão "imediata". A **dissuasão geral** consiste no efeito combinado de todos os esforços nacionais e internacionais para proteger os defensores, isto é, tudo o que contribuirá para criar uma convicção geral de que os ataques contra os defensores são inaceitáveis e têm conseqüências negativas. Para isto, você pode recorrer a amplas campanhas de imprensa, ou à formação e informação sobre a proteção dos defensores. Por outro lado, a dissuasão imediata envia uma mensagem concreta a um agressor determinado para o dissuadir de ataques a um alvo específico. A **dissuasão imediata** é necessária quando a dissuasão geral falha ou resulta insuficiente, e quando os esforços de proteção se centram em casos específicos.

A **persuasão** é um conceito mais amplo. Poderia ser definido como o resultado dos atos que induzem um oponente a não levar a termo uma ação hostil previamente considerada. O argumento racional, ou reclamo moral, um aumento de cooperação, uma melhora da compreensão humana, a distração, a adoção de políticas não ofensivas e a prevenção, todos poderiam ser utilizados para se obter a persuasão. Os defensores utilizam todas estas táticas no âmbito nacional ou internacional em diferentes situações. Evidentemente, os defensores não podem utilizar as "ameaças" diretas muito freqüentemente: a estratégia se baseia, sobretudo, em recordar aos demais que as decisões que tomem **poderiam** gerar uma série de conseqüências.

Colocando a dissuasão em marcha

Para poder medir se a dissuasão foi efetiva, é necessário cumprir com uma série de requisitost:

1 ♦ **Os defensores devem especificar e comunicar claramente ao agressor que tipo de ações são inaceitáveis.** A dissuasão não funciona se o agressor desconhece as ações que provocarão uma resposta.

2 ♦ **A organização dos defensores deve expressar seu compromisso em dissuadir o ator de realizar a agressão, de forma que este esteja consciente disso.** A organização também deve estabelecer uma estratégia para conseguir tal dissuasão.

3 ♦ **A organização dos defensores dever ser capaz de implementar a estratégia de dissuasão, e assegurar-se de que o agressor é consciente disso.** Se uma ameaça de mobilização nacional ou internacional não é crível, não existe nenhuma razão para esperar que tenha um efeito protetor.

4 ♦ **Os defensores devem saber quem é o agressor.** Os grupos de ataque costumam trabalhar na obscuridade da noite e raramente assumem a responsabilidade. Portanto, nos vemos obrigados a analisar quem poderia sair beneficiado com o ataque. Em caso de suspeita de "responsabilidade estatal", ainda que ela seja correta, deverá ser acompanhada de informação mais específica sobre que parte do poder estatal se esconde atrás do ataque para poder, assim, melhorar a efetividade de uma reação nacional ou internacional.

5 ♦ **O agressor deve ter considerado seriamente o ataque e depois ter decidido não o fazer** porque os custos – graças ao compromisso dos defensores – poderiam ser maiores que os benefícios.

É difícil que os defensores consigam persuadir um agressor que não se vê em absoluto afetado por argumentos de dissuasão: isso acontece quando a comunidade internacional pode punir os governos, mas estes não podem punir o ator violador dos direitos humanos. Por exemplo, os exércitos privados ou milícias poderiam estar fora do alcance do governo ou não compartilhar seus interesses. Nestes casos, o agressor poderia, inclusive, beneficiar-se de atacar os defensores dos direitos humanos, porque os ataques colocariam o governo numa posição difícil e danificariam sua imagem.

Os defensores nunca saberão com antecipação se seu "compromisso de dissuasão" é suficientemente forte para dissuadir um possível ataque. O agressor poderia estar na expectativa de obter benefícios que os defensores ignoram. Avaliar a situação de forma detalhada representa um constante desafio e poderia, inclusive, resultar impossível devido à falta de informação básica. As organizações de defensores devem, portanto, desenvolver planos de emergência muito flexíveis e sua habilidade de responder com rapidez a acontecimentos inesperados.

Tabela: Prevenir um ataque direto – diferentes resultados protetores

Prevenir um ataque direto: Diferentes resultados de proteção	
1 Mudanças no comportamento do agressor: dissuasão do agressor através de aumento do custo potencial de uma agressão. →	**Confrontando** e **reduzindo ameaças** (agindo diretamente contra a fonte, ou contra qualquer ação tomada pela fonte).
2 Mudanças no comportamento de autoridades estatais responsáveis pela implementação da Declaração da ONU sobre Defensores [2] : dissuasão dos agressores aumentando a probabilidade de que as autoridades tomaram uma atitude para proteger o defensor ou punir o agressor em caso de ataque. →	
3 Redução da possibilidade de um ataque: Reduzindo a exposição do defensor, melhorando o ambiente de trabalho, administrando adequadamente o medo e estresse, elaborando planos de segurança, etc. →	Reduzindo v**ulnerabilidades**, aumentando **capacidades.**

2 Veja o Capítulo 1.1. Por exemplo, após um defensor denunciar ameaças, a promotoria ou a polícia ou ainda outros órgãos tomam a iniciativa de investigar o que aconteceu e isso leva a uma ação contra aqueles que ameaçaram o defensor. Ao menos isso tem como objetivo prevenir uma agressão.

CAPÍTULO 1.7

Preparando um plano de segurança

Purpose:

Aprender a elaborar um plano de segurança.

Drafting a security plan

Agora que você já preparou o mapa de proteção dos atores chave, determinou as forças de campo, avaliou o risco, reconheceu suas estratégias existentes, e estabeleceu sua estratégia global, não será difícil elaborar um plano de segurança.

Segurança é algo complexo e representa a combinação de vários fatores. Alguns estão sempre presentes. Outros podem ser adicionados quando necessário. Juntos eles constituem o plano de segurança.

Eles precisam ser implementados em nível individual, organizacional e inter-organizativo.

Como proceder? Aqui está o processo representado em somente alguns passos:

1 ♦ **Os componentes do plano.** A finalidade do plano de segurança é reduzir seu risco. Ele terá, portanto, no mínimo três objetivos baseados em sua avaliação de risco:

- Reduzir o grau de ameaça que você está enfrentando;
- Reduzir suas vulnerabilidades;
- Aumentar suas capacidades.

Um plano de segurança deveria também incluir regras do dia-a-dia, medidas e protocolos para gerir situações específicas.

Regras e medidas para a rotina diária de trabalho:

- Trabalho de incidência (lobby) permanente, networking, código de ética, cultura de segurança, gestão de segurança, etc.
- Medidas permanentes, para garantir que a rotina de trabalho seja feita de acordo com os requisitos de segurança.

Protocolos para situações específicas:

- Protocolos preventivos: por exemplo como preparar uma conferência de imprensa ou uma visita a uma área remota.
- Protocolos de emergência para reagir a problemas específicos, como detenções ou desaparecimentos.

Quando mais as regras e medidas do dia-a-dia são implementadas, tanto melhor funcionarão os protocolos para situações específicas.

Alguns exemplos:

■ se um conjunto de regras e medidas permanentes a respeito de controle de informação for implementado, uma invasão do escritório (emergência) terá menos impacto se não existissem estas regras.

■ Se um conjunto permanente de regras e medidas sobre relações públicas for implementado, um alerta inicial gerado por um ataque contra um defensor de direitos humanos terá maiores possibilidades de resultar numa reação por parte dos atores chave, atingindo assim os objetivos definidos pelo defensor no caso de um ataque.

Para atingir este último objetivo o plano de segurança deve incluir incidência (lobby) permanente em relação às autoridades responsáveis e aos atores chave. Será preciso uma política de comportamento ético em funcionamento em relação a todos os aspectos do trabalho da organização, tanto nos níveis individual e organizacional quanto inter-organizativo.

■ No caso de uma detenção ou prisão, se um plano permanente estiver em vigor incluindo uma política de comportamento ético dos indivíduos, então eventuais contravenções à lei podem ser razoavelmente excluídas como causa da detenção e assim o protocolo de emergência pode ser implementado. Certamente, uma infração à lei pode ser um pretexto, mas os advogados ou juristas da organização saberão o que fazer. Além do mais, um defensor detido saberá quais passos estão sendo tomados detalhadamente, e poderá "relaxar" (impacto psicológico) sabendo que o trabalho para sua liberação fora do centro de detenção já começou. Não há necessidade de desafiar as autoridades e expor-se pessoalmente a mais risco do que já está sofrendo.

■ Em caso de missões de campo a regiões perigosas, os atores chave relevantes foram avisados previamente e estarão em alerta até que o defensor retorne a salvo.

2 ♦ **Responsabilidades e recursos para implementar o plano.** Para assegurar-se da implementação do plano, devemos integrar a segurança às atividades diárias:

- Incluir regularmente nas agendas de trabalho uma avaliação do contexto e os pontos de segurança;

- Registrar e analisar os incidentes de segurança.
- Designar responsabilidades;
- Designar recursos, isto é, o tempo e os fundos, para segurança.

3 ♦ **Elaborar o plano – por onde começar**. Se você realizou uma valoração do risco de um defensor ou organização, com certeza terá uma longa lista de vulnerabilidades, vários tipos de ameaças e um número de capacidades. É praticamente impossível cobrir tudo ao mesmo tempo. E assim, por onde começar? É muito simples:

- **Selecione algumas ameaças**. Dê prioridade às ameaças que você enumerou na lista, mesmo que sejam atuais ou potenciais, utilizando **um** dos seguintes critérios: a ameaça mais séria – as ameaças de morte, por exemplo; **OU** a ameaça mais séria e provável – se outras organizações similares à sua foram atacadas, isto representa uma clara ameaça potencial para você; **OU** a ameaça que mais se aproxime de suas vulnerabilidades – porque você corre um maior risco com essa ameaça específica.
- **Faça uma lista das vulnerabilidades relevantes**. Você deve concentrar-se, primeiro, nestas vulnerabilidades, e lembre que nem todas as vulnerabilidades estão relacionadas com todas as ameaças.
- **Faça uma lista das capacidades relevantes**.

Exemplo

de seleção de um processo que leva à elaboração de um plano de segurança:

O líder de uma organização de defensores (seja rural ou urbana) recebeu sérias ameaças de morte. A organização realiza uma avaliação de risco da ameaça e lista suas vulnerabilidades e capacidades.

Concluindo, a organização decide implementar as seguintes medidas de segurança: trancar todos os armários, colocar barras de ferro para proteger as janelas, comprar telefones celulares novos para seus membros em risco e publicamente denunciar as ameaças de morte.

Em geral, o ponto é perguntar e demonstrar como cada medida contribuirá para reduzir o risco específico (em outras palavras, como aumentará a segurança relacionada ao risco especifico).

Portanto: como todas estas medidas reduzirão na prática a ameaça específica contra o líder. (Certamente elas poderão enfrentar a questão de segurança global da organização mas este não é o momento correto para fazer isso).

Pergunte a você mesmo: Qual é a probabilidade de a ameaça de morte ser efetivada no escritório sabendo-se que há pessoas no local? O líder precisa estar fisicamente no escritório para ser morto? O líder ameaçado não estará sempre no escritório. Portanto, há muitas outras vulnerabilidades, tais como deixar o escritório sozinho à noite, viajar a locais isolados, ignorar medidas de segurança em casa...

Apesar de trancar os armários ser importante, não reduzirá a ameaça ou as vulnerabilidades do líder. O mesmo vale para as barras de ferro nas janelas. O que poderiam fazer contra um atirador de precisão ou uma granada?

Como um telefone celular vai reduzir o risco? O que pode ser feito com um celular para evitar que alguém mate o líder?

Pode ser mais útil reduzir a exposição deste líder durante seus deslocamentos entre sua casa e o escritório ou durante os fins-de-semana. Estas são as vulnerabilidades que precisam ser resolvidas primeiro, pois elas são mais relevantes para a ameaça.

Se o processo de seleção for correto e você estiver na posição de resolver as ameaças, vulnerabilidades e capacidades específicas de seu plano de segurança, você pode estar razoavelmente certo de que poderá reduzir o risco já no início do processo.

Não se esqueça de que este é um sistema ad hoc para elaborar um plano de segurança. Existem outros métodos "formais" para fazê-lo, mas este método é simples e faz com que você se concentre nos temas de segurança mais urgentes – sempre e quando sua avaliação de risco seja correta – e que você consiga um plano "ativo" e "realista"; essa é a parte importante da segurança. (*Veja no final deste Capítulo uma lista detalhada dos possíveis componentes do plano de segurança que também podem ser de utilidade na hora de avaliar os riscos.*)

Possíveis elementos a serem incluídos num plano de segurança

O seguinte "cardápio" enumera uma proposta detalhada de elementos a serem incluídos num plano de segurança. Uma vez realizada a avaliação de risco, você poderá escolher e combinar estes elementos para completar seu plano de segurança.

Um plano de segurança inclui elementos que se tornam procedimentos políticos (como encontrar autoridades de órgãos nacionais e internacionais, pedir proteção devida do Estado) e procedimentos operacionais (tais como rotinas de preparação para uma missão de campo).

Elementos para políticas organizacionais permanentes e medidas para o trabalho ordinário:

- O mandato, a missão e os objetivos gerais da organização (conhecê-los e respeitá-los).
- Uma declaração por parte da organização sobre a política de segurança.
- A segurança deve abarcar todos os aspectos do trabalho diário: a análise do contexto, a valoração do risco e a análise de incidentes, assim como a avaliação da segurança.
- Como assegurar que todos os trabalhadores tenham um conhecimento adequado da segurança e que quando as pessoas saiam da organização, sejam transferidas suas responsabilidades de segurança.
- Designação das responsabilidades: quem deve fazer o quê e em que situações.

- Como atuar numa crise de segurança: organizar um comitê ou grupo de crise, delegar um responsável para se ocupar dos meios de comunicação, da comunicação com os familiares, etc.

- Responsabilidades de segurança organizacional: planejamento, seguimento, seguros, responsabilidade civil, etc.

- Responsabilidades individuais de segurança: reduzir sempre o risco, como administrar o tempo livre, registrar e informar sobre os incidentes de segurança, sanções (alguns destes pontos podem ser incluídos nos contratos de trabalho, se for o caso).

- Políticas organizacionais sobre:
  - O descanso, o tempo livre e o estresse;
  - A segurança de vítimas e testemunhas;
  - Saúde e prevenção de acidentes;
  - Relações com autoridades, forças de segurança e grupos armados;
  - Documentar e arquivar a informação, a gestão dos documentos confidenciais;
  - Sua própria imagem em relação aos valores religiosos, sociais e culturais;
  - A gestão da segurança em escritórios e residências (incluindo para visitantes);
  - Manuseio de dinheiro e objetos de valor;
  - Meios de comunicação e protocolos;
  - Manutenção de veículos;
  - Segurança de mulheres defensoras;
  - Segurança de defensores LGBTI;
  - ...

Elementos de medidas específicas para situações extraordinárias

- Protocolos de prevenção e reação:
  - Preparando viagens de campo;
  - Minas terrestres;
  - Reduzindo o risco de se envolver em crimes comuns, incidentes armados ou ataques sexuais;
  - Reduzindo o risco de acidentes em viagens a áreas perigosas;
  - Protocolos de reação sobre: emergências médicas e psicológicas (também em missões de trabalho);
  - Ataques, incluindo os ataques sexuais;
  - Roubo;
  - Reagir se uma pessoa não se reporta quando deve fazê-lo;
  - Prisão ou detenção;
  - Rapto, desaparecimento;
  - Incêndio e outros acidentes;
  - Evacuação;

- Desastres naturais;
- Buscas legais ou ilegais ou invasões ilegais em escritórios ou residências;
- Incidentes armados (se alguém se encontra num tiroteio, por exemplo, ou num bombardeio);
- Se matam alguém;
- Se há um golpe de estado.
- ...

Implementando um plano de segurança

Os planos de segurança são importantes, mas nem sempre resultam fáceis de serem colocados em prática. A implementação é muito mais que um processo técnico – é um processo organizativo, o que implica buscar pontos de entrada e oportunidades para desenvolvê-lo, assim como detectar quais são os obstáculos e problemas.

Um plano de segurança deve ser implementado, pelo menos, em três níveis:

1 ♦ Nível **individual**. Cada indivíduo deve seguir o plano para que ele funcione.

2 ♦ Nível **organizativo**. A organização, em sua totalidade, deve seguir o plano.

3 ♦ Nível **inter-organizativo**. Normalmente, para manter a segurança, é necessário um certo grau de cooperação entre organizações.

Exemplos

de **pontos de entrada** e **oportunidades** na hora de implementar um plano de segurança:

- Ocorreram vários incidentes menores em sua organização ou em outra organização similar e alguns trabalhadores estão preocupados a respeito.
- Existe uma preocupação geral sobre a segurança devido à situação do país.
- Foram incorporados novos trabalhadores que poderiam se capacitar e implementar boas práticas em segurança com maior facilidade.
- Uma organização nos oferece uma formação sobre segurança.

Exemplos

de **problemas** e **obstáculos** na hora de implementar um plano de segurança:

- Algumas pessoas pensam que um maior número de medidas de segurança equivale a incrementar ainda mais o volume de trabalho.
- Outras opinam que a organização já dispõe de uma boa segurança.
- "Não temos tempo para estas coisas!"
- "Tudo bem, tiraremos algum momento para discutir o tema da segurança nos sábado pela manhã, mas que não se fale mais disso!"
- "Devemos nos concentrar mais nas pessoas a quem queremos ajudar, não em nós mesmos."

■ **Aproveite as oportunidades e os pontos de entrada** para confrontar os problemas e superar os obstáculos.

■ **Proceda passo a passo.** Não vale a pena achar que se pode fazer tudo ao mesmo tempo.

■ **Enfatize a importância da segurança para fazer um bom trabalho pelo bem das vítimas.** A segurança das vítimas e testemunhas é primordial para o trabalho e a melhor maneira de lidar com isto é integrando boas práticas de segurança em todos os âmbitos de trabalho. Utilize exemplos de formação/debate que mostrem o possível impacto negativo que pode exercer sobre as testemunhas e as vítimas uma segurança pouco rigorosa.

■ Se o plano é elaborado por dois "especialistas" e for apresentado para toda a organização é provável que seja um grande fracasso. Em segurança, a **participação é fundamental**.

■ **Um plano deve ser realista e realizável.** Se você faz uma longa lista de coisas para fazer antes de cada viagem ao campo, isto não funcionará. Enumere somente as que sejam imprescindíveis para garantir a segurança. Esta é outra das razões porque é necessário envolver aqueles que realmente fazem o trabalho – como por exemplo as pessoas que costumam viajar ao campo.

■ **O plano não é um documento inalterável** – deve ser revisado e atualizado com freqüência.

■ **O plano não deve ser considerado como "mais trabalho", mas como "uma melhor forma de trabalhar".** As pessoas têm de ver as vantagens do plano: evitar, por exemplo, duplicar os relatórios. Assegure-se de que os relatórios das visitas externas tenham um anexo de segurança; faça com que os assuntos de segurança passem a ser um ponto comum de pauta nas reuniões de equipe, integre aspectos da segurança em outras formações, etc.

■ **Enfatize que a segurança não é uma escolha pessoal.** As decisões, atitudes e comportamentos individuais que causam um impacto na segurança podem gerar conseqüências na segurança das testemunhas, dos familiares das vítimas e de colegas. É necessário chegar a um compromisso coletivo para poder implementar boas práticas de segurança.

■ **É necessário designar o tempo e os recursos para** poder implementar o plano, visto que, para melhorar a segurança, não devemos fazer uso do "tempo livre". Para que as atividades de segurança sejam consideradas "importantes", devem ser colocadas junto a outras atividades "importantes".

■ **Todo mundo deve ser visto seguindo o plano,** sobretudo os diretores e os responsáveis pelo trabalho de outras pessoas. É necessário implantar sanções para os indivíduos que se neguem a seguir o plano.

Resumo

A Um plano de segurança deve diminuir as vulnerabilidades e aumentar as capacidades de modo que as ameaças sejam reduzias ou se tornem menos prováveis de serem executadas. Assim o risco é reduzido.

Um plano de segurança deve se adequar às necessidades atuais e do ambiente de trabalho.

O ponto principal não é cobrir um grande espaço sociopolítico, mas de cobrir dentro do espaço correto, o ambiente de trabalho tanto quanto possível através de trabalho em rede e juntamente com outras organizações. Determinar procedimentos de segurança que transcendem diferenças políticas.

Segurança é uma preocupação de todos e é individual, organizacional e inter-organizativa.

Segurança é tema complexo e constitui-se no resultado de vários fatores. Alguns sempre estarão presentes. Outros serão adicionados em momentos específicos. Juntos eles constituem um plano de segurança.

Seu plano de segurança deve incluir políticas organizacionais para o dia-a-dia, medidas e protocolos para situações específicas.

Ambos incluem procedimentos políticos e operacionais.

Melhorando a segurança no trabalho e nas residências particulares

Objetivos:

Avaliar a segurança em escritórios e residências.

Planejar, melhorar e supervisionar a segurança nestes lugares.

A segurança no trabalho e em casa

A segurança dos escritórios centrais da organização, dos escritórios e das residências dos trabalhadores é de vital importância para o trabalho dos defensores de direitos humanos. Portanto, veremos em profundidade como se pode analisar e melhorar a segurança de um escritório ou casa. (*Para simplificar, a partir de agora utilizaremos o termo "escritório", mas a informação que segue também faz referencia à segurança em residências particulares*).

Aspectos gerais da segurança no escritório

Nosso objetivo para melhorar a segurança, pode ser resumido em cinco palavras: **evitar o acesso não autorizado.** Estes exemplos aplicam-se tanto em escritórios situados em áreas urbanas como rurais. Em casos excepcionais, também é necessário proteger o escritório de um possível ataque (um atentado a bomba, por exemplo).

Isto nos leva à primeira consideração geral: as vulnerabilidades de um escritório, porque elas podem aumentar o risco, dependendo do tipo de ameaça que você enfrenta. Por exemplo, se existe o risco de que alguém roube material ou informação, você deve eliminar as vulnerabilidades correspondentes. Um alarme noturno (eléctrico, se tem acesso a eletricidade, ou uma vigia noturno, ou mesmo um cachorro) não servirá muito se ninguém se prontificar a ver o que ocorreu. Por outro lado, caso se tratar de um roubo violento em pleno dia, os reforços das trancas da porta não serão de grande ajuda. Em resumo, decida que medidas tomar de acordo com as ameaças que você enfrenta e o contexto em que trabalha.

As vulnerabilidades de um escritório devem ser avaliadas de acordo com as ameaças que enfrente.

Entretanto, é importante encontrar um equilíbrio entre impor as medidas de segurança apropriadas e dar a impressão às pessoas de fora de que se "esconde" ou "guarda" algo dentro, já que isto poderia, por si só, supor um risco. Na segurança do escritório, você se encontrará na obrigação de decidir entre manter um perfil baixo ou tomar mais medidas visíveis segundo convenha. Por outro lado, o agressor potencial saberá que seu escritório contem objetos de valor e informação contenciosa e que você "precisa" proteger.

A segurança de um escritório
é igual a de seu ponto mais fracot.

Se alguém quer entrar no escritório passando despercebido, não escolherá ponto de acesso mais difícil para fazê-lo. Lembre que, às vezes, a forma mais simples de entrar num escritório e observar o que ocorre em seu interior é, simplesmente, batendo à porta.

A localização do escritório

Independentemente do fato de ser uma área rural ou urbana, os fatores para se ter em vista ao montar um escritório são: a vizinhança, se o edifício tem alguma relação com alguma pessoa ou atividades do passado; se é possível implantar medidas de segurança necessárias; acessibilidade de transporte público e privado; risco de acidentes, etc. (*Veja também 'Avaliação de risco da localização' abaixo*).

É conveniente revisar as medidas de segurança adotadas na vizinhança por outros. Se há muitas, poderia significar que se trata de uma zona perigosa em relação ao crime comum, por exemplo. Também é importante falar com as pessoas da região sobre a situação da segurança local. Em todo caso, é importante assegurar-se de que é possível tomar medidas de segurança sem chamar muita atenção. Também é conveniente relacionar-se com a população local, já que podem informar sobre qualquer assunto suspeito que ocorra na vizinhança.

Também é importante comprovar quem é o proprietário. Que reputação tem? Poderia ser suscetível à pressão das autoridades? Aceitará que você adote medidas de segurança?

Ao escolher o escritório, é necessário ter em conta quem o freqüentará. As necessidades de um escritório onde estarão vítimas em busca de uma assessoria jurídica serão completamente distintas das de um escritório que atue principalmente como um lugar de trabalho para os empregados. É importante ter em conta o fácil acesso ao transporte público, se é perigoso o trajeto que vai do escritório às residências dos trabalhadores, ou a áreas onde se realizam a maioria das atividades, etc. Também é preciso avaliar os arredores, especialmente para evitar ter que cruzar zonas perigosas durante os deslocamentos.

Em alguns casos, o escritório pode simplesmente ser a casa do defensor (veja áreas rurais, abaixo). Ainda assim, as considerações mencionadas acima devem ser levadas em consideração.

Uma vez escolhida a localização, é importante realizar avaliações periódicas de aspectos da localização que podem mudar, por exemplo, um "elemento indesejável" se muda para a vizinhança.

Pontos a considerar para a escolha de uma boa localização para o escritório	
Vizinhança:	Estatísticas de crime; proximidade de possíveis alvos de ataques armados, como instalações militares ou governamentais; lugares seguros para refugiar-se; outras organizações nacionais ou internacionais com as quais relacionar-se.
Relações:	Tipo de gente na vizinhança; proprietário/locador, prévios locatários; prévios usos do edifício.
Acessibilidade:	Uma ou várias boas rotas de acesso (quantas mais melhor. Lembre que o elemento indesejado também terá dessa forma uma escolha maior); acessibilidade de transporte público e privado.
Serviços básicos:	Água e eletricidade, telefone.
Iluminação pública	Dos arredores.
Suscetibilidade a acidentes ou riscos naturais:	Incêndios, inundações graves, detritos tóxicos, fábricas com processos industriais perigosos, etc.
Estrutura física:	Solidez das estruturas, facilidade para instalar o material de segurança, portas e janelas, perímetro e barreiras de proteção, pontos de acesso (veja mais abaixo).
Para veículos:	Uma garagem ou, ao menos, um pátio ou um espaço fechado, com uma barreira de estacionamento.

Caso o escritório seja localizado numa área restrita, remota ou sem serviços próximos, o resultado do checklist acima indicará que vários itens não existem em sua área. Capacidades deverão ser desenvolvidas para compensar estas vulnerabilidades específicas. Por exemplo, se não houver outra organização por perto, você pode recorrer à comunidade. Ou, em caso de falta de água ou extintores de incêndio, certifique-se de que você tenha um recipiente grande para água sempre cheio.

Acesso de terceiros ao escritório: barreiras físicas e procedimentos para as visitas

Agora já sabemos que o objetivo principal da segurança do escritório é impedir o acesso a pessoas não autorizadas. Uma ou mais pessoas poderiam entrar e roubar, obter informação, colocar algo que poderia ser utilizado contra você, como drogas ou armas, ameaçar, etc. Cada caso é diferente, mas o objetivo é sempre o mesmo: evitá-lo.

O acesso a um edifício está controlado por meio de **barreiras físicas** (valas, portas, grades), de **medidas técnicas** (como alarmes com iluminação) e de **procedimentos de acesso para as visitas**. Toda barreira e procedimento representam um **filtro** pelo qual deve passar todo indivíduo que queira entrar no escritório. O ideal seria que estes filtros estivessem combinados, formando várias capas de proteção capazes de impedir diferentes tipos de entrada não autorizada.

Barreiras físicas.

As barreiras servem para bloquear **fisicamente** a entrada de visitantes não autorizados. A utilidade das barreiras físicas dependerá de sua **solidez** e habilidade de cobrir todos os **buracos vulneráveis** dos muros.

Seu escritório pode dispor de barreiras físicas em três zonas:

1 ♦ O perímetro **externo**: valas, muros ou similares, do outro lado do jardim ou pátio. Na falta de perímetro externo você pode definir a extensão do perímetro externo que estará sob seu controle.

2 ♦ O perímetro do **edifício ou do local**.

3 ♦ O perímetro **interno**: barreiras que podem ser instaladas no interior de um escritório para proteger uma ou mais salas. É prático, sobretudo em escritórios com um fluxo grande de visitantes, já que permite separar uma área pública de outra mais privada que pode estar protegida com barreiras adicionais.

O perímetro externo

O escritório deve estar rodeado por um perímetro externo claramente delimitado, possivelmente com obstáculos altos ou baixos, mas preferivelmente sólidos e suficientemente altos para dificultar mais o acesso. As grades metálicas que permitem ver através deixarão mais visível o trabalho da organização e, portanto, podem ser preferíveis os muros de tijolo ou algo parecido.

Na falta de um perímetro cercado claramente identificado, você pode decidir quanto de extensão estará visualmente dentro do seu controle, para que você diminua a possibilidade de elementos indesejáveis chegarem perto do escritório. Você pode utilizar espelhos convexos para isso.

O perímetro do edifício ou do local

Este inclui paredes, portas, janelas e teto ou telhado. Se as paredes são sólidas, todas as aberturas ou telhado deverão ser também. As portas e janelas devem ter fechaduras apropriadas e devem estar reforçadas com grades, preferivelmente com barras tanto verticais como horizontais bem incrustadas na parede. Se há um teto, este deve oferecer uma boa proteção – não uma simples folha de zinco ou uma capa de telhas. Se o telhado não pode ser reforçado, bloqueie todos os acessos possíveis ao telhado, desde o solo ou desde os edifícios vizinhos.

Se as janelas de seu escritório dão vista para a rua ou para um espaço público, coloque sua mesa de maneira que você possa ver para fora mas não possa ser visto de fora para dentro. Se as janelas dão vista para vegetação, certifique-se de que ninguém conseguirá se esconder ali.

Alguns escritórios possuem mais portas e uma delas pode servir como "saída de emergência". Lembre que uma saída de emergência também pode ser um ponto de entrada para elementos indesejáveis.

Em lugares com risco de ataque armado, é importante estabelecer zonas de segurança no interior do escritório (veja o Capítulo sobre segurança em zonas de conflito armado).

O perímetro interno

Aplica-se o mesmo que no edifício ou local. Resulta muito prático dispor de uma zona de maior segurança no interior do escritório, e costuma ser muito fácil de organizar. Inclusive uma caixa forte poderia ser considerada como um perímetro interno de segurança.

Seu escritório pode ter apenas uma sala. Neste caso você pode considerar partições móveis para manter um espaço privado longe da vista de algum visitante.

Uma observação sobre as chaves

- Nenhuma chave deve estar visível ou acessível a visitas. Mantenha todas as chaves num armário ou gaveta com chave de combinação cujo código somente conheçam os trabalhadores. Assegure-se de alterar o código de vez em quando, para maior segurança.

- Se as chaves estão etiquetadas individualmente, não escreva uma descrição da sala, armário ou gaveta correspondentes, já que isto facilitaria o roubo. É melhor que utilize um código de números, letras ou cores.

Medidas técnicas: iluminação e alarmes

(caso seu escritório tenha acesso a eletricidade ou esteja equipado com um gerador de eletricidade).

As medidas técnicas como olho mágico, interfones, câmeras de vídeo reforçam as barreiras físicas ou os procedimentos de acesso de visitas (veja mais abaixo). Isto porque as **medidas técnicas somente são práticas para dissuadir intrusos quando estão ativadas**. Para que funcione uma medida técnica, é necessário que possa provocar uma reação em concreto, como por exemplo, atrair a atenção dos vizinhos, da polícia ou de uma empresa privada de segurança. Se isto não ocorre, e o intruso sabe que não ocorrerá, estes tipos de medidas são muito pouco práticas e limitar-se-ão a prevenir furtos menores ou a gravar as pessoas que entram.

- A **iluminação** ao redor do edifício (de pátios, jardins, calçada) é fundamental.

- Os **alarmes** devem ter várias finalidades, que incluam a detecção de intrusos e evitar o ingresso de possíveis intrusos ou fazer que desistam de um novo intento.

Um alarme pode ativar um aviso sonoro no interior do escritório; uma luz de segurança, um tom, timbre ou ruído forte e geral; ou um sinal numa empresa externa de segurança. Um alarme sonoro é prático para chamar a atenção, mas pode ser contraproducente em situações de conflito ou caso se imagina que os residentes locais ou outros não reagirão a ele. É necessário escolher cuidadosamente entre um alarme sonoro ou um luminoso (uma luz fixa potente, ou uma luz

vermelha intermitente). Esta última pode ser suficiente para dissuadir o intruso, já que sugere que a detecção inicial pode desencadear uma reação contra ele.

Os alarmes devem ser instalados em pontos de acesso (pátios, portas e janelas, e em zonas vulneráveis tais como os lugares que contenham informação confidencial). Os alarmes mais sensíveis são os sensores de **movimento**, que ativam uma luz, emitem um som ou ativam uma câmera quando detectam algum movimento.

- Os alarmes devem:
  - Incluir baterias, para que continuem funcionando em caso de apagão;
  - Dispor de um intervalo antes de ser ativado para que possa ser desativado pelos empregados, em caso de ter sido ativado acidentalmente;
  - Incluir uma opção de ativação manual, em caso de que os empregados necessitem ativá-lo;
  - Ser de fácil instalação e manutenção;
  - Ser fácil de distinguir de um alarme de incêndio.

Câmeras de vídeo

As câmeras de vídeo podem ajudar a melhorar os procedimentos de acesso (veja abaixo) ou gravar as pessoas que entram no escritório. Entretanto, as câmeras deveriam estar colocadas em pontos fora do alcance dos intrusos porque, caso contrário, eles poderiam abrir a câmera e destruir a fita.

É preciso ter em conta que as câmeras podem intimidar as pessoas que vão ao escritório, como vítimas ou testemunhas, ou se pelo contrário, podem ser consideradas como um bem luxuoso que atrai ladrões. É recomendável colocar uma nota advertindo sobre a presença de câmeras ativadas (o direito à privacidade também é um direito humano).

Iluminação e alarmes caso seu escritório não tenha acesso a eletricidade ou não esteja equipado com um gerador de eletricidade.

Simplesmente evite ficar no escritório quando escurecer.

O alarme elétrico pode ser substituído por outro sistema de alarme: um vigia noturno, vizinhos, familiares, a comunidade, cachorros: obtenha seu apoio e veja como eles podem se tornar seu sistema de alarme.

Empresas de segurança privadas

Este tema requer muito cuidado. Em muitos países, os trabalhadores das empresas privadas de segurança são antigos membros das forças de segurança. Existem casos documentados onde estas pessoas eram responsáveis pela vigilância e pelos ataques aos defensores dos direitos humanos ao mesmo tempo.

Portanto, é sensato não confiar nas empresas de segurança quando se têm razões para suspeitar que se está sendo vigiado ou se teme um ataque das forças de segurança. Se uma empresa de segurança tem acesso a seu escritório, podem instalar microfones ou permitir o acesso de outras pessoas.

Se decidir usar os serviços de uma empresa de segurança, você deve assegurar-se de ter um acordo conciso sobre o que seu pessoal pode fazer e não fazer, e a que partes do edifício podem ter acesso. Evidentemente, é necessário vigiar para comprovar que estes acordos sejam respeitados.

Por exemplo:

> *Se você contratou um serviço de segurança que envia um guarda quando dispara o alarme, este guarda pode entrar em áreas reservadas de seu escritório e ativar aparatos de escuta em sua sala de reuniões.*

É preferível que se lembre (e se possível controle) exatamente quais empregados trabalham para você, mas isto não costuma ser possível.

Se os guardas de segurança vão armados, é importante para uma organização de direitos humanos informar-se detalhadamente sobre quais são suas regras de uso. Contudo, é mais importante ainda fazer um balanço das possíveis vantagens do uso de armas e de suas desvantagens. As armas de mão não representam nenhum obstáculo para os agressores com uma maior capacidade de fogo (tal como costuma ser o caso), mas se os agressores sabem que há homens dentro do imóvel com espingardas, poderiam decidir entrar preparados para disparar, para protegerem-se durante o ataque. Em outras palavras, uma capacidade armada (armas pequenas) provavelmente incentive os atacantes a utilizar armas de maior capacidade. Neste ponto, se você necessita de guardas com metralhadoras, vale a pena questionar-se se dispõe do espaço sociopolítico mínimo necessário para poder realizar seu trabalho.

Filtros no procedimento de acesso

As barreiras físicas devem ser acompanhadas por um "filtro" no **procedimento de acesso**. Estes procedimentos determinam quando, como e quem pode entrar em qualquer parte do escritório. O acesso a espaços privados, como chaves, informação ou dinheiro, deve ser restringido.

O método mais simples para entrar num escritório onde trabalha um defensor dos direitos humanos é batendo à porta e entrando. Muita gente faz isso todos os dias. Para poder conciliar o caráter aberto de um escritório de direitos humanos com a necessidade de controlar quem quer visitá-lo e por quê, você necessitará de processos de acesso apropriados.

No geral, as pessoas que batem à sua porta e querem entrar o fazem por uma razão concreta. Em geral, querem perguntar ou entregar algo, sem ter necessariamente de pedir permissão para isso antes. Examinemos caso por caso:

Alguém liga e pede permissão para entrar por uma razão em concreto.

Siga três passos simples:

1 ♦ **Pergunte a identidade da pessoa e por que quer entrar.** Se ele/a quer ver alguém do escritório, consulte esta pessoa. Se a pessoa não está, peça ao visitante que volte em outro momento ou que espere fora da zona restrita do escritório.

É importante utilizar os visores, câmeras ou interfones para evitar abrir ou aproximar-se da porta, especialmente se você quer impedir a entrada de alguém ou deve enfrentar uma entrada violenta ou forçada. Portanto, é bom dispor de uma sala de espera fisicamente separada da entrada interna do escritório. Se é imprescindível dispor de uma área pública de fácil acesso, assegure-se de dispor de barreiras físicas que bloqueiem o acesso a áreas restritas do escritório.

Alguém poderia solicitar entrar para comprovar ou reparar a instalação de água ou eletricidade ou fazer alguma manutenção. Também poderia afirmar ser um jornalista, um funcionário estatal, etc. Antes de permitir a entrada, comprove sempre sua identidade com a companhia ou organização a quem diz representar. Lembre que nem um uniforme e nem um cartão de identificação são garantias de uma identificação correta e segura, especialmente numa situação de risco médio ou elevado.

2 ♦ **Decida se deve permitir ou não o acesso.** Uma vez estabelecida a razão da visita, você deverá decidir se permite ou não o acesso. O simples fato de que alguém dê um motivo para entrar não é razão suficiente para deixar entrar. Se você não está seguro de qual é seu objetivo, não deixe entrar.

3 ♦ **Supervisione as visitas até que saiam.** Uma vez que a visita entrou no escritório, assegure-se de que alguém as supervisione todo o tempo até sua saída. É conveniente dispor de uma área separada para reunir-se com as visitas fora das áreas restritas.

Para cada visitante deve-se anotar seu nome, organização, razão da visita, com quem se reuniu, hora de entrada e de saída. Esta informação pode ser de grande utilidade no momento de analisar os possíveis erros após um incidente de segurança.

Alguém vem ou liga fazendo perguntas.

Apesar do que possa dizer uma visita ou alguém por telefone, não comunique sob nenhuma hipótese a localização de um colega ou de outra pessoa próxima, nem ofereça nenhum tipo de informação pessoal. Em caso de que insistam, diga para que deixem uma mensagem, que venham ou voltem a ligar mais tarde ou que peçam uma reunião com a pessoa que desejam ver.

Algumas vezes, a pessoa pode parecer enganada, perguntando se o Senhor Tal vive aqui ou se vende algo, etc. Outras vezes, querem vender alguma coisa, e os mendigos podem vir pedir ajuda. Se você nega o acesso e informação a estas pessoas, estará evitando todo risco de segurança.

Alguém quer fazer entrega de um objeto ou pacote.

O risco que se corre com um pacote ou objeto é que o conteúdo poderia comprometer ou ferir alguém (em caso de um pacote ou carta bomba). Por mais

inocente que pareça, não toque ou manipule um pacote ou carta até que não tenha seguido três simples passos:

1 ♦ **Comprove se o destinatário a quem é dirigido está esperando o pacote.** Não é suficiente que o destinatário conheça o remetente, porque a identidade deste poderia ser facilmente falsificada. Se o destinatário não espera um pacote, deverá comprovar se o suposto remetente realmente enviou algo. Se o pacote está simplesmente dirigido ao escritório, comprove quem o enviou. Espere e discuta o assunto antes de tomar uma decisão final.

2 ♦ **Decida se aceita ou não o pacote ou a carta.** Se você não pode determinar quem enviou ou pacote, ou se levará tempo para fazer isso, a melhor opção é não aceitar, sobretudo num ambiente de risco médio ou elevado. Você sempre pode pedir que lhe entreguem mais tarde, ou retirar nos correios.

3 ♦ **Não perca o pacote de vista enquanto estiver no interior do escritório.** Assegure-se de que sabe, em todo momento, em que lugar do escritório se encontra o pacote até que o destinatário o tenha recolhido.

Em alguns países, um pacote é anunciado pelo telefone e é o defensor quem tem de retirá-lo. Pode ser um truque para atrair o defensor e expô-lo a uma agressão. Como o telefone pode não registrar as chamadas, seria impossível rastrear a origem da ligação. Se o defensor verificar a origem do pacote, poderá também verificar o remetente e perguntar qual a rota do envio. O defensor poderá, então, decidir se é seguro retirar o pacote ou não. Ele pode também pedir que a pessoa que ligou informando sobre o pacote venha até o escritório trazer o item e então seguir os procedimentos acima. Muito provavelmente, em caso de um pretexto, o interlocutor não virá ao escritório.

Durante atos ou festas.

Nestas circunstâncias a norma é simples: ninguém que você não conheça pessoalmente poderá entrar. Somente devem entrar os conhecidos de companheiros de confiança, e somente quando este companheiro estiver presente e possa identificar seu convidado. Se uma pessoa aparece afirmando conhecer alguém do escritório que não está presente, não o deixe entrar.

Os defensores podem hesitar e achar difícil fazer perguntas a um visitante e mandá-lo embora. Entretanto, eles não precisam fazer isso. Podem simplesmente dizer que não estão autorizados a deixar o visitante entrar.

Além disso, para todos os procedimentos de admissão, lembre que se um visitante for genuíno, ele reconhecerá o empenho da organização em zelar pela segurança e se o visitante não for genuíno ficará sabendo que a organização também implementa procedimentos de segurança. Então, qualquer que seja o caso, os defensores devem dar a eles mesmo a autoridade de negar a entrada a um visitante desconhecido. Se isso ajudar, podem usar a seguinte desculpa: "não e... não estou autorizado a deixar visitantes desconhecidos entrarem, mas se você deixar seu cartão de visita eu certamente o informarei sobre futuras atividades públicas da organização."

Manter um registro de chamadas e de visitas.

É prático manter um registro das chamadas de telefone e dos números e tomar nota das pessoas que visitam a organização (algumas organizações solicitam aos visitantes novos a apresentação de um documento de identidade e a organização registra o número do documento).

Horas extras no escritório.

Devem existir certos procedimentos para o pessoal que fica trabalhando fora do horário normal. Os membros de uma organização que tenham de fazê-lo devem avisar a cada certa hora a outro membro designado, ter um cuidado especial ao sair do edifício, etc.

LISTA DE REVISÃO: IDENTIFICAR OS PONTOS FRACOS DOS PROCEDIMENTOS DE ACESSO
♦ **Quem** tem acesso habitual a **que** zonas e **por quê**? Restrinja o acesso a não ser que seja absolutamente necessário mantê-lo público.
♦ Distinguir os diferentes **tipos** de visitantes (mensageiros, trabalhadores de manutenção, técnicos de informática, membros de ONG em reuniões, VIPs, convidados a atos, etc.) e **desenvolva procedimentos de acesso apropriados para cada um.** Todo o pessoal deve estar familiarizado com os diferentes procedimentos de cada tipo de visitas, e assumir a responsabilidade de implementá-los**.**
♦ O visitante tem acesso aos pontos mais fracos uma vez dentro do escritório? Desenvolva estratégias para evitar isso.
LISTA DE REVISÃO: ACESSO A CHAVES
♦ **Quem** tem acesso a **que** chaves e **quando**.
♦ Onde e como **se guardam** as **chaves** e suas **cópias** correspondentes?
♦ Há um **controle das cópias** de chaves que estão em circulação?
♦ Existe algum risco de que alguém faça cópia **não autorizada da chave**?
♦ O que ocorre se **alguém perde uma chave**? Você deverá mudar a fechadura, a não ser que esteja totalmente convencido de que se perdeu acidentalmente e de que ninguém pode identificar o proprietário da chave ou seu endereço. Lembre que uma chave pode ser roubada – num roubo organizado, por exemplo – para poder entrar no escritório.

Todos os trabalhadores têm a obrigação de agir em relação a qualquer pessoa que não siga corretamente os procedimentos de acesso. Deveriam também registrar em livro de incidentes de segurança todos os movimentos de pessoas ou veículos suspeitos. Isto é também aplicável a qualquer objeto situado fora do edifício, para descartar o risco potencial de uma bomba. Se há uma suspeita de bomba, não a ignore, **não a toque**, e assegure-se de contatar a polícia.

Quando se mudar para um novo escritório, ou se perderam ou foram roubadas as chaves, é essencial mudar no mínimo todas as fechaduras de entrada.

Lista de revisão: procedimentos gerais da segurança de escritório

- Dispor de extintores e lanternas (com pilhas). Assegurar-se de que todos os empregados saibam como utilizá-los.
- Dispor de um gerador elétrico se há uma alta possibilidade de apagão. Os apagões podem por em perigo a segurança (luzes, alarmes, telefones, etc.), sobretudo em zonas rurais.
- Ter uma lista a mão com os telefones locais de emergência, da polícia, bombeiros, ambulância, hospitais de urgência próximos, etc.
- Se existe um risco de combate nas proximidades, mantenha uma provisão de comida e água em reserva.
- Confirme a localização de outras zonas de segurança externas ao escritório em caso de emergência (os escritórios de outras organizações por exemplo).
- Nunca deixe uma pessoa externa à organização **sozinha** numa área restrita com acesso a chaves, informação ou objetos de valor.
- **Chaves**: nunca deixe as chaves num lugar onde as visitas possam ter acesso a elas. Nunca "esconda" as chaves fora da entrada do escritório – isto as torna acessíveis.
- **Procedimentos de acesso**: As barreiras de segurança não oferecem proteção alguma se se permite o acesso ao escritório a um possível intruso. Os pontos principais a se ter em conta são:
  - Todos os trabalhadores são igualmente responsáveis pelo controle e entrada dos visitantes.
  - Todas os visitantes deverão estar supervisionados em todo momento, enquanto permaneçam no interior do escritório.
- Se você se encontrar com um visitante não autorizado no escritório:
  - Nunca confronte alguém que parece disposto a fazer uso de violência para obter o que quer (se estiverem armados, por exemplo). Nestes casos, avise a seus companheiros, busque um lugar seguro para esconder e tente pedir ajuda à polícia.
  - Dirija-se à pessoa com cuidado, ou busque ajuda no escritório, ou chame a polícia se for adequado.

- Em situações de elevado risco, controle sempre a localização dos objetos vulneráveis, como a informação do disco rígido do computador, para que permaneçam inacessíveis ou para poder levá-los em caso de uma evacuação urgente.

- Tenha em conta que, em caso de confrontação com um possível intruso, os trabalhadores do escritório estão na primeira linha. Assegure-se de que recebam, em todo momento, formação suficiente e apoio sobre como atuar em cada situação sem se colocarem numa situação de risco.

Inspeções regulares de segurança no escritório

A supervisão ou inspeção regular da segurança do escritório é de grande importância, porque as situações e procedimentos de segurança variam com o tempo, como por exemplo, quando se deteriora o material ou quando há uma grande circulação de pessoal. Também é importante que os empregados adotem um certo sentido de apropriação das regras de segurança do escritório.

A pessoa responsável pela segurança deverá realizar, pelo menos, uma revisão de segurança de escritório a **cada seis meses**. Com a ajuda da seguinte lista, levará, tão-somente, uma ou duas horas. A pessoa responsável pela segurança deve assegurar-se de obter a opinião dos colegas antes de escrever o relatório final, e apresentá-lo à organização para que se tomem as decisões e as ações correspondentes. Em seguida, o relatório deve ser arquivado até a próxima revisão de segurança.

Lista de Revisão da Segurança no Escritório

Revisão de:
Realizada por:
Data:

1. Contatos de emergência:

- Há uma lista atualizada com os números de telefone e endereços de outras ONGs locais, hospitais de emergência, polícia, bombeiros e ambulância à mão?

2. Barreiras técnicas e físicas (externas, internas e interiores):

- Certifique o estado e o funcionamento das grades/valas, portas que dão acesso ao edifício, janelas, paredes e telhado.
- Certifique o estado e funcionamento da iluminação externa, câmeras ou vídeo, interfones da entrada.
- Certifique os procedimentos das chaves, incluindo as chaves que estão **sob segurança** e **etiquetadas em código**, designação de **responsabilidade** para controlar as chaves e suas cópias, e que estas **funcionem corretamente**. Assegure-se de que se troquem os miolos quando as chaves se perderem ou forem roubadas, e que tais incidentes sejam **registrados**.

3. Procedimentos de acesso das visitas e "filtros":

- Estão ativados os procedimentos de acesso para todo tipo de visitantes? Os empregados estão familiarizados com eles?
- Revise todos os incidentes de segurança registrados, relacionados com os procedimentos de ingresso ou "filtros".
- Pergunte aos empregados que costumam encarregar-se dos procedimentos de acesso se eles funcionam corretamente, e que melhoras são necessárias.

4. Segurança em caso de acidentes:

- Certifique o estado dos extintores contra incêndios, das válvulas/canos de gás e torneiras de água, das conexões elétricas e geradores de eletricidade (caso seja relevante).

5. Responsabilidade e formação:

- Foi designada a responsabilidade pela segurança do escritório a alguém? É efetiva?
- Existe algum programa de formação sobre a segurança de escritório? Ele cobre todas as áreas mencionadas nesta revisão? Todos os empregados foram treinados? O treinamento é efetivo?

Em áreas rurais:

Defensores trabalham em áreas rurais tanto em vilas (pequena) como em áreas isoladas ou remotas. Eles podem não ter muitas escolhas em relação à localização do escritório. Ainda assim eles precisam proteger seu espaço de visitantes e objetos indesejáveis.

Vilas: se for comparável com uma micro área urbana, a maioria das considerações acima podem ser levadas em consideração e completadas com as seguintes dicas.

Localização remota ou isolada: certifique-se de que a comunidade local, sua família e amigos possam contribuir para seu sistema de alarme. Tente que eles verifiquem regularmente se você está bem e se seu escritório está seguro (ou sua casa). Você pode considerar também manter um cachorro que pode ser treinado para latir para visitantes. Certifique-se de que ele não atacará as pessoas e de que não será facilmente envenenado.

Evite áreas escuras.

Você pode considerar estabelecer comunicação através de recados com pessoas confiáveis para garantir uma reação rápida em caso de necessidade.

Resumo

O objetivo das medidas de segurança no escritório/casa é reduzir o risco de acessos indesejados.

A segurança de um escritório não é maior do que seu ponto fraco.

Independentemente de seu escritório/casa ser localizado numa área urbana ou rural, você poderá usar a equação para reduzir risco de aceso indesejado.

Ameaças podem ser assimiladas a conseqüências de riscos.

Liste todas suas ameaças e conseqüências de risco de acessos indesejados. Então faça uma lista das respectivas vulnerabilidades e capacidades para cada ameaça/conseqüência e comece a trabalhar com elas.

CAPÍTULO 1.9

Segurança para mulheres defensoras dos direitos humanos

Objetivos

Ver a segurança na perspectiva das mulheres defensoras dos direitos humanos.

Oferecer a ambos mulheres e homens defensores de direitos humanos conhecimento e ferramentas adicionais de segurança e proteção.

Introdução

Apesar de a segurança das mulheres defensoras dos direitos humanos estar relacionada com a segurança de todos os defensores de direitos humanos, decidimos dedicar um capítulo específico para a segurança das mulheres defensoras dos direitos humanos porque a experiência no terreno nos mostra que este assunto não é sistematicamente integrado. Há múltiplas razões para isso e, em última análise a maioria se origina de contextos sociais, culturais e religiosos.[1] É por esta razão que decidimos introduzir este tópico com uma curta compilação de comentários recolhidos diretamente da experiência no terreno, e que trazem luz à convergência de interesses e colaboração necessários entre mulheres e homens defensores de direitos humanos.

Mulheres defensoras de direitos humanos

As mulheres sempre foram importantes atoras na promoção e proteção dos direitos humanos. Entretanto, este papel nem sempre foi reconhecido. As mulheres trabalham sozinhas ou ao lado de homens na defesa dos direitos humanos.

Infelizmente, com muita freqüência:

- Elas enfrentam não apenas violência de gênero fora de suas organizações mas também preconceito e discriminação dentro das próprias organizações de direitos humanos.

[1] Ética da Atenção (Ethic of Care). Em seu livro "*In a different voice*" (1982), Carol Gilligan (Psicóloga de Harvard) afirma que ao passo que a moral masculina é baseada em justiça e direitos, a moral feminina é baseada no reconhecimento da importância das relações humanas e na atenção demonstrada para as necessidades dos outros. É legítimo, portanto, acreditar que se os homens seguissem a ética da atenção, haveria menos violência.

- Existe uma desculpa para "adiar" os direitos das mulheres da agenda ou fazê-los itens "extraordinários", como se houvesse ordem de prioridade ao invés da interdependência dos direitos humanos. Isso acontece em organizações mistas de defensores de direitos humanos.

- Mulheres defensoras de direitos humanos ainda são consideradas por seus pares masculinos como auxiliares. Colegas homens geralmente recusam tarefas vistas como menos fundamentais, como se sua masculinidade dependesse disso.

Sexismo, classismo, racismo, 'castas', xenofobia e homofobia são todos mais ou menos facetas sutis da mesma lógica subjacente às violações de direitos humanos contra homens, mulheres, pessoas de diferente orientação sexual, crianças, idosos, grupos étnicos, pessoas pobres... Todos eles têm um impacto na segurança: por exemplo, em alguns lugares, párias não são considerados de maneira alguma no plano de segurança: nem positivamente (por exemplo como pessoas que conhecem a vizinhança) nem negativamente (por exemplo como potenciais informantes dos agressores).

O conceito de violência é geralmente distorcido:

- lutar contra "violência contra as mulheres" ao invés de lutar contra violência masculina.

- "violência doméstica" como eufemismo para violência masculina.

Ao trabalhar para por um fim à violência masculina, a violência doméstica deveria diminuir como resultado. Estes não são assuntos separados.

As mulheres são geralmente consideradas como seres humanos inferiores, apesar de a ciência moderna ter estabelecido que diferenças de gênero não implicam uma ordem de capacidades. Soa óbvio, mas a experiência no campo e em oficinas com defensores tem demonstrado que esta idéia não está totalmente integrada. Isto explica nossa insistência.

Desde que as mulheres passaram a ter acesso à escola e educação elas provaram ser tão inteligentes quanto os homens (apenas para mencionar o uso da inteligência na escola). Existe uma confusão entre inteligência e acesso à informação. O mesmo pode ser dito de minorias étnicas e qualquer outro grupo discriminado: não se trata de uma questão antropológica, mas social. Um indivíduo ou grupo educado poderá participar de uma discussão dialética substantiva e desafiar o establishment. Isto explica o porquê de muitas meninas e mulheres ainda não terem acesso à educação.

As mulheres notam contradições entre defender direitos humanos por um lado e, de outro, discriminar contra as mulheres. Inevitavelmente, algumas vezes, as mulheres gostariam de dizer a seus colegas homens para voltarem ao 'bê-á-bá' e retornarem quando estiverem atentos a estes fatos e preparados para mudarem seu comportamento. Entretanto, as mulheres continuam a trabalhar com seus

colegas homens: mais mulheres se unem a ações de direitos humanos organizadas por homens do que homens se unem a atividades organizadas por mulheres.

Onde a violência é perpetrada contra as mulheres, seja mesmo contra uma só mulher (ou outro grupo ou indivíduo), não se trata de uma questão de cultura ou religião, mas de poder.

No caso de Nelson Mandela e Desmond Tutu, por exemplo, o apartheid não acabou porque a dignidade das pessoas negras foi repentinamente reconhecida, mas porque algumas pessoas brancas reconheceram que tinham perdido a sua. O mesmo se aplica à discriminação de gênero e para muitos outros tipos de discriminação.

Enquanto homens defensores de direitos humanos falharem em ver que a discriminação de gênero se origina da mesma lógica perversa que legitima outros tipos de discriminação, o movimento de direitos humanos continuará a ter apenas a metade de seu potencial. Ainda, continuará a servir os propósitos dos violadores de direitos humanos: dividir para reinar.

Direitos das mulheres não são apenas direitos das mulheres.

Este capítulo não tenta mudar mentes ou valores, mas ver como discriminação de gênero e outros tipos de discriminação impactam na segurança e proteção de mulheres, primeiramente, mas também de homens defensores. Ao passo que uma mudança de mentalidade possa ser um objetivo muito ambicioso, dissuasão não é. E isso envolve mudanças de comportamento. Neste caso, a solidariedade masculina em questões de segurança das mulheres contribui para a segurança de todos os defensores de direitos humanos.

Mais material foi produzido sobre este tema no contexto da Consulta Internacional sobre Mulheres Defensoras de Direitos Humanos, realizada em Colombo, Sri Lanka, em 2005.[2]

http://defendingwomen-defendingrights.org/pdf/WHRD-Proceedings.pdf

Ataques a mulheres defensoras dos direitos humanos

Em seu **Informe anual de 2002 à Comissão de Direitos Humanos** da ONU, Hina Jilani, então Representante Especial do Secretário-Geral da ONU para os Defensores dos Direitos Humanos afirmou:

> *As mulheres defensoras dos direitos humanos estão em igualdade com seus homólogos masculinos ao situar-se na primeira linha da promoção e proteção dos direitos humanos. Entretanto, em sua atuação, como mulheres, enfrentam a riscos específicos para seu gênero que se somam àqueles que enfrentam os homens.*

2 Você encontrará um guia muito prático sobre mulheres defensores de direitos humanos na página web do UNHCHR em http://www.unhchr.ch/defenders/tiwomen.htm. Veja também o Relatório: Debate sobre as Mulheres Defensoras de Direitos Humanos com a Representante Especial do Secretário-Geral da ONU para os Defensores de Direitos Humanos, 4-6 abril de 2003, Publicado por Asia Pacific Forum on Women, Law and Development, e Atores Essenciais de Nosso Tempo: os defensores de direitos humanos nas Américas, Anistia Internacional.

Em primeiro lugar, como mulheres, ***resultam mais visíveis****. Isto é, as mulheres defensoras podem despertar uma maior hostilidade que seus colegas masculinos porque como mulheres defensoras dos direitos humanos podem chocar com as normas culturais, religiosas ou sociais sobre a feminilidade e o papel da mulher num país ou sociedade em particular. Neste contexto, não somente devem enfrentar violações dos direitos humanos devido a seu trabalho como defensoras dos direitos humanos, mas ainda mais por causa de seu gênero e o fato de que* ***seu trabalho pode se opor a estereótipos*** *sociais sobre a natureza submissa das mulheres, ou desafiar os conceitos da sociedade sobre a condição das mulheres.*

Em segundo lugar, não resulta improvável que a hostilidade, intimidação e repressão a que se defrontam as mulheres defensoras possa, por si mesma, tomar uma forma específica baseada no gênero, que vai, por exemplo, desde o abuso verbal dirigido exclusivamente a mulheres por seu gênero até a intimidação ou assédio sexual e o estupro.

A este respeito, a ***integridade profissional das mulheres e sua posição na sociedade pode ser ameaçada e desacreditada*** *em formas que são específicas para elas, tais como os tão conhecidos pretextos que questionam sua probidade quando – por exemplo – reivindicam seu direito a saúde sexual e reprodutiva, ou à igualdade com os homens, que inclua uma vida livre de discriminação e violência. Neste contexto, por exemplo, as mulheres defensoras dos direitos humanos foram julgadas com base em leis que penalizam uma conduta que vem a ser o legítimo uso e exercício de direitos protegidos sob a lei internacional baseando-se em falsas acusações apresentadas contra elas em virtude de suas opiniões e trabalho de apoio na defesa dos direitos das mulheres.*

Em terceiro lugar, os abusos aos direitos humanos perpetrados contra mulheres defensoras dos direitos humanos podem, por sua vez, ter repercussões que estão, por si mesmas baseadas na questão de gênero. Por exemplo, ***o abuso sexual*** *de uma mulher defensora dos direitos humanos sob custódia e seu* ***estupro pode representar uma gravidez e enfermidades sexualmente transmissíveis, incluindo o HIV/AIDS.***

Alguns direitos específicos de mulheres são quase exclusivamente promovidos e protegidos por mulheres defensoras dos direitos humanos. Promover e proteger os direitos das mulheres pode ser um fator de risco adicional, já que a reafirmação de tais direitos é considerada como uma ameaça ao ***patriarcado e como transformador de tradições culturais, religiosas e sociais****. A defesa dos*

direitos da mulher à vida e liberdade em alguns países tem resultado na violação da vida e liberdade das próprias defensoras. Do mesmo modo, protestos contra práticas discriminatórias resultaram numa ação judicial contra uma destacada defensora dos direitos humanos da mulher acusada de apostasia.

Fatores tais como a idade, a etnia, a educação, a orientação sexual e o estado civil devem também ser tomados em consideração, já que os diferentes grupos de mulheres defensoras enfrentam a muitos desafios diferentes e, portanto, têm diferentes necessidades de proteção e segurança.

A avaliação das necessidades de proteção das mulheres defensoras ajudará a esclarecer as especificidades e diversas necessidades, vulnerabilidades e estratégias de resistência das mulheres defensoras. Desta forma, suas situações poderão ser atendidas de maneira mais adequada em situações de emergência e em seu dia-a-dia.

A Declaração sobre a eliminação da Violência contra a Mulher (1993) define a violênciacontra a mulher como:

Qualquer ato de violência com base em gênero, sexo, que resulte em, ou que é provável resultar em dano físico, sexual, mental ou sofrimento para a mulher, incluindo as ameaças de tais atos, coerção ou privação arbitrária de liberdade, ocorrida em público ou na vida particular. (Artigo 1)

Entender-se-á que a violência contra a mulher abarca os seguintes atos, ainda que não se limite a eles:

a) ♦ A violência física, sexual e psicológica que se produza na família, incluídos os maus tratos, ou abuso sexual das meninas no lar, a violência relacionada com o dote, o estupro pelo marido, a mutilação genital feminina e outras práticas tradicionais nocivas para a mulher, os atos de violência perpetrados por outros membros da família e a violência relacionada com a exploração;

b) ♦ A violência física, sexual e psicológica perpetrada dentro da comunidade em geral, inclusive o estupro, o abuso sexual, o assédio e a intimidação sexuais no trabalho, em instituições educacionais e em outros lugares, o tráfico de mulheres e a prostituição forçada;

c) ♦ A violência física, sexual e psicológica perpetrada ou tolerada pelo Estado, onde quer que ocorra. (Artigo 2)

A segurança das mulheres defensoras de direitos humanos

As mulheres defensoras de direitos humanos pagam um elevado preço por seu trabalho de proteção e promoção de direitos humanos. As defensoras têm que enfrentar riscos que estão relacionados com seu gênero, e sua segurança portanto requer uma atenção específica.

As causas devem ser levadas em consideração nas políticas organizacionais e protocolos de segurança. Aqui apresentamos uma lista não exaustiva de causas mencionadas no Relatório 2002 de Hina Jilani, mencionado acima:

- As mulheres podem atrair uma atenção não desejada.
- As mulheres defensoras podem ter que infringir leis patriarcais e tabus sociais.
- Existem formas de ataque específicas contra mulheres defensoras.
- As mulheres defensoras podem sentir-se forçadas a "demonstrar" sua integridade.
- Os homens defensores poderiam não compreender, ou inclusive rechaçar o trabalho das mulheres defensoras.
- As mulheres defensoras podem ser vítimas da violência doméstica.
- As mulheres defensoras geralmente têm obrigações familiares adicionais.
- Todas estas pressões supõem uma carga adicional de trabalho e estresse para as mulheres defensoras.

Rumo a uma melhor segurança e proteção para as mulheres defensoras de direitos humanos: Medidas e políticas globais permanentes de segurança

Integrando a participação das mulheres

Em poucas palavras, isto significa assegurar uma maior participação de mulheres junto a homens na tomada de decisões, colocando as questões de segurança das mulheres na pauta, e situando as mulheres em igualdade com os homens na tomada de decisões sobre medidas de segurança. É importante incluir as experiências e opiniões das mulheres e assegurar-se de que as mulheres definam normas e procedimentos de segurança, assim como observar seu desenvolvimento e avaliá-los.

Assegurar-se de resolver as necessidades de segurança e proteção específicas de gênero

Assim como outras necessidades de segurança, é muito importante, em toda organização ou grupo de defensores que estes determinem responsabilidades para lidar com a violência de gênero e com os riscos de segurança das defensoras. As pessoas responsáveis pela segurança deverão ter bom conhecimento das necessidades específicas das mulheres defensoras. Em algumas ocasiões,

talvez seja necessário alocar responsabilidade a outra pessoa que possa aportar um conhecimento e percepção específicos para esta tarefa. Por exemplo, uma pessoa poderia ser responsável pela segurança, mas a organização decide mais tarde designar a outra pessoa com experiência prática e teórica para lidar com a violência de gênero. Neste caso, ambas pessoas devem trabalhar conjuntamente para assegurar que todos os procedimentos de segurança funcionem sem dificuldade e respondam às diferentes necessidades das pessoas.

Formação

A formação de todas as pessoas que trabalham numa organização de direitos humanos é um elemento chave para melhorar a segurança e proteção e deve incluir ou criar consciência sobre as necessidades específicas das mulheres defensoras.

Sensibilização

- Sobre qualquer confusão entre valores sociais, culturais e religiosos e direitos das mulheres e direitos humanos.
- Sobre violência doméstica contra as mulheres. Isto inclui danos físicos, sexuais e psicológicos dentro da família como surras, estupro marital, mutilação genital feminina e outras práticas tradicionais que são danosas e trazem risco às vidas das mulheres.
- Dentro das famílias de mulheres defensoras de direitos humanos. E a necessidade de levar estes mesmos cursos de ação utilizados contra violência fora do ambiente doméstico. As organizações deveriam considerar qualquer contradição entre seus objetivos e membros concordarem com violência doméstica. Desde um ponto de vista de segurança, isto implicaria desacreditar toda a organização com a possível conseqüência de diminuir o apoio de atores chave.
- Sobre o fato de que muitas mulheres serão influenciadas, no que tange à segurança, pelo fato de que elas devem cuidar de filhos e outros parentes além de terem seu próprio trabalho. Sobre como homens podem promover tarefas domésticas compartilhando-as sem afetar sua masculinidade.
- Sobre o fato de ambos mulheres e homens defensores de direitos humanos estarem condenados a dedicarem seus esforços em prol de outros ao invés de suas famílias.

Em resumo,

As diferenças nas necessidades de segurança das mulheres estão relacionadas aos diferentes papéis, os diferentes tipos de ameaças e as diferentes situações (tais como a detenção, o trabalho de campo, etc.). O propósito é poder desenvolver respostas sensíveis à violência de gênero contra as mulheres e demais defensoras.

Comentário adicional

A violência de gênero tem recebido **atenção insuficiente**. A consciência geral sobre a violência de gênero na organização ou grupo pode ajudar a que as pessoas identifiquem ameaças ou incidentes de gênero específicos. Os trabalhadores dispostos a colaborar podem também atuar como "pontos de acesso" para que mulheres e homens que queiram buscar soluções para as ameaças ou violência vinculadas ao gênero, contra eles ou outras pessoas da organização ou da comunidade.

Agressões sexuais e segurança pessoal

Estatisticamente, estupros afetam mais mulheres do que homens. Alguns homens defensores de direitos humanos que foram vítimas falam disso como tortura sexual e estão conscientes de que é isso que as mulheres sofrem. Estupro é tortura em si mesmo pois atenta contra a integridade física e psíquica da pessoa.

Crimes comuns são geralmente uma cobertura quando se trata de defensores de direitos humanos. Se formos proporcionais, podemos falar de crime comum de estupro e de crime de tortura sexual[3] no caso de um crime político (repressão ao trabalho dos defensores de direitos humanos onde as vítimas podem ser pré-selecionadas ou alvos oportunistas).

Trata-se de um crime de poder e de violência. Tortura sexual é uma alternativa para o agressor demonstrar seu poder sobre a vítima.

Tortura sexual é uma das conseqüências da agressão física. Portanto, a prevenção deve começar com a implementação de todas as medidas de segurança descritas anteriormente para reduzir o risco de agressão. É por esta razão que a prevenção de ataques sexuais pode ser similar à de outras agressões.

Recordemos que, em muitos casos, as mulheres que são seqüestradas por um agressor, são estupradas (e são espancadas ou ainda assassinadas). Portanto, as mulheres deveriam tomar a decisão firme de não se deslocarem com um agressor potencial para outra localização (a não ser que sua recusa pudesse colocar em perigo sua vida ou a de outros).

Todas as mulheres defensoras de direitos humanos enfrentam o risco de tortura sexual mas nem todas as defensoras de direitos humanos são iguais diante dessa situação. Tudo depende do contexto político, social, cultural e religioso. Algumas mulheres terão de lidar com as conseqüências psicológicas e de saúde física. Outras com a saúde física, psicológica, conseqüências culturais, sociais e ainda o sofrimento de ter de relatar o fato e ser questionada sobre isso durante o procedimento judicial.

3 Convenção da ONU contra a Tortura: "(…) o termo "tortura" designa qualquer ato pelo qual uma violenta dor ou sofrimento, físico ou mental, é infligido intencionalmente a uma pessoa por ou instigada por uma autoridade pública, com o fim de se obter dela ou de uma terceira pessoa informações ou confissão; de puní-la por um ato que ela ou uma terceira pessoa tenha cometido ou seja suspeita de ter cometido; de intimidar ou coagir ela ou uma terceira pessoa. (…)"

Agressões sexuais devem ser abordadas a partir de todas as perspectivas e conseqüências, incluindo a dimensão psicossocial. Como em todo tipo de tortura, a pessoa sexualmente torturada poderá sofrer sentimentos de culpa, "perda de dignidade", falta de confiança, e em caso de estupro, também o sentimento de sujeira... As organizações podem considerar a possibilidade de analisar o conceito de dignidade: o que é dignidade? Quem decide sobre a dignidade de outra pessoa? Quem realmente perdeu sua dignidade: aquele que desceu ao ponto de torturar ou o/a torturado/a?

Uma política organizacional permanente deveria incluir:

- integração de necessidades específicas de mulheres defensoras de direitos humanos.
- resolver problemas de discriminação de gênero na organização.
- considerar o impacto cultural nas vítimas de abuso sexual e tortura.
- ...

Protocolos específicos:

- mulheres defensoras de direitos humanos em missões de campo.
- relações públicas com atores chave sobre proteção.
- lidar com as conseqüências de abuso sexual e tortura tais como gravidez indesejada e HIV/AIDS.

Ao definir estes protocolos, não esqueça de que:

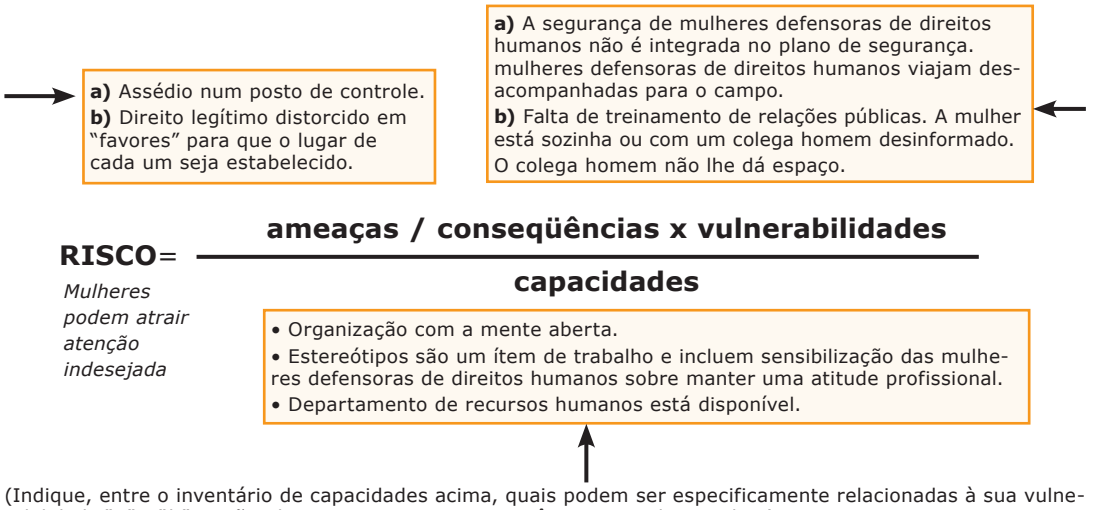
- Algumas mulheres defensoras de direitos humanos não ousam mencionar que foram vítimas de abuso sexual e tortura com seus colegas homens pois temem ser estigmatizadas ou desacreditadas (lembre-se que as vítimas geralmente sentem um sentimento de culpa apesar de totalmente injustificado).
- Em alguns países, organizações mistas raramente falam sobre isso.
- Alguns homens defensores de direitos humanos têm opiniões muito fortes sobre o aborto. Por outro lado, eles não estão preparados para criar uma criança indesejada. Em muitos países o aborto não é permitido seja pela lei, cultura ou religião. Nestes casos infanticídios tornaram-se opções comuns tanto quanto abandono de crianças. Este último caso contribui com o fenômeno de bruxaria infantil e pelo aumento de crianças soldados, além de muitas outras mazelas sociais. Ademais, as mulheres podem considerar tomar a pílula do dia seguinte (pílula que induz a menstruação independentemente do fato da mulher estar ou não grávida).
- Não há escolha certa ou errada, apenas conseqüências que devem ser analisadas pela organização.
- **É importante que você use a ferramenta de análise de risco.**

Exemplo:

Risco: *mulheres podem atrair atenção indesejada.*

Liste todas as possíveis ameaças e conseqüências dessas ameaças que podem ser consideradas um risco. Então, para cada ameaça ou conseqüência, liste as respectivas vulnerabilidades e capacidades. Então determine as capacidades desejáveis para reduzir as vulnerabilidades e trabalhar sobre elas.

Em outras palavras, o risco precisa ser desdobrado tanto quanto possível, como descascar uma cebola. Para cada camada (ameaça/conseqüência) determine as vulnerabilidades e capacidades relativas.



(Indique, entre o inventário de capacidades acima, quais podem ser especificamente relacionadas à sua vulnerabilidade "a" e "b". Então, determine quais outras você necessita desenvolver).

Reação frente a uma agressão sexual[4]

As opções de resposta no momento de uma agressão sexual são limitadas e dependerão estritamente da vítima. Não existe uma reação "correta" ou "equivocada". Em todo caso, o objetivo primordial é sobreviver. As opções disponíveis para a vítima no momento de uma agressão sexual podem incluir o seguinte:

1 ♦ **Ceder:** se a vítima teme por sua vida, talvez escolha submeter-se à agressão sexual.

2 ♦ **Resistência passiva:** fazer ou dizer qualquer cosa desagradável ou repugnante para arruinar o desejo de contato sexual do atacante. Poderia dizer que tem AIDS (apesar de o agressor poder reagir dizendo que também tem, e então tornar-se ainda mais agressivo).

3 ♦ **Resistência ativa:** utilizar toda a força possível para desvencilhar-se do atacante, como golpear, dar chutes, morder, arranhar, gritar e escapar.

4 A maior parte desta informação foi adaptada do livro Vam Brabant: *Operational Security in Violent Environments* e dos Manuais de Segurança de World Vision e World Council of Churches.

Em todos os casos:

- Se possível, tente mencionar o preservativo. Em algumas culturas e religiões, falsamente se considera como "consentimento", mas no fim do dia este é um problema deles. O seu poderá ser ainda maior pois terá de viver com uma possível gravidez, conseqüências de saúde e, além de todo o resto o pensamento de "e se?". Isto significa que as mulheres defensoras de direitos humanos poderiam considerar levar preservativos em sua bolsa ou usar preservativos femininos quando em missão a áreas perigosas. Isto quer dizer que o assunto deve ser discutido na organização e deve haver um orçamento para tal. O mesmo vale para a pílula do dia seguinte e qualquer outro tratamento hospitalar necessário. (ver mais abaixo: PEP)

- Se possível, tente recolher informação sobre o (s) agressor (es). Pode ser útil concentrar em algum detalhe que poderá ajudar no julgamento deles e diminuir a probabilidade de impunidade.

- Se possível, tente concentrar-se mentalmente para separar o corpo da alma.

Em qualquer caso, é preciso fazer o que se tenha de fazer para sobreviver. "Siga seus instintos". Ninguém sabe como reagirá numa situação como esta (ou qualquer outro tipo de tortura) e sua reação será a apropriada para você e sua situação em concreto.

Em muitos locais, tortura sexual toma proporções inimagináveis. Quando a lógica básica de segurança lhe diz para não ir a uma missão de campo antes de ter construído suficiente poder de dissuasão pois o risco de ser torturada sexualmente por grupos em disputa é extremamente alto, algumas organizações de defensores de direitos humanos e mulheres defensoras decidem ir além de seu pensamento de segurança para pensar nas outras vítimas. Apesar de a linha entre o que é aceitável ou não ser muito pessoal, nós não podemos deixar de insistir nas regras básicas de segurança. Durante as oficinas, as discussões já chegaram a considerar as seguintes opções em caso de agressão sexual durante uma missão de campo: a mulher defensora pode dizer que tem AIDS (mesmo que seja uma tortura sexual coletiva ou não) e criar dúvidas pois nem todos estarão seguros se têm AIDS ou não ou se serão afetados. Ela pode também dizer ao agressor que ela estaria menstruada. Para isso ela usaria toalhas sanitárias manchadas durante toda a missão de campo. Ela poderia usar roupas manchadas na esperança de que o socorro chegue a tempo.

HIV/AIDS é uma mazela na sociedade e não tem barreiras de gênero. Em alguns países onde a tortura sexual de mulheres se tornou uma arma de guerra, muitas mulheres estão considerando encontrar com os agressores para "explicar" como isso lhes afeta também: como o ponto não é da tortura sexual das mulheres para reprimir, mas que isso está levando a uma morte coletiva: A questão tornou-se de vida ou morte para todos, incluindo os agressores. É uma bomba relógio, para não mencionar o genocídio cultural.

Muitos homens defensores de direitos humanos também trabalham sobre torturas sexuais contra mulheres e a rejeição cultural relacionada a isso. A pesar disso, muitos deles dizem que repudiariam suas mulheres se isso acontecesse com elas.

Um homem defensor de direitos humanos uma vez questionou um colega (trabalhando para mudar atitudes familiares em relação a mulheres torturadas sexualmente) o que significaria adultério para ele. A resposta foi: "depende do quanto sua mulher representa para você".

Esta é a questão subjacente. Com muita freqüência, uma mulher é considerada apenas um objeto ou propriedade sexual. Uma vez "quebrado", deixe-a e pegue outra.

Uma mulher é geralmente considerada a mulher, filha, irmã, mulher de um homem. Raramente uma mulher é ela mesma com sua própria identidade. Afortunadamente, muitas mulheres podem contar com o apoio de seus colegas homens que dão apoio genuíno a elas.

Todas as organizações e grupos defensores dos direitos humanos devem dispor de planos de prevenção e reação para casos de agressões sexuais.

Quando possível, e dependendo do contexto local e do acesso a laboratórios médicos, os seguintes cuidados devem estar disponíveis:

- a administração de assistência médica efetiva (mesmo antes de limpar-se, para colher amostras para análise inclusive de DNA).
- fotos da vítima.
- assistência psicológica.
- denúncia às autoridades competentes.

Em todos os casos, o plano de reação deve incluir, no mínimo, a administração de assistência **médica efetiva, incluindo assistência psicológica**, seguido de assistência jurídica.

Para prevenir gravidez a vítima deve receber a pílula do dia seguinte (dentro de 24 horas): este é um contraceptivo de emergência (não uma pílula abortiva).

Apesar de não ser garantido, dependerá de muitas variáveis. Você pode considerar a Profilaxia Pós-Exposição (Post-exposure Prophylaxis, PEP). Um kit pós-estupro está disponível em alguns hospitais, contendo tratamento direcionado para interromper a transmissão de diversas doenças para vítimas que tenham recebido tratamento dentro de 72 horas após o estupro. Em qualquer caso, verifique imediatamente e regularmente a contaminação por doenças sexualmente transmissíveis.[5]

É necessário encontrar um justo equilíbrio entre assegurar-se de que a vítima obtenha o apoio de especialistas e assegurar o apoio e a reação apropriada por parte da organização.

Veja também *Prevenção e reação aos ataques* no Capítulo 1.5.

Resumo

As mulheres sofrem abuso de gênero, assédio e tortura determinados por uma cultura patriarcal. Organizações de direitos humanos mixas com freqüência reproduzem isso em seu microcosmo. A segurança de mulheres defensoras de direitos humanos é também a segurança de todos os defensores de direitos humanos.

É preciso integrar o tema dentro das políticas de segurança e protocolos das organizações. É preciso fazer mais do que simplesmente uma avaliação de risco. Este trabalho requer ainda:

- discutir os papéis e atitudes.
- trabalhar sobre presunções falsas e mudar atitudes derivadas de diferenças de gênero.
- fazer discriminação positiva para auxiliar as mudanças.
- que o orçamento de segurança inclua preservativos, a pílula do dia seguinte, terapia PEP, ...

Mais uma vez, não há garantia de resultados. A tortura sexual ocorre após agressão física. Ao reduzir a exposição a agressões, a probabilidade de tortura sexual também será reduzida.

5 Para mais informação acesse o site da Cruz Vermelha Internacional (CCVI): http://icrc.org/web/eng/siteeng0.nsf/html/congo-kinshasa-feature-201207A

A segurança em zonas de conflito armado

Objetivo:

Reducing the risks inherent in areas of armed conflict.

O risco em situações de conflito

Os defensores dos direitos humanos que trabalham em zonas de conflito estão expostos a riscos específicos, sobretudo nas situações de conflito armado: muitos dos assassinatos de civis são devidos a práticas indiscriminadas da guerra, mas muitos outros são o resultado de que civis se convertem em objetivos militares diretos, e é necessário que reconheçamos estes fatos como tais – a ação política é sempre necessária para afirmar estes fatos e tentar detê-los.

Apesar de não exercer qualquer tipo de controle sobre uma ação militar em curso, você pode adaptar sua conduta para evitar que o conflito o afete ou para reagir apropriadamente se algo vier a acontecer.

Se você está localizado numa zona onde ações armadas são freqüentes, é muito provável que já tenha estabelecido muitos dos contatos necessários para proteger sua família e os que trabalham com você, ao mesmo tempo em que dá continuidade ao seu trabalho.

Entretanto, se você não está localizado numa zona de conflito armado, deve **considerar três pontos desde o começo**:

a ♦ Que grau de risco você está preparado a assumir? Isto também é aplicável à(s) organização/pessoas com a(s) que você trabalha.

b ♦ Sua presença na região traz maiores vantagens que riscos? O trabalho de direitos humanos não pode ser mantido no longo prazo quando equivale a estar continuamente exposto a um risco elevado.

c ♦ O simples fato de "conhecer a zona" ou "saber muito sobre armas" não oferecerá nenhuma proteção aos disparos de um ataque com morteiros ou de franco-atiradores.

Tipos de fogo

Você pode estar exposto ao fogo de rifles, metralhadoras, morteiros, bombas e mísseis de terra, ar ou mar. O fogo pode estar mais ou menos orientado, e compreende desde um franco-atirador ou um helicóptero com boa visibilidade até morteiros ou artilharia. O fogo também pode ser da variedade de "saturação", dirigido a "varrer" uma zona inteira.

Quanto mais dirigido estiver o fogo, menor será o risco – sempre e quando o fogo não for dirigido a você, a sua zona em geral ou a uma zona vizinha, nestes casos o risco diminui se você pode se retirar de lá. **Em qualquer caso, lembre que você se encontra na linha de fogo, resultará difícil determinar se é dirigido a você. Estabelecer isso não é uma prioridade,** tal como veremos mais abaixo.

Tomar precauções: reduzir sua vulnerabilidade ao fogo cruzado

1 ♦ **Evite os lugares perigosos**.

Em uma zona de combate ou de ação terrorista, evite assentar lugar (ter um escritório ou permanecer durante um longo período) próximo de um possível alvo, como uma guarnição ou uma instalação de telecomunicações. Isto também é aplicável a zonas estratégicas como as entradas e saídas das zonas urbanas, os aeroportos ou os pontos estratégicos que controlam a zona circundante.

2 ♦ **Busque proteção adequada do ataque.**

Uma das principais causas de ferimentos são os estilhaços de vidro destruídos das janelas próximas. Cobrir as janelas com tábuas ou com fita adesiva reduzirá o risco de que isto ocorra. Em caso de ataque, fique longe das janelas e busque proteção imediata no solo, sob uma mesa, preferivelmente num quarto central com paredes grossas, ou, melhor ainda, no sótão.

Os sacos de areia podem ser práticos, mas somente se os demais edifícios também estão equipados com eles – se não, você corre o risco de chamar uma atenção desnecessária.

Se não há nada mais disponível, o solo ou qualquer buraco podem oferecer ao menos uma proteção parcial.

Um simples muro de tijolos ou a porta de um carro não podem proteger de um rifle ou de armas de fogo mais pesadas. Os bombardeios e os mísseis podem matar num raio de vários quilômetros, assim que não é necessário estar muito próximo do combate para que ele o alcance.

As explosões de bombas ou morteiros podem danificar seus ouvidos. Cubra-os com ambas as mãos e abra um pouco a boca.

A clara sinalização do escritório central, sua localização ou dos veículos pode ser útil, mas lembre que **isto é unicamente aplicável se os agressores respeitam seu trabalho.** Se não é o caso, isso causará exposição desnecessária. Se você quer ser identificado, faça-o com uma bandeira ou com cores ou sinais nas paredes e nos telhados (caso exista risco de ataque aéreo).

3 ♦ **Deslocamento em veículos.**

Se disparam diretamente contra seu veículo, você pode pensar em analisar a situação, mas é muito difícil fazer uma avaliação acertada nestas circunstâncias. No geral, **é aconselhável imaginar que o veículo é ou pode ser um alvo, e que a reação apropriada é, portanto, sair e proteger-se imediatamente**. Um veículo é um alvo perfeito. Não somente é vulnerável, mas além do fogo direto pode causar outros ferimentos com os vidros que se quebram ou ainda da explosão do tanque de gasolina. Se o fogo não é próximo, continue o deslocamento no veículo até que encontre um lugar próximo onde se proteger.

Minas e artefatos explosivos não detonados (Unexploded ordnance, UXO)[1]

As minas e artefatos explosivos não detonados supõem uma séria ameaça para os civis em zonas de conflito armado. Podem ter diferentes formas:

- **Minas:**
  - ♦ As minas antitanque costumam estar colocadas em estradas e caminhos e podem destruir um veículo normal.
  - ♦ As minas anti-pessoais são menores e podem encontrar-se em qualquer lugar onde se supõe que circulam pessoas. A maioria das minas anti-pessoais está enterrada no solo. Não se esqueça de quem coloca minas numa estrada pode também minar as margens, os campos e os caminhos próximos à estrada.
- **Bombas armadilha (booby-traps):**
  - ♦ As bombas armadilha são pequenos explosivos escondidos num objeto de aspecto normal ou atrativo (com cores, por exemplo), que explodem ao serem tocados. O termo também é utilizado para as minas presas a um objeto que pode ser movido ou ativado (pode ser qualquer coisa, desde um cadáver até um carro abandonado).
- **Projéteis não detonados:**
  - ♦ Qualquer tipo de munição que foi disparada mas que não explodiu.

Atualmente percebemos um recrudescimento no uso de bombas de fragmentação (cluster bombs). Elas são tão freqüentes quanto as minas anti-pessoais. As munições de de fragmentação são remanescentes de bombas de fragmentação[2]. Cada bomba de fragmentação é feita de centenas de sub-munições ejetadas em todas as direções. Elas são desenhadas para cobrir áreas grandes e explodir ao impacto. Entretanto, nem todas elas explodem quando atiradas e o percentual de falhas é grande.[3] Elas são mais instáveis do que as minas e portanto podem explodir a qualquer momento. Algumas são coloridas e portanto atraem a atenção de crianças.

---

1 Grande parte da informação desta seção foi adaptada do excelente manual de Koenraad vam Brabant: *Operational Security Management in Conflict Areas* (veja a Bibliografia selecionada).

2 Veja *Principes de droit des conflits armés*, Eric David (ULB, Brylant, 2002). Veja também a recente campanha da Handicap International, Anistia Internacional etc.; www.clustermunition.org, www.controlarms.org.

3 Estimativas da taxa de falha encontram-se entre 5 e 80%, dependendo do tipo de munição de fargmentação e da consistência ou dureza do solo. Elas se tornam, de fato, praticamente a mesma coisa que minas anti-pessoais.

Prevenção contra as minas e os projéteis não detonados.

A única forma de evitar as zonas minadas é sabendo onde estão. Se você não se encontra ou não vive na zona, a única forma de determinar a localização dos campos minados é perguntando de forma contínua e ativa aos moradores locais, ou aos especialistas[4], se houve explosões ou combates na região. É aconselhável utilizar estradas asfaltadas, ou caminhos transitáveis de uso habitual, ou seguir as trilhas de outros veículos. **Não saia da estrada, nem sequer na margem ou beira da estrada, com ou sem o veículo**. As minas, ou outro tipo de artilharia não detonada, podem permanecer escondidas e ativas durante anos.

Os artefatos não detonados pode encontrar-se em qualquer zona onde tenha havido um combate ou fogo armado, e podem ser visíveis. A regra de ouro é: **não se aproxime, não os toque, marque o lugar se puder e transmita a informação imediatamente.**

As bombas armadilha costumam encontrar-se, normalmente, nas zonas de onde se retiraram os combatentes. Nestas áreas, é imperativo não tocar nem mover nada e permanecer afastado dos edifícios abandonados.

Se uma mina explode debaixo de um veículo ou de uma pessoa próximos.

Existem duas regras de ouros:

- Onde há uma mina sempre há mais.
- Nunca atue de forma impulsiva, ainda que haja feridos.

Se você precisa se retirar, volte sobre seus passos se eles ainda forem visíveis. Se você viaja num veículo e suspeita que pode haver minas antitanque, abandone o veículo e retire-se seguindo de volta as trilhas das rodas.

Se você quer se aproximar de uma vítima ou retirar-se de uma zona minada, a única forma de fazê-lo é de joelhos, agachado e examinando o chão introduzindo um pedaço fino de madeira ou de metal pontiagudo (prodder) delicadamente na terra num ângulo de 30 graus, para detectar com cuidado qualquer objeto duro. Se você encontrar algum objeto duro, limpe a área ao redor com cuidado até que possa ver o que é. As minas também podem explodir por meio de arames presos a elas. Se você encontrar algum arame ou fio, não corte.

Tudo isso, evidentemente, requer uma quantidade de tempo considerável.[5]

4 ONGs especializadas em limpeza de áreas minadas ou Forças de Paz da ONU. Algumas ONGs internacionais também possuem mapas de zonas minadas e desminadas.

5 Você pode encontrar manuais e recursos sobre a conscientização e educação sobre minas na página eletrônica da Campanha Internacional para Proibir as Minas Terrestres (International Campaign to Ban Ladmines): http://www.icbl.org

A segurança nas comunicações e a tecnologia da informação

(Com a colaboração de Privaterra – www.privaterra.org)

Objetivo:

Os grandes vazios da tecnologia da informação presentes em todo o mundo afetam também os defensores dos direitos humanos. Este capítulo trata principalmente das tecnologias da informação – isto é, os computadores e a Internet[1]. Os defensores sem acesso a computadores ou Internet talvez considerem parte do conteúdo irrelevante. Entretanto, podem vir a necessitar obter urgentemente os meios e a formação necessários para o uso das tecnologias da informação na defesa dos direitos humanos.

Guia dos problemas de segurança em comunicação e como evitá-los

Conhecimento é poder, e conhecendo a origem de seus possíveis problemas de comunicação, você se sentirá mais seguro para realizar seu trabalho. A seguinte lista resume as diferentes formas de acesso ou de manipulação ilegal de informação ou do sistema de comunicação, e sugere várias medidas para evitar estes problemas de segurança.

Falar

Não é necessário que a informação passe pela Internet para que tenham acesso a ela ilegalmente. Quando você discute temas confidenciais, considere os seguintes pontos:

1 ♦ Você confia na pessoa com quem está falando?

2 ♦ Eles precisam saber da informação que você lhes está dando?

3 ♦ Você está num ambiente seguro? É possível que se coloquem microfones escondidos ou outros dispositivos de escuta em áreas que as pessoas consideram seguros, tais como escritórios particulares, ruas com muita circulação, quartos da casa e carros.

1 Este Capítulo é baseado no trabalho realizado por Roubert Guerra, Katitza Rodríguez e Caryn Mladen da Privaterra, uma ONG que trabalha por todo o mundo em segurança de Tecnologia da Informação para os defensores de direitos humanos oferecendo cursos e informação. (Este texto foi ligeiramente adaptado em alguns parágrafos por Enrique Eguren).Outras páginas oferecendo informações idênticas são: http://security.ngoinabox.org and http://www.tacticaltech.org

É difícil responder à terceira pergunta, porque podem ter instalado gravadores ou microfones escondidos na sala para gravar ou transmitir tudo que se diz ali. Também podem ter microfones laser apontados para as janelas para escutar as conversas a partir de grande distância. As cortinas grossas, assim como a instalação de janelas duplas, podem proteger em parte destes microfones laser. Alguns edifícios mais seguros têm dois conjuntos de janelas nos escritórios para reduzir o risco destes aparelhos de escuta por laser.

O que fazer?

■ **Sempre imagine que há alguém escutando.** Uma atitude de paranóia saudável pode ajudá-lo a ser mais cauteloso com assuntos confidenciais.

■ **Detectores de microfones ou rastreadores podem detectar os aparelhos de escuta,** mas podem ser caros e difíceis de adquirir. Além disso, às vezes, os próprios encarregados de detectar os microfones são os responsáveis por instalá-los. Durante uma varredura, poderiam ser encontrados alguns "descartáveis" (microfones ocultos muito baratos, e feitos justamente para serem encontrados) ou curiosamente não encontrar nada e declarar seus escritórios "limpos".

■ **O pessoal de limpeza pode representar uma grave ameaça de segurança,** porque podem ter acesso a seus escritórios fora do horário de trabalho e levam o lixo a cada noite. Todo o pessoal deveria ser examinado cuidadosa e regularmente por algum dispositivo de segurança, já que poderiam ser comprometidos, uma vez que foram incorporados à organização.

■ **Mude as salas de reuniões com tanta freqüência quanto seja possível.** Quanto maior o número de salas ou lugares onde troquem informação, maior o número de pessoal e equipes serão necessários para a escuta.

■ **Suspeite dos presentes dados a você para que leve consigo todas as horas,** como uma caneta cara, um broche de lapela; ou para que utilize em seu escritório, como um peso de papel bonito ou um quadro grande. No passado, temos registros deste tipo de objetos sendo usados para escutar conversas.

■ **Imagine que uma parte de sua informação está exposta sempre**. Talvez você decida mudar de planos e códigos freqüentemente, oferecendo a seus interlocutores apenas fragmentos da informação verídica. Você pode repassar informação falsa para comprovar se alguém faz uso ou responde a ela.

■ Para minimizar a efetividade dos microfones laser, **discuta os assuntos confidenciais num sótão ou numa sala sem janelas.** As tempestades ou outras mudanças climáticas podem reduzir a efetividade de alguns dispositivos de escuta.

■ **Coloque uma gravação de ruído alto ou uma canção popular** de fundo para que interfiram na recepção do som. Alguns equipamentos conseguem captar conversar a até 50 metros de distância. Ou seja, o seu escritório não necessita ter uma escuta fisicamente presente. Somente alta tecnologia pode filtrar os ruídos sobrepostos a uma conversação.

■ **Os espaços abertos podem ser tão práticos como nocivos.** Se você se reúne num lugar isolado, será mais fácil comprovar se alguém os observa, mas será impossível se esconder entre as pessoas e escapar. As multidões podem ajudar a passar despercebido, mas também é muito mais fácil ser visto e ouvido nelas.

■ **Se o seu escritório for numa área rural (aberta),** pergunte a um membro da organização para permanecer fora e reportar se ele/a consegue ouvir a conversa e peça que vigie elementos indesejáveis que passem pelo local.

Telefones celulares

Se o operador da escuta possui uma boa capacidade tecnológica, poderá escutar todo tipo de chamadas telefônicas. Nenhum tipo de chamada pode ser considerada segura. Os telefones celulares digitais são mais seguros que os telefones celulares analógicos e as linhas fixas são mais seguras ainda que os dois anteriores.

A vigilância de celulares pode detectar sua localização e suas conversas. Para identificar seu paradeiro, não é necessário que esteja falando – basta que você tenha o celular ligado para que seja encontrado.

Não guarde informação confidencial como nomes e números de telefone na memória de seu telefone. Se você for roubado, esta informação pode ajudá-los a localizar e comprometer as pessoas que você quis proteger.

Para emergências, onde possível procure ter dois telefones não identificados (pré-pagos ou de cartão). Eles só podem ser usados para chamar um ao outro ou para serem chamados por um número "já conhecido". Não os use de locais onde você pode ser facilmente identificado. Lembre de não deixá-los no seu telefone celular quando não estão em uso pois podem ser rastreados. Troque-os regularmente. Use discrição durante as conversas como se estivesse usando o telefone usual.

A segurança do material de informação do escritório

Mantenha o escritório fechado com chave todas as horas, incluindo portas e janelas. Utilize chaves que requeiram uma autorização específica para fazer uma cópia e não perca de vista nenhuma das cópias. NÃO dê chaves a terceiros, nem sequer ao pessoal de limpeza ou de manutenção, e assegure-se de que você ou alguém de confiança esteja sempre presente quando pessoas estranhas ao escritório estejam presentes. Se isso não for possível, assegure-se de dispor de uma sala com acesso limitado para guardar os arquivos confidenciais. Procure fechar com chave todas as portas do escritório e, ao finalizar o dia, deixe todos os resíduos não-confidenciais no corredor.

Utilize um triturador de papel para todos os documentos confidenciais. As tiras de papel trituradas são quase completamente inúteis. Se você quer se desfazer de um material extremamente confidencial, pode queimar os restos, pulverizar as cinzas e jogar fora no banheiro.

Segurança básica de computadores e arquivos[2]

Se possível, procure guardar os computadores sob chave ao sair do escritório. Vire as telas dos computadores das janelas.

Utilize um protetor de sobrecarga para todas as tomadas elétricas (as variações de corrente elétrica podem danificar seu computador).

Guarde as cópias de segurança, incluindo arquivos de papel, num lugar seguro e separado. Assegure-se de que as cópias de segurança estejam protegidas, guardando-as num disco rígido encriptado com dados seguros da organização, ou protegido com cadeados sofisticados.

Para reduzir o risco de acesso ao seu computador, proteja-o com uma senha e desligue-o sempre que saia de perto dele.

Encripte seus arquivos acaso alguém consiga ter acesso a seu computador ou descobrir a senha.

Crie cópias de segurança diariamente para poder recuperar seus arquivos em caso roubo ou destruição do computador. Mantenha os documentos de segurança encriptados longe de seu escritório, num lugar seguro.

Os arquivos apagados não poderão ser reconstruídos se você utiliza o PGP Wipe ou outro programa de utilitário, ao invés de apenas os deletar e colocá-los na lixeira ou arquivo de reciclagem do computador.

Seu computador pode ser programado, sem que você perceba, para enviar seus arquivos fora ou para deixá-lo indefenso. Para evitar isso, adquira seu computador de uma fonte segura, limpe o computador (isto é, reformate o disco rígido) ao iniciá-lo, e instale apenas os programas que você realmente necessite. Permita somente aos técnicos de confiança que façam a manutenção do computador e observe-os todo o tempo.

Desconecte o modem/conexão telefônica de seu computador, ou senão desconecte da Internet, quando deixar o computador desatendido. Desta forma, os programas maliciosos que ligam no meio da noite não funcionarão. Nunca deixe seu computador conectado se pensa em passar o dia fora. Procure instalar um programa que invalide o acesso após certo tempo determinado de inatividade. Desta maneira, seu computador não estará exposto enquanto você toma um café ou faça cópias, por exemplo.

Em suas preferências de Internet, ative as extensões de arquivos para saber que tipo de arquivo é antes de o abrir. Você poderá ser contaminado com um vírus se abrir um arquivo executável, pensando que se trata de um arquivo de texto. Se você utiliza *Internet Explorer*, clique duas vezes no *Painel de controle* de seu computador e depois em *Opções*. Clique em *Ver* e confira se o quadro de *Ocultar as extensões de arquivo para tipos de arquivo conhecidos* NÃO esteja ativado.

2 Se você deseja informação mais detalhada sobre a segurança de computadores, consulte a Front Line através do e-mail info@frontlinedefenders.org ou a Privaterra no e-mail info@privaterra.org

Seu email não passa diretamente de seu computador ao computador do destinatário, mas passa por várias conexões e vai deixando informação no caminho. **É possível ter acesso a sua mensagem em qualquer parte do caminho (não somente em seu país, mas também a partir do seu país!).**

Alguém pode estar olhando por cima de seu ombro enquanto tecla. Isto é particularmente problemático nos cafés com Internet. Se você está conectado a uma rede, todo mundo no escritório tem acesso a seu email. Seu sistema administrativo pode ter alguns privilégios (de administração) especiais para acesso a todos os correios eletrônicos.

Seu provedor de Internet (ISP) tem acesso a seus correios eletrônicos, e qualquer pessoa com influência sobre seu ISP pode pressioná-lo para conseguir que o envie cópias de todos seus correios eletrônicos ou para impedir que passem certas mensagens.

Ao passar pela Internet, seus e-mails passam por centenas de sites inseguros. Os piratas de informática podem ter acesso às mensagens de e-mail enquanto elas são transmitidas. O ISP de seu destinatário também pode ser vulnerável, da mesma forma que sua rede interna e seu escritório.

Segurança de Internet básica

Os vírus e outros problemas, tais como os "Cavalos de Tróia" ou os "Trojans", podem vir de qualquer parte; inclusive seus amigos podem propagar um vírus sem saber. Utilize um bom programa antivírus e mantenha-o atualizado, com conexões automáticas à Internet. Constantemente, se criam e se descobrem novos vírus, por isso você deve consultar a *Biblioteca de Informação sobre Vírus* em www.vil.nai.com para saber as últimas atualizações de proteção.

Os vírus costumam ser propagados através do e-mail, assim, procure fazer uso seguro do correio eletrônico (veja abaixo). Os vírus são programas únicos, construídos para replicar e podem ou não ser nocivos. Os "Trojans" são programas construídos para oferecer o acesso de seu computador a terceiros (ou a qualquer um!).

Um bom "firewall" pode ajudá-lo a passar despercebido ante os piratas de computador e manter longe os intrusos que tentam ter acesso a seu sistema. Desta forma, seu computador não poderá conectar-se a Internet sem autorização e isso também impede que programas como os "Trojans" enviem informação ou abram as "portas traseiras" de seu computador para deixar entrar os piratas de informática.

O sistema de "key logger" pode localizar cada tecla que você aperta. Estes programas podem ser instalados tendo acesso a seu computador em sua ausência, ou por meio de um vírus ou um "Trojan" que ataca seu sistema pela Internet. Os "Key loggers" localizam as pulsações de seu teclado e informam sobre suas atividades, normalmente pela Internet. É possível acabar com eles utilizando uma senha para proteger seu computador, fazendo uso do e-mail de forma segura, utilizando um programa antivírus, e um programa para digitar sua senha com um "mouse". Também é possível incapacitar os "Key loggers", desconectando fisicamente o computador do acesso a Internet – normalmente você apenas tem

de tirar a conexão telefônica do computador da tomada – quando não estiver utilizando.

O endereço de e-mail pode ser "spoofed" (manipulado/falsificado) ou utilizado por uma pessoa que não é o proprietário real. O pirata de computadores pode conseguir este acesso ao provedor de serviços de Internet do computador dessa pessoa e obter o acesso e sua senha, ou ainda utilizando um endereço quase idêntico. Por exemplo, se mudamos a letra "l" minúscula pelo número "1", teremos um endereço muito parecido e quase ninguém notará a diferença. Para evitar ser enganado por um "spoof", escreva frases coerentes na linha de Assunto e formule perguntas periodicamente que somente a pessoa em questão possa responder. Confirme todo pedido de informação, por meio de outro sistema de comunicação.

Mantenha a privacidade de sua atividade de navegação não aceitando "cookies" e eliminando seu arquivo de internet temporário cada vez que terminar de navegar na "web". Em *Internet Explorer*, clique em *Ferramentas*, e depois em *Opções*. Em *Netscape Navigator*, clique em *Edição*, e logo em *Preferências*. Uma vez dentro de qualquer destes menus, apague todo o seu histórico, todos os cookies que possa ter e esvazie seu arquivo de internet temporário (área de memória rápida). Lembre-se de apagar também todos seus favoritos. Os navegadores também arquivam as páginas "Web" que você visitou, em fichas de arquivo de internet temporário (área de memória rápida); assim você deve verificar que fichas devem ser apagadas de seu sistema.

Atualize todos os navegadores de Internet para que adotem uma encriptação de 128-bits. Isto ajudará a proteger qualquer informação que queira enviar através da Internet, incluindo senhas e outros dados confidenciais em formulários. Instale as atualizações de segurança mais atuais em todo os programas que você utiliza, sobretudo no *Microsoft Office, Microsoft Internet Explorer e Netscape.*

Não utilize um computador que contenha informação confidencial para conexões à Internet não essenciais.

Segurança básica do e-mail

Existem métodos seguros para utilizar o e-mail que você, seus amigos e associados deveriam colocar em prática. Informe seus amigos e associados de que não abrirá suas mensagens a não ser que pratiquem uma correspondência eletrônica segura.

1 ♦ NUNCA abra uma mensagem de um desconhecido.

2 ♦ NUNCA reenvie uma mensagem de um desconhecido, ou originada por um desconhecido. Todas estas mensagens tipo "Tenha pensamentos felizes", que as pessoas enviam, podem conter vírus. Ao enviar para seus amigos e associados, você pode infectar seus computadores. Se você gosta tanto do texto, reescreva-o e envie você mesmo. Se não vale a pena perder tempo reescrevendo, é sinal de que não era tão importante.

3 ♦ NUNCA baixe ou abra um arquivo anexo sem saber o que ele contém e se é seguro. Desconecte as opções de "download" automático de seu

programa de e-mail. Muitos vírus e "Trojans" se auto-propagam em forma de "vermes" e os vermes modernos costumam ser enviados por um conhecido. Os vermes inteligentes copiam sua agenda de endereços, sobretudo se você utiliza *Microsoft Outlook* ou *Outlook Express*, e a replicam fazendo-se passar por arquivos anexos legítimos de contatos legítimos. Se você usa o PGP para assinar seu e-mail, com ou sem arquivos anexos, você reduzirá em grande parte a confusão sobre os arquivos anexos sem vírus que possa enviar a seus companheiros (PGP é um programa elaborado para encriptar informação, veja mais abaixo em "Encriptação")

4 ♦ NÃO utilize HTML, MIME ou um formato de texto enriquecido (rich text format) em seu e-mail - unicamente um texto normal. Os correios eletrônicos enriquecidos podem conter programas incorporados, que permitem o acesso ou danificam os arquivos de seu computador.

5 ♦ Se você utiliza Outlook ou Outlook Express, desconecte a opção de vista prévia da tela.

6 ♦ Codifique seu e-mail sempre que possa. Um e-mail sem encriptar é como um cartão postal que pode ser lido por todo aquele que vê ou tem acesso a ele. Um e-mail encriptado é como uma carta num envelope dentro de uma caixa forte.

7 ♦ Titule suas mensagens com frases significativas para que o destinatário o reconheça. Peça a todos seus amigos e colegas que façam sempre um comentário pessoal na linha de Assunto para assegurar que são realmente eles quem enviam a mensagem. Caso contrário, alguém pode estar praticando spoofing com eles, ou um "Trojan" pode ter enviado um programa infectado a toda sua agenda de endereços, incluindo você mesmo. No entanto, não utilize as linhas de Assunto para revelar informação confidencial de mensagens encriptadas. Não se esqueça de que a linha de Assunto não está encriptada e pode revelar o tema da mensagem encriptada, o que pode desencadear ataques. Atualmente, há muitos programas de piratas de computador copiam mensagens de e-mail com títulos "interessantes" como "relatório", "confidencial", "privado" e outros, para indicar que a mensagem é de interesse.

8 ♦ NUNCA envie um e-mail a um grande grupo utilizando as linhas "Para" ou "CC". Envie a mensagem a você mesmo e inclua o nome dos demais nas linhas de "Bcc" (Blind carbon copy, ou cópia carbono oculta). Isto é por pura cortesia e ao mesmo tempo, é uma boa prática de privacidade. De outra maneira, você estará enviando meu endereço a pessoas que não conheço, uma prática que pode ser vista como mal-educada, ofensiva e provavelmente tão frustrante quanto perigosa.

9 ♦ NUNCA responda ao e-mail spam, mesmo se as proposições são de que você necessita fazê-lo para removê-lo da lista. Os servidores de spam enviam mensagens a grandes quantidades de endereços e nunca sabem quais estão "ativas" - isto quer dizer que o endereço de e-mail está sendo

utilizado ativamente. Ao responder, o servidor o reconhece como uma conta "ativa" e como conseqüência enviará mais spams.

10 ♦ Se possível, mantenha um computador separado, que não esteja conectado a nenhum outro e que não contenha nenhum arquivo de dados, para a correspondência eletrônica geral.

11 ♦ Você pode também utilizar dois endereços eletrônicos apenas para comunicar-se entre eles (como o exemplo dos dois números de telefone de emergência e com as mesmas regras). Ou um único endereço eletrônico, cuja caixa de entrada é acessível às pessoas mais confiáveis de sua organização: e-mails viajarão apenas uma vez e serão consultados por mais pessoas. Lembre-se de que quanto mais pessoas souberem disso, menos segura será o esquema. Mude o endereço de tempos em tempos.

Encriptação: Perguntas e Respostas

A seguir você encontrará uma lista com perguntas e respostas mais freqüentes. Para qualquer consulta não hesite em contatar a ONG Privaterra em www.privaterra.org

P: O que é a encriptação?

R: Encriptar significa transformar dados num código secreto que pode ser decifrado unicamente pela parte interessada. Contando com tempo e capacidade informática suficiente, todas as mensagens encriptadas podem ser decodificadas, mas é necessário investir grande quantidade de tempo e recursos. Para simplificar, a encriptação é uma forma de esconder seus arquivos e e-mail da vista dos espiões. Seus arquivos se traduzem com um código – aparentemente uma coleção de números e letras escolhidos aleatoriamente – que não guardam sentido algum para quem o vê. Para encriptar um arquivo, você pode "bloqueá-lo" com uma tecla, que representa uma senha. Para encriptar uma mensagem, você bloqueia com duas teclas utilizando sua senha. Somente o destinatário poderá abrir este e-mail, utilizando sua própria senha.

P: Por que os grupos de direitos humanos devem utilizar a encriptação?

R: Todo mundo deve utilizar a encriptação, porque as comunicações digitais são intrinsecamente inseguras. Entretanto, os ativistas de direitos humanos correm um maior risco que a maioria das pessoas e seus arquivos e comunicações são mais confidenciais. É fundamental que os trabalhadores dos direitos humanos utilizem a encriptação para proteger-se a si mesmos e às pessoas que tentam ajudar.

A tecnologia digital representa uma vantagem para os grupos de direitos humanos, já que lhes permite uma comunicação mais fácil, uma maior eficácia e mais oportunidades. Entretanto, toda vantagem traz também certos perigos. O simples fato de colocar o cinto de segurança não significa que você terá um acidente cada vez que dirija. Quando você dirige numa situação mais perigosa, como numa competição, você está mais propenso a utilizar o cinto de segurança, simplesmente por segurança.

Os trabalhadores de direitos humanos são conhecidos alvos de vigilância. Como é possível ter acesso e ler os correios eletrônicos encriptados com certa facilidade, torna-se quase inevitável que suas mensagens encriptadas sejam interceptadas em algum momento. De fato, talvez seu correio já tenha sido interceptado por seus oponentes e você nunca saberá. Os adversários das pessoas que você ajuda com seu trabalho também são seus adversários.

P: O uso da encriptação é ilegal?

R: Às vezes. Na maioria dos países do mundo o uso da encriptação é completamente legal. Entretanto, existem exceções. Na China, por exemplo, as organizações devem solicitar uma permissão para utilizar a encriptação, e qualquer programa de encriptação de seu computador portátil deve ser declarado ao entrar no país. Cingapura e Malásia têm leis que exigem que toda pessoa que deseje utilizar a encriptação notifique suas senhas privadas. Na Índia, está tramitando uma lei parecida. Também existem outras exceções.

O Centro de Informação Eletrônica Privada (EPIC) publica um *Relatório Internacional sobre a Política de Encriptação* (International Survey of Encryption Policy) que examina as leis da maioria dos países em http://www2.epic.org/reports/crypto2000/. Sua última atualização é de 2000. Se você se preocupar, antes de utilizar encriptação num país em concreto consulte a Privaterra.

P: O que necessitamos para manter nossos sistemas de Tecnologia da Informação (TI) seguros?

R: Depende de seu sistema e de suas atividades, mas no geral todo mundo deve ter:

- Um firewall;
- Encriptação do disco;
- Encriptação de e-mail que também realize assinaturas digitais como o PGP;
- Software para a detecção de vírus;
- Segurança de reserva: envie por e-mail todo o material a um site seguro e faça cópias de segurança semanalmente em CD-Rom. Depois, armazene num lugar separado e seguro;
- Senhas que sejam fáceis de lembrar, mas não de adivinhar;
- Uma hierarquia de acesso – nem todo mundo na organização necessita acessar todos os arquivos;
- Consistência – nenhuma das ferramentas funcionará se não as utiliza todo o tempo!

Mas ter o software correto não é a solução para tudo. **As pessoas costumam ser o elo mais fraco, não a tecnologia**. A encriptação não funciona se as pessoas não a utilizam continuamente, se compartilham as senhas indiscriminadamente ou as fazem visíveis num canto da tela, por exemplo. Em caso de um incêndio ou ataque, o "software" de reserva não se salvará se você não mantém a cópia de segurança num lugar separado e seguro. A informação confidencial deve ser compartilhada quando necessária e não com todos da organização; é necessário criar hierarquias

e protocolos. No geral, é importante ter presentes a privacidade e a segurança em suas atividades diárias. É o que denominamos uma "paranóia saudável".

P: Como decido que software de encriptação usar?

R: Normalmente, pode consultar seus amigos – e confirmar conosco. Você necessitará comunicar-se com certas pessoas e certos grupos, e se já estão utilizando um sistema de encriptação específico, deve utilizar o mesmo para facilitar a comunicação. Entretanto, consulte-nos primeiro. Alguns pacotes de "software" simplesmente não funcionam bem, enquanto outros são potes de mel. Os potes de mel atraem, oferecendo o uso gratuito de um "software" aparentemente excelente, mas é oferecido pela mesma gente que quer espiá-lo. Qual a melhor maneira de ler suas comunicações mais confidenciais que a de ser o supervisor de seu "software" de encriptação? Ainda assim, existem muitas marcas de confiança, tanto de "software" privado como de "software" gratuito – simplesmente não se esqueça de se informar antes de usar.[3]

P: O uso da encriptação aumenta o risco de que se adotem medidas severas contra mim?

R: Ninguém saberá que você está utilizando encriptação, a não ser que sua correspondência eletrônica já estiver sendo vigiada. Se é assim, sua informação particular já está sendo lida. Isso significa que quem te vigia já adotou essas medidas severas. Existe a inquietude de que os espiões possam utilizar outras opções se não podem continuar lendo seus correios eletrônicos, assim, é importante conhecer seus colegas e implementar políticas de reserva seguras e uma gestão de trabalho sólida quando começar a utilizar a encriptação.

(Nota: não dispomos de informação de casos onde o uso da encriptação tenha causado problemas aos defensores. Entretanto, considere esta possibilidade com atenção antes de iniciar a encriptação, sobretudo se você está num país com conflito armado pesado – a inteligência militar pode suspeitar que você está passando informação relevante sob um ponto de vista militar – ou se muito poucos defensores utilizam a encriptação – este pode despertar um interesse não desejado contra você).

P: Por que é necessário encriptar o e-mail e os documentos todo o tempo?

R: Se você somente usa a encriptação para os assuntos confidenciais, aqueles que estão vigiando seus clientes podem adivinhar, quando se está realizando uma atividade crítica, e ser mais propensos a tomar medidas enérgicas nestes momentos. Enquanto não possam ler suas comunicações codificadas, não poderão saber se os arquivos foram encriptados ou não. Um incremento repentino da encriptação pode incentivar um ataque, por esta razão é aconselhável começar a utilizar a encriptação antes de iniciar os projetos especiais. De fato, é melhor assegurar-se de que a comunicação flui sem problemas. Envie correios eletrônicos encriptados com intervalos regulares, inclusive quando não tenha

3 Por exemplo, PGP – "Pretty Good Privacy" (Privacidade Realmente Boa) – é um método conhecido e seguro. Pode ser baixado em http://www.pgpi.org

nada a informar. Desta forma, quando necessitar enviar informação confidencial, não chamará tanto a atenção.

P: Se já tenho um "firewall", por que necessito encriptar meu e-mail?

R: Os "firewall" impedem que os piratas tenham acesso a seu disco rígido e rede mas, uma vez que você envie o e-mail pela Internet, ele fica exposto ao mundo. Você precisa protegê-lo antes de enviá-lo.

P: Ninguém vai entrar e roubar em meu escritório, então por que deveria utilizar um "software" de privacidade?

R: Você não sabe se alguém entrou em seu sistema ou está filtrando informação. Sem comunicações codificadas, segurança física ou protocolos de privacidade, todo mundo pode ter acesso a seus arquivos, ler seu e-mail e manipular seus documentos sem seu conhecimento. Suas comunicações transparentes também podem expor os demais ao risco, sobretudo em lugares onde podem ocorrer ataques por motivações políticas. Se você fecha as portas com chave, deve encriptar seus arquivos. É simples assim.

P: Não dispomos de acesso a Internet e temos de usar um Internet café. Como podemos proteger as comunicações enviadas desde um computador externo?

R: É possível encriptar seu e-mail e seus arquivos. Antes de ir ao Internet café, codifique todos os arquivos que vai enviar por e-mail e copie-os num formato codificado em seu disquete ou CD. Uma vez no Internet café, inscreva-se num serviço de encriptação como www.hushmail.com ou num serviço de anonimato como www.anonymizer.com, e utilize-os quando enviar seus e-mails. Assegure-se de que as pessoas que recebam seu e-mail se inscrevam nestes serviços também.

P: Se é tão importante assegurar nossos arquivos e comunicações, por que todo mundo não faz isso?

R: Esta tecnologia é relativamente nova, mas seu uso está se expandindo. Os bancos, as empresas multinacionais, as agências de imprensa e os governos, todos utilizam a encriptação, considerando-a um investimento sólido e um custo necessário para seus negócios. As ONGs correm um maior risco que as empresas, que costumam ser bem acolhidas pela maioria dos governos. É maior a probabilidade que as ONGs sejam um alvo de vigilância e, portanto, necessitem tomar a iniciativa de implementar esta tecnologia. Os trabalhadores dos direitos humanos se dedicam a proteger a pessoas ou grupos perseguidos e possuem arquivos que podem identificar e localizar as pessoas. Se estes arquivos fossem acessíveis, estas pessoas podem ser assassinadas, torturadas, seqüestradas, ou "persuadidas" a não voltar a contatar a ONG. A informação destas fichas pode também ser utilizada como prova contra a ONG e seus clientes em processos judiciais políticos.

P: Um de nossos princípios é a transparência. Estamos trabalhando para que o governo tenha uma maior transparência. Como podemos utilizar a tecnologia de privacidade?

R: A privacidade é compatível com a transparência. Se o governo deseja solicitar publicamente seus arquivos, pode fazê-lo seguindo os procedimentos corretos e reconhecidos. A tecnologia de privacidade evita que se tenha acesso a sua informação de forma clandestina.

P: Seguimos todos os protocolos de privacidade e segurança e nossa informação continua sendo filtrada. O que está acontecendo?

R: Talvez haja um espião dentro da organização ou alguém simplesmente incapaz de guardar informação confidencial. Modifique sua hierarquia de informação, reduzindo o número de pessoas com acesso a informação confidencial – e esteja especialmente alerta a essas pessoas. As grandes corporações e organizações divulgam regularmente várias peças de informação falsas a certas pessoas específicas como simples tática. Se a informação falsa é filtrada, você descobrirá que o filtro vem do empregado a quem se deu essa informação.

Regras básicas do uso da encriptação:

- **Utilize** a encriptação continuamente. Se você apenas codifica o material confidencial, a pessoa que controla sua correspondência eletrônica saberá quando está a ponto de ocorrer algo importante. Um aumento repentino no uso da encriptação pode causar um ataque.

- **NÃO** coloque informação confidencial na linha de Assunto. Elas não costumam estar codificadas, ainda que a mensagem esteja.

- **Utilize** uma senha que contenha letras, números, espaços e pontuação que somente você possa lembrar. Algumas técnicas de criação de senhas são o uso de desenhos de seu teclado ou palavras ao azar juntadas entre elas por símbolos. No geral, quanto mais longa for a senha, mais segura.

- **NÃO** utilize uma única palavra, um nome, uma frase popular ou um endereço de sua agenda como senha. Poderiam descobri-la em questão de minutos.

- **Faça** uma cópia de segurança de sua chave privada (o arquivo que contém sua senha privada para a encriptação do "software") num único lugar seguro, como codificado num disquete ou num diminuto disco portátil USB ou "pen drive" (dispositivo de memória).

- **NÃO** envie material confidencial a alguém simplesmente por ter recebido uma mensagem sua encriptada com um nome conhecido. Qualquer um pode "spoof" (falsificar) um nome criando um endereço de e-mail parecido ao de alguém conhecido. Comprove sempre a identidade antes de confiar na fonte – comunique-se pessoalmente, por telefone, ou envie outro e-mail para reconfirmar.

■ **Ensine** aos demais a utilizar a encriptação. Quanto mais pessoas a utilizarem, mais seguros estaremos todos.

■ **NÃO** esqueça de assinar e encriptar a mensagem. Você necessita que seu destinatário saiba se a mensagem sofreu alterações durante ou trajeto.

■ **Encripte** separadamente os arquivos que queira anexar. No geral, não são encriptados automaticamente quando você envia um e-mail encriptado.

Guia para uma gestão mais segura do escritório e da informação

Gestão de escritório mais segura

Para conseguir uma gestão de escritório mais segura, é necessário criar certos hábitos. Os hábitos na gestão do escritório podem ser úteis ou nocivos. Para desenvolver bons hábitos, convém compreender o raciocínio que se esconde por trás deles. Elaboramos uma lista de hábitos que podem ser de utilidade para administrar sua informação de uma maneira mais segura – mas somente se forem desenvolvidos estes hábitos e reflexões, pois são importantes.

O que é mais importante para a privacidade e a segurança na administração do escritório?

- Ser consciente de sua informação e de quem tem acesso a ela.
- Desenvolver hábitos seguros e usá-los constantemente.
- Utilizar as ferramentas apropriadamente.

Administração

Muitas organizações possuem um sistema administrador ou alguém com privilégios administrativos para ter acesso ao e-mail, à rede de computadores e supervisionar a instalação de novos programas. Se alguém abandona a organização ou não está disponível, o administrador pode ter acesso à sua informação e o projeto pode continuar sem interrupção. Isto também significa que há um responsável por assegurar que o sistema de "software" esteja limpo e que venha de uma fonte de confiança.

O problema é que algumas organizações consideram este papel como um simples suporte técnico e dão a um trabalhador externo estes privilégios administrativos. Este administrador tem um controle efetivo sobre toda a informação da organização, e deve, portanto, ser de absoluta confiança. Algumas organizações dividem o papel de administrador entre o diretor da organização e outra pessoa de confiança.

Existem organizações que optam por agrupar as chaves privadas e senhas do PGP, encriptá-las e guardá-las de forma segura e num lugar remoto, como por exemplo outra organização de confiança. Isto evita problemas em caso de que alguém esqueça sua senha ou perca sua chave privada. Entretanto, a localização dos arquivos deve ser completamente segura e de confiança, e devem ser criados protocolos específicos e extensos em relação ao acesso aos arquivos.

As regras:

1 ♦ NUNCA conceda privilégios administrativos a um trabalhador externo. Não apenas são menos confiáveis do que gente da organização, mas em caso de emergência, pode resultar difícil contatar com alguém externo ao escritório.

2 ♦ Somente devem ser concedidos privilégios administrativos a pessoas da maior confiança.

3 ♦ Decida a que informação poderá ter acesso o administrador: a todos os computadores, senhas do computador, senhas para iniciar a sessão, chaves e senhas do PGP, etc.

4 ♦ Se você decide manter cópias de senhas e chaves privadas do PGP em outra organização, deverá criar certos protocolos de acesso.

5 ♦ Se uma pessoa abandona a organização, suas senhas e códigos de acesso pessoais deverão ser alterados imediatamente.

6 ♦ Se alguém com privilégios administrativos abandona a organização, todas as senhas e códigos de acesso deverão ser alterados imediatamente.

Administração de "softwares"

O uso de "software" pirata pode expor uma organização à denominada "polícia de software". Os policiais podem tomar medidas drásticas com uma organização que usa um software ilegal, impondo multas muito elevadas e até mesmo fechando a organização. Nestes casos, a organização não poderá contar com a simpatia ou apoio dos meios de comunicação ocidentais, porque mais que um ataque a uma ONG de direitos humanos, verão um ataque contra a pirataria. Seja extremadamente cuidadoso com suas licenças de software e não permita que sejam copiadas indiscriminadamente. O software pirateado pode também ser inseguro já que pode conter vírus. Utilize sempre um programa antivírus quando instalar um software ou aplicativo.

O administrador deve controlar a instalação do novo software para comprová-lo primeiro. Não permita a instalação de um software supostamente inseguro, e instale apenas o software que necessitar.

Instale as atualizações de segurança mais recentes em todo software, sobretudo no *Microsoft Office*, *Microsoft Internet Explorer* e *Netscape*. As piores ameaças à segurança vêm dos "software" e suportes físicos criados com vulnerabilidades intencionais. Melhor, portanto, utilizar um software de *Código Aberto*, que não está baseado no modelo de "Segurança por Obscuridade", mas que convida tanto a especialistas de segurança e a piratas a provar rigorosamente todos os códigos. O uso do software de *Código Aberto* e de qualquer outro que não seja Microsoft tem a vantagem adicionada de ser menos vulnerável aos vírus e aos piratas em geral. São poucos os vírus criados para os sistemas operativos Linux ou Macintosh, porque a maioria ainda utiliza Windows. *Outlook* é ou programa de e-mail mais conhecido, e portanto, o alvo mais conhecido dos piratas de informática.

Hábitos do correio eletrônico (e-mail)

A encriptação do e-mail deve se converter num hábito. É mais simples encriptá-lo sempre do que criar uma política de quando deve encriptar-se o e-mail e quando não. Lembre que se se encripta sempre o e-mail, quem vigia sua correspondência não saberá nunca quando suas comunicações passam a ser mais importantes e confidenciais.

Outros pontos importantes:

- Guarde sempre o e-mail codificado num formato encriptado. Sempre será possível desencriptá-lo, mas se alguém tem acesso a seu computador, será tão vulnerável como se nunca houvesse sido codificado.

- Lembre a todo mundo com quem troca e-mails encriptados que não decodifiquem e reenviem as mensagens, ou que não respondam sem encriptá-los. A preguiça individual é a maior ameaça para suas comunicações.

- Seria interessante criar algumas contas de correio seguras para as pessoas no campo, que não se utilizam geralmente e assim não cairão em mãos de servidores de "spam". Estes endereços devem ser revisados constantemente, mas não utilizados, exceto pelo pessoal de campo. Desta forma, poderá eliminar endereços eletrônicos que recebam muito correio "spam", sem que sua base de contatos corra riscos.

Conselhos gerais para cafés Internet, cibercafés e outros

Os correios eletrônicos enviados num texto legível ou decodificados pela Internet, podem ser lidos por muitas partes diferentes, se estiverem dispostas a isso. Uma delas é seu Provedor de Internet local (ISP) ou qualquer outro ISP por onde passam todos seus correios eletrônicos. Um e-mail passa por muitos computadores para poder chegar do remetente ao destinatário; ignora fronteiras geopolíticas e poderia passar por servidores de outros países, ainda que o e-mail esteja dirigido ao mesmo país.

Alguns conselhos gerais sobre assuntos comumente mal interpretados por usuários de Internet:

Some general tips on issues commonly misunderstood by internet users:

- Proteger um arquivo com uma senha protege tão pouco o arquivo que não vale a pena fazê-lo com documentos confidenciais. Apenas proporciona uma falsa sensação de segurança.

- Comprimir um arquivo não o protege de ninguém que queira comprovar seu conteúdo.

- Se quer enviar um arquivo ou e-mail de forma segura, utilize a encriptação (veja www.privaterra.com).

■ Se quer enviar um e-mail ou um documento de forma segura, utilize a encriptação durante todo o trajeto até seu destinatário final. Não é suficiente enviar um e-mail codificado desde um escritório externo até Nova Iorque ou Londres ou qualquer outro lugar, se logo se reenvia este mesmo correio decodificado a outra pessoa.

■ A Internet é universal por natureza. Não há nenhuma diferença entre enviar um e-mail entre dois escritórios de Manhattan ou enviá-lo desde um café Internet da África do Sul a um computador do escritório de Londres.

■ Utilize a encriptação com tanta regularidade quanto possível, ainda que o e-mail ou a informação que você envia não seja confidencial.

■ Assegure-se de que o computador que você utiliza possui um antivírus. Muitos vírus são criados para extrair informação de seu computador, tanto do conteúdo de seu disco rígido como de seus arquivos de e-mail, incluindo a agenda de endereços do e-mail.

■ Assegure-se de que seu software esteja autorizado/licenciado. Se você utiliza um software sem licença, automaticamente se converte num pirata do software aos olhos do governo e dos meios de comunicação. A melhor opção é utilizar um software de código aberto - é gratuito!

■ Não existe uma solução 100% segura para o uso da Internet. Tenha em conta que uma pessoa pode "piratear socialmente" um sistema fazendo-se passar por outra pessoa que não tem acesso ao telefone ou e-mail. Use sempre seu próprio juízo e senso comum.

Resumo

Lembre que os grupos interessados em seu trabalho não esperam a tecnologia perfeita para tentar conseguir informação sua.

Muitos defensores de direitos humanos são relutantes em usar tecnologia da informação segura. Ainda assim, procedimentos básicos são simples.

Procedimentos básicos: discrição ao telefone e comunicação pessoal, PGP na comunicação por e-mail e para arquivos sensíveis, senha para acessar seu computador.

Mas ter o software correto não é toda a solução. **Os indivíduos são o elo mais fraco, não a tecnologia.**

PARTE II

SEGURANÇA ORGANIZACIONAL

Nesta segunda parte do Manual trataremos do nível de segurança organizacional, isto é, maneiras de melhorar a segurança das organizações de defensores.

Segurança/proteção não significa apenas ter um plano de segurança.

Requer apropriar-se de todo o processo, começando por melhorar o nível de segurança orga

nizacional inicial, implementar o plano, e mais tarde melhorar o processo.

Apropriar-se de todo o processo é parte da própria segurança.

O processo de segurança organizacional é pragmático e inclusivo.

Ele precisa ser realista e se adaptar ao perfil da organização.

Apesar de que serão necessários recursos, mudar comportamentos é grátis e constitui um fator crucial na melhora da segurança.

ÍNDICE DA SEGUNDA PARTE:

CAPÍTULO 2.1

Avaliando a performance da segurança organizacional: a "roda da segurança"

Objetivos:

Examinar a forma com que você lida com sua segurança.

Avaliar em que grau a segurança está integrada no trabalho de um grupo de defensores de direitos humanos.

Para realizar essa tarefa, sugerimos uma abordagem dupla:

- Auto-avaliação pela organização de sua performance de segurança: a organização olha para sua própria performance recolhendo informação objetiva. O processo de auto-avaliação pode ser coletivo e/ou individual. É interessante na verdade ver como os membros de uma mesma organização chegam a conclusões diferentes sobre a performance de segurança de toda a organização.

- Como 'outros' percebem a organização.

Auto-avaliação de segurança organizacional

A roda da segurança

A auto-avaliação organizacional pode objetivamente ser realizada implementando-se a roda de segurança e seus oito raios.

Uma roda deve ser redonda; em outras palavras todos os raios devem ter o mesmo comprimento.

O mesmo ocorre com a roda de segurança e seus oito raios (ou componentes) representando a administração da segurança em uma organização ou grupo de defensores.

Esta avaliação pode ser feita em grupos:

- Desenhem a roda.
- Preencham cada raio de acordo com o desenvolvimento de cada uma.

- Listem as razões (faça um brainstorming) porque alguns dos raios não foram desenvolvidos suficientemente, e proponham diferentes soluções para estes problemas. Uma vez que vocês tenham enumerado as possíveis soluções, escolha objetivos e processos relevantes, antecipem possíveis problemas e sugiram soluções.
- Uma vez completada a avaliação, conservem o resultado e o diagrama. Quando repetirem o exercício alguns meses mais tarde, vocês poderão comparar o novo diagrama com o anterior e comprovar, ponto por ponto, se a situação melhorou ou não.

Os oito raios (componentes) da roda da segurança

■ **Experiência prática de segurança e coesão:** conhecimento prático e partilhado de segurança e proteção, reunidos através do trabalho. São os pontos de partida e de chegada da avaliação.

■ **Formação em segurança:** pode se obter formação em segurança com um curso ou por iniciativa própria durante seu trabalho diário.

■ **Consciência e atitude com relação à segurança:** se as pessoas e a organização, em sua totalidade, consideram a proteção e a segurança como uma necessidade e se estão dispostas a trabalhar para garanti-las.

■ **Planejamento de segurança:** capacidade de planejamento de segurança no trabalho. Planejamento para a proteção.

■ **Designação de responsabilidades:** quem é responsável por quais aspectos da segurança e da proteção? E em caso de emergência?

■ **Grau de apropriação das normas de segurança/cumprimento:** em que medida se cumprem as normas e os procedimentos de segurança?

■ **Análise e reação aos incidentes de segurança:** em que medida estão sendo analisados os incidentes de segurança? A organização está respondendo corretamente?

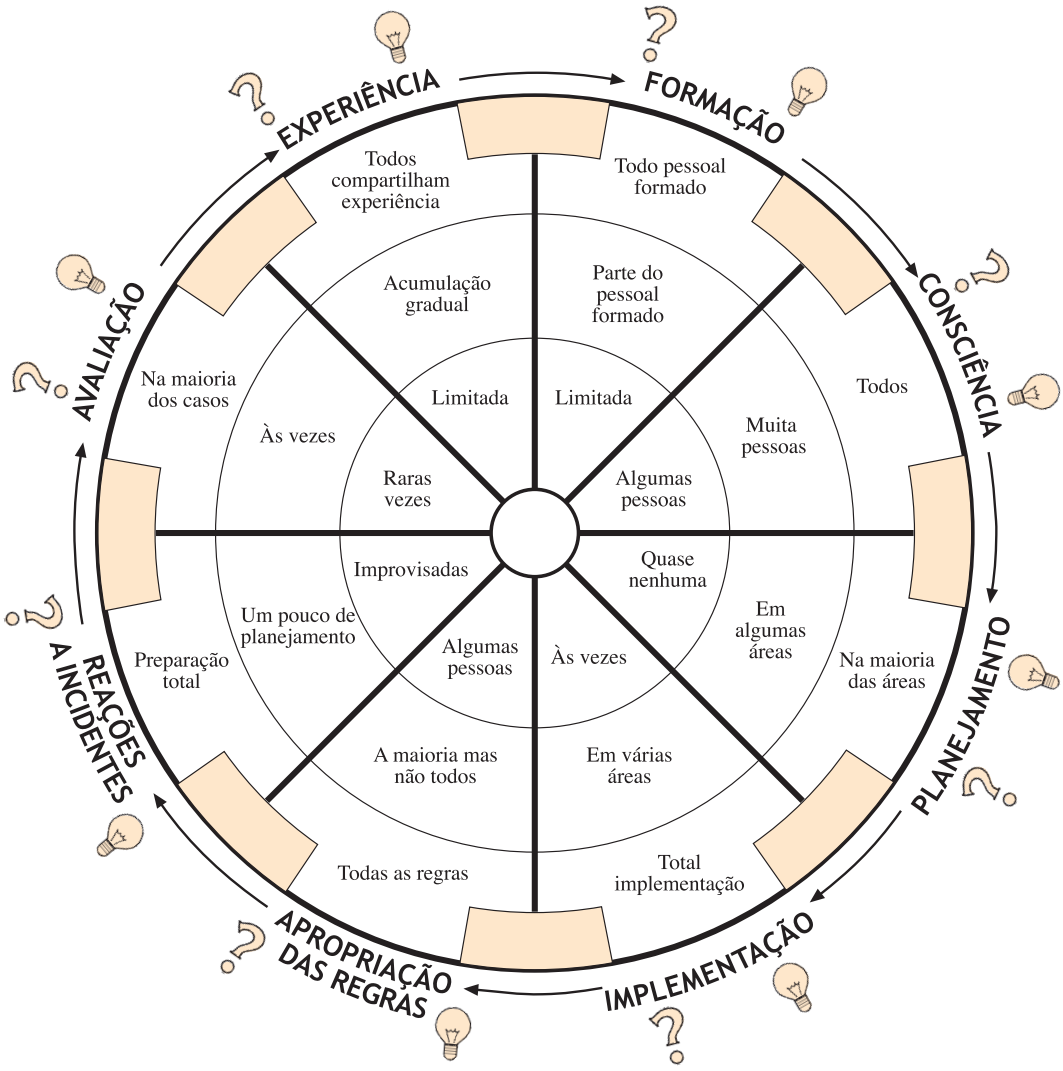
■ **Avaliação da segurança e da gestão da proteção:** Que entendimento é que a organização tem da sua gestão de segurança e proteção e em que medida é que esta gestão está atualizada?

Exemplo de uma roda de segurança:

A roda da segurança nunca é perfeita: alguns de seus componentes estão mais desenvolvidos que outros. Portanto, é melhor examinar o grau de desenvolvimento de cada um. Desta forma, você poderá identificar quais são as ações prioritárias que devem ser tomadas para melhorar sua proteção e segurança. As linhas de pontos concêntricas, que vão do centro para fora, ilustram quão desenvolvido está cada componente.

? Possíveis problemas relacionados a esta parte da roda...

...e possíveis soluções para os problemas.



Faça cópia da roda e pinte com cores os espaços entre os raios. Assim, você obterá a estrutura da roda de seu grupo ou sua organização, e isso o ajudará a comprovar que algumas partes estão mais ou menos desenvolvidas.

Análise passo a passo da "roda de segurança"

Uma análise bem feita da política de segurança de uma organização requer tempo para examinar o atual significado de cada componente individual da roda de segurança.

1 • Experiência de segurança e coesão adquirida através de trabalho e compartilhamento

Conhecimento prático acumulado e coesão entre segurança e proteção. O começo e o fim da análise.

Tenha em mente que a experiência de apenas poucos membros não quer dizer experiência em segurança em nível organizacional, mas na verdade o total de experiência de seus membros: compartilhar experiências contribuirá, portanto, para a coesão da segurança.

O conhecimento total será refletido nos raios; uma vez que você desenvolva todos os componentes até sua satisfação, o conhecimento total crescerá ainda mais com o resultado. Conhecimento de segurança será provavelmente melhor desenvolvido e os outros raios seguirão. É uma atividade que nunca acaba pela simples razão de que os membros da organização vão e vêm, e o contexto político muda assim como a segurança. Entretanto, a boa notícia é que como este é o resultado de todos os outros 7 raios, para este raio específico você não precisa fazer nada (contrariamente ao que acontece com os 7 outros raios).

2 • Formação em segurança

Indique o treinamento de segurança que você já fez, seja um curso, ou através de uma iniciativa própria em seu trabalho.

Perguntas que necessitam aprofundamento:

O treinamento em procedimentos de segurança está disponível para todo mundo? Temos de atualizá-lo? Os novos membros do staff são treinados? Que dificuldades você encontraria para treinar alguém? Quais são as possíveis soluções?

3 • Aumentando a sensibilização sobre segurança e atitudes corretas

Perguntas utilizadas para determinar o nível atual de conhecimento:

Todos são realmente conscientes sobre segurança e proteção? Como podemos alcançar isso?

Sensibilização não quer dizer implementação (por exemplo, fumantes sabem quão perigoso fumar é, mas continuam fumando).

Perguntas para sensibilizar:

Que fatores acionam uma revisão de segurança?

Quais são as histórias contadas sobre segurança na organização e qual o conhecimento informal sobre o assunto?

Quais problemas encontramos em aumentar o conhecimento? Quais são as possíveis soluções?

4 • Planejamento de segurança

Perguntas para determinar o atual nível de planejamento de segurança:

- Planejamos a segurança e proteção em nosso trabalho?
- A questão de segurança é integrada na abordagem institucional? (missão, planos estratégicos, áreas de trabalho, temas transversais)?
- Segurança é um item na agenda nas principais reuniões (e não o último item da lista)?
- Qual é a estratégia do orçamento (é ad hoc para segurança (ou é incluído em outras categorias) e da administração financeira?
- Você realiza uma análise do ambiente de trabalho – em grupos de trabalho (incluindo níveis local, regional e nacional)?

E nós:

- Analisamos o impacto do trabalho e como a organização é percebida por outros atores que podem representar uma ameaça?
- Realizamos análises de risco completas: ameaças, vulnerabilidades e capacidades?
- Compilamos todos os documentos de segurança: revisão de seu conteúdo para ver como foram usado?
- Elaboramos e atualizamos documentos de segurança? Verificamos se eles estão atualizados e como podem ser alcançados/ Verificamos se o impacto de seu trabalho e os fatores de risco foram levados em conta? Verificamos se os processos de consulta diária sobre segurança estão em funcionamento?

Nós temos esquemas de segurança que são:

- Simples e claros? Eles contêm toda a informação necessária em linguagem clara?
- Elaborados em cooperação com todas as pessoas afetadas?
- Apropriados a qualquer contexto de trabalho?
- Melhorados, desenvolvidos e atualizados graças a iniciativas de diferentes pessoas do grupo de trabalho?
- Genuíno e adaptado ao "mundo real"?

Nossos esquemas de segurança cobrem:

- Todos os itens necessários?
- Comunicação, TI, e administração de informações?
- Administração de pessoal (incluindo recrutamento)? gestão de estresse?

Estão todos os empregados informados de que um grupo de trabalho com boa estrutura, boa comunicação interna, boas relações públicas e boa cooperação é um requisito básico de segurança?

Questões para melhorar ainda mais o planejamento de segurança:

Que problemas enfrentaríamos se tentássemos resolver cada um dos itens acima?

Quais poderiam ser as soluções?

5 • Atribuição de responsabilidades

Perguntas para definir o atual nível de atribuição de responsabilidades de segurança:

- Nós sabemos claramente quem é responsável por cada aspecto de segurança e proteção? E em caso de emergências?
- Existem responsabilidades organizacionais e deveres dos trabalhadores e colaboradores (incluindo seu comportamento fora do trabalho e com a família)?
- Todos assumem sua responsabilidade pela segurança e há responsabilidades específicas para diferentes aspectos da segurança? (Quais são as dificuldades que encontramos)?

Perguntas para melhorar a atribuição de responsabilidades pela segurança:

Que problemas encontraríamos se tentássemos designar e compartilhar responsabilidades de segurança?

Quais poderiam ser as soluções?

Atribuir responsabilidades contribui com a segurança compartilhada.

6 • Grau de apropriação das regras de segurança e seguimento das mesmas

Perguntas para determinar o atual nível de apropriação das regras de segurança e o seguimento por parte dos empregados:

- Em que medida as pessoas respeitam as regras e procedimentos de segurança?
- Em que medida cada indivíduo e o grupo como um todo contribuem na elaboração do plano de segurança e cumprem com as regras de segurança e proteção?
- É possível dizer que as regras de segurança não estão sendo seguidas? E se não estão, por quê?
- As pessoas seguem as regras de segurança por medo de reprimendas ou porque eles/as estão convencidos/as de que seguí-las diminui as conseqüências de riscos? (por exemplo, um motorista pode usar o cinto de segurança por medo de uma multa, ou porque ele está convencido de que fazendo isso diminuirá as conseqüências de um possível acidente automobilístico)

Perguntas para melhorar o grau de apropriação das regras de segurança e seguimento:

Que problemas você encontraria para melhorar o nível de respeito às regras?

Quais são as possíveis soluções?

7 ● Análise de incidentes de segurança e reações

Questões usadas para determinar o nível atual de análise de incidentes de segurança e suas reações:

- Em que medida os incidentes de segurança estão sendo analisados? Eles geram algum tipo de feedback da organização? Que incidentes de segurança ocorreram? Como foram tratados e qual foi o dano causado?
- Nós escrevemos relatórios (e como)?
- Nós realizamos nossas análises (como e em que nível)?
- Qual é o feedback (prazos, procedimento, responsabilidades)?
- Como avaliamos o feedback?
- Treinamento dentro da organização é baseado em incidentes (ele é feito para todos? Há canais institucionais para isso?)?
- Em resumo, o que é feito em caso de incidentes?
- Existe um procedimento para coletar, investigar e analisar incidentes de segurança para criar um feedback e uma base para nossas estratégias e planos? Estas conclusões são integradas em nosso trabalho e avaliações (onde necessário)?
- Há planos claros e responsabilidades cobrindo reações em caso de emergências?
- Para que tipos de emergências eles são aplicáveis?

Perguntas para melhorar a análise e reação a incidentes de segurança:

Quais são os problemas para melhorar cada item da lista acima?

Quais são as possíveis soluções?

8 ● Avaliando a gestão de segurança e proteção

Perguntas para determinar o atual nível de avaliação da gestão de segurança e proteção:

- Em que medida a organização avalia sua gestão de segurança e proteção e em que medida ela é atualizada?
- A avaliação é uma atividade institucionalizada?
- Estamos conscientes que o trabalho diário e as reações em caso de incidentes de segurança devem ser avaliados desde uma perspectiva de segurança para que possam contribuir com o conhecimento e experiência de cada pessoa e de toda a organização?

Perguntas para melhorar a avaliação da gestão de segurança e proteção:

Que problemas encontraríamos para melhorar a avaliação da gestão de segurança e proteção?

Quais seriam as possíveis soluções?

Segurança e nossa própria imagem

É importante olhar para o ambiente da organização para ver como sua imagem organizacional é percebida e se ela corresponde à imagem que a organização quer externar. É importante também descobrir como outros percebem a proteção e segurança da organização. Isso deve ser feito a partir dos seguintes pontos de vista:

- Do ponto de vista das pessoas com quem trabalhamos: contrapartes, beneficiários.
- Colegas e organizações similares.
- Instituições financiadoras e patrocinadores (alguns serão mais receptivos do que outros).
- Autoridades com quem temos relações.
- Outros atores que podem ser agressores em potencial.
- ...

É importante certificar que nível de cooperação na segurança existe com outras organizações ou redes, com contrapartes, com as pessoas com as quais trabalhamos, etc.

Duas listas não exaustivas de perguntas temáticas:

I ♦ Imagem organizacional e impacto da organização. Como podemos avaliar isso?

- Como ficamos informados sobre a imagem da organização?
- Como explicar para outros?
- Qual é o propósito da organização?
- Quais são nossas atividades?
- Como nossas atividades afetam atores armados ou outros?
- Que capacidades ou poder temos para manter nosso espaço de trabalho aberto?
- O que fazemos para mantê-lo aberto?
- Como pensamos que nossos potenciais agressores nos vêem?
- Somos percebidos como uma organização que lida bem com questões de proteção e segurança?

- Há alguém que destaca nosso trabalho ou nossa gestão de segurança? Por quê? Como você sabe?

II ♦ Imagem organizacional e impacto do trabalho da organização. Como somos vistos?

Tente responder às questões abaixo do ponto de vista de outra pessoa (você será "eles" e o entrevistado será "nós").

- Quem são eles?
- O que eles esperam?
- Qual é o seu trabalho?
- Como eles atrapalham nosso trabalho?
- Quais são os limites para nosso trabalho?
- O que podemos fazer?
- Como podemos nos proteger?
- Como podemos obter o que queremos?

Uma vez que você tenha analisado a percepção dos outros, você precisará ver como mudar sua imagem e se isso lhe é conveniente. Nem todas as percepções podem mudar, obviamente. Mas é bom estar atento a elas e ao impacto que elas têm sobre sua segurança e proteção.

Resumo

Para avaliar sua segurança você necessita uma abordagem dupla:

Auto-avaliação e avaliação de como os outros veem você.

A auto-avaliação pode ser feita através da roda de segurança e seus oito raios.

Trata-se de uma fotografia instantânea de seu atual nível de segurança e proteção.

Ela permite o desenvolvimento de cada elemento, de modo a atingir uma roda redonda.

Para desenvolver sua roda de segurança você precisa começar por um inventário de sua situação atual, definir objetivos e decidir os processos de melhoria relevantes. Tente antecipar possíveis obstáculos durante o progresso até seus objetivos. Tente antecipar soluções.

Avaliação de como os outros o veem pode ser realizada tentando imaginar como eles estariam falando de você.

Você pode fazer perguntas a atores confiáveis.

Você precisará encontrar maneiras de mudar as percepções que não lhe convêm. Nem todas as percepções podem ser modificadas. Mas é bom estar atento a elas e ao impacto que elas têm sobre sua segurança e proteção.

Capítulo 2.2

Assegurar-se do cumprimento das normas e procedimentos de segurança

Objetivo:

Pensar nas razões pelas quais os trabalhadores e as organizações não podem ou não estão dispostos a seguir os planos e procedimentos de segurança, e encontrar soluções apropriadas.

A segurança é assunto de todos

É complicado conseguir que as pessoas e as organizações cumpram realmente os procedimentos e normas de segurança. Pode-se traçar um bom plano de segurança, completo, com normas preventivas e procedimentos de emergência; designar à segurança uma posição capital na agenda de todas as reuniões importantes, etc., e, apesar disso, as pessoas continuarem sem observar as normas de segurança da organização.

Isto poderia parecer incrível, tendo em conta que os defensores de direitos humanos se encontram sob pressão e ameaça constantes, mas ocorre.

Se alguém necessita averiguar algo sobre seu trabalho, não o fará por meio da pessoa mais cuidadosa da organização. Tentarão aproximar-se de alguém que costuma embriagar-se nos sábados à noite, por exemplo. Ainda assim, se alguém quer assustar sua organização, provavelmente não atacará a pessoa que tomou todas as precauções necessárias; ao contrário, abordará alguém que costuma ser bastante descuidado com sua própria segurança. Pela mesma razão, poderia suceder que se ataque uma pessoa cuidadosa, se a pessoa descuidada deixar a porta aberta... Isto vem demonstrar que uma pessoa descuidada pode colocar todos numa situação de maior risco. A segurança é apenas tão boa quanto os seus elementos mais fracos – neste caso a negligência de um indivíduo.

É por isso que deveríamos definir a segurança como um assunto que não diz respeito somente às pessoas envolvidas mas a toda a organização. Se somente três de 12 pessoas cumprem as normas de segurança, toda a organização, incluindo os que respeitam as normas, corre um risco. Se a situação melhora e nove pessoas começam a seguir os procedimentos de segurança, o risco diminui. Mas o risco seria ainda menor se as 12 pessoas seguissem as normas.

Segurança é um assunto para toda a organização, mas também para as pessoas envolvidas no seu trabalho.

Um bom plano de segurança não tem sentido se ele não é cumprido. Sejamos realistas: muita gente não observa as normas ou procedimentos. A falta de cumprimento é a soma das diferenças entre boas intenções e a prática na realidade. Entretanto, é mais fácil enfrentar este problema do que suas possíveis conseqüências.

Por que as pessoas não cumprem as normas de segurança? E como podemos evitar isso desde o princípio?

Em primeiro lugar, a palavra "cumprir" tem conotações de submissão e docilidade e, portanto, deve ser evitada. As pessoas tendem a cumprir as normas que entendem e aceitam, porque podem adotá-las como próprias. A palavra-chave portanto é "apropriação".

Para que um procedimento de segurança se cumpra, é necessário que seja adotado por todas as pessoas da organização. Isto não ocorre de forma imediata. Para que o pessoal faça seu um procedimento de segurança devemos permitir sua participação na elaboração e na implementação do mesmo. Também são importantes a formação, a compreensão e a aceitação dos procedimentos.

Quadro 1: A relação entre as pessoas e as organizações em termos de segurança

Conceito	Enfoque: " Todo mundo deve seguir as normas!"	Enfoque: "O indivíduo e a organização concordaram com as normas"
Enfoque	Baseado nas normas.	Baseado nas necessidades de segurança das pessoas e da organização.
Tipo de relação entre o indivíduo e a organização	Normativa ou "paternalista".	Baseada no diálogo.
Por que cumprimos as normas?	Por obrigação, para evitar uma sanção ou uma expulsão.	Por respeito a um acordo, com um margem de crítica e melhora (apropriação e persuasão são conquistados quando estamos convencidos que o acordo se encaixa nas nossas necessidades e que irá diminuir a praticabilidade e conseqüências de um risco e contribuir para poder ajudar a proteger os nossos companheiros e as pessoas por/com quem trabalhamos).
Responsabilidade da segurança	Não compartilhada.	Compartilhada.

A apropriação não significa simplesmente "cumprir as normas", mas estabelecer um acordo sobre as normas que faça com que as pessoas as cumpram porque as

entendem, porque consideram que são apropriadas e efetivas, e porque pensam que as afeta pessoalmente. Por esta razão, as normas deveriam ser ajustadas também ao critério moral e ético e às necessidades básicas das pessoas.

A apropriação não significa simplesmente "cumprir as normas", mas respeitar um acordo entre a organização e os indivíduos referente à segurança.

Para poder manter o acordo entre os indivíduos e a organização é importante que **a(s) pessoa(s) responsável(is) pela segurança mantenha(m) os demais continuamente envolvidos** por meio de sessões informativas, lembretes sobre aspetos do acordo, e consultando as pessoas sobre quão apropriadas e efetivas as normas têm resultado na prática.

No entanto, esta participação não terá muito valor se não existe uma **cultura organizacional da segurança,** que penetre nos programas de trabalho e nos procedimentos, tantos os formais como os informais.

Em resumo, é possível que os indivíduos se apropriem das normas e procedimentos de segurança, seguindo estes passos:

- Desenvolver o conceito de que a segurança é importante para proteger as vítimas, testemunhas, familiares e colegas de trabalho, e assim fazer com que o trabalho continue;
- Desenvolver e valorar uma cultura organizacional da segurança;
- Promover a apropriação das normas e procedimentos de segurança;
- Assegurar-se de que todos os indivíduos participem na elaboração e na melhora das normas e procedimentos de segurança;
- Treinar as pessoas em temas de segurança;
- Assegurar-se de que todo o pessoal está convencido da idoneidade e efetividade das normas e procedimentos de segurança;
- Estabelecer um acordo entre a organização e as pessoas sobre o respeito às normas e procedimentos de segurança;
- Pedir aos responsáveis pela segurança que informem e formem as pessoas, lembrem o pessoal sobre os termos do acordo e a solicitem suas opiniões sobre quão apropriadas e efetivas as normas resultam na prática.

Por que não se observam as normas e procedimentos de segurança?

Não existe um protótipo do defensor de direitos humanos que não cumpre as normas de segurança. Muita gente dentro de uma mesma organização costuma cumprir algumas das normas mas não todas, ou as observam esporadicamente.

São muitas as possíveis razões pelas quais as pessoas não cumprem as normas e procedimentos. Para mudar esta situação e garantir a apropriação, é importante estabelecer as causas e buscar as soluções junto às demais pessoas

envolvidas. Também resultará prático distinguir as diferentes razões que podem levar as pessoas a descumprir as normas, já que elas variam muito.

Possíveis razões para o descumprimento das normas e procedimentos de segurança:

Descumprimento não intencional:

- O defensor desconhece as normas;
- Ele/a não aplica as normas corretamente.

Descumprimento intencional:

Problemas gerais:

- As normas são muito complicadas e difíceis de seguir;
- Os procedimentos não estão à mão no escritório ou foram elaborados de forma que fica difícil seu uso cotidiano.

Problemas individuais:

- As normas chocam com necessidades ou interesses individuais e este conflito não foi resolvido;
- O indivíduo não está de acordo com algumas ou todas as normas e as considera desnecessárias, inapropriadas ou ineficientes, baseando-se em sua experiência pessoal, numa informação ou formação prévia ou em suas crenças pessoais.

Problemas de grupo:

- A maioria dos indivíduos do grupo não cumpre as normas, ou os "líderes" do grupo não as cumprem suficientemente, porque não existe uma cultura organizacional de segurança;
- Uma falta de motivação geral no trabalho pode fazer com que as pessoas ignorem as normas de segurança.

Problemas organizacionais:

- Não há recursos econômicos suficientes ou técnicos que facilitem o cumprimento das normas;
- Existe uma contradição entre as normas e algumas áreas concretas de trabalho. Por exemplo, as normas foram estabelecidas pelos responsáveis de segurança, mas ignoradas ou não implementadas corretamente pelo pessoal que trabalha em programas ou na contabilidade. Algumas normas poderiam ser adequadas para algumas áreas e inadequadas para outras;
- As pessoas têm um grande volume de trabalho e um tempo limitado, e não priorizam nenhuma ou apenas algumas das normas;
- Uma falta de motivação generalizada por causa do estresse, das disputas de trabalho, etc.

A cultura organizacional é tão formal como informal, e deve ser desenvolvida não apenas na totalidade da organização, mas também nas equipes de trabalho. Uma boa cultura organizacional se reconhece por suas conversas informais, piadas, brincadeiras, festas, etc.

Monitorando o cumprimento das normas e procedimentos de segurança

Seguimento direto:

Podemos incluir as normas e procedimentos nas avaliações gerais do trabalho e nas "listas de controle"; assim como nas reuniões anteriores e posteriores a missões in loco, nos relatórios de trabalho, nas agendas de reuniões, etc.

Também podem ser realizadas, conjuntamente com as equipes em questão, revisões periódicas de questões como o cuidado com a informação confidencial dos manuais de segurança e das cópias; os protocolos de segurança para visitar os escritórios centrais; a preparação para sair em missão, etc.

Seguimento indireto:

Solicitar a opinião das pessoas sobre as normas e procedimentos (se são corretas e fáceis de seguir, etc.) pode mostrar se o pessoal é realmente consciente das normas, se foram totalmente aceitas ou se existe um desacordo sobre o que se fazer.

Também se pode revisar, assim, o uso do manual de segurança por parte dos trabalhadores e das normas e protocolos existentes.

Resulta muito proveitoso recopilar e analisar, conjuntamente com as pessoas ou as equipes em questão, as opiniões e avaliações sobre as normas e procedimentos de segurança. Isto também poderia ser realizado de forma confidencial/anônima ou mediante uma terceira pessoa.

Seguimento retrospectivo:

A segurança pode ser revisada, analisando os incidentes de segurança à medida que vão surgindo. Para isso, devemos atuar com especial precaução. A pessoa que sofreu um incidente de segurança poderia sentir-se culpada ou pensar que a análise poderia representar sanções. Poderia, portanto, sentir a tentação de ocultá-lo, não informando sobre o incidente ou sobre alguns aspectos dele.

Quem realiza o seguimento?

Dependendo de como funcione o grupo, o seguimento pode ser feito pelas pessoas responsáveis pela segurança ou por pessoas responsáveis por outras áreas de trabalho ou de recursos humanos.

O que fazemos se não se respeitam as normas e procedimentos de segurança?

1 ♦ Determinar as causas, buscar soluções e colocá-las em prática. A lista de opções do quadro 1 anterior pode servir como guia.

2 ♦ Se o problema é intencional e está relacionado a uma pessoa, procure:

- a • Estabelecer um diálogo com a pessoa para saber a(s) causa(s) ou motivo;

b • Trabalhar junto à equipe do indivíduo (dependendo do caso, isso pode não ser apropriado);

c • Estabelecer um sistema de advertências ou avisos, para que a pessoa que descumpre as normas esteja totalmente consciente do problema;

d • Utilizar um sistema de sanções graduais (que poderiam culminar na demissão da pessoa).

3 ♦ Incluir uma cláusula em todos os contratos trabalhistas ou de voluntariado sobre o cumprimento das normas e procedimentos de segurança, para que todos os empregados estejam perfeitamente conscientes de como é importante para a organização.

Conclusão...

Haverá quem sustente que organizar um debate sobre as razões pelas quais as pessoas não cumprem as normas de segurança é uma perda de tempo, já que há coisas mais urgentes ou importantes que fazer. Os que assim opinam, costumam pensar simplesmente que as normas são feitas para serem cumpridas, e ponto final. Outras pessoas são conscientes de que as coisas nem sempre funcionam assim.

Seja qual for sua opinião, convidamos você para que dê um passo atrás e analise até que ponto estão sendo cumpridas as normas e procedimentos de segurança na organização onde você trabalha. O resultado pode ser surpreendente, e vale a pena dedicar um pouco de tempo para evitar problemas no futuro...

Resumo

Segurança é um assunto de todos.

Segurança é uma questão de toda a organização, assim como dos indivíduos envolvidos.

As razões para as pessoas não seguirem regras de segurança podem ser:

- não intencionais (problema individual).
- intencionais (gerais, individuais, grupais, problemas organizacionais).

Conhecê-las contribuirá para encontrarmos maneiras apropriadas para resolvê-las. Entretanto, monitoramento (indireto, direto ou retrospectivo) através de um órgão é recomendável.

É fundamental desenvolver uma cultura organizacional de segurança.

Administrando mudanças organizacionais para uma melhor política de segurança

Objetivos:

Aprender a administrar mudanças organizacionais para uma melhora na política de segurança.

Passos e questões a partir dos quais o processo é ser construído:

- melhorar a gestão da estratégia de segurança.
- melhorar o processo de implementação da gestão de segurança.
- qual é seu ponto de entrada? Quem (que órgão) é responsável por isso? Qual é o ponto de partida? Como proceder? E a implementação? Quais são os pontos positivos e negativos? Quais são os obstáculos?

Tratando de desafios de segurança: gestão de segurança passo a passo

Gestão de segurança nunca acaba e é sempre pragmática, parcial e seletiva. Isto porque:

- Há limites à quantidade de informação que você pode utilizar – nem todos os fatores afetando a segurança podem ser agrupados e tratados simultaneamente;

- Trata-se de um processo complexo – tempo e esforço são necessários para sensibilizar, criar consenso, treinar as pessoas, lidar com mudanças de pessoal, implementar atividades, etc.

Gestão de segurança raramente toma uma visão compreensiva, de longo prazo. Sua contribuição está na habilidade de prevenir ataques e indicar a necessidade de estratégias organizacionais para superá-los. Isto pode não parecer muito ambicioso, mas não podemos esquecer que pouquíssimos recursos são destinados para segurança!

Quando revisamos as medidas práticas de um defensor ou de uma organização, podemos encontrar algum tipo de guia, plano, medidas ou padrões de comportamento já em funcionamento. Forças conflitantes estarão envolvidas, desde

idéias estereotípicas sobre práticas de segurança à relutância em aumentar carga de trabalho ao incorporar novas atividades de segurança.

A prática de segurança é tipicamente um trabalho contínuo, intuitivo e fragmentado. A gestão da segurança deveria fazer mudanças passo a passo para melhorar sua performance. Regras e procedimentos de segurança tendem a surgir de partes da organização trabalhando sobre áreas específicas, como logística, a equipe de campo preocupada com sua segurança, um diretor apreensivo com preocupações dos financiadores com a segurança, etc.

Gestão da segurança passo a passo abre a porta para processos informais e que abrirão espaço para novas práticas serem enraizadas. Eventos inesperados, como incidentes de segurança, induzirão decisões urgentes, de curto prazo que, se não forem administradas corretamente, darão forma a práticas de segurança de longo prazo de toda a organização.

Melhorias na estratégia de segurança: possíveis pontos de entrada

Uma vez que a necessidade de melhorar a segurança foi estabelecida, ela precisa ser promovida. Há vários pontos de entrada para isso (tanto dentro quanto fora da organização):

Dentro da organização

- Diretores, Conselho ou líderes;
- Níveis intermediário e executivo;
- Staff, funcionários;
- Combinação de todas as possibilidades mencionadas acima.

Fora da organização

- Doadores;
- Parceiros e contrapartes;
- Organizações similares trabalhando na mesma rede.

Vamos comparar suas vantagens e desvantagens

Possível ponto de entrada para promover a necessidade de mudanças?	Vantagens	Desvantagens	Possíveis soluções
Pontos de entrada **dentro** da organização			
Diretoria, Conselho ou líderes	• podem convocar uma reunião ou assembléias-gerais. • possuem memória histórica. • autoridade moral. • apoio institucional. • ...	• percebidos como "impondo a segurança" e geram desinteresse. Tornam as coisas muito rígidas, formais, distantes e condescendentes. • veem a segurança como uma questão que só afeta eles. • desvalorizam a questão, dizendo que não é uma prioridade. • ...	• Reuniões ou assembléias gerais. • ...
Nível intermediário / executivo	• Vista dos níveis superiores e inferiores. • Fácil acesso a ambos os níveis. • Comunicação convivial entre ambos os níveis. • Capacidade técnica de implementar mudanças de segurança.	• Geralmente este nível não existe. • Foco parcial: uma área ou lado apenas. • Distraído por interesses pessoais de carreira. • "Muito" técnico se não estiver envolvido em atividades políticas ou de campo.	• Procedimento de envolvimento tanto dos diretores quando dos membros em geral. • ...
Staff, funcionários • ...	• Podem mobilizar as pessoas. • Conscientes dos mecanismos e detalhes do trabalho diário. - ...	• Podem ter problemas com os diretores ou outra hierarquia. • ...	• Em geral, como um grupo, reconhecem o problema, a necessidade da contribuição de cada um e de soluções. Então, delegam a busca da solução para um grupo de trabalho. • ...
Pontos de entrada **de fora** de organização			
Doadores, organização parceira • ...	• Maior distância. • Nenhum interesse direto. • Podem ter experiência mais ampla. • Poderiam convocar uma reunião com qualquer dos níveis acima sem conflito de interesse. • ...	• Podem ter problemas de credibilidade ou pouco conhecimento sobre o trabalho que é feito. • Abordagem muito "técnica". • ...	• Apontam para interesses comuns de segurança. • Organização doadora prefere investir numa organização que se preocupa com sua segurança do que arriscar perder seu investimento numa organização que ignora segurança. • Segurança inter-organizacional depende de atitudes e regras comuns de segurança. • ...

Este processo de entrada, ou de partida, pode ser implementado por todas as organizações, independentemente de seu tamanho, estabilidade, localização.

Qual o órgão responsável pelo processo de melhoria?

Agora que o ponto de entrada foi superado (a necessidade foi promovida e reconhecida), alguma parte da organização deve liderar o processo. Que órgão será responsável pelo processo de melhoria da segurança? Há várias possibilidades:

- Membros aleatórios da organização (eles são parte da organização e são escolhidos por ela (geralmente eles também tem outras responsabilidades). Isso pode ser um grupo de trabalho (composto por pessoas de várias áreas de trabalho).
- Uma pessoa de fora: a pessoa é parcialmente envolvida no trabalho e interage próxima e continuamente com as pessoas da organização (por exemplo alguém que costumava trabalhar na organização).
- Um consultor ou assessor: interage com a pessoa da segurança ad hoc ou com o grupo de trabalho (uma interação de curto prazo).

Vamos examinar as vantagens e desvantagens destas diferentes abordagens.

Órgão responsável pelo processo de melhoria	Vantagens	Desvantagens	Possíveis soluções
Pessoa ad hoc escolhida pela organização	• Informação centralizada. • Fácil acesso à informação. • Claridade em termos de responsabilidade. • Processo de decisão facilitado – menos pessoas envolvidas. • Escolhida por suas habilidades. • ...	• Carga de trabalho excessiva - Dependência excessiva em uma só pessoa. • Possível falta de contribuições aos planos e idéias. • ...	• Distinção entre promoção/ coordenação e implementação. • Redução temporária da carga de trabalho para permitir foco na segurança. • Pessoal de apoio. • Constante circulação de estratégias a fim de garantir feedback contínuo.
Grupo de trabalho	• Abordagem compartilhada e ampla da segurança no trabalho. • Experiências diversas e extensas. • Mais recursos humanos. • Distribuição de responsabilidades: mais claridade para iniciativas e atividades. • Maior probabilidade de protocolos serem seguidos. • ...	• Carga de trabalho excessiva. • Consenso lento ao tomar decisões. • Circulação de informação menos fluída – maior número de pessoas para ser treinado para as tarefas. • ...	• Adequada distribuição de habilidades e tarefas. • Envolvimento dos diretores. • Rotação, treinamento e comprometimento ativo na circulação progressiva de resultados de modo a receber feedback e compartilhar o processo. • ...

Uma pessoa de fora/de dentro	• Maior objetividade na análise de risco. • Pessoa habilidosa, com confiança da organização. • Comprometimento total. • Receptividade comprovada, ciente das forças e debilidades. • ...	• Descontinuidade. • Pode enfraquecer o comprometimento do grupo. • Pode enfraquecer a apropriação do grupo do processo e do assunto. • ...	• Treinar um ou dois membros da equipe. • Contínua circulação de resultados de progresso e feedback para toda a equipe. • Construção de consenso e de pontos de acordo. • ...
Um consultor ou assessor	• Pode treinar a equipe. • Consultor especializado. • Claridade sobre o processo de monitoramento. • Assessoria reconhecida. • Processo de seguimento ativo. • Menos afetado por questões organizacionais. • ...	- Pode gerar dependência de habilidades. - Pode ser visto como "alguém para fazer o trabalho" ao invés de "alguém para facilitar o trabalho". - Pode enfraquecer a confiança dentro da organização. - Custos adicionais. - Consultores nesta área são raros. - Dificuldades em organizar os horários de trabalho. - Pode não ter conhecimento suficiente do contexto. - Pode produzir um plano e regras inapropriados para o contexto de trabalho. - ...	• Esclarecer o quanto possível com todos o seu papel de consultor, escopo. • Aumentar a importância da segurança com outras agências para atacar e compartilhar o problema. • Organizar treinamentos de segurança para futuros treinadores em organizações e instituições. • Informado sobre o contexto de trabalho. • ...

Qual é o ponto de partida do processo?

Agora que a entrada foi ganha e que o/a responsável pelo processo foi indicado/a, onde começamos?

O ponto de partida deve ser a avaliação da segurança de todo o processo de implementação da política de segurança da organização. Começando pela avaliação (ou diagnóstico), que determinará as prioridades e as possíveis soluções (melhores práticas de acordo com as necessidades declaradas, perfil organizacional e mandato). O plano será então desenhado com o objetivo de estruturar um processo de melhoria. O plano incluirá objetivos intermediários para monitorar o progresso atingido. Além disso, o plano vai esclarecer o papel e as responsabilidades da(s) pessoa(s) a cargo do processo e dos membros da organização. O plano incluirá ainda um calendário. Ao final do processo de planejamento será realizada uma avaliação dos resultados alcançados.

Diagnósticos ⇨ prioridades ⇨ possíveis soluções ⇨
plano de melhoria ⇨ avaliação

Uma vez que as prioridades foram determinadas, a decisão sobre sua ordem de implementação será mais fácil se os seguintes critérios forem estabelecidos: emergência, recursos disponíveis, etc.

Flexibilidade é um fator essencial durante todo o processo. Entretanto, qual é o mínimo necessário para que o processo de melhoria tenha uma oportunidade genuína de alcançar resultados positivos? Responder a esta questão antes do início do processo é fundamental.

Diagnóstico e plano de melhoria

O diagnóstico pode ser realizado usando a "avaliação de risco" e a "roda de segurança", descritas em capítulos anteriores deste Manual (qualquer revisão organizacional da metodologia pode ser útil para este processo também).

Sabe-se que este passo deveria envolver todas as pessoas e equipes dentro da organização.

O plano de melhoria deve ser **realista** e **apropriado** ao perfil e necessidades da organização. Aqui indicamos uma possível seqüência de passos:

1 ♦ Identify 1. Identifique as expectativas da organização e os resultados esperados de um plano de melhoria da segurança.

2 ♦ Diagnostique conjuntamente, chegue a um consenso e compartilhe idéias sobre a atual estrutura da gestão de segurança (uso da "análise de risco" e da "roda de segurança"): indique progresso, falhas e necessidades.

3 ♦ Indique e discuta melhores práticas a serem implementadas para resolver as falhas e necessidades reveladas.

4 ♦ Indique os objetivos desejáveis para o plano de melhoria.

5 ♦ Esboço de atividades requeridas para alcançar estes objetivos e o que pode ser razoavelmente esperado de cada atividade (isto facilitará progresso rumo aos objetivos).

6 ♦ Esboço dos recursos necessários (financeiros, humanos, tempo, recursos técnicos). Defina as responsabilidades e o horário de trabalho.

7 ♦ Defina quais riscos surgem se atingirmos estes objetivos e resultados.

8 ♦ Defina indicadores para monitorar o progresso e os resultados finais.

9 ♦ Compartilhe o plano com todas as partes envolvidas para receber feedback, melhorá-lo e gerar a aprovação necessária para sua implementação.

10 ♦ Implemente o plano e decida os prazos para monitorar progresso e possíveis mudanças no processo.

O processo: implementando o plano de melhoria.

O processo inclui uma serie de reuniões e entrevistas com pessoas e equipes trabalhando dentro da organização ou em contato com ela (neste caso, deve haver concordância prévia da organização, indicando as pessoas específicas e/ou organizações com quem a segurança deve ser discutida). A troca pode começar com uma reunião introdutória geral, a qual terá seqüência com outras reuniões. Estas reuniões criarão o espaço no qual definiremos o diagnóstico e discutiremos a implementação do plano de melhoria. Ademais, as reuniões podem tratar de itens específicos ou acompanhar o trabalho específico da organização de um ponto de vista de segurança e proteção.

Resistência ao plano de melhoria

Agora que a entrada foi ganha, as pessoas responsáveis indicadas e o ponto de partida e o processo definidos, que resistência encontraremos entre os indivíduos?

Assim como processos que levam a mudanças numa organização, o plano de melhoria pode encontrar resistência. Entretanto, também encontrará apoio e aprovação. O ponto é ver como conseguir o apoio e argumentar o caso contra possíveis resistências.

A maneira mais apropriada para enfraquecer a resistência é ouvi-la genuinamente e tentar entender as razões. Novamente aqui, participação, ouvindo atentamente todos os pontos de vista e expectativas, é fundamental para um bom processo.

É essencial que o plano de melhoria preveja maneiras de reduzir possíveis resistências de modo a evitar uma posterior improvisação e o risco de o plano falhar simplesmente por causa de possíveis resistências haverem sido negadas anteriormente.

Nesta tabela estão alguns estereótipos comuns de resistência, o raciocínio por trás destes estereótipos e possíveis respostas para superar as forças de resistência.

Estereótipos comuns de resistência	Raciocínio por trás do estereótipo	Respostas para superar a resistência
"Nós não estamos sendo ameaçados" ou "nosso trabalho não é exposto ou contencioso como o de outras organizações".	• O risco permanece igual, não muda ou depende do fato de o contexto de trabalho deteriorar ou de algum cenário mudar.	• Risco depende do contexto político e este é dinâmico: assim como o risco.
"O risco é inerente ao nosso trabalho como defensores" e "nós já estamos cientes a respeito do que estamos expostos".	• Os defensores aceitam o risco e ele não parece afetar seu trabalho. Ou, o risco não pode ser reduzido, o risco está lá e ponto final.	• Encontrar com o risco inerente não quer dizer aceitá-lo. • O risco tem ao menos um impacto psicológico em nosso trabalho: ele induz pelo menos ao estresse, o qual prejudica o trabalho. • O risco é feito de elementos objetivos: ameaças, vulnerabilidades e capacidades: vulnerabilidades e capacidades pertencem ao defensor e são variáveis com as quais ele pode trabalhar. Ao reduzir vulnerabilidades e aumentar capacidades, o risco pode ser reduzido. Ele não pode ser eliminado totalmente, o que não significa que não possa ser reduzido tanto quanto possível.

“Nós já temos conhecimento sobre como lidar com o risco”, ou “nós sabemos como cuidar de nós mesmos”e “nós temos bastante experiência”.	• A atual administração da segurança não pode ser melhorada e não vale à pena fazê-lo”. • O fato de que não sofremos nenhum dano no passado garante que não ocorrerá no futuro.	• A administração da segurança é baseada em elementos objetivos que podem ser trabalhados. • Olhe ao seu redor e veja quantos defensores sofreram algum dano apesar de serem muito experientes.
“Sim, o assunto é interessante mas também temos outras prioridades”.	• Há coisas mais importantes do que a segurança de defensores.	• A vida é a prioridade. Se a perdemos não poderemos lidar com todas as outras prioridades.
“E como vamos pagar por isso?”	• A segurança é cara e eles não podem incluir o tema em propostas de financiamento.	• Quanto você acha que custa a segurança? Um número de fatores de segurança são comportamentais e não custam nenhum centavo. • Investidores prefeririam dar fundos a uma organização que se ocupa de questões de segurança ao invés de arriscar perder seu investimento.
“Se prestarmos tanta atenção à segurança, não poderemos fazer o que é realmente importante, que é trabalhar com as pessoas e nós devemos isso a eles”.	• O fato de que somos afetados por problemas de segurança não afeta as pessoas com quem trabalhamos. A qualidade de nosso trabalho para as pessoas não depende de nos sentirmos mais seguros ou não.	• Segurança é uma questão de vida ou morte. • Em função do fato de trabalharmos para outras pessoas, não podemos correr o risco de perder nossas vidas. • As pessoas correm risco ao confiar-nos seus casos e se não trabalharmos nossa segurança isso lhes afetará também; eles podem escolher outra organização que já tem sua segurança planificada e portanto dará mais segurança às pessoas.
“Nós não temos tempo porque estamos sobrecarregados”.	• É impossível encontrar tempo em nossos horários.	- Quanto tempo leva pensar em segurança? - Quanto tempo gastamos reagindo a emergências ao invés de preveni-las? (provavelmente muito mais tempo do que o tempo necessário para colocar o plano de segurança em funcionamento).
“A comunidade está conosco: quem se atreveria a nos machucar?”	• Nós somos parte da comunidade. A comunidade não é fragmentada, não muda tanto tem termos de pessoas quanto de opinião. • A comunidade não pode ser influenciada.	- A comunidade não é homogênea e é composta de pessoas que poderão ser afetadas por nosso trabalho.
“Em nossa comunidade, as autoridades demonstraram compreensão e colaboração”.	• As autoridades locais não são afetadas pelo nosso trabalho de direitos humanos e não mudarão suas opiniões. • Não há hierarquia entre autoridades locais ou nacionais.	• A memória histórica da organização terá exemplos de autoridades locais que se opõe ao trabalho de direitos humanos quando seus limites de tolerância se excedem. • As autoridades locais implementam ordens que vêm de cima. As autoridades são compostas de pessoas que podem ter interesse em proteger eventuais agressores. • Contextos políticos mudam.

Agora que você já iniciou o processo, um departamento responsável foi indicado e definiu tanto o ponto de partida quanto o processo, e ainda a resistência individual foi desmontada, que fatores organizacionais podem atrapalhar ou facilitar as mudanças?

Fatores organizacionais que podem impedir ou facilitar mudanças organizacionais visando uma melhor política de segurança.

Dentro da organização	Fatores impedindo mudanças	Fatores facilitando mudanças
Cultura organizacional	• Superficialidade. Improvisação. Orientação individual. • Segurança não é integrada. • ...	• Trabalho em equipe, sensibilização sobre o impacto do trabalho, escuta ativa, consulta, processos de tomada de decisão consensuais. • Integração da segurança. • ...
Atitude da diretoria	• Autoritária e ditatorial. Direcionada para resultados. Distante. Importância dada apenas para líderes e portanto inclinada a criar e respeitar regras que sejam adequadas a suas necessidades. • Expectativa não recíproca de que outros membros estão ali para servir os diretores. • Auto concessão de privilégios. • ...	• Em contato com todos os membros. • Reconhecimento da importância da contribuição de todos para alcançar os objetivos da organização. • Atenção dada para preocupações dos funcionários. • Abertura. • Respeito às regras. • ...
Estrutura organizacional	• Rígida. • Compartimentada. • Inapropriada para o trabalho. • ...	• Flexibilidade apropriada. • Coordenação e comunicação fluída entre os níveis. • Reflete as necessidades de todas as pessoas e do trabalho. • ...
Conhecimento de questões de segurança	• Centralização. Parcialidade. Baixo conhecimento de questões de segurança no terreno. Falta de objetividade. Pouco conhecimento efetivo ou substantivo das questões. • ...	• Compartilham experiências e conhecimento. Inclusivo. Factual. • Compilação sistemática de informação e atualizações regulares. • ...
Instabilidade na organização; cansaço	• Rotação de funcionários. • Falta de memória histórica. • Tensão devido a mudanças contínuas. Falta de continuidade no trabalho. • ...	• Descrição do trabalho e contratos claros com o comprometimento declarado da organização de dar aviso prévio com tempo adequado e de transmissão das habilidades e conhecimento antes da saída. • Avaliações regulares. • Distribuição de tarefas que se encaixam no tempo disponível para os funcionários. Introdução e treinamento. • ...
Sobrecarga de trabalho	• Recursos humanos insuficientes ou inadequados. Estresse. Perda de foco. • ...	• Priorização e (re)distribuição de trabalho. • Espaço para relaxar. • ...

Planejamento do trabalho	• Segurança não é claramente priorizada. • Segurança não é considerada no plano de trabalho. • O plano de trabalho é espontâneo e não encaixa os fins e os objetivos. • ...	• Planejamento de segurança adequado no trabalho. Segurança é integrada ao plano de trabalho Consideração adequada é dada às atividades para as quais a segurança é insuficiente e as decisões subseqüentes são tomadas no sentido de melhorar estas condições deficitárias.

Fatores que não influenciam especificamente as mudanças organizações para uma melhor política de segurança:

- Tamanho da organização;
- O fato de as pessoas responsáveis pela segurança não terem educação superior;
- Religião;
- Gênero.
- ...

Padrões ou boas práticas para administrar a proteção e segurança

Agora que o ponto de entrada foi garantido, um departamento responsável foi indicado e definiu tanto o ponto de partida quanto o processo, e ainda a resistência individual foi desmontada, os fatores organizacionais que podem atrapalhar ou facilitar as mudanças foram considerados, quais são as melhoras práticas de gestão de segurança e proteção que dependem de modelos estruturais?

Há vários modelos de administração de segurança dentro de uma organização, e pode ser difícil tomar uma decisão sobre qual seria a melhor escolha. Nesta tabela discutiremos três modelos e seus pontos positivos e negativos, assim como algumas soluções.

Modelos estruturais	Onde são tomadas as decisões de segurança	Vantagens	Desvantagens	Possíveis soluções
Modelo central	• No nível de diretoria, dentro de um departamento dedicado.	• Mais fácil de verificar se a experiência e conhecimento adequados existem dentro da organização. • ...	• A carga de trabalho pode inibir a habilidade de tomada de decisões. • Pode estar desconectado do trabalho em algumas áreas. • ...	• Uma pessoa no nível intermediário com habilidades executivas atua em nome da direção. • A segurança é definida no nível diretivo, mas sem habilidades executórias. • ...

MODELO INTER-MEDIÁRIO	• Decisões globais e importantes: nível diretivo. Decisões específicas: feitas pela pessoa responsável em cada área.	• A diretoria não fica sobrecarregada. • Combinação de habilidades e o nível apropriado. Mais próximo do trabalho real em cada área. • ...	• Conflitos sobre segurança podem aparecer entre os níveis de diretoria e as diferentes áreas da organização. • ...	• Cada pessoa responsável por uma área específica toma a responsabilidade pela segurança desta área. Um consultor de segurança pode ser nomeado para toda a organização; uma pessoa ligada à uma área específica, por exemplo administração ou logística, toma a responsabilidade pela segurança e interage com a pessoa responsável por cada outra área que não seja a sua. • ...
MODELO DESCEN-TRALIZADO	• Decisões de segurança são tomadas em todos os níveis porque cada pessoa tem uma responsabilidade explícita.	• Melhor cumprimento, contribuição à cultura da organização preocupada com segurança. • ...	• Discussões podem levar mais tempo. Talvez se aplique melhor a organizações menores. • ...	• Pode ou não haver uma pessoa dedicada exclusivamente à segurança. • Cada pessoa pode ter uma responsabilidade descrita em seu contrato de trabalho ou em seu trabalho anterior. • ...

Organisation staff/members' training

Agora que o ponto de entrada foi garantido, um departamento responsável foi indicado e definiu tanto o ponto de partida quanto o processo, e ainda a resistência individual foi desmontada, os fatores organizacionais que podem atrapalhar ou facilitar as mudanças foram considerados, os padrões ou melhores práticas de segurança foram estabelecidos, que tal o treinamento dos funcionários?

O treinamento pode ser realizado com recursos internos (talvez haja pessoas treinadas para dar treinamento sobre segurança). O treinamento pode também ser realizado conjuntamente com outras organizações (enviar pessoas juntas de organizações diferentes para treinamentos). Se for este o caso, construir sua capacidade conjuntamente com outra organização pode facilitar trocas de informação sobre segurança no futuro e até mesmo a criação de redes para melhorar a proteção. A confiança entre organizações participando de um treinamento de segurança é fundamental. Além disso, é útil que as organizações compartilhem interesses e tenham áreas e ambientes parecidos de trabalho; organizações rurais ou urbanas por exemplo possuem necessidades de segurança muito distintas.

O treinamento pode ser implementado de muitas maneiras diferentes. As mais comuns são:

- Oficinas (preferentemente em grupos pequenos de 10-15 pessoas);
- treinamento individual (útil para tarefas complexas ou responsabilidades específicas, com treinamento no trabalho);
- Modo conversacional ou semi-formal de reuniões (aconselhamento, conselhos concretos).

É recomendável organizar ao menos um treinamento fora do ambiente de trabalho para facilitar a concentração e evitar as tensões diárias do trabalho. Entretanto, é contraproducente realizar estas atividades fora do horário de trabalho (por exemplo durante os fins-de-semana) pois isso envia a mensagem errada: a de que segurança significa trabalho adicional – sobretudo hora extra, e que a segurança não é importante o suficiente para ser incluída no horário normal de trabalho.

Como melhorar o respeito às regras de segurança

Agora que o ponto de entrada foi garantido, um departamento responsável foi indicado e definiu tanto o ponto de partida quanto o processo, e ainda a resistência individual foi desmontada, os fatores organizacionais que podem atrapalhar ou facilitar as mudanças foram considerados, os padrões ou melhores práticas de segurança foram estabelecidos, os funcionários foram treinados, como se pode melhorar o respeito às regras de segurança?

As condições necessárias para o respeito às regras e planos de segurança são alcançadas através dos seguintes passos:

- Existência e desenvolvimento de uma cultura organizacional de segurança.
- Apropriação das regras e planos de segurança. Participação no desenho e nos processos de melhoria. Treinamento para esclarecer e compreendê-los. Persuasão de sua adequação e efetividade.
- Elaborar um acordo entre indivíduos e a organização em relação ao cumprimento dos planos e regras de segurança.
- Intervenções regulares por parte das pessoas responsáveis pela segurança ou por razões de treinamento e informação, lembrando às pessoas de seus acordos recíprocos e recolhendo opiniões das pessoas sobre a adequação e efetividade das regras.

O que se pode fazer em caso de não cumprimento das regras e planos de segurança?

I • Descubra e resolva as causas do não cumprimento (veja o Capítulo 2.2).

II • Se a causa do descumprimento for intencional e depender meramente da vontade de um indivíduo, siga os seguintes passos:

a • Converse com a pessoa (como o fim do processo anterior destinado a resolver as causas do não cumprimento) para gerar motivação e comprometimento.

b • Leve o assunto à pessoa relevante no grupo, na presença do indivíduo em questão (este passo às vezes não é o mais adequado, dependendo da situação).

c • Aplique um sistema de avisos (entre 2 e 3 avisos).

d • Aplique um sistema de sanções graduais que pode culminar na demissão do indivíduo.

É importante incluir no acordo uma cláusula referente ao cumprimento dos planos e regras de segurança para que todos os defensores estejam totalmente conscientes da importância destinada à segurança pela organização.

Resumo

Ter um plano de segurança não quer dizer que este será respeitado e implementado. Um processo apropriado deve ser pensado para administrar a implementação da segurança, seu cumprimento e como melhorá-lo. Quanto mais inclusivo o processo, mais informação sobre necessidades de segurança serão recolhidas e mais apropriação por parte das pessoas envolvidas será alcançada.

Não há estrutura organizacional certa ou errada: há vantagens e desvantagens. É portanto útil analisá-las para criar um processo conveniente e com as maiores chances possíveis de sucesso.

A melhoria do plano deve ser **realista** e **apropriada** ao perfil e necessidades da organização.

Estes são os passos sucessivos de um processo para melhorar a política de segurança:

- ♦ É preciso um ponto de entrada para a segurança;
- ♦ Um departamento ou órgão deve ser nomeado;
- ♦ O órgão responsável precisa encontrar o ponto de partida e planejar o processo;
- ♦ Resistências individuais precisam ser neutralizadas ouvindo-se os argumentos para compreendê-los e articular um contra argumento (não é suficiente apenas dar uma visão oposta ao estereótipo de resistência; é preciso determinar as razões por trás de fazê-lo). Se a resistência ao pensamento de um indivíduo está certo, também estará sua resistência;
- ♦ Fatores organizacionais impedem ou facilitam as necessidades de mudança e precisam ser considerados;
- ♦ Padrões ou melhores práticas de segurança e proteção precisam ser determinados pelos funcionários;
- ♦ os membros precisam ser treinados;
- ♦ O cumprimento das regras de segurança precisa ser melhorado.

PARTE III

PROTOCOLOS, PLANOS EMERGÊNCIAE MAIS POLÍTICAS ORGANIZATIVAS

Eles são baseados em boas práticas compartilhadas e aprendidas em oficinas que organizamos.

Eles não são, entretanto, completos ou uma garantia de bons resultados, pois o Manual não pode reproduzir todas as variáveis de um determinado contexto.

Todo este processo é um trabalho em construção, e apreciamos seus comentários, assim como novas sugestões de protocolos e planos.

Publicaremos atualizações e novas ferramentas no sítio www.protectionline.org, so that defenders can benefit from them as sopara que os defensores possam beneficiar delas tão logo quanto possível. Também incluiremos atualizações em novas edições do Manual. Por enquanto, veja o *Anexo IV – Elementos de Risco Geral para um Perfil Específico de Defensor de Direitos Humanos*.

ÍNDICE DA TERCEIRA PARTE:

Como reduzir os riscos relacionados a uma busca e/ou assalto ao escritório

Uma busca pode ser descrita como uma entrada forçada a uma casa, escritório ou espaço privado. Uma busca é legal quando o Estado decide sobre ela e a realiza de acordo com as leis em vigor. Uma busca é ilegal quando a entrada forçada é contra a lei (por exemplo um roubo durante a noite, uma busca por forças de segurança sem um mandado judicial ou a busca à força por parte de um ator armado).

Apesar de o caso que segue como exemplo ser o resultado de uma busca legal, os defensores também podem derivar regras aplicáveis a buscas ilegais e completá-las com informação contida no capítulo sobre segurança em residências e escritórios.

O Estado pode legalmente realizar uma busca. A lei em vigor precisará estar em linha com os padrões internacionais de direitos humanos e de proteção das liberdades democráticas. Entretanto, pode vir a ser um problema se, contrariamente aos padrões internacionais, as buscas são usadas como método padrão para continuadamente importunar e criminalizar os defensores de direitos humanos e movimentos sociais através de buscas rotineiras.

Nenhum defensor pode alegar que uma busca é um evento "inesperado" (como qualquer outro risco), sobretudo porque a busca pode ser absolutamente legal. Nenhum risco pode ser reduzido a zero. Nós precisamos portanto reduzir ao máximo o risco de possíveis ameaças/ ou conseqüências desta busca.

Como podemos atingir isso? Usando a equação de risco e listando todas as ameaças/ e conseqüências (conseqüências podem ser assimiladas a ameaças). Então, para cada ameaça/conseqüência, liste as vulnerabilidades e capacidades respectivas, e comece a trabalhar sobre elas...

Ameaças/conseqüências relacionadas a buscas

Uma busca gera ameaças/conseqüências:

a • A ameaça de que durante a busca alguém sofra algum dano físico ou psicológico.

b • A ameaça de que a informação seja levada, perdida ou destruída.

c • Relacionado a isso, que a informação possa ser usada inadequadamente por uma terceira pessoa.

d • A ameaça de que objetos contenciosos possam ser "escondidos" (armas, drogas, documentos) para mais tarde processar "legalmente" a organização.

e • A ameaça/conseqüência de que dinheiro e outras propriedades (computadores, etc.) sejam roubados ou destruídos.

f • ...

a ♦ A ameaça de que durante a busca alguém sofra algum dano físico ou psicológico.

Ninguém pode prever como uma busca será realizada e qual será seu impacto. Entretanto, possuir antecipadamente tanta informação quanto possível sobre a busca pode contribuir para evitar estresse e comportamentos que poderiam levar a danos físicos e psicológicos. Pode ainda contribuir para aumentar a conscientização sobre riscos e para que se mantenha sempre um comportamento positivo.

Vulnerabilidades:

- Não saber sobre o que é a busca;
- Acreditar que opor-se à busca ajudará na situação;
- Nenhum seguro médico;
- ...

Capacidades:

- Saber como uma busca autorizada legalmente pode ser realizada;
- Saber qual departamento ou órgão pode emitir mandados de busca e ter o nome do funcionário responsável (antes e durante a busca);
- Saber a aparência de um mandado de busca;
- Saber quais os direitos da organização ou pessoa sendo objeto de uma busca (incluindo o direito de pedir para ver o mandado de busca e possivelmente pedir assistência jurídica);
- Ter acesso a assistência jurídica (durante e depois da busca);
- Saber como não exercer resistência indevida;
- Se a busca for realizada sem violência, é importante que as pessoas fiquem em grupo para reduzir a chance de ser maltratado individualmente;
- ...

A organização considera pendurar num local visível:

- Um exemplo de mandado de busca;
- Toda a legislação correspondente (direitos e deveres de ambas as partes);

■ Uma lista dos nomes e telefones dos advogados, médicos, psicólogos da organização e do hospital mais próximo... (A lista deveria também estar visível em todas as partes do escritório para aumentar a possibilidade de acesso rápido por parte de todos os funcionários presentes).

Esta informação é legal e pública. Ela pode portanto estar visualmente acessível para todos. Isto pode não prevenir uma busca (com ou sem um mandado de busca). Mas pode, no entanto, ajudar a reduzir o estresse entre aqueles que são revistados. Isso pode também contribuir para avisar a pessoa que efetua a busca que o indivíduo ou a organização estão cientes de seus direitos e que eles tomarão as ações necessárias caso a busca vá além da prescrição legal (dissuasão).

b ♦ A ameaça de que a informação seja levada, perdida ou destruída.

Em geral, a maioria das organizações mantém mais informação do que o necessário. Uma grande quantidade raramente é usada e não é confidencial. Em outras palavras, apenas uma pequena quantidade é confidencial e ela não deveria estar acessível a buscas. Informação absolutamente confidencial normalmente inclui: lista de pessoas (beneficiários de projetos, testemunhas de casos); provas fundamentais em casos jurídicos; casos específicos e análises.

A informação considerada pública ou não contenciosa pode ser mantida no escritório para as buscas (da mesma forma quando alguém viaja com dinheiro, e mantém uma pequena quantidade visível que poderia ser levada no caso de um roubo ou assalto).

Uma política de segurança de informação apropriada significa que as conseqüências da perda, roubo ou destruição de informação são consideravelmente reduzidas.

Isso também significa que o defensor não deveria sentir a necessidade de se expor para proteger informação (em qualquer caso, a vida vem em primeiro lugar); isso diminuirá a probabilidade de estresse em caso de buscas, reduzindo ainda o risco de violência e ferimentos tanto físicos quando psicológicos. (resolvendo assim a questão referida acima de ameaça/conseqüências).

Vulnerabilidades:

- Informação não arquivada de acordo com a distinção entre confidencial e não confidencial.
- Informação sensível mantida em papel.
- Informação eletrônica não criptografada (arquivos e anexos).
- Segurança inadequada do escritório e de residências: falta de barreiras e filtros para prevenir acesso de pessoas indesejáveis ou ao menos que permitam tempo para desligar o computador ou esconder um documento.
- ...

Capacidades:

- Cópias de segurança regulares (ao menos semanalmente) das informações guardadas no computador, e armazenadas em um lugar seguro. No caso de uma busca você saberá quanta informação está efetivamente exposta (dependendo da data da busca e da última cópia de segurança).
- Cópias ou fotocópias, ou melhor ainda cópias digitalizadas, para manter os registros num lugar seguro. Se necessário elas podem ser distribuídas entre outros locais seguros.
- Medidas de segurança adequadas para o escritório e residências.
- Alerta no início de uma busca para conseguir apoio jurídico (advogados) e pedidos a outras organizações para que sejam testemunhas e auxiliem vocês, pelo menos do lado de fora. Isso colocará pressão nos perpetradores, na esperança de que se atenham a cumprir com a lei durante a busca.
- ...

Comparação entre diferentes sistemas de backup

Meio de armazenamento	Vantagens	Desvantagens
CDs/DVDs	Muitos computadores possuem drive para gravar CDs e DVDs. É fácil e seguro transportar e armazenar a cópia de segurança em CDs/DVDs.	No caso de muita informação, muitos CDs são necessários, o que faz o processo mais longo e complexo. Qualquer pessoa que tenha acesso aos CDs terá acesso a todos os dados.
Pen drive	Mesma coisa.	Como acima, mas ainda mais fácil de armazenar e portanto menos provável que cairá em mãos erradas.
Disco rígido externo	Armazena grande quantidade de informação e não leva muito tempo para copiar. Pode ser equipado com senhas de acesso para proteger a informação.	Custo (200-300 US $).
Servidor remoto	Pode armazenar toda a informação, é rápido e não pode ser perdido ou roubado.	Você precisa uma conexão internet rápida e criptografia. Os servidores podem ser "forçados" a entregar os arquivos aos agressores ("argumento de segurança do Estado").

c ♦ A ameaça/conseqüência de que a informação possa ser usada inadequadamente por uma terceira pessoa.

Alta probabilidade de conseqüências para a organização e para as pessoas mencionadas na informação roubada.

Conseqüências para a organização alvo de buscasfetada

Vulnerabilidades:

- Nenhuma consideração antecipada foi dada para possíveis procedimentos de reação.
- Negligência ética, controle financeiro deficiente, software pirata (pode representar açõesprocedimentos legais contra a organização).
- ...

Capacidades:

- Cópias de segurança.
- Plano de reação funcionando.
- ...

Conseqüências para as pessoas mencionadas na informação.

Vulnerabilidades:

- Não ter discutido previamente essa possibilidade com as pessoas envolvidas.
- Não possuir contato rápido com elas.
- ...

Capacidades:

- Ter explicado a existência do risco e certificado-se de que não ocorrerá novamente por causa de negligência de pessoas ou da organização.
- Ter feito um plano conjunto de reação de emergência (utilizando-se do plano rapidamente, medidas de proteção, esconderijos, etc.).
- ...

d ♦ A ameaça de que objetos contenciosos possam ser "escondidos" (armas, drogas, documentos) para mais tarde processar "legalmente" a organização.

Vulnerabilidades:

- Office o espaço do escritório está cheio de objetos e papéis não relacionados ao trabalho (objetos pessoais, revistas espalhadas)... fica mais

difícil encontrar alguma coisa que tenha sido escondida intencionalmente durante a busca, ou se um visitante anterior escondeu ou deixou algum objeto ou documento contencioso que pode ser 'casualmente' encontrado pelas pessoas que realizam a busca.

- Nenhum inventário de material de escritório, muito menos um inventário registrado com um advogado.
- Apenas uma pessoa da organização está presente durante a busca.
- ...

Capacidades:

- Onde possível (no caso de uma busca legal)[1] , as pessoas estão preparadas para ficarem em cantos/ das salas do escritório (por exemplo cada pessoa em sua sala de trabalho) para observar o que acontece durante a busca. É mais fácil notar se alguma coisa está sendo levada ilegalmente.
- Após a busca (não importa que tipo de busca), a organização realiza uma verificação do escritório (se possível com o auxílio de observadores externos), gravando (mesmo com fotos) tudo que puder ser encontrado e não pertence ao escritório/ ou não estava lá antes da busca. Isso deve ser claramente relatado e não deve ser tocado (lembre-se das impressões digitais). Faça um registro também de itens não encontrados.
- Envie um relatório para a polícia e siga as normas legais vigentes.
- ...

e ♦ A ameaça/conseqüência de que dinheiro e outras propriedades (computadores, etc.) sejam roubados ou destruídos.

Uma busca ilegal provavelmente incluirá o roubo de alguns itens.

Vulnerabilities:

- Grande quantidade de dinheiro e bens valiosos no escritório.
- Itens desprotegidos.
- Nenhum inventário de materiais do escritório, muito menos um inventário registrado com um advogado, como recomendável.
- Nenhum seguro contra roubot.
- ...

1 Se a busca é realizada sem violência, é importante que as pessoas permaneçam em grupo para evitar o risco de serem maltratados individualmente.

Capacidades:

- Coloque funcionários do escritório em vários locais para observar a busca.[2]
- Alerta no início de uma busca para conseguir apoio jurídico (advogados) e pedidos a outras organizações para que sejam testemunhas e auxiliem vocês, pelo menos do lado de fora. Isso colocará pressão nos perpetradores na esperança de que se atenham a cumprir com a lei durante a busca.
- ...

Como confrontar e reduzir a ameaça de uma busca

Se uma busca segue a legislação internacional e tem um objetivo legítimo e legal, então não há sentido em pensar em confrontar ou reduzir a ameaça de uma busca. Você deve abrir a porta do escritório e considerar apenas os passos prévios relativos às conseqüências. No entanto, se as buscas são usadas sistematicamente para atrapalhar o trabalho de defensores de direitos humanos e movimentos sociais, então uma ação correspondente deve ser levada a cabo.

Para confrontar ou reduzir a ameaça de uma busca legal, a melhor estratégia é aumentar o custo político através de campanhas públicas de incidência, de preferência em parceria com outras organizações ou institutos.

Se existe o risco de uma busca ilegal (ou roubo) é importante melhorar tanto quanto possível a segurança da residência ou escritório.

Isto tudo se aplica tanto para casos de escritórios em áreas rurais quanto em áreas urbanas.

2 Novamente, se a busca dor realizada sem violência, é importante que as pessoas fiquem em grupo para reduzir os riscos de serem maltratados individualmente.

Resumo

Como reduzir o risco de uma busca.

Buscas podem ser legais e ilegais (quando se trata de uma busca ilegal, trata-se de uma invasão).

E assim como para qualquer outro risco específico, aumente o custo político das buscas.

Use a equação e desenvolva cada elemento ao máximo.

Liste as ameaças/conseqüências e suas respectivas vulnerabilidades e capacidades e trabalhe sobre elas:

a • A ameaça que durante a busca alguém sofra algum dano físico ou psicológico.

b • A ameaça de que a informação seja levada, perdida ou destruída.

c • Relacionado a isso, que a informação seja usada inadequadamente por terceiros.

d • A ameaça de que objetos contenciosos possam ser "escondidos' (armas, drogas, documentos) para posterior ação "legal" contra a organização.

e • A ameaça/conseqüência de dinheiro e outras propriedades (como computadores) serem roubados ou destruídos.

f • ...

Detenção, prisão, rapto ou seqüestro de um defensor

"Nenhuma notícia do defensor".

Quando não se tem notícias do paradeiro de um defensor, o primeiro desafio é descobrir exatamente o que lhe aconteceu, e isso pode levar tempo. Muitas coisas podem ter acontecido:

- O defensor pode não **querer, ou pode ter esquecido de**, contatar a organização: ela/e pode ter decidido sair por um fim de semana, ou visitar alguém sem informar a ninguém (ou talvez queira se "desconectar"). Ela/e pode ter ficado sem telefone ou outro meio de comunicação, ou pode não ter se dado conta de avisar. Eles podem querer que ninguém saiba o que estão fazendo (com êxito algumas vezes). Eles podem (e essa é a opção menos freqüente) ter esquecido ou ignorado o fato de que seu paradeiro pode ser uma preocupação para seus colegas.

- O/A defensor(a) pode não ter conseguido contatar a organização por **questões técnicas**: isso pode acontecer quando o defensor é desconectado dos meios de comunicação num local mais remoto inesperadamente ou de modo imprevisível. Isso pode acontecer durante uma viagem quando o defensor se encontra, inesperadamente, num local sem comunicação, ou onde a estrada está bloqueada, ou ele/a tem de tomar um caminho alternativo, ou ele/a tem de fazer uma improvisação no plano sem comunicação. Pode ser também que os meios de comunicação estejam com problemas (celular quebrado, sem cartão de crédito, bateria exausta, colapso da rede telefônica, etc.)

- O/A defensor(a) pode estar impossibilitado de contatar a organização por causa de uma **doença ou se for hospitalizado** (por exemplo num acidente de trânsito, uma doença repentina, ou a piora na condição de saúde por causa de uma doença preexistente).

- O/A defensor(a) pode ter sido **detida**, **presa**, **raptada** ou **seqüestrada**. A característica comum é que o/a defensor(a) está privada de sua liberdade de movimento e pode experimentar

desde uma pressão leve a uma tentativa contra sua vida[1]. Em alguns casos, o/a defensor(a) pode chegar a conseguir falar com a organização, o que significa que a organização terá mais informação sobre sua situação.

Detenção significa que membros da organização estão sob o controle de um grupo (de soldados, ou milícia, ou autoridade local, etc.). **Prisão** é o termo usado para descrever a detenção pelas forças de segurança (quando o princípio da lei pode ser invocado). **Rapto** refere-se à captura forçada e remoção do defensor de uma maneira ilegal por razões políticas. **Seqüestro** refere-se à captura forçada e detenção sem o propósito explícito de obtenção de concessões da pessoa cativa ou de outros. Neste Capítulo usaremos preferencialmente o termo **detenção** para simplificar as coisas.

Em geral nós deveríamos dizer que na maioria dos casos quando não temos notícias do(a) defensor(a), trata-se de um dos dois primeiros casos (não querer ou esquecer de comunicar, ou não ser possível por razões técnicas) Vejamos como prevenir e reagir a estes casos.

Dicas de prevenção para evitar uma situação "Sem Notícias" em relação ao paradeiro de um defensor.

O defensor não quer, ou se esqueceu de, contatar a organização.

- Cada membro da organização e particularmente aqueles em situação de maior risco devem estar conscientes do fato de que outros estarão preocupados com eles em caso de falta de notícias sobre sua localização. Se eles quiserem ficar sem contato, eles deveriam avisar os colegas sobre isso, incluindo detalhes de quando estarão de volta em contato regular. No caso de um defensor de alto risco, pode ser desaconselhável para ele/a permanecer sem contato regular.
- É importante estabelecer rotinas de verificação para ficar em contato com a organização (geralmente com uma ou duas pessoas específicas). Isso torna-se essencial se o risco aumenta para um defensor (porque estão viajando numa área de risco ou se receberam ameaças, etc.).

O defensor não é capaz de contatar a organização por razões técnicas.

- Combinar uma verificação previamente pode ser feito, e os problemas de comunicação devem ser antecipados para estes períodos: por exemplo, se um horário de conferência coincide com uma viagem, deve-se pensar em como será possível comunicar-se (por telefone celular, fixo ou outro meio) para certificar-se que isso será possível e também garantir que problemas como interrupção de comunicações, vencimento do cartão de crédito, fim da bateria... não impedirão a comunicação.
- Planeje meios alternativos de comunicação (através de terceiros, por exemplo).

[1] Neste Capítulo utilizaremos alguns conteúdos do Manual de segurança escrito por van Brabant (2000) (Capítulo 13)

O/A defensor não é capaz de se comunicar porque ele/a está doente ou hospitalizado/a.

- Mantenha listas de números de telefones e endereços de todos os hospitais e centros médicos na área visitada, e onde possível detalhes de como receber atualizações sobre acidentes de trânsito (companhias de ônibus, polícia rodoviária, contatos ao longo da rota, etc.).
- Defensores não deveriam realizar viagens a menos que estejam em boa saúde.
- Use o meio mais seguro de transporte (incluindo ônibus ou outros meios).
- Defensores deveriam ter seguro de saúde e acidentes em dia.

Prevenindo detenções.

Não é fácil antecipar como prevenir uma detenção. O objetivo crucial é reduzir as razões que podem expor ou facilitar a detenção de qualquer membro da organização.

- O comportamento ético de indivíduos e da organização é crucial para razoavelmente excluir infrações individuais ou organizacionais à lei. Infrações à lei podem ser usadas como pretexto, mas o advogado da organização saberá o que fazer. Além disso, o defensor preso saberá os passos que estão sendo tomados e poderá permanecer "calmo" (impacto psicológico) sabendo que uma ação exterior está sendo realizada em seu favor. Não há necessidade de desafiar as autoridades ou dar uma oportunidade para expor-se a mais risco do que já está sendo submetido.
- Em casos onde infrações à lei são usadas para ação política, é necessária uma análise de risco completa e uma estratégia de limitação de danos deve ser preparada, dado o risco enfrentado pelos defensores.
- É claro que uma detenção legal pode ser um pretexto. Pode ou não ser baseada num mandado e pode acontecer a qualquer momento, no escritório/em casa ou durante uma viagem. O essencial seria prevenir uma detenção quando o defensor está sozinho para reduzir as conseqüências da própria detenção. O que é necessário é uma estratégia de ação política para dissuadir as autoridades de prenderem os defensores; apesar disso, a tendência em muitos países parece ser a de judicializar os defensores e prendê-los por várias razões, incluindo razões desconectadas de seu trabalho.
- Não é fácil impedir um rapto. Ademais de realizar uma detalhada análise de risco quando existe a ameaça de um rapto, é crucial reduzir a exposição em áreas onde a ameaça pode ser realizada, garantir que a pessoa nunca ficará sozinha, e avaliar qualquer ação que possa facilitar um rapto.
- Rapto pode ser realizado por criminosos comuns (seja um pretexto ou não) ou por atores legais e/ou paralegais, e/ou grupos políticos armados, etc. Pode potencialmente ocorrer em qualquer lugar, mas provavelmente ocorrerá quando a oportunidade é criada pelos potenciais agressores, ou apresentada a eles pelo defensor, e preferencialmente sem testemunhas por perto. Portanto, um rapto é menos provável no escritório durante o horário de trabalho, em casa durante o dia, etc. (veja exemplos de ameaças de morte contra um líder de uma organização no Capítulo 1.7)

  As diferenças entre procedimentos ilegais e uma detenção legal e uma agressão/rapto são tão tênues que os defensores de direitos humanos

deveriam considerar todas estas possibilidades não como mutuamente excludentes, mas mutuamente complementares. Entretanto, nós consideramos importante explicar a diferença entre o atual significado entre detenção e rapto por questões práticas e psicológicas.

- A prevenção da agressão/rapto deveria levar em conta o dia-a-dia de trabalho do defensor e na sua área usual de trabalho, tempo livre, atividades, etc., e definitivamente durante missões de campo, sejam elas planejadas pela organização e/ou como convidados. Seja vigilante, verifique duas vezes os convites de pessoas desconhecidas.

We suspect that a defender has been detained (or arrested, abducted or kidnapped)...

Quando suspeitamos que um defensor foi levado contra sua vontade? Bem, se não tivermos notícias diretas do defensor, devemos suspeitar algo quando temos razões para imaginar que alguma destas três coisas aconteceu... Realisticamente, o procedimento de reação a uma detenção ou suspeita de detenção segue o procedimento de razão usado quanto uma pessoa não entra em contato e ela havia combinado isso.

Portanto, quando não temos notícias do defensor, devemos começar a procurar para poder ignorar as três primeiras opções. É difícil certificar-se de que excluímos qualquer uma das três primeiras opções. Por esta razão, é importante definir um prazo limite antes de considerar a quarta opção: 3 horas sem notícias, 6 horas, 12 horas... Dependendo do contexto, das circunstâncias, do nível de risco, da ciência do defensor de que deveria reportar-se, etc. Quanto menor o tempo, maior será o risco de cometer erros se emitirmos um alerta; quanto maior o prazo, maior também será o tempo para tomar alguma ação necessária. Essa não é uma decisão fácil!

Aviso: um relatório (de viagem) pode não ocorrer por descuido, por negligência da pessoa que deveria fazê-lo, ou por falta de meios de comunicação – estes fatores deveriam ser antecipados quando planejamos um programa de relatórios periódicos para a missão.

Lembre-se: nós podemos reagir a uma suspeita de detenção ou a uma detenção já confirmada.

É fundamental que a reação daqueles que foram detidos e da organização seja harmonizada, e tente atingir os mesmos objetivos. É por esta razão que todos os membros da organização deveriam estar familiarizados com procedimentos de reação.

Detenção (prisão, rapto, seqüestro):

Uma detenção (prisão, rapto, seqüestro) pode variar em duração entre algumas horas ou mesmo anos. A resolução do caso geralmente será alcançada com a liberação da pessoa, ou pode ser que no caso de um seqüestro o objetivo a ser alcançado é outro e vai além da própria detenção, ou em alguns casos sérios de rapto que podem levar a ferimentos, à morte ou a "desaparecimentos".

Detenção deveria ser tratada a partir de três pontos de vista:

- Do ponto de vista do(s) defensor(es) detido(s).
- Do ponto de vista da organização da qual depende a(s) pessoa(s) detida(s).
- Do ponto de vista da família e parentes da(s) pessoa(s) detida(s).

Objetivos gerais ao tratar de uma detenção:

- Reduzir a possibilidade de que ocorra uma detenção.
- Estar informado assim que possível sobre as possíveis chances de uma detenção.
- Esboçar como reagir a uma situação assim:
  - Reação imediata.
  - Reação de médio prazo.

Para manter este Manual o mais simples possível, trataremos de detenção (incluindo prisões) e seqüestro separadamente.

Detenção de um defensor: reação imediata

Objetivos e passos de uma reação imediata a uma detenção:

Estabelecer um grupo de trabalho ad hoc para reagir à detenção.

1 ♦ Proteger a vida e a liberdade dos membros da organização.

2 ♦ Localizar geograficamente as pessoas detidas, usando um mapa, o plano de viagem, os últimos contatos feitos, ligar para contatos e atores no campo, etc...

3 ♦ Definir qual grupo armado deteve a pessoa, porquê, e para que finalidade.

- Usando a localização geográfica da(s) pessoa(s) detida(s), assim como conhecimento prévio (você poderá ter de supor as causas da detenção se você ainda não as sabe). Será então possível chegar a uma suposição razoável sobre quem está detendo a(s) pessoa(s), ou ao menos chegar a uma lista curta de possíveis suspeitos.
- Contate as autoridades (caso seja adequado, necessário e possível).

4 ♦ Consiga a soltura do defensor da detenção ileso.

■ Como uma regra geral, é importante não focar em não chegar a um acordo mas chegar a uma saída concreta ou soltura, deixando as negociações para depois que o defensor tenha sido liberado.

■ Avalie o grupo armado em questão (em colaboração com autoridades regionais quando possível/necessário), tanto diretamente no caso de forças de segurança, ou usando intermediários – a assistência de órgãos como igrejas, sábios, autoridades locais, o Comitê Internacional da Cruz Vermelha, etc... Por esta razão é crucial poder contar com estes contatos. Esta avaliação tem como objetivo definir as razões para a detenção, e tentar obter a soltura imediata do defensor detido.

■ Considere alertar outros defensores de direitos humanos e organizações humanitárias para que eles estejam cientes, e para ajudarem com passos conjuntos para reforçar a ação. Quando há suspeita de rapto com ferimento ao defensor (como um rapto realizado por um "grupo de extermínio"), é importante agir o mais rápido possível e focar a ação tanto quanto possível.

■ Alerte os consulados se a pessoa detida for de outro país.

Detenção de um defensor: reação de médio prazo

Se um defensor for detido, e não podemos antecipar a possibilidade de liberá-lo no curto prazo, objetivos e passos de médio prazo devem ser introduzidos sem perder o foco nos objetivos de curto prazo.

Objetivos e passos de uma reação de médio prazo a uma detenção.

1 ♦ Mantenha o foco nos objetivos da reação de curto prazo.

2 ♦ No caso de uma prisão, além de identificar rapidamente quem está detendo o defensor, tente obter a transferência para a custódia legal (do Estado) ou para um serviço de segurança que possa ser influenciado. Neste caso, tente obter apoio jurídico adequado assim que possível (preferencialmente antecipadamente). O risco de tratamento desumano e de tortura pode ser reduzido assim.

3 ♦ Se o defensor permanecer detido, tente atender suas necessidades pessoais – segurança, comida, cuidados de saúde, contato com familiares e a organização, etc. – desde o princípio e durante todo o processo (isso pode ser planejado com antecipação – veja abaixo: medidas para familiares e parentes).

Reações por parte das pessoas detidas

- Lembre-se dos passos e planos preparados previamente tendo em vista a possibilidade de tais situações. É importante saber a seqüência correta dos passos no caso de uma detenção ou prisão, para poder minimizar a incerteza, usar a força das pessoas de uma maneira controlada e planejar objetivos simples de resistência.
- Permaneça calmo. Os defensores sabem do protocolo de reação da organização e os passos que estão sendo tomados; eles podem repeti-los para eles mesmos e permanecerem calmos.
- Tudo o que for dito ou feito deve ter como objetivo preservar a vida e a segurança das pessoas detidas.
- Faça contato com o chefe do grupo armado, e incentive-o a dialogar, usando argumentos institucionais básicos com o objetivo de obter a liberação das pessoas detidas e seu retorno, ou a liberação para outro local seguro (não tente negociar um "acordo").
- Se isso não for permitido, solicite permissão para usar outros meios disponíveis para alertar a organização sobre sua posição; não tente chamá-los sem permissão se você estiver sendo vigiado, pois isso poderá causar mais riscos do que não fazer nada.
- Se a detenção for resultado de forças de segurança, use os argumentos legais da organização para estes casos.
- Permaneça calmo e não se esqueça de que a organização está rapidamente implementando todos seus sistemas de segurança.

Medidas com o objetivo de apoiar a família e parentes:

- Informe a família e parentes se a pessoa não for liberada logo. Estabeleça e mantenha confiança.
- Estabeleça uma abordagem clara com relação à família. Ofereça apoio e mantenha-os informados (nomeie uma pessoa de contato para a família).
- A família precisará de tempo e atenção da organização. Espere atitudes flutuantes e iniciativas por parte da família.
- No caso de prisões de longo prazo, é importante planejar o apoio à família do defensor.

Rapto e seqüestro de um defensor[2]

Desde o ponto de vista da organização

Administrar uma crise de seqüestro é um processo de mudança que pode durar entre algumas horas, meses ou mesmo anos. As questões chave são a mobilização de uma equipe de crise competente; lidar com a família, com as autoridades e a imprensa; comunicações e negociação com os seqüestradores.

Comunicando e negociando com os seqüestradores

Seqüestro, conforme entendido aqui, tem um objetivo deliberado. Os seqüestradores geralmente estabelecem contato para deixar claras suas condições e exigências.

A equipe de gerenciamento da crise deveria manter o controle das negociações, mas evitar fazer contato direto com os seqüestradores; o propósito é criar uma diferença de tempo para permitir consultas internas e externas e então tomar decisões. Você pode, caso necessário, pedir uma prova de vida ou da identidade dos seqüestradores e incentivar e exigir bom tratamento dos seqüestrados.

Um seqüestro é um caso de risco real. É importante ter acordado previamente as regras e procedimentos em relação a resgates e pedidos dos seqüestradores, e quando possível que isso esteja em linha com outras organizações. Dê publicidade a este guia. Em qualquer caso, eventos similares do passado poderão trazer informações sobre os estágios prováveis de um seqüestro.

Do ponto de vista do defensor seqüestrado

■ Os momentos mais perigosos, quando os seqüestradores estarão mais tensos, serão durante o rapto, quando o seqüestrado tiver de ser movido rapidamente por medo de os seqüestradores serem encontrados, durante uma situação de cerco e durante a liberação.

■ Seus captores vão querer que você fique quieto; você pode permanecer vendado, ser agredido e mesmo drogado. Não faz sentido chorar ou lutar para opor-se a estas táticas: permanecer quieto pode ajudar a evitar estas táticas (a menos que você possa razoavelmente esperar que, durante um seqüestro, gritar por ajuda pode fazer com que alguém lhe ajude).

2 Para este tema, utilizaremos extensivamente a obra de van Brabant (2000).

■ O local e as condições nas quais o seqüestrado será mantido variam muito. Você poderá ser mantido num mesmo local ou ser movido várias vezes; você pode ficar sozinho ou com outros seqüestrados. É comum para seqüestrados desenvolverem algum tipo de relação com seus guardas e achar difícil adaptar-se à mudança de guardas.

■ Obedeça as ordens de seus captores sem parecer servil; evite surpreendê-los ou alarmá-los.

■ Tente manter a saúde física e mental.

■ Se você estiver em um grupo, deveria tentar não ficar separado, pois estar com uma outra pessoa pode ser uma fonte de apoio. É importante entretanto estar preparado para a separação e para mudanças, e em geral para a incerteza que cada dia vai trazer e que precisará ser enfrentada.

■ Conseguir a liberação não é seu problema, mas de sua organização. Nunca se envolva diretamente nas negociações para sua liberação. Isso apenas complicará as coisas. Se pedirem para que fale no rádio, telefone ou em vídeo diga o que lhe pedirem e recuse negociar mesmo que seus captores exijam.

Procedimentos de prevenção: reduzindo riscos de detenção ou rapto durante uma viagem

Riscos de detenção ou rapto são particularmente altos durante uma viagem de campo porque o defensor está mais exposto, tem menos contato com seu entorno regular, e com aqueles com quem se relaciona e isso pode atrasar a reação a um ataque ou ameaça. Por esta razão, nós explicitamos os riscos relacionados a viagens de campo pois incluem a maioria das ameaças e conseqüências relacionadas ao trabalho dos defensores como um todo.

Por exemplo:

Pontos de controle ⇨ prisão ⇨ detenção ⇨...
Agressão ⇨ rapto ⇨ violência ⇨...
Perda de informação ⇨ impacto sobre testemunhas ⇨ impacto na organização ⇨...
Transporte ⇨ público/particular ⇨...
Tempo de lazer quando no campo ⇨ abaixar a guarda ⇨ incidentes de segurança ⇨...
Comunicação ⇨ telefone ⇨ cara a cara ⇨...

Nós gostaríamos de insistir no risco de detenção/rapto durante uma viagem de campo e recomendamos protocolos de prevenção para estas viagens que incluam ao menos o seguinte:

- Preparação para todas as missões, tanto de campo quanto em áreas urbanas, onde for relevante.
- Não viaje sozinho.
- Informação adequada do contexto da área e dos atores a serem visitados (mapeamento dos atores, análise de campos de força, veja Capítulo 1.1).
- Defensores deveriam conhecer rotas de entrada e saída dos locais da missão.

- Cada pessoa envolvida na missão deve ter documentos de identidade válidos.
- Alerte os contatos de emergência da organização que estarão em alerta durante toda a missão de campo (do momento que você sai até o seu retorno).
- Prepare a missão de acordo com procedimentos: inclua a agenda e o trabalho a ser realizado, e isso deveria ser parte do Manual de segurança organizacional.
- Planeje atualizações regulares sobre o estado da missão (geralmente por telefone, conforme combinado anteriormente). Isso implica, se possível, verificar se a rota e a destinação final possuem recepção telefônica. Se não for possível checar a recepção, você pode pedir ajuda a pessoas confiáveis morando no caminho para confirmar que a equipe foi vista e está bem.

  É importante decidir quanto tempo a pessoa designada estará em alerta para receber uma chamada de atualização sem se preocupar após tentar contatar a equipe em viagem e não ter conseguido. Lembre-se que é mais fácil reconstruir um rapto dentro de um período de algumas horas do que de muitas horas.
- Avalie a segurança dos meios de transporte (isso pode muitas vezes ser o veículo da organização e outras vezes tratar-se de transporte público por estar rodeado de testemunhas potenciais). No caso de transporte púbico, avalie se é melhor sentar junto ou separado de seu colega. Isso pode dar a possibilidade de uma pessoa fingir que não conhece a outra e também de alertar a organização. Tentar intervir para impedir o rapto pode fazer perder esta chance.
- Se as viagens são feitas em veículo, ele deve estar revisado sempre (respeite os limites de velocidade e o código de trânsito). Não dê caronas.
- Quando relevante, distribua informação apropriada para autoridades civis, militares e comunitárias, assim como para aqueles responsáveis pela missão (para que a responsabilidade por sua segurança seja ampliada e não possam dizer apenas que "não sabiam").
- Apresente um argumento preparado que explique os objetivos da viagem a o mandato da organização, de modo que seja acessível a grupos armados e forças de segurança (é melhor não adaptar o argumento para o grupo armado, pois pode ser difícil identificá-lo e poderia representar um grave erro).
- Avalie o melhor momento para sair do terreno (às vezes, por causa do tempo quente, é preferível sair de madrugada apesar da segurança). No caso de um ataque após a saída, entretanto, os contatos de emergência da organização talvez ainda não estejam operacionais; os primeiros momentos após um rapto são cruciais para rastrear o paradeiro da pessoa.
- Não viaje quando anoitecer.
- Em nenhuma hipótese deixe objetos de valor visíveis (tais como câmeras ou máquinas fotográficas).
- Comporte-se de maneira apropriada durante a viagem.
- Geralmente, peça para que a organização consiga uma permissão para trabalhar com a comunidade visitada (e quando possível negocie pelo menos a tolerância dos grupos armados).

Em caso de uma missão de campo após uma chamada de um terceiro, também:

- Certifique-se da identidade da pessoa que chama (cruze a informação com organizações confiáveis).
- Cruze informações sobre os eventos mencionados.
- Avalie se é de fato importante fazer a visita no terreno ou se não seria mais seguro para todos se a informação viajasse até à organização (ver gerenciamento da informação: protocolo de prevenção e reação).
- Avalie se é necessário ir ao local logo após a chamada, especialmente se a pessoa é desconhecida (a informação deve, pelo menos, ser cruzada antes). Além disso, deve-se considerar que a missão ao campo não impedirá os eventos pois eles já ocorreram, e por isso a razão da chamada. Em geral, o melhor conselho é evitar improvisações e mudanças de planos enquanto se está visitando uma área de risco.

Resumo

Nós entendemos que a detenção de uma pessoa pode ser um procedimento legal. Quando ocorre fora dos limites legais, ela pode ser considerada uma privação injustificada da liberdade de alguém. Sua duração pode variar de algumas horas a anos...

Objetivos gerais ao tratar de uma detenção:

- Do ponto de vista da pessoa detida.
- Do ponto de vista da organização da qual depende a pessoa detida.
- Do ponto de vista da família e parentes da pessoa detida.

General objectives when dealing with detention:

- Reduzir a possibilidade de que ocorra uma detenção.
- Estar informado rapidamente sobre as chances de uma detenção.
- Esboçar como reagir em tal situação: reação imediata e reação de médio prazo.

Rapto é um ato ilegal e pode ocorrer a qualquer momento, geralmente quando a oportunidade aparece. Este é um das várias conseqüências possíveis de uma "agressão". Portanto, as medidas de segurança serão parecidas àquelas destinadas a prevenir uma agressão (veja Capítulo 1.5): reduza a exposição física ao máximo...

CAPÍTULO 3.3

Administração segura da informação

Organizações de defesa dos direitos humanos administram informação que num ambiente hostil pode ser usada contra os defensores para afetar a segurança da organização, outras pessoas ou instituições. Faz-se portanto crucial estabelecer procedimentos de administração de informação seguros e um plano de reação para qualquer incidente afetando a segurança da informação gerida pela organização.

Administração segura da informação: procedimento de prevenção

Dados mantidos por organizações de direitos humanos podem, em termos gerais, ser agrupados em duas categorias de acordo com seu nível de sensibilidade: alta confidencialidade e baixa confidencialidade.

Qualquer peça de informação administrada por nós segue quatro passos distintos antes de chegar às nossas mãos e sair dela (quando relevante). Detalharemos as necessidades de segurança em cada etapa deste longo caminho.

1 • Fonte - coleta da informação, num ponto de encontro.

2 • Transferência da informação.

3 • Processamento e armazenamento.

4 • Distribuição.

1 • Fonte - coleta da informação num ponto de encontro.

O principal problema aqui é a proteção da informação e das pessoas afetadas por ela.

A pessoa que passa a informação requer uma rota entre sua casa/escritório e o ponto de encontro; um ponto de encontro (o local onde a pessoa que passará a informação encontra um membro da organização); este ponto de encontro pode ser a casa da pessoa ou local de trabalho, o escritório da organização ou qualquer outro lugar; e a rota para deixar o escritório da organização (viagens de ida e volta ao pontos de encontro).

São necessários um local e condições seguras para o encontro, assim como uma rota para que o informante possa chegar e deixar o local, e a rota para a chegada e saída dos membros da organização que irão receber a informação.

A segurança da administração da informação começa mesmo *antes* de recebê-la.

- A organização precisa mesmo receber esta informação?

  A organização será capaz de usar os dados para melhorar seu trabalho ou para melhorar o alcance de seus objetivos? Caso contrário, é melhor que a organização **não receba** a informação; se ela não for da sua esfera de competência, nossa organização pode referir a pessoa a outra organização, sem tocar no conteúdo da informação ou no caso.

- Comunique à pessoa dando a informação de quem somos, quais são nossos objetivos e qual é nosso trabalho, como a informação será usada pela organização; o tipo de informação que requeremos, como vamos usá-la e resguardá-la - e o que podem esperar de nós. É fundamental e ético que a pessoa dando a informação deva saber antecipadamente (diretamente ou por um terceiro) os riscos de passar esta informação adiante e os usos que a organização fará deste material.

Não é suficiente supor que a pessoa em questão está consciente de tudo isso. É importante que expliquemos a ela(s) para que estejamos seguros de que compreende(m) o risco. Também é importante definir com ela(s) possíveis medidas de segurança.

O local do encontro deve ser tão seguro e anônimo quando possível. De qualquer forma, a casa da pessoa não será um local seguro, pois a chegada de um membro da organização seria notada facilmente. Os escritórios da organização podem oferecer mais segurança (isso se a confidencialidade for respeitada), ou outro local público no qual as pessoas vêm e vão freqüentemente (por exemplo, o edifício de uma paróquia, um centro comunitário) isso sempre caso a confidencialidade possa ser resguardada. Se o encontro for marcado para um local inapropriado, ele deve ser adiado ou remarcado para um local mais seguro de acordo com a sensibilidade da informação que está sendo transmitida.

Pode-se considerar também recorrer a uma história oficial para encobrir o encontro: a pessoa deixa sua casa com um pretexto oficial. A pessoa precisará inventar um pretexto: visita ao dentista por causa de uma dor de dente, uma consulta médica (qualquer doença), mercado, etc. A pessoa precisará voltar para casa com provas do motivo real (uma prescrição médica por exemplo, ou compras que não encontraria normalmente em casa).

Não esqueça de que os problemas de segurança para a pessoa que passou a informação podem surgir após uma reunião num local pré-determinado.

2 ● Transmissão da informação

A informação pode ser coletada através de vários meios: disco de memória, impressora, notas escritas à mão ou no computador, fotos, etc...

O método rotineiro mais seguro para transferir informação é através de um laptop, de um pen drive ou CD Rom equipado com criptografia de segurança. O encontro pode ser gravado, fotos podem ser guardadas e notas podem ser levadas. Todos os outros meios são considerados menos seguros, o que aumenta o risco do processo de transmissão.

Informação confidencial deveria ser carregada apenas por membros da organização que sabem o que estão carregando.

Com muita freqüência, defensores de direitos humanos viajam com todas as suas notas contendo informação importante não necessariamente relacionada àquela missão específica. Eles mantêm o caderno de anotações cheio ao invés de viajar com apenas a quantidade de papel que necessitam. Isso também vale para o pen drive, computadores e outros meios de informação.

3 ● Armazenamento e processamento da informação

Uma vez que a informação chegou ao escritório da organização está geralmente mais segura (de acordo com as debilidades do escritório – veja Capítulo sobre segurança em residências e escritórios).

Padrões de relevância específica da informação:

Arquivo físico de documentos impressos: isso poderia ser usado quando necessário; documentação necessária em casos particulares deveria ser entregue pessoalmente. Informação em papel deveria ser guardada em arquivos de metal com chave; o uso de um quarto fechado deveria ser considerado para manter estes arquivos.

Pode-se considerar também a possibilidade de distribuir papéis entre vários locais seguros ou mandá-los para outros locais com o mesmo cuidado ilustrado em "transmissão da informação". Informação também pode ser digitalizada, criptografada e enviada a uma organização segura (um parceiro internacional, por exemplo).

Sistemas de criptografia e códigos deveriam ser usados de maneira apropriada.

Faça cópias de segurança semanalmente e mantenhas estas cópias, também criptografadas seguramente num cofre ou outro local seguro.

4 ● Distribuição da informação

Critérios gerais em relação à distribuição da informação incluem os seguintes pontos:

- Verifique a informação.

- Quando a organização for a única fonte de informação sobre certos fatos, haverá um risco aumentado e serão necessários planos de contingência.

- O consentimento informado deveria ser conseguido das pessoas que lhe dão informação, particularmente quando estas pessoas são identificáveis localmente como a única fonte de informação.

- Qualquer informação escrita que deixe a organização ou organizações parceiras deve ser considerada "pública" devido ao risco de cair em mãos erradas, ou às irregularidades normais diárias dos meios de comunicação.

- É crucial para a organização que publica a informação possuir uma política dedicada de publicação; isso deveria incluir os principais padrões de segurança aplicáveis a publicação de informação (entre eles estão as regras de tratamento da informação).

Acesso à informação por pessoas que não são membros da organização (ajudantes, voluntários, etc...)

Para a segurança da organização, o acesso de terceiros, ajudantes, voluntários deve ser restrito aos arquivos digitais e físicos (decida caso a caso) e este acesso deve ser responsabilidade de um membro específico da organização.

Pode ser útil incorporar ao contrato ou acordo de trabalho de ajudantes e voluntários uma cláusula de confidencialidade a qual deve ser respeitada sempre. Esta cláusula de confidencialidade deveria também ser incluída nos contratos de todo o pessoal subcontratado da organização.

Administração segura de dados: procedimentos de reação em casos de roubo ou perda de dados

Roubo ou perda (as vezes é difícil definir o que ocorreu) de dados mantidos pela organização deveria causar uma reação como se a informação fosse cair em mãos erradas, e que será feito um uso malicioso desta informação e isto conseqüentemente afetará a terceiros (seja aqueles que repassaram a informação ou colegas de trabalho, etc...) ou à própria organização.

Se, apesar de todos os procedimentos de prevenção, ainda assim ocorrer a perda ou roubo de informação, isso deveria ser tratado como uma quebra de segurança séria, e os seguintes passos deveriam ser tomados:

1 ♦ Informar imediatamente as pessoas da organização.

2 ♦ Avaliar a quantidade e sensibilidade da informação roubada ou perdida, se: Ela coloca em risco as pessoas diretamente afetadas pela informação, terceiros ou a organização, e por quê (vetores de risco). Esta avaliação deve ser realizada para cada tipo de informação roubada quando vários tipos de informação forem roubados (por exemplo, listas de pessoas, referências a informação coletada para casos individuais).

3 ♦ Avalie a necessidade de informar as pessoas e instituições potencialmente afetadas para que possam tomar suas próprias medidas para protegerem-se (isso deve ser feito discretamente).

4 ♦ Avalie se deve informar as autoridades e relatar o ocorrido.

5 ♦ Quando necessário, inicie qualquer dos passos acima para evitar maior dano no caso de a informação roubada ou perdida ser usada.

A organização também deverá decidir quanto seus membros podem se expor ao risco para proteger a informação: por exemplo no caso de uma busca violenta, deve-se considerar se é realmente 'válido' resistir.

Resumo

A administração segura da informação requer protocolos de prevenção e de reação.

Prevenção deve considerar 4 momentos:

1 • Fonte – coleta da informação, no local de encontro.

2 • Transferência da informação.

3 • Processamento e armazenamento.

4 • Distribuição.

Reação requer ao menos:

1 • Informar as pessoas responsáveis da organização.

2 • Avaliar a quantidade e sensibilidade da informação perdida ou roubada.

3 • Avaliar se deve informar subseqüentemente às pessoas e instituições potencialmente afetadas.

4 • Avaliar se deve informar as autoridades e relatar o ocorrido.

5 • Passos necessários para evitar danos maiores no caso de a informação roubada ou perdida ser utilizada.

Segurança e tempo livre

Reflexão:

Em termos gerais, regras de segurança são seguidas se elas não se opõem aos interesses pessoais. Será, portanto, mais fácil lidar com a segurança do escritório do que com o tempo livre das pessoas. Ainda assim o tempo livre é um aspecto fundamental tanto da segurança pessoal quanto organizacional. Isso requer discussão e compreensão sobre como as necessidades pessoais interferem com a segurança.

Tempo livre

Aqui há poucas questões e reflexões para ajudar a organização a elaborar uma política sobre tempo livre. É importante, assim como qualquer outro item da segurança, explorar tanto quanto possível mesmo que a exploração possa invadir a privacidade (incidentes de segurança podem violar a privacidade também…).

Nós começamos com duas importantes reflexões:

- Se alguém pretende atacar uma organização, eles provavelmente não atacarão a pessoa mais bem protegida ou aquela que segue as regras de segurança, mas atacarão o ponto fraco, sobretudo durante o tempo livre (à noite e fins de semana, etc...).
- Se uma organização possui 10 membros, dos quais um ou dois não seguem as normas de segurança durante o seu tempo livre, será toda a organização, não apenas os dois indivíduos, que estará em risco porque toda a organização será afetada por um ataque contra estas duas pessoas.

A questão subjacente é sempre: "existe um risco de segurança envolvido em..." Se a resposta dor "não", então tudo bem. Se a resposta for "sim", então é necessário explorar a situação e decidir se existe outra maneira de satisfazer a necessidade pessoal num ambiente protegido ou decidir adiar esta necessidade para um momento mais seguro pois é incompatível com a segurança de um defensor de direitos humanos.

Nós nos preocupamos com segurança apenas durante o horário de trabalho ou 24/7?

Apesar de ser difícil fazer a distinção entre as políticas da organização e a autonomia de cada indivíduo durante seu tempo livre, a prevenção a ataques e as reações a eles não fazem diferenças entre o horário de trabalho e o tempo livre... Nós não podemos nos esquecer de que se alguém decide atacar a organização através de seus membros, eles não farão apenas através de seus membros, eles não farão durante o horário de trabalho, mas nos momentos em que os defensores estão mais vulneráveis. A pessoa planejando um ataque contra um defensor procurará a melhor oportunidade para fazê-lo. Nós devemos ter sempre em mente que um ataque à noite, na saída de uma boate, etc., será muito mais fácil de encobrir…

Em países onde beber álcool é um hábito social, beber ao ponto de ficar bêbado pode ser um risco de segurança?

Embriagar-se num espaço público tem um impacto definitivo na segurança. O defensor pode falar, seu comportamento estará alterado e ele poderá não perceber que está sendo deliberadamente questionado ou desafiado. Existe um impacto definitivo na imagem da organização, mesmo que não seja a segurança física dos defensores de direitos humanos. E lembre-se de que um defensor embriagado dá a oportunidade para um grupo hostil utilizar-se desta vantagem para realizar um ataque à organização (o mesmo é válido para o uso de drogas). O uso de álcool e drogas em relação à segurança não deveria ser examinado desde uma perspectiva moral ou de saúde, mas como um fato objetivo que afeta a segurança.

Pode uma relação amorosa secreta afetar a segurança?

- Já ocorreram casos de defensores de direitos humanos não contatando a organização porque estavam tendo um caso amoroso. A organização já havia alertado seus contatos de emergência para então descobrir que o defensor estava bem e sem saber do problema que havia causado. Este tipo de situação obviamente dá aos outros a oportunidade de desacreditar a organização e o defensor em questão ao chamar atenção para as implicações éticas e a imagem dos dois. Alguns contatos de emergência podem até decidir retirar-se do sistema de alerta da organização.

- O problema não é o caso, mas como o caso pode afetar a comunicação e a segurança. Nós reiteramos que isso não é uma questão moral ou de saúde, mas de segurança. É importante que a organização seja capaz de lidar com estas questões de uma maneira clara e procure maneiras de resolvê-la.

- E se o/a amigo/a do/a defensor é visto com suspeita dentro da organização? A organização pode interferir?

- De que maneiras podemos passar informação a amigos, familiares, parentes? O defensor de direitos humanos é responsável por como a informação será usada?

Como os defensores usam seu tempo livre tem portanto um impacto potencial de na segurança. O ponto não é o de negar o desfrute do tempo livre mas ver como se pode desfrutar dele.

Todas as organizações de defensores em risco necessitam uma política de tempo livre, das noites às férias. Menção especial é necessária para o uso público de álcool e outras drogas, como casos amorosos podem interferir na segurança e como o tempo livre pode afetar a imagem e a segurança da organização?

Como devemos tratar a confidencialidade da informação?

E porque a informação pode vazar a qualquer momento, mesmo durante o tempo livre, aqui vai uma consideração adicional relacionada à segurança da informação.

A organização deveria criar dois níveis diferentes de confidencialidade na sua informação (isso sempre dentro da organização):

a ♦ O que apenas poucos membros deveriam saber.

b ♦ O que todos os membros podem saber.

Este processo pode reduzir o risco de informação confidencial vazar, seja por um comportamento negligente ou por infiltração. Pode ajudar também a organização a ver quem estaria vazando este tipo de informação.

Podem alguns aspectos do nosso comportamento durante nosso tempo livre afetar a imagem de nossa organização?

♦ Como outros nos vêem?

♦ Em que medida outros colegas sabem o que fazemos em nosso tempo livre? Qual é o impacto da imagem da organização na sua segurança?

♦ …

Resumo

Um defensor em risco deve cuidar da segurança 24 horas por dia, 7 dias por semana em todos os aspectos de sua vida, incluindo o tempo livre.

O tempo livre necessita de avaliação apropriada.

A questão subjacente é sempre: "existe um risco de segurança envolvido em..."Se a resposta for "não", então tudo bem. Se a resposta for "sim", então a questão precisa ser mais bem explorada e uma decisão tomada sobre se há maneiras de satisfazer a necessidade pessoal num ambiente protegido ou se a necessidade precisa ser adiada até tempos mais seguros ou simplesmente adiada pois incompatível com as necessidade de segurança de um defensor de direitos humanos.

Todas as organizações de defensores em situação de risco necessitam uma política de desfrute do tempo livre, como as noites e as férias. Especial menção é necessária ao uso de álcool e outras drogas em público, como relacionamentos amorosos secretos podem interferir com a segurança, e como a imagem da organização sobre o uso do tempo livre pode afetar sua segurança.

Como o tempo livre envolve riscos, é importante não esquecer de realizar uma avaliação detalhada dos riscos.

ANEXO I

Declaração da ONU sobre Defensores de Direitos Humanos[1]

NAÇÕES UNIDAS

A

Assembléia geral

Distr.
GENERAL
A/RES/53/144
8 de Março de 1999

Quinquagésima-terceira sessão
Item da Agenda 110 (b)

RESOLUÇÃO ADOTADA PELA ASSEMBLÉIA GERAL

[sobre relatório do Terceiro Comitê (A/53/625/Add.2]

53/144. Declaração sobre o Direito e o Dever dos Indivíduos, Grupos e Instituições de Promover e Proteger os Direitos Humanos e as Liberdades Fundamentais Universalmente Reconhecidos

A Assembleia Geral,

Reafirmando a importância da realização dos objectivos e princípios da Carta das Nações Unidas para a promoção e protecção de todos os direitos humanos e liberdades fundamentais de todas as pessoas em todos os países do mundo,

Tomando nota da resolução 1998/7 da Comissão dos Direitos do Homem, de 3 de Abril de 1998, na qual a Comissão aprovou o texto do projecto de declaração sobre o direito e a responsabilidade dos indivíduos, grupos ou órgãos da sociedade de promover e proteger os direitos humanos e liberdades fundamentais universalmente reconhecidos,

Tomando também nota da resolução 1998/33 do Conselho Económico e Social, de 30 de Julho de 1998, na qual o Conselho recomendou o projecto de declaração à Assembleia Geral para adopção,

Consciente da importância da adopção do projecto de declaração no contexto do quinquagésimo aniversário da Declaração Universal dos Direitos do Homem[2],

1. *Adopta* a Declaração sobre o Direito e a Responsabilidade dos Indivíduos, Grupos ou Órgãos da Sociedade de Promover e Proteger os Direitos Humanos e Liberdades Fundamentais Universalmente Reconhecidos, anexa à presente resolução;

2. *Convida* os Governos, as agências e organizações do sistema das Nações Unidas e as organizações intergovernamentais e não governamentais a intensificarem os seus esforços para divulgar a Declaração e para promover o respeito universal e a compreensão da mesma, e solicita ao Secretário-Geral que inclua o texto da Declaração na próxima edição da obra Direitos Humanos: Compilação de Instrumentos Internacionais.

85.ª reunião plenária
9 de Dezembro de 1998

1 Fonte: Gabinete de Documentação e Direito Comparado, Portugal: http://www.gddc.pt/direitos-humanos/textos-internacionais-dh/tidhuniversais/o-defensores-dh.html

2 Resolução 217 A (III)

ANEXO

Declaração sobre o Direito e a Responsabilidade dos Indivíduos, Grupos ou Órgãos da Sociedade de Promover e Proteger os Direitos Humanos e Liberdades Fundamentais Universalmente Reconhecidos

A Assembleia Geral

Reafirmando a importância que assume a realização dos objectivos e princípios da Carta das Nações Unidas para a promoção e protecção de todos os direitos humanos e liberdades fundamentais de todas as pessoas em todos os países do mundo,

Reafirmando também a importância da Declaração Universal dos Direitos do Homem[3] e dos Pactos Internacionais sobre Direitos Humanos[4] enquanto elementos essenciais dos esforços internacionais para promover o respeito universal e efectivo dos direitos humanos e liberdades fundamentais, bem como a importância de outros instrumentos de direitos humanos adoptados no âmbito do sistema das Nações Unidas e a nível regional,

Sublinhando que todos os membros da comunidade internacional deverão cumprir, em conjunto e separadamente, a sua solene obrigação de promover e estimular o respeito dos direitos humanos e liberdades fundamentais para todos sem qualquer distinção baseada, nomeadamente, na raça, cor, sexo, língua, religião, opinião política ou outra, origem nacional ou social, condição económica, nascimento ou outra situação, e reafirmando a particular importância de conseguir a cooperação internacional para cumprir essa obrigação em conformidade com a Carta das Nações Unidas,

Reconhecendo o importante papel da cooperação internacional e o importante contributo do trabalho dos indivíduos, grupos e associações para a efectiva eliminação de todas as violações de direitos humanos e liberdades fundamentais dos povos e dos indivíduos, nomeadamente no que diz respeito a violações em massa, flagrantes e sistemáticas como as que resultam do apartheid, de todas as formas de discriminação racial, do colonialismo, do domínio ou ocupação estrangeira, da agressão ou ameaças à soberania nacional, unidade nacional ou integridade territorial e da recusa em reconhecer o direito dos povos à autodeterminação e o direito de todos os povos a exercerem a sua plena soberania sobre as suas riquezas e recursos naturais,

Reconhecendo a relação entre a paz e a segurança internacionais e o gozo dos direitos humanos e liberdades fundamentais, e consciente de que a ausência de paz e segurança internacionais não constitui desculpa para o desrespeito destes direitos e liberdades,

Reiterando que todos os direitos humanos e liberdades fundamentais são universais, indivisíveis, interdependentes e indissociáveis e deverão ser promovidos e realizados de forma justa e equitativa, sem prejuízo da realização de cada um desses direitos e liberdades,

Sublinhando que a responsabilidade e o dever primordiais de promover e proteger os direitos humanos incumbem ao Estado,

Reconhecendo que os indivíduos, grupos e associações têm o direito e a responsabilidade de promoverem o respeito e o conhecimento dos direitos humanos e liberdades fundamentais a nível nacional e internacional,

Declara:

Artigo 1.º

Todas as pessoas têm o direito, individualmente e em associação com outras, de promover e lutar pela protecção e realização dos direitos humanos e das liberdades fundamentais a nível nacional e internacional.

3 Resolution 217 A (III).
4 Resolution 2200 A (XXI), annex.

Artigo 2.º

1. Cada Estado tem a responsabilidade e o dever primordiais de proteger, promover e tornar efectivos todos os direitos humanos e liberdades fundamentais, nomeadamente através da adopção das medidas necessárias à criação das devidas condições nas áreas social, económica, política e outras, bem como das garantias jurídicas que se impõem para assegurar que todas as pessoas sob a sua jurisdição, individualmente e em associação com outras, possam gozar na prática esses direitos e liberdades;

2. Cada Estado deverá adoptar as medidas legislativas, administrativas e outras que se revelem necessárias para assegurar que os direitos e liberdades referidos na presente Declaração são efectivamente garantidos.

Artigo 3.º

O direito interno conforme à Carta das Nações Unidas e às demais obrigações internacionais do Estado no domínio dos direitos humanos e liberdades fundamentais constitui o quadro jurídico no âmbito do qual os direitos humanos e liberdades fundamentais deverão ser realizados e gozados e no âmbito do qual deverão ser conduzidas as actividades referidas na presente Declaração para a promoção, protecção e realização efectiva desses direitos e liberdades.

Artigo 4.º

Nenhuma disposição da presente Declaração deverá ser interpretada de maneira a prejudicar ou contradizer os objectivos e princípios da Carta das Nações Unidas ou como uma restrição ou derrogação das disposições da Declaração Universal dos Direitos do Homem, dos Pactos Internacionais sobre Direitos Humanos e de outros instrumentos internacionais e compromissos aplicáveis neste domínio.

Artigo 5.º

A fim de promover e proteger os direitos humanos e liberdades fundamentais, todos têm o direito, individualmente e em associação com outros, a nível nacional e internacional:

a) De se reunir ou manifestar pacificamente;

b) De constituir organizações, associações ou grupos não governamentais, de aderir aos mesmos e de participar nas respectivas actividades;

c) De comunicar com organizações não governamentais ou intergovernamentais.

Artigo 6.º

Todos têm o direito, individualmente e em associação com outros:

a) De conhecer, procurar, obter, receber e guardar informação sobre todos os direitos humanos e liberdades fundamentais, nomeadamente através do acesso à informação sobre a forma como os sistemas internos nos domínios legislativo, judicial ou administrativo tornam efectivos esses direitos e liberdades;

b) Em conformidade com os instrumentos internacionais de direitos humanos e outros instrumentos internacionais aplicáveis, de publicitar, comunicar ou divulgar livremente junto de terceiros opiniões, informação e conhecimentos sobre todos os direitos humanos e liberdades fundamentais;

c) De estudar e debater a questão de saber se todos os direitos humanos e liberdades fundamentais são ou não respeitados, tanto na lei como na prática, de formar e defender opiniões a tal respeito e, através destes como de outros meios adequados, de chamar a atenção do público para estas questões.

Artigo 7.º

Todos têm o direito, individualmente e em associação com outros, de desenvolver e debater novas ideias e princípios no domínio dos direitos humanos e de defender a sua aceitação.

Artigo 8.º

1. Todos têm o direito, individualmente e em associação com outros, de ter acesso efectivo, numa base não discriminatória, à participação no governo do seu país e na condução dos negócios públicos.

2. Este direito compreende, entre outros aspectos, o direito de, individualmente ou em associação com outros, apresentar aos organismos governamentais e às agências e organizações que se ocupam dos negócios públicos críticas e propostas para aperfeiçoar o respectivo funcionamento e chamar a atenção para qualquer aspecto do respectivo trabalho que possa prejudicar ou impedir a promoção, protecção e realização dos direitos humanos e liberdades fundamentais.

Artigo 9.º

1. No exercício dos direitos humanos e liberdades fundamentais, nomeadamente na promoção e protecção dos direitos humanos enunciados na presente Declaração, todos têm o direito, individualmente e em associação com outros, de beneficiarem de recursos adequados e de serem protegidos na eventualidade de violação de tais direitos.

2. Para este fim, todas as pessoas cujos direitos ou liberdades tenham alegadamente sido violados têm o direito, pessoalmente ou através de representantes legalmente autorizados, de apresentar queixa e de que esta queixa seja rapidamente examinada em audiência pública perante uma autoridade judicial ou outra autoridade independente, imparcial e competente estabelecida por lei e de obter dessa autoridade uma decisão, em conformidade com a lei, que lhe atribua uma reparação, incluindo qualquer indemnização que seja devida, caso a pessoa tenha sido vítima de uma violação dos seus direitos ou liberdades, e garanta a execução da eventual decisão e o cumprimento da obrigação de reparar, tudo isto sem demora indevida.

3. Para o mesmo fim, todos têm o direito, individualmente e em associação com outros, nomeadamente:

(a) De se queixar das políticas e acções de funcionários individuais e organismos públicos que consubstanciem uma violação dos direitos humanos e liberdades fundamentais, através de petição ou outro meio adequado, às autoridades judiciais, administrativas ou legislativas competentes nos termos da lei nacional ou a qualquer outra autoridade competente prevista nos termos do ordenamento jurídico interno do Estado, que deverão proferir a sua decisão sobre a queixa sem demora indevida;

b) De comparecer às audiências, diligências e julgamentos públicos, de forma a formar uma opinião sobre a conformidade dos mesmos com a lei nacional e as obrigações e compromissos internacionais aplicáveis;

c) De oferecer e prestar assistência jurídica profissionalmente qualificada ou outro tipo de aconselhamento e assistência relevantes para a defesa dos direitos humanos e liberdades fundamentais.

4. Para o mesmo fim, e em conformidade com os instrumentos e procedimentos internacionais aplicáveis, todos têm o direito, individualmente e em associação com outros, de acesso irrestrito aos organismos internacionais com competência genérica ou específica para receber e considerar comunicações sobre questões de direitos humanos e liberdades fundamentais e de se comunicarem livremente com os mesmos.

5. O Estado deverá proceder a uma investigação imediata e imparcial ou garantir a instauração de um inquérito caso existam motivos razoáveis para crer que ocorreu uma violação de direitos humanos em qualquer território sob a sua jurisdição.

Artigo 10.º

Ninguém deverá participar, por acção ou por omissão caso tenha o dever de actuar, na violação de direitos humanos e liberdades fundamentais e ninguém será sujeito a um castigo ou acção hostil de qualquer género por se recusar a fazê-lo.

Artigo 11.º

Todos têm o direito, individualmente e em associação com outros, de exercer legitimamente a sua ocupação ou profissão. Todos aqueles que, em resultado da sua profissão, possam afectar a dignidade humana, os direitos humanos e as liberdades fundamentais de terceiros deverão respeitar esses direitos e liberdades e observar o cumprimento das relevantes normas nacionais e internacionais de conduta ou ética profissional.

Artigo 12.º

1. Todos têm o direito, individualmente ou em associação com outros, de participar em actividades pacíficas contra violações de direitos humanos e liberdades fundamentais.

2. O Estado deverá adoptar todas as medidas adequadas para garantir que as autoridades competentes protegem todas as pessoas, individualmente e em associação com outras, contra qualquer forma de violência, ameaças, retaliação, discriminação negativa de facto ou de direito, coacção ou qualquer outra acção arbitrária resultante do facto de a pessoa em questão ter exercido legitimamente os direitos enunciados na presente Declaração.

3. A este respeito, todos têm o direito, individualmente e em associação com outros, a uma protecção eficaz da lei nacional ao reagir ou manifestar oposição, por meios pacíficos, relativamente a actividades, actos e omissões imputáveis aos Estados, que resultem em violações de direitos humanos e liberdades fundamentais, bem como a actos de violência perpetrados por grupos ou indivíduos que afectem o gozo dos direitos humanos e liberdades fundamentais.

Artigo 13.º

Todos têm o direito, individualmente e em associação com outros, de solicitar, receber e utilizar recursos para o fim expresso da promoção e protecção dos direitos humanos e liberdades fundamentais através de meios pacíficos, em conformidade com o artigo 3.º da presente Declaração.

Artigo 14.º

1. O Estado tem o dever de adoptar medidas adequadas no plano legislativo, judicial, administrativo e outros a fim de promover a compreensão por todas as pessoas sujeitas à sua jurisdição dos respectivos direitos civis, políticos, económicos, sociais e culturais.

2. Tais medidas deverão incluir, entre outras:

a) A publicação e disponibilização generalizada das leis e regulamentos nacionais e dos aplicáveis instrumentos internacionais fundamentais em matéria de direitos humanos;

b) O acesso pleno e em condições de igualdade aos documentos internacionais no domínio dos direitos humanos, nomeadamente aos relatórios periódicos apresentados pelo Estado em causa aos órgãos criados pelos tratados internacionais de direitos humanos de que seja parte, bem como as actas das sessões em que tenham sido discutidos e os relatórios oficiais desses órgãos.

3. O Estado deverá garantir e apoiar, sempre que necessário, a criação e o desenvolvimento de novas instituições nacionais independentes para a promoção e protecção dos direitos humanos e liberdades fundamentais em todos os territórios sob a sua jurisdição, quer se tratem de provedores de justiça, comissões nacionais de direitos humanos ou qualquer outra forma de instituição nacional.

Artigo 15.º

O Estado tem o dever de promover e facilitar a educação em matéria de direitos humanos e liberdades fundamentais em todos os níveis do ensino e de garantir que todos os responsáveis pela formação dos juristas, funcionários responsáveis pela aplicação da lei, pessoal das forças armadas e funcionários públicos incluem elementos adequados para o ensino dos direitos humanos nos programas de formação destinados a estes grupos profissionais.

Artigo 16.º

Os indivíduos, as organizações não governamentais e as instituições competentes têm um importante contributo a dar na sensibilização do público para as questões relativas aos direitos humanos e liberdades fundamentais, através de actividades como a educação, a formação e a investigação nessas áreas com o fim de reforçar, nomeadamente, a compreensão, a tolerância, a paz e as relações amigáveis entre as nações e entre todos os grupos raciais e religiosos, tendo em conta a diversidade das sociedades e comunidades onde as suas actividades se desenvolvem.

Artigo 17.º

No exercício dos direitos e liberdades enunciados na presente Declaração, ninguém, agindo individualmente e em associação com outros, estará sujeito senão às limitações que estejam em conformidade com as obrigações internacionais aplicáveis e sejam estabelecidas pela lei com vista exclusivamente a garantir o devido reconhecimento e respeito dos direitos e liberdades dos outros e de satisfazer as justas exigências da moral, da ordem pública e do bem-estar geral numa sociedade democrática.

Artigo 18.º

1. Todos têm deveres para com a comunidade e no seio desta, fora da qual o livre e pleno desenvolvimento da respectiva personalidade não é possível.

2. Os indivíduos, grupos, instituições e organizações não governamentais têm um papel importante a desempenhar e a responsabilidade de defender a democracia, proteger os direitos humanos e liberdades fundamentais e contribuir para a promoção e progresso das sociedades, instituições e processos democráticos.

3. Os indivíduos, grupos, instituições e organizações não governamentais têm também um papel importante a desempenhar e a responsabilidade de contribuir, conforme necessário, para a promoção do direito de todos a que reine, no plano social e no plano internacional, uma ordem capaz de tornar plenamente efectivos os direitos e liberdades enunciados na Declaração Universal dos Direitos do Homem.

Artigo 19.º

Nenhuma disposição da presente Declaração pode ser interpretada de maneira a conferir a qualquer indivíduo, grupo ou órgão da sociedade ou a qualquer Estado o direito de se entregar a qualquer actividade ou de praticar qualquer acto destinado a destruir os direitos e liberdades enunciados na presente Declaração.

Artigo 20.º

Nenhuma disposição da presente Declaração pode ser interpretada de maneira a permitir que os Estados apoiem e promovam actividades de indivíduos, grupos de indivíduos, instituições ou organizações não governamentais contrárias às disposições da Carta das Nações Unidas.

ANEXO[1] II

CONSELHO DA UNIÃO EUROPÉIA

Brussels, 9 de Junho de 2004
10056/1/04
REV 1
LIMITE
PESC 435
COHOM 17

NOTA

De:	Comitê Político e de Segurança
Para:	Coreper/Conselho
Assunto:	**Esboço de Conclusões sobre as Orientações da UE sobre Defensores de Direitos Humanos**

1 Durante sua reunião em 8 de Junho, o Comitê Político e de Segurança discutiu e finalizou a versão preliminar abaixo das mencionadas Conclusões do Conselho, que são reproduzidas no anexo.

2 Em sua reunião de 1 de Junho, o Comitê Político e de Segurança aprovou o texto "At its meeting on 1 June, the Political and Security Committee had endorsed the text «Garantir a proteção – Orientações da União Européia sobre os defensores dos direitos do Homem» preparado em consulta com o Grupo de Trabalho sobre Direitos Humanos (Council Working Party on Human Rights, COHOM), e que estão agora anexados a estas Conclusões do Conselho.

3 O Coreper é convidado a recomendar que o Conselho aprove esta versão das Conclusões e as Orientações em anexo como o item A de sua reunião de 14/15 de junho.

ANEXO

Conclusões Preliminares do Conselho

1. O Conselho dá as boas vindas e adota as Orientações da UE sobre Defensores de Direitos Humanos (cópia anexa). As Orientações serão parte integral de um processo de reforço da política de direitos humanos da União Européia em suas relações externas. O Conselho observa que as Orientações melhorarão as atividades da União Européia na proteção e apoio aos defensores de direitos humanos.

2. O Conselho observa que o apoio aos defensores de direitos humanos já é um elemento consolidado da política de relações externas em direitos humanos da União Européia. O propósito das Orientações sobre Defensores de Direitos Humanos é o de dar sugestões práticas para melhorar a atuação da UE em relação a este tema. As Orientações podem ser usadas em contatos com terceiros países em todos os níveis, assim como com organizações multilaterais de direitos humanos, de modo a apoiar e encorajar o respeito ao direito de defender direitos humanos. As Orientações também apresentam intervenções para a União no caso de defensores de direitos humanos em situação de risco e sugerem medidas práticas de apoio e assistências aos defensores de direitos humanos.

3. O Conselho observa que pese que as Orientações se referem a questões específicas de defensores de direitos humanos, elas contribuirão para reforçar a política de direitos humanos da União Européia como um todo.

1 Tradução não oficial. Texto original das Orientações (Anexo do Anexo) em português.

Anexo do Anexo

GARANTIR A PROTEÇÃO – ORIENTAÇÕES DA UNIÃO EUROPÉIA SOBRE OS DEFENSORES DOS DIREITOS DO HOMEM

I. OBJETO

1. O apoio aos defensores dos direitos do Homem faz, desde há longa data, parte integrante da política externa da União Européia em matéria de direitos humanos. As presentes orientações, que têm por fim apresentar sugestões concretas que permitam incrementar a ação da UE neste domínio, poderão ser utilizadas nos contatos estabelecidos com países terceiros, a todos os níveis, e nas instâncias multilaterais competentes na matéria, a fim de apoiar e consolidar os esforços que a União tem vindo a desenvolver para promover e incentivar a observância do direito à defesa dos direitos humanos. Prevêem igualmente que a União interceda a favor dos defensores dos direitos humanos objeto de ameaças e propõem meios concretos para os apoiar e lhes prestar assistência.
   Um dos principais elementos das presentes orientações reside no apoio aos procedimentos especiais do Conselho das Nações Unidas para os Direitos do Homem, designadamente ao Relator Especial sobre os Defensores dos Direitos Humanos e aos mecanismos regionais que tenham sido criados especificamente para os proteger. Por outro lado, as presentes orientações servirão para ajudar as representações da UE (embaixadas e consulados dos Estados-Membros e delegações da Comissão Européia) a definirem a sua abordagem em relação aos defensores dos direitos humanos. Embora tenham por principal objetivo tratar questões que lhes estejam especificamente ligadas, as presentes orientações contribuem igualmente para reforçar a política de direitos humanos da UE em geral.

II. DEFINIÇÃO

2. As presentes orientações baseiam-se na definição de defensores dos direitos humanos dada no artigo 1.º da "Declaração sobre o Direito e a Responsabilidade dos Indivíduos, Grupos ou Órgãos da Sociedade de Promover e Proteger os Direitos Humanos e Liberdades Fundamentais Universalmente Reconhecidos" (ver Anexo I), segundo o qual "Todas as pessoas têm o direito, individualmente e em associação com outras, de promover e lutar pela proteção e realização dos direitos humanos e das liberdades fundamentais a nível nacional e internacional".
3. São defensores dos direitos humanos todos os indivíduos, grupos e órgãos da sociedade que promovam e protejam os direitos humanos e as liberdades fundamentais universalmente reconhecidos. Os defensores dos direitos humanos lutam pela promoção e proteção dos direitos cívicos e políticos e procuram também promover, proteger e fazer cumprir os direitos econômicos, socais e culturais. Promovem e defendem igualmente os direitos dos membros de determinados grupos, como as comunidades indígenas. Não se incluem nesta definição os indivíduos ou grupos que cometam atos de violência ou a propaguem.

III. INTRODUÇÃO

4. A UE apóia os princípios consignados na Declaração sobre o Direito e a Responsabilidade dos Indivíduos, Grupos ou Órgãos da Sociedade de Promover e Proteger os Direitos Humanos e Liberdades Fundamentais Universalmente Reconhecidos. Embora a principal responsabilidade pela promoção e defesa dos direitos humanos incumba aos Estados, a UE reconhece que os indivíduos, grupos e órgãos da sociedade desempenham todos eles um papel importante na defesa da causa dos direitos humanos. Entre as ações dos defensores dos direitos humanos refiram-se:
   - chamar a atenção para as violações cometidas;
   - ajudar as vítimas de tais violações a fazerem valer os seus direitos perante a justiça, prestando-lhes apoio jurídico, psicológico, médico ou de outra natureza;
   - combater a cultura da impunidade, que favorece o encobrimento de violações sistemáticas e recorrentes dos direitos humanos e das liberdades fundamentais.
5. No trabalho dos defensores dos direitos humanos está freqüentemente implícita uma crítica às políticas e ações dos Governos. Todavia, estes não deverão encará-la negativamente. O princípio de que devem poder existir independência de espírito e liberdade de opinião sobre as políticas e ações dos Governos

é fundamental, além do que constitui um meio comprovadamente eficaz de incrementar o nível de proteção dos direitos humanos. Os defensores dos direitos humanos podem ajudar os Governos a promover e proteger tais direitos. A sua participação no processo de consulta permite-lhes desempenhar um papel fundamental em termos de apoio à elaboração de legislação adequada e de planos e estratégias nacionais sobre direitos humanos, papel esse que deverá igualmente ser reconhecido e apoiado.

6. A UE está ciente de que as ações dos defensores dos direitos humanos têm vindo a ser cada vez mais valorizadas e garantes de maior proteção às vítimas de violações desses direitos. Contudo, este progresso teve custos elevados: os próprios defensores são cada vez mais alvo de ataques e os seus direitos estão a ser violados em muitos países. A UE considera importante preservar a segurança dos defensores dos direitos humanos e proteger os seus direitos, sem deixar de atender, neste contexto, à questão da igualdade entre homens e mulheres.

IV. ORIENTAÇÕES OPERACIONAIS

7. A vertente operacional das presentes orientações destina-se a definir meios que, no quadro da Política Externa e de Segurança Comum, permitam agir eficazmente em prol da promoção e proteção dos defensores dos direitos humanos.

Acompanhamento, elaboração de relatórios e avaliação

8. Os Chefes de Missão da UE ficam desde já convidados a apresentar relatórios periódicos sobre a situação em matéria de direitos humanos nos respectivos países de acreditação. O Grupo dos Direitos do Homem (COHOM) aprovou, nas suas grandes linhas, fichas informativas que se destinam a facilitar tal tarefa. De acordo com essas fichas, as Missões da UE deverão passar a focar a situação dos defensores dos direitos humanos nos seus relatórios, neles assinalando, nomeadamente, quaisquer ameaças ou ataques de que aqueles tenham sido alvo. Neste contexto, os Chefes de Missão deverão ter em mente que o quadro institucional pode contribuir significativamente para que os defensores dos direitos humanos possam realizar o seu trabalho em condições de segurança. Nesta matéria revestem-se de grande importância as medidas legislativas, judiciárias e administrativas, ou outras que se afigurem adequadas, adotadas no quadro do exercício legítimo dos direitos referidos na Declaração das Nações Unidas sobre os Defensores de Direitos Humanos, que tenham sido tomadas pelos Estados com vista a proteger os cidadãos contra atos de violência, ameaças de retaliação, discriminações de fato ou de jure, pressões ou quaisquer outros atos arbitrários.
   Sempre que necessário, os Chefes de Missão deverão dirigir ao COHOM recomendações relativas a eventuais ações da UE que tenham por objetivo condenar, nomeadamente, as ameaças e ataques a defensores dos direitos humanos, bem como efetuar diligências e emitir declarações públicas sempre que se verifiquem situações de risco iminente ou grave para os defensores desses direitos. Nos seus relatórios, os Chefes de Missão deverão também analisar até que ponto são eficazes as ações empreendidas pela UE.
9. Os relatórios dos Chefes de Missão e outras informações pertinentes, como os relatórios e recomendações do Relator Especial sobre os Defensores dos Direitos Humanos, dos demais relatores especiais das Nações Unidas, dos órgãos de acompanhamento dos tratados, do Comissário do Conselho da Europa para os Direitos Humanos e das organizações não-governamentais, permitirão ao COHOM e a outros grupos competentes identificar as situações que requeiram a intervenção da UE e decidir sobre as medidas a tomar ou, se for caso disso, formular recomendações nesse sentido ao CPS/Conselho.

Papel das missões da UE no que respeita ao apoio e à proteção aos defensores dos direitos humanos

10. Em muitos países terceiros, as missões da UE (embaixadas de Estados-Membros da UE e delegações da Comissão Européia) constituem o primeiro ponto de contato entre a União e seus Estados-Membros e os defensores dos direitos humanos no terreno. Têm, pois, um papel importante a desempenhar em termos de concretização da política da UE em relação aos defensores dos direitos humanos, pelo que deverão adotar uma política antecipatória neste contexto e, paralelamente, ter presente que, em determinados casos, as ações da UE podem desencadear ameaças ou ataques a esses defensores. Como tal, devem discutir, sempre que necessário, com os defensores dos direitos humanos as eventuais ações projetadas. As missões da UE deverão velar por que o defensor dos direitos humanos visado e/ou os seus familiares sejam informados das ações empreendidas em nome da UE, podendo tomar para tal as seguintes medidas:

- proceder a uma estreita coordenação e trocar informações sobre os defensores dos direitos humanos, nomeadamente sobre aqueles que se encontrem em situação de risco;
- manter contatos apropriados com os defensores dos direitos humanos, recebendo-os inclusive na missão e visitando as zonas onde trabalham e, eventualmente, nomear agentes de ligação específicos repartindo, se necessário, as tarefas confiadas a cada um;
- assegurar, sempre que necessário ou pertinente, o reconhecimento público dos defensores dos direitos humanos e do trabalho que desenvolvem, recorrendo à publicidade, a visitas ou a convites;
- eventualmente, visitar os defensores dos direitos do Homem e assistir ao seu julgamento, na qualidade de observadores.

Promoção do respeito pelos defensores dos direitos humanos nas relações com países terceiros e nas instâncias multilaterais

11. A UE tem por objetivo incitar os países terceiros a cumprirem a obrigação de respeitar os direitos dos defensores dos direitos humanos e de os proteger dos ataques e ameaças de intervenientes não estatais. Nos seus contatos com países terceiros, a UE sublinhará, sempre que assim o entender, a necessidade de todos os países adotarem e cumprirem as normas e padrões internacionais pertinentes, em especial a Declaração das Nações Unidas acima mencionada. O objetivo geral deverá ser criar um clima que permita aos defensores dos direitos humanos atuar livremente. A UE dará a conhecer os seus objetivos como elementos intrínsecos da sua política de direitos humanos e sublinhará a importância que atribui à proteção dos defensores desses direitos. Como forma de apoiar esses objetivos, desenvolver-se-ão, nomeadamente, as seguintes ações:
    - no âmbito das suas missões em países terceiros, a Presidência, o Alto Representante para a Política Externa e de Segurança Comum, o Representante Pessoal do SG/AR para os Direitos do Homem, os representantes ou enviados especiais da UE e os representantes dos Estados-Membros e da Comissão Européia participarão, se necessário, em reuniões com defensores dos direitos humanos durante as quais serão evocados casos particulares, bem como questões levantadas pelos trabalhos dos defensores dos direitos humanos.
    - na vertente "direitos humanos" do diálogo político estabelecido pela UE com países terceiros e organizações regionais focar-se-á, sempre que pertinente, a situação dos defensores dos direitos do Homem. A UE sublinhará o seu apoio aos defensores dos direitos humanos e ao trabalho que desenvolvem, abordando, se necessário, casos particulares preocupantes.
    - estabelecer-se-á uma estreita cooperação com outros países que assumam a mesma postura, nomeadamente no âmbito do Conselho das Nações Unidas para os Direitos do Homem e da Assembléia Geral da ONU.
    - promover-se-á o reforço dos mecanismos regionais existentes que visam proteger os defensores dos direitos humanos – como sejam o ponto focal que se dedica a esta problemática e as instituições nacionais competentes do Gabinete das Instituições Democráticas e dos Direitos Humanos da OSCE, o Comissário do Conselho da Europa para os Direitos Humanos, o Relator Especial sobre a situação dos defensores dos direitos do Homem da Comissão Africana de Direitos Humanos e dos Povos e a Unidade Especial para os defensores dos direitos humanos da Comissão Inter--Americana dos Direitos Humanos –, bem como a criação de mecanismos adequados em regiões onde não existam.

Apóio aos procedimentos especiais do Conselho das Nações Unidas para os Direitos do Homem, designadamente ao Relator Especial sobre os Defensores dos Direitos Humanos

12. A UE reconhece que os procedimentos especiais do Conselho das Nações Unidas para os Direitos do Homem (relatores especiais, representantes especiais, peritos independentes e grupos de trabalho) têm um papel determinante no que toca aos esforços desenvolvidos no plano internacional para proteger os defensores dos direitos humanos, dada a sua independência e imparcialidade, bem como a sua capacidade de agir e denunciar as agressões de que são vítimas os defensores dos direitos humanos em todo o mundo e ainda de se deslocarem aos países em causa. Se bem que o Relator Especial sobre os Defensores dos Direitos Humanos desempenhe um papel muito específico nesta matéria, os mandatos

confiados aos restantes procedimentos especiais são também importantes para os defensores dos direitos humanos. Entre as ações a desenvolver pela UE para apoiar os procedimentos especiais contam-se, nomeadamente, as seguintes:

- exortar os Estados a que, por uma questão de princípio, acedam aos pedidos de visita apresentados no âmbito dos procedimentos especiais das Nações Unidas;
- promover, por intermédio das missões da UE, o recurso aos mecanismos temáticos das Nações Unidas por parte das comunidades locais que atuam no domínio dos direitos humanos e dos seus defensores, facilitando inclusive (mas não exclusivamente) o estabelecimento de contatos e o intercâmbio de informações entre os mecanismos temáticos e os defensores dos direitos do Homem;
- por sua vez, os Estados-Membros apoiarão a afetação de fundos suficientes do orçamento geral ao Alto Comissariado das Nações Unidas para os Direitos do Homem, dado ser impossível aos procedimentos especiais cumprirem o seu mandato se não dispuserem dos recursos necessários.

Medidas concretas de apoio aos defensores dos direitos humanos, nomeadamente no quadro da política de desenvolvimento

13. Os programas da União Européia e dos Estados-Membros que visam contribuir para a implementação de processos e instituições democráticos e para promover e proteger os direitos humanos nos países em desenvolvimento, como o Instrumento Europeu para a Democracia e os Direitos Humanos, fazem parte de um vasto leque de medidas concretas de apoio aos defensores dos direitos do Homem. Neles se incluem, entre outros, os programas dos Estados-Membros no domínio da cooperação para o desenvolvimento. Entre essas medidas concretas refiram-se, nomeadamente, as seguintes:
    - programas bilaterais de democratização e direitos humanos da Comunidade Européia e Estados-Membros deveriam levar em consideração a necessidade de assistir no desenvolvimento de processos e instituições democráticos, e a promoção e proteção dos direitos humanos em países em desenvolvimento através de, entre outros, apoiar os defensores dos direitos humanos mediante a realização de atividades que visem reforçar as suas capacidades ou de campanhas de;
    - fomentar e apoiar a criação de organismos nacionais de promoção e defesa dos direitos humanos estabelecidos de acordo com os princípios de Paris, nomeadamente instituições nacionais de defesa dos direitos do Homem, gabinetes de mediação e comissões de direitos humanos, bem como as ações por eles desenvolvidas;
    - participar na criação de redes internacionais de defensores dos direitos humanos, designadamente facilitando a organização de reuniões entre eles, tanto dentro como fora da UE;
    - procurar garantir que os defensores dos direitos humanos nos países terceiros tenham acesso a recursos, nomeadamente financeiros, provenientes do estrangeiro;
    - assegurar que os programas educativos em matéria de direitos do Homem promovam, entre outros, a Declaração sobre os Defensores de Direitos Humanos.

Papel dos grupos do Conselho

14. Conforme previsto no seu mandato, o COHOM deverá, em estreita coordenação e cooperação com outros grupos competentes do Conselho, supervisionar a aplicação e o seguimento dado às presentes orientações. Para tanto, caber-lhe-á:
    - promover a integração da questão dos defensores dos direitos humanos nas políticas e ações pertinentes da UE;
    - proceder regularmente a um balanço da aplicação das presentes orientações;
    - continuar a estudar, se for caso disso, novas formas de cooperação com as Nações Unidas e outros mecanismos internacionais e regionais de apoio aos defensores dos direitos humanos;
    - dar conhecimento ao Conselho – se necessário todos os anos –, por intermédio do CPS e do COREPER, dos progressos registrados no que respeita à aplicação das presentes orientações.

Anexo I ao Anexo do ANEXO
(Declaração sobre DDH)

Declaração da ONU sobre os Direitos e Responsabilidades de Indivíduos, Grupos e Órgãos da Sociedade de Promover e Proteger Direitos Humanos e Liberdades Fundamentais Universalmente Reconhecidos

Anexo II ao Anexo do ANEXO

Instrumentos internacionais pertinentes

- Declaração Universal dos Direitos do Homem
- Pacto Internacional sobre os Direitos Civis e Políticos
- Pacto Internacional sobre os Direitos Econômicos, Sociais e Culturais
- Convenção contra a Tortura e outras Penas ou Tratamentos Cruéis, Desumanos ou Degradantes
- Convenção sobre os Direitos da Criança
- Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres
- Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial
- Convenção Européia dos Direitos do Homem, respectivos Protocolos e jurisprudência pertinente do Tribunal Europeu dos Direitos do Homem
- Carta Social Européia / Carta Social Européia (revista)
- Carta Africana dos Direitos do Homem e dos Povos
- Convenção Americana sobre Direitos Humanos
- Convenções de Genebra para a Proteção das Vítimas de Guerra e respectivos protocolos, bem como as regras habituais do direito humanitário aplicáveis aos conflitos armados
- Convenção de 1951 relativa ao Estatuto dos Refugiados e respectivo Protocolo de 1967
- Estatuto de Roma do Tribunal Penal Internacional
- Declaração sobre o Direito e a Responsabilidade dos Indivíduos, Grupos ou Órgãos da Sociedade de Promover e Proteger os Direitos Humanos e Liberdades Fundamentais Universalmente Reconhecidos

ANEXO III

Recomendações de incidência (advocacy) da Protection International para defensores relacionadas a Missões Diplomáticas da União Européia (UE), Embaixadas e Representantes Especiais de Estados Membros da UE (mais dicas disponíveis em www.protectionline.org)

Desde a adoção da Declaração da ONU, os seguintes mecanismos foram criados para proteger os DDH ao redor do mundo:

- The O Mandato de **Representante Especial do Secretário-Geral da ONU sobre Defensores de direitos Humanos**, criado pela Comissão de Direitos Humanos da ONU.
- O mandato de **Relator Especial da Comissão Africana sobre Direitos Humanos e dos Povos**.
- **Resolução sobre a proteção dos defensores de direitos humanos da África** da Comissão Africana de Direitos Humanos e dos Povos, reunida em sua 35ª sessão ordinária, realizada entre 21 de maio e 4 de junho de 2004 em Banjul, Gâmbia.
- A **Unidade de Defensores de Direitos Humanos da Comissão Interamericana de Direitos Humanos**.
- A **UE** também adotou **Orientações específicas sobre Defensores de Direitos Humanos** como uma ferramenta que as missões diplomáticas da UE deveriam implementar em terceiros países.
- Conselho da Europa: Adoção da Declaração do Comitê de Ministros por uma melhor proteção aos defensores de direitos humanos, **18 de fevereiro de 2008**.
- Comissão Asiática de Direitos Humanos.

Em 2004, o Conselho de Ministros adotou as Orientações da UE sobre Defensores de Direitos Humanos. As Orientações da UE reiteram a Declaração da ONU e contém recomendações diretas específicas a todos os Estados Membros da UE e missões de Estados Membros. As recomendações da UE tem como objetivo:

- A adoção de políticas proativas de proteção dos defensores de direitos humanos.
- O uso de canais diplomáticos para obter, de autoridades locais e nacionais, o comprometimento de respeitar integralmente os direitos dos defensores de direitos humanos.

As Orientações da UE também podem ser obtidas nas Embaixadas de Estados Membros da UE.

As Missões da UE (Embaixadas de Estados Membros da UE e Delegações da Comissão da UE) constituem o primeiro ponto de contato entre a UE, o Estado membro e os defensores locais de direitos humanos (DDH).

A PI recomenda que os DDH ao menos:

- Ask pedir que as Orientações da UE sejam traduzidas para a língua dos DDH e distribuídas para organizações de direitos humanos, autoridades locais e nacionais.
- Enviar informação regular e atualizações sobre seu trabalho e a situação de direitos humanos para os Chefes de Missão da UE e para ONGs nacionais e internacionais para aumentar o conhecimento e aumentar a coordenação entre estes vários atores.

- Manter contato regular com as missões da UE para que os DDH estejam informados sobre as Orientações da UE e iniciativas da UE para a proteção dos DDH. Este contato regular permitirá às missões da UE estarem informadas sobre a situação dos DDH e suas recomendações de proteção e medidas de apoio a serem tomadas.
- Pedir às missões da UE que compartilhem e implementem práticas de proteção e estratégias de médio prazo.
- Convidar o chefe da missão da UE e os oficiais de direitos humanos para visitar sua área de trabalho, especialmente quando os DDH estão em risco particular (por exemplo, aras de conflito onde os DDH já foram atacados ou estão ameaçados).
- Pedir ações urgentes quando os DDH de direitos humanos são ameaçados ou detidos.
- Pedir um local seguro e assistência integral a DDH em risco.
- Solicitar ou aceitar convites e promoção de Missões da UE quando os DDH tiverem realizado uma análise de risco sobre o impacto de seu perfil ser elevado com estas ações. Enfatize as possíveis conseqüências de segurança e peça apoio à proteção. Peça assistência e que observem um evento como um julgamento contra um defensor de direitos humanos. Isso pode garantir um julgamento justo mas a presença será necessária durante todo o procedimento (desde a leitura do indiciamento até a leitura da sentença) para garantir a independência. Peça para que os observadores se comuniquem com a pessoa sendo julgada. Peça para observadores da UE estarem presentes em julgamentos contra violadores de direitos humanos para evitar a impunidade por seus crimes.
- Esteja atualizado sobre visitas aos DDH de seu país por parte da Presidência da UE, do Alto Representante do Conselho de Política Externa e Segurança Comum, de Representantes Especiais da UE ou de Membros da Comissão da UE, e peça para encontrar-se com eles.
- Peça para que a situação dos DDH de direitos humanos seja incluída na agenda política oficial de diálogo entre a UE, os DDH do país e organizações regionais.
- Peça para ações políticas coordenadas entre outros atores, em particular com o Conselho de Direitos Humanos e a Assembléia Geral da ONU. Peça por coordenação entre órgãos regionais para a proteção dos direitos humanos e os DDH eles mesmos, como a Comissão Africana de Direitos Humanos e dos Povos, a Unidade de Defensores da Comissão Interamericana de Direitos Humanos e a Comissão Asiática de Direitos Humanos.
- Peça para que os informes dos Chefes de Missão da UE sejam públicos e acessíveis aos DDH.

Levantamento de fundos/captação de recursos

Os DDH podem levantar fundos diretamente com embaixadas (programas de direitos humanos) e com a UE através do Instrumento Europeu para Democracia e Direitos Humanos (European Instrument for Democracy and Human Rights,EIDHR). O EIDHR permite que a Comissão Européia aloque fundos para ONGs sem a aprovação do governo do terceiro país. http://ec.europa.eu/europaid/projects/eidhr/index_en.htm ou simplesmente EIDHR. Mais informações sobre outros instrumentos financeiros disponíveis através do mesmo link.

Além disso:

Apesar de as Orientações da UE cobrirem missões da UE, instituições da UE e Estados Membros da UE e suas embaixadas, os DDH deveriam lembrar que podem conseguir apoio através de outros corpos diplomáticos e organizações internacionais pois a Declaração da ONU é válida para ser usada com todos os atores.

ANEXO IV

Delineamentos de Risco Geral para o Perfil Específico de Defensor de Direitos Humanos

Objetivo:

Definir risco para o perfil específico para o perfil de DDH de modo a levar em consideração na elaboração de planos de segurança/proteção e políticas de promoção organizacionais.

Além dos riscos comuns enfrentados por todos os DDH, o capítulo 1.9 ilustra as especificidades que um grupo de DDH deve levar em consideração ao elaborar um plano de segurança/proteção, seja no plano individual, organizacional ou inter-organizativo.

O Manual não pode ser exaustivo ao explorar todos os perfis de DDH trabalhando em diferentes contextos políticos. Cada grupo e cada situação mereceriam pelo menos um capítulo inteiro, se não todo um manual de proteção: instituições religiosas, comunidades indígenas, grupos trabalhando sobre direitos econômicos, sociais e culturais, grupos trabalhando sobre direitos das crianças, advogados e juristas, jornalistas, organizações rurais, ambientalistas, sindicalistas, minorias, LGBTI[1], …

Além disso, seria necessário uma contínua atualização do contexto político, pois se trata de algo dinâmico, e portanto também do risco.

Entretanto, não nos esqueçamos que a lógica de análise do risco subjacente permanece a mesma para todos os grupos de DDH e indivíduos. Ela apenas precisa ser implementada de acordo com o perfil específico e as ameaças, vulnerabilidades e capacidades relacionadas a esta pessoa ou grupo.

Abaixo apresentamos uma tabela não exaustiva sobre como dados específicos podem ser ilustrados através de discussões. Pode ser considerado um ponto de partida que cada grupo de DDH necessita explorar e detalhar ainda mais pois cada elemento possui vários matizes.

Por exemplo, instituições e redes religiosas podem ser cristãs (católicas, apostólicas, evangélicas, mórmons, Quakers...), islâmicas (sunni, shi'a, sufi…), hinduísta, budista, etc.; elas podem estar trabalhando em áreas rurais ou urbanas; em contextos políticos mais orientados aos direitos humanos ou não; sobre mais ou menos os mesmos assuntos polêmicos, etc.

A mesma ameaça pode ser veiculada de diferentes maneiras, por exemplo uma ameaça de agressão pode ser contra pessoas, materiais...

Cada perfil (tabela 3 (página 32-35) precisa ser usado para complementar esta informação.

1 Manual de Proteção para Defensores LGBTI, PI©2009.

Delineamentos de risco geral para o perfil específico de defensor de direitos humanos - ddh (não exaustivo)			
Perfis	**Áreas de trabalho**	**Ameaças devido ao trabalho/impacto**	**Vulnerabilidades/ capacidades**
Redes religiosas (…)	• Direitos humanos, Direito Internacional Humanitário, segurança alimentar e valores religiosos • Grupo de denominação múltipla • (…)	• Desacreditados quando taxados de "defensores de grupos armados ilegais" • Agressões por causa do rótulo • (…)	• Isolamento geográfico • Falta de apoio institucional • Acesso a redes • Trabalham com um elemento convergente (crença religiosa) • (…)
Organizações de direitos econômicos, sociais e culturais	• Empoderamento individual e organizacional • Segurança alimentar, gestão de meio ambiente E proteção, projetos agrários, educação • Identidade e direitos das minorias • (…)	• Força organizacional quebra a hegemonia dos atores armados • Embargos Econômicos • Infiltração • (…)	• Expostos a grupos armados nas regiões onde trabalham • Isolamento geográfico • Acesso a redes tratando de temas menos contenciosos que outros temas de direitos humanos como prisioneiros políticos, por exemplo • Acesso a algum tipo de aceitação a seu trabalho que gera benefícios imediatos para as comunidades local • (…)
Organizações legais ou judiciais	• Defesa dos direitos humanos geralmente através de casos emblemáticos • Treinamento sobre direitos humanos • Luta contra a impunidade e por observações de julgamentos • Consultorias jurídicas e políticas • Denúncias públicas de violações de direitos humanos • Campanhas políticas temáticas • (…)	• Descrédito • Criminalização • Judicialização • Ataques contra sua imagem social • Infiltração • (…)	• Distância de autoridades civis e políticas • Apoio político interno limitado • Perfil institucional relativamente alto • Apóio Institucional • Acesso a redes homólogas internacionais • (…)
Instituições religiosas	• Assistência humanitária • (…)	• Estigmatização e perseguição • (…)	• Exposição • Confiança exagerada (Deus querendo / com a proteção de Deus/ reencarnação/ …) • Legitimidade • Redes e recursos – Credibilidade • Incidência política e hierárquica • Hierárquica • Identidade Ideológica • (…)

Delineamentos de risco geral para o perfil específico de defensor de direitos humanos - DDH (não exaustivo)			
Perfis	**Áreas de trabalho**	**Ameaças devido ao trabalho/impacto**	**Vulnerabilidades/ capacidades**
Comunidades rurais	• Luta pela terra • (…)	• Controle territorial por terceiros • Deslocados ou confinados • Intimidação de fazendeiros poderosos • (…)	• Isolação • Liderança fraca • Pobreza • Habilidades para aumentar produtos • Conhecimento do território • Habilidades organizacionais • Acesso difícil à informação e educação • Acesso difícil a eletricidade e água • Território agrícola compartilhado • Composição e interesses heterogêneos • (…)
Sindicados	• Direitos humanos trabalhistas • (…)	• Descrédito e criminalização • Demissões • (…)	• Membro registrado de uma Organização social mundial • Exposto a atitudes de protagonismo • Posição político-partidária • Trabalho em redes • Capacidade de mobilizar grande número de membros e não membros • Capacidade de ter impacto sobre áreas econômico-social chave • Reconhecimento Social • Relutância em colaborar com DDH • Identidade Política • Estrutura Hierárquica • (…)
Jornalistas	• Investigação e publicação de violações de direitos humanos. • (…)	• Descrédito • Agressão • (…)	• Expostos a corrupção e a magnatas da mídia • Acesso a redes internacionais a associações de jornalistas • Acesso à mídia • Imagem Pública • Cão de guarda da democracia • Indivíduos • (…)

Delineamentos de risco geral para o perfil específico de defensor de direitos humanos - DDH (não exaustivo)			
Perfis	**Áreas de trabalho**	**Ameaças devido ao trabalho/impacto**	**Vulnerabilidades/ capacidades**
LGBTI	• Direitos LGBTI • (…)	• Difamação, descrédito e criminalização • Campanha Pública anti LGBTI • Legislação Anti LGBTI • (…)	• Expostos a preconceitos morais/religiosos/ culturais/sociais • Acesso a redes internacionais • Geralmente excluídos por outros DDH • Algumas vezes tem o perfil baixo • Difícil promoção de seus direitos • Transversal a todas as organizações de DDH • Facilmente reconhecível • Expostos a homo e trans fobias também de autoridades supostamente encarregadas de proteger todos os cidadãos • Expostos a pressão psicológica e estresse • (…)
GRUPOS DE MINORIAS ÉTNICAS • (…)	• Direito à identidade • (…)	• Descrédito e exclusão • Restrição aos direitos civis e cívicos • (…)	• Compartilham identidade étnica e cultural • Podem ser assentados em diferentes áreas geográficas • Tendência de trabalhar em círculos fechados • Isolação • Acesso difícil a outros grupos de direitos humanos • Dificuldade em promover conscientização sobre sua causa • (…)

Bibliografia e recursos adicionais

Bibliografia

- Amnesty International (2003): "*Atores Essenciais do Nosso Tempo: defensores dos direitos humanos nas Américas*". Secretariado Internacional AI (Índice AI: AMR 01/009/2003/s
- AVRE and ENS (2002): "*Afrontar la amenaza por persecución sindical*". Escuela de Liderazgo Sindical Democrático. Published by the Escuela Nacional Sindical and Corporación AVRE. Medellín, Colombia.
- Bettocchi, G., Cabrera, A.G., Crisp, J., and Varga, A (2002): "*Protection and solutions in situations of internal displacement*". EPAU/2002/10, UNHCR.
- Cohen, R. (1996): "*Protecting the Internally Displaced*". World Refugee Survey.
- Conway, T., Moser, C., Norton, A. and Farrington, J. (2002) "*Rights and livelihoods approaches: Exploring policy dimensions*". DFID Natural Resource Perspectives, no. 78. ODI, London.
- Dworken, J.T "*Threat assessment*". Series of modules for OFDA/InterAction PVO Security Task Force (Mimeo, included in REDR Security Training Modules, 2001).
- Eguren, E. (2000): "*Who should go where*? Examples from Peace Brigades International", in "*Peacebuilding: a Field Perspective. A Handbook for Field Diplomats*", by Luc Reychler and Thania Paffenholz (editors). Lynne Rienner Publishers (London).
- Eguren, E. (2000), "T*he Protection Gap: Policies and Strategies*" in the ODI HPN Report, London: Overseas Development Institute.
- Eguren, E. (2000) "*Beyond security planning: Towards a model of security management. Coping with the security challenges of the humanitarian work*". Journal of Humanitarian Assistance. Bradford, UK.
  www.jha.ac/articles/a060.pdf
- Eriksson, A. (1999) "*Protecting internally displaced persons in Kosovo*". http://web.mit.edu/cis/www/migration/kosovo.html#f4
- Lebow, Richard Ned and Gross Stein, Janice. (1990) "*When Does Deterrence Succeed And How Do We Know?*" (Occasional Paper 8). Ottawa: Canadian Inst. for Peace and International Security.
- Mahony, L. and Eguren, E. (1997): "*Unarmed bodyguards. International accompaniment for the protection of human rights*". Kumarian Press. West Hartford, CT (USA).
- Martin Beristain, C. and Riera, F. (1993): "*Afirmación y resistencia. La comunidad como apoyo*". Virus Editorial. Barcelona.

- Paul, Diane (1999): "*Protection in practice: Field level strategies for protecting civilians from deliberate harm*". ODI Network Paper no. 30.
- SEDEM (2000): *Manual de Seguridad. Seguridad en Democracia*. Guatemala.
- *Sustainable Livelihoods Guidance Sheets* (2000). DFID. London, February 2000
- Sutton, R. (1999) *The policy process: An overview*. Working Paper 118. ODI. London.
- ACNUR (2004): "*About Human Rights Defenders*" (extensive information): http://www.unhchr.ch/defenders/about1.htm
- ACNUR (2004): "*Human Rights Defenders: Protecting the Right to Defend Human Rights*". Fact Sheet no. 29. Geneva.
- ACNUR (2004): On women defenders: www.unhchr.ch/defenders/tiwomen.htm
- ACNUR (1999): *Protecting Refugees: A Field Guide for NGO*. Geneva.
- ACNUR (2001): *Complementary forms of protection. Global Consultations on International Protection*. EC/GC/01/18 4 September 2001
- ACNUR (2002) *Strengthening protection capacities in host countries. Global Consultations on International Protection*. EC/GC/01/19 * / 19 April 2002
- ACNUR-Department of Field Protection (2002) *Designing protection strategies and measuring progress: Checklist for UNHCR staff*. Mimeo- Geneva.
- Van Brabant, Koenraad (2000): "*Operational Security Management in Violent Environments*". Good Practice Review 8. Humanitarian Practice Network. Overseas Development Institute, London.

Recursos adicionais

A Protection International oferece, desde 2000, formação e assessoria sobre análise de risco, proteção e segurança para defensores de direitos humanos.

Por favor contate-nos em pi@protectioninternational.org ou escreva para: PI, Rue de la Linière, 11-1060, Bruxelas, Bélgica

Tel: + 32 (0)2 609 44 05 +32 (0)2 609 44 07

Fax: +32 (0)2 609 44 06

www.protectioninternational.org

www.protectionline.org

Tactical Technology Collective: **www.tacticaltech.org** (desde 2003 – experiência técnica em segurança digital): "NGO in a Box".

Índice dos capítulos

Índice temático

Luis Enrique Eguren

Espanha), médico e especialista em proteção, membro da Unidade de Pesquisa e Capacitação da Protection International. Ele trabalhou com a PBI em El Salvador, Sri Lanka e Colômbia, assim como em missões curtas em outros países com outras organizações internacionais. Consultor, instrutor e pesquisador, ele já publicou diversos artigos e livros sobre o tema de proteção.

Marie Caraj

Intérprete e especialista em proteção. Membro da Unidade de Pesquisa e Capacitação da Protection International. Ela trabalhou com a PBI e PBI-BEO entre 1985 e 2007. Teve uma sucessão de missões curtas na África, Ásia e América Latina. Consultora, instrutora e pesquisadora.

"(...) a gravidade dos riscos enfrentados pelos defensores de direitos humanos todos os dias é tanta que é também importante perseguir meios para reforçar sua proteção. Neste sentido, espero que este Manual de Proteção apoiará os defensores de direitos humanos a desenvolver seus próprios planos de segurança e mecanismos de proteção. Muitos defensores de direitos humanos estão tão focados em seu trabalho protegendo outros que eles prestam atenção insuficiente à sua própria segurança. É importante que todos nós envolvidos em direitos humanos possamos entender que devemos estar preocupados com a nossa segurança e aquela das pessoas para quem e com quem trabalhamos."

(Hina Jilani, ex-Representante Especial do Secretário-Geral da ONU para Defensores de Direitos Humanos)

"Desde que tivemos esta formação, muitas coisas mudaram em nossa organização, apenas porque muitas das coisas que aprendemos durante o curso nós obviamente não tinhamos conhecimento anterior. Agora, somos mais fortes por causa desta formação, e sabemos muito melhor como avaliar os riscos que corremos todos os dias, assim como julgar incidentes de segurança, ameaças e a probabilidade de um ataque ser realizado."

(...) Seus métodos de ensino são ativos e inclusivos, e isso é um extra considerável pois nos permite intercambiar informação. Temos certeza de que os resultados nos darão muitas perspectivas novas.".
"Eu sinto que recebi uma formação de muito boa qualidade sobre como ser um verdadeiro defensor de direitos humanos. Vou mudar a maneira de trabalhar depois disso."

(Defensores na República Democrática do Congo)

Parabéns pelos esforços e o formato pois foi muito instrutivo e nos ajudou a resolver nossa situação diária."

(Um defensor na Guatemala)

"Eu aprendi muito sobre um mundo o qual conheço há muito tempo, mas para o qual eu não havia ainda olhado daquela maneira antes."

(Um defensor do México)

"(...) Este é um tópico muito novo para mim. Apesar de estar trabalhando nesta área onde sempre há ameaças à nossa segurança, nós nunca pensamos na necessidade de tal treinamento ou nunca tivemos o tempo para pensar sobre nossa segurança. Mas depois do treinamento, eu pessoalmente senti que o assunto deveria ser mantido em alto nível antes de lançar qualquer outro programa. Em outras palavras, o treinamento é realmente essencial para todos."

(Um defensor no Nepal)

PROTECTION international

Com o apoio de:

ifa Institut für Auslandsbeziehungen e. V.

Auswärtiges Amt

Iniciativa Europeia para a Democracia e os Direitos do Homen IEDDH

KINGDOM OF BELGIUM
Federal public service
Foreign Affairs, Foreign Trade and Development Cooperation

O Novo Manual de Proteção de Defensores de Direitos Humanos foi pesquisado e escrito por Enrique Eguren e Marie Caraj, da Unidade de Formação e Pesquisa da Protection International.

Protection International, Rue de la Linière, 11, B-1060, Bruxelas
Tel.: +32(0)2 609 44 05 / +32 (0) 2 609 44 07, Fax: +32 (0) 2 609 44 07
e-mail: pi@protectioninternational.org www.protectioninternational.org

Um sítio único sobre proteção dos defensores dos direitos humanos: www.protectioninternational.org