Manual de Proteção para Defensores de Direitos Humanos

Pesquisado e escrito por Enrique Eguren,
Escritório Europeu de Peace Brigades International (PBI BEO)

Publicado por Front Line
Fundação Internacional para a Proteção dos Defensores de Direitos Humanos

Publicado por Front Line 2005
Fundação Internacional para a Proteção dos Defensores de Direitos Humanos
16 Idrone Place, Off Bath Place, Blackrock County, Dublin, Irlanda.

Para pedir cópias deste manual, escreva para:
info@frontlinedefenders.org ou pbibeo@biz.tiscali.be ou ainda
manual@protectionline.org
Preço: 20 Euros além do custo de envio

Alternativamente, para pedir um manual por favor contate

PBI-European Office
38 Rue Saint-Christophe, 1000 Bruxelas ,Bélgica.
Tel./Fax + 32 (0) 2 511 14 98
manual@protectionline.org
pbibeo@protectionline.org ou pbibeo@biz.tiscali.be

Front Line
16 Idrone Place, Off Bath Place, Blackrock County, Dublin, Irlanda.
Tel. + 353 1212 37 50 Fax + 353 1212 1001
protectionmanual@frontlinedefenders.org

Este manual será traduzido por Front Line para o inglês, francês, russo e árabe (assim como para outros idiomas, de acordo com as possibilidades)

ISBN: 0-9547883-1-1

Prefácio, 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 das Nações Unidas.[1] 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 apoie 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
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 instituções de promover e proteger os direitos humanos e as liberdades fundamentais universalmente reconhecidos, 1998.

FRONT LINE

Front Line foi fundada em Dublin em 2001 com o objetivo específico de proteger aos defensores de os direitos humanos, pessoas que trabalham, de maneira não violenta, por qualquer dos direitos defendidos na Declaração Universal de Direitos Humanos. Front Line tem como objetivo se ocupar de algumas das necessidades identificadas pelos mesmos defensores, incluindo a proteção, contatos, a formação e acesso aos mecanismos temáticos e de países da ONU e de outros organismos regionais.

Front Line se ocupa principalmente dos defensores de direitos humanos em situação de risco, tanto temporalmente como permanentemente, por seu trabalho em nome de seus cidadãos. Front Line tem um pequeno programa de bolsas para o propósito específico de fortalecer a proteção dos defensores de direitos humanos. Front Line mobiliza campanhas e grupos de pressão em nome dos defensores que estão em perigo iminente. Em situações de emergência, Front Line pode assistir no deslocamento temporal.

Front Line pesquisa e publica relatórios sobre a situação dos defensores de direitos humanos em países específicos. Também desenvolvemos materiais e pacotes de formação para os defensores de direitos humanos, além de facilitar contatos e intercâmbios entre os defensores de diferentes partes do mundo. Os projetos da Front Line costumam ser realizados em associação com organizações específicas de direitos humanos.

Front Line promove a difusão da Declaração Universal de os Direitos Humanos e atua para assegurar o conhecimento, respeito e adesão aos princípios e os normas reconhecidos na "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" (conhecida como a "Declaração sobre defensores de direitos humanos").

Front Line tem status consultivo especial ante o Conselho Econômico e Social das Nações Unidas (ECOSOC).
Front Line tem status "*charitable*" (CHY NO 14029), é independente e imparcial.

Para apoiar seu trabalho, Front Line depende inteiramente da generosidade do financiamento de organizações e pessoas. Front Line tem a felicidade de ter sido financiada, desde seu lançamento em 2001, a partir de uma variedade de fontes de financiamento, e também recebe doações de pessoas individuais.

Conselho de Administração (*Board of trustees)*: Denis O´Brien (*chairman*), Mary Lawlor (Diretora), Pierre Sané, Kieran Mulvey, Noeline Blackwell, Michel Forst, David Sykes.

Conselho Consultivo: Hanan Ashrawi, Robert Badinter, Bono, His Holiness The Dalai Lama, Indai Lourdes Sajor, Wangarai Muta Maathai, Martin O´Brien, Adolfo Pérez Esquivel, Desmond Tutu.

Peace Brigades International (PBI)

Peace Brigades International (PBI) é uma organização não governamental que protege aos defensores de direitos humanos e promove a transformação não violenta de conflitos.

Mediante convite, a PBI envia equipes de voluntários a zonas onde há conflito e repressão. Os voluntários acompanham defensores de direitos humanos e suas organizações que estejam ameaçados por violência política. Aqueles que realizam violações de direitos humanos normalmente não querem que a comunidade internacional seja testemunha de suas ações. A presença física dos voluntários como observadores, junto com suas ações de incidência (*advocacy*) e de criação de redes e uma ampla rede de apoio internacional, contribui para dissuadir agressores de cometerem hostilidades e ataques contra os defensores. Desta maneira a PBI contribui para criar espaço para que os defensores realizem seu trabalho a favor dos direitos humanos e da justiça social.

PBI tem um Conselho Internacional, um Escritório Internacional em Londres e Grupos de País ou associados em 17 países, assim como vários projetos no terreno.

O Escritório Europeu da PBI está localizado em Bruxelas, Bélgica. Os conteúdos deste Manual são um dos resultados do trabalho de sua Unidade de Pesquisa e Formação.

Para mais informação sobre a PBI, acesse http://www.peacebrigades.org.

Para mais informação sobre o Escritório Europeu da PBI, acesse http://www.peacebrigades.org/beo.html

Apresentação

Front Line foi fundada com o mandato de trabalhar exclusivamente para a proteção dos defensores de direitos humanos. Lamentavelmente, nosso trabalho diário nos mostra quanta proteção e segurança é ainda preciso para os defensores em um mundo em que se encontram cada vez mais atacados. Nosso principal foco é incrementar a pressão em torno aos governos que ademais de serem responsáveis perante o direito internacional de proteger os defensores, são frequentemente os perpetradores de ataques e medidas repressivas contra os defensores. No entanto, resta claro que a partir da informação proporcionada pelos próprios defensores, poder-se-ia fazer muito mais para desenvolver sua própria capacidade para melhorar sua segurança.

Por esta razão nos pareceu muito interessante quando soubemos do projeto que sob o título de “Priorizando a proteção” estava desenvolvendo Peace Brigades International, e particularmente o manual proposto para defensores de direitos humanos. Rapidamente nos colocamos de acordo com eles para financiar a pesquisa e a publicação deste manual.

Foi um prazer trabalhar com Enrique Eguren, o autor deste manual. Junto com seus colegas, trouxe a riqueza da experiência sobre temas de proteção e segurança. PBI realizou também um número de oficinas com defensores no terreno, para tentar assegurar que o manual se beneficiasse da experiência daqueles que estão trabalhando na primeira linha. Duas destas oficinas foram feitas em colaboração com Front Line em Bukavu e Goma, na região leste da República Democrática do Congo, em maio de 2004.

O objetivo de Front Line ao publicar o manual é prover um recurso prático que os defensores possam usar ao desenvolver suas estratégias e planos de proteção e segurança. Neste sentido o manual é oferecido como um trabalho aberto sobre o qual esperamos poder construir com a experiência de tantos defensores que trabalham em ambientes hostis. Os conteúdos do manual também tomaram em conta as discussões sobre segurança e proteção realizadas na Primeira e Segunda Plataformas de Dublin para Defensores de Direitos Humanos, que tiveram lugar em 2002 e 2003. Haverá outra oportunidade para uma discussão sistemática e comentários sobre o manual na Terceira Plataforma de Dublin de outubro de 2005.

O manual tenta aprofundar como analisar riscos e ameaças e como desenvolver estratégias e planos efetivos de segurança e proteção. Esperamos que seja uma ferramenta útil para os responsáveis de segurança em ONGs de direitos humanos e um apoio para a formação de defensores. Nossa intenção é publicar um manual mas curto com conselhos e sugestões práticos para complementar o manual de formação. Front Line está também envolvida num projeto com Privaterra para publicar um manual e um conjunto de ferramentas especiais para o tema de segurança e comunicações eletrônicas, em parte resumido no capítulo 12 deste manual, que será lançado em 2005.

Temos de reconhecer a contribuição de várias pessoas sem as quais este manual não teria sido publicado.

Marie Caraj, Pascale Boosten, MichaO Schools and Christoph Klotz, queridos colegas do Escritório Europeu da PBI, foram chave para este projeto: sem seu compromisso e experiência não teríamos conseguido nada.

O texto foi revisado e corrigido por Mary Lawlor, Andrew Anderson, James Mehigan, e Dmitri Vitaliev (capítulo 12), de Front Line. Kristin Hulaas Sunde revisou uma versão anterior do texto.

O capítulo 12 é baseado no trabalho de Robert Guerra, Katitza Rodríguez e Caryn Madden, de Privaterra (Canadá).

Estamos em divida com os aportes e comentários recebidos de Arnold Tsunga (Zimbabwe Lawyers for Human Rights), Sihem Bensedrine (Túnez, Conseil National pour les Libertés en Tunisie), Padre Brendan Forde (Franciscanos Itinerantes, Colombia), Indai Sajor (ex-Diretora do Asian Centre for Women´s Human Rights, Filipinas), James Cavallaro (Brasil, Diretor Associado do Programa de Direitos Humanos de 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 de SEDEM (Guatemala), Claudia Samayoa (Guatemala), Jaime Prieto (Colombia), Emma Eastwood (UK) e Cintia Lavandera (Programa de Defensores de Direitos Humanos da Anistia Internacional em Londres).

Carmen Díez Rozas diagramou cuidadosamente todo o manual e completou sua montagem, e Montserrat Muñoz colaborou com assessoria na montagem e ilustrações.

Estamos também agradecidos ao apoio proporcionado por Development Cooperation Ireland.

Impresso por “Print and Display”.

(do autor)
Também muitas pessoas contribuíram para reunir o conhecimento necessário para escrever o manual. É impossível nomeá-las aqui, mas gostaria de mencionar alguns nomes como:

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

A Danilo, Clemencia e Abilio e seus colegas da Comisión Intereclesial de Justicia e 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.

Às pessoas comprometidas com o programa de formação em segurança para defensores da *Consejería en Proyectos,* na Colômbia, e aos colegas de *Pensamiento e Acción Social* (PAS) na Colômbia.

Ao 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, Croácia, Sérvia, Kosovo, Ruanda, República Democrática do Congo, Ingushetia, etc... um mar de conversões, lágrimas, sorrisos e 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.

Agradecemos a contribuição de todas as pessoas mencionadas, e aos muitos defensores com quem trabalhamos e de quem tanto temos aprendido. No entanto, o texto final e qualquer erro que possa constar nele, são tão somente de responsabilidade conjunta de Front Line e do autor. Esperamos que este 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 devem assumir sua responsabilidade elas mesmas. Esperamos seus comentários e opiniões.

Front Line
Escritório Europeu de Peace Brigades International
7 de março de 2005

Isenção de responsabilidade com respeito ao texto

Os conteúdos deste manual não necessariamente representam as posições ou pontos de vista de Peace Brigades International, nem de Front Line (International Foundation for the Protection of Human Rights Defenders).

Nem o autor nem quem o publica 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.

Índice de capítulos

Introdução .....
Cap. 1.- Cenários de trabalho: contextualizando as decisões sobre segurança e proteção
Cap. 2.- Valoração do risco: ameaças, vulnerabilidades e capacidades
Cap. 3.- Conhecimento e avaliação das ameaças
Cap. 4.- Incidentes de segurança: definição e análise.
Cap. 5.- Prevenir e reagir aos ataques.
Cap. 6.- Preparação de uma estratégia e de um plano de segurança.
Cap. 7.- Avaliar o rendimento da segurança de sua organização: a roda da segurança.
Cap. 8.- Assegurar-se do cumprimento das normas e procedimentos de segurança.
Cap. 9.- Melhorar a segurança no trabalho e nas residências particulares.
Cap. 10.- A segurança e as mulheres defensoras dos direitos humanos.
Cap. 11.- A segurança em zonas de conflito armado.
Cap. 12.- A segurança nas comunicações e a tecnologia da informação.
Anexo: A Declaração da ONU sobre Defensores de direitos humanos.
Bibliografia selecionada e outros recursos
Índice temático

Manual de Segurança e Proteção para Defensores dos Direitos Humanos

Introdução: O risco dos defensores dos direitos humanos

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

Nos últimos anos, aumentou a consciência geral do enorme risco que correm os defensores dos direitos humanos em seu trabalho. O risco é fácil de identificar 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 correm risco também quando a lei autoriza plenamente o trabalho em direitos humanos por um lado, mas por outro, não pune aqueles que ameaçam ou atacam os defensores. Em situações de conflito armado, o risco se faz mais patente ainda.

Excetuando algumas situações caóticas nas quais a vida de um defensor pode estar nas mãos de soldados durante um controle na estrada, 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 dos direitos humanos devam implementar estratégias amplas e ativas 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 manobras dirigidas a melhorar a gestão da segurança dos defensores.

As lições de segurança mais efetivas procedem 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 re-compilemos mais informação por parte dos defensores de direitos humanos que trabalham na linha de frente. Também há lições que 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 (de governos e da sociedade civil) a pressionar e atuar contra aqueles que dia após dia ameaçam, perseguem e matam aos defensores. Por isto, 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 dos 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 dos 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 o de proporcionar aos defensores de direitos humanos um conhecimento adicional e alguns instrumentos que possam ser de utilidade imediata para melhorar sua segurança e proteção. O manual lhes ajudará 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.

O presente manual é o resultado de um projeto de longo prazo da PBI sobre a proteção dos defensores. Tivemos a oportunidade de aprender e compartilhar experiências e conhecimentos com centenas de defensores no campo, ou igualmente em oficinas, reuniões e debates sobre segurança. A maior parte do conteúdo do manual já foi colocada em prática, ou 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 dele 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 sobrecarregadas agendas de trabalho, do acentuado estresse e, inclusive, do medo que sofrem muitos dos defensores. 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. O presente 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. 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...

Melhoremos 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:

protectionmanual@frontlinedefenders.org
pbibeo@biz.tiscali.be

Ou por correio para Front Line ou PBI:

PBI – Escritório Europeu
38, Rue Saint-Christophe, 1000 Bruxelas, Bélgica
Tel./fax: + 32 (0)2 511 14 98

Front Line
16 Idrone ane, Off Bath Pace, Backrock, Dublin, Irlanda
Tel.: +353 1212 3750 fax: +353 1212 1001

****

Uma pequena introdução aos defensores de direitos humanos.

“Defensor dos 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 dos 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 os defensores.

Em 1998 a Assembléia Geral das Nações Unidas aprovou a "Declaração sobre o Direito e o Dever dos Indivíduos, os Grupos e as Instituições da Sociedade de Promover e Proteger os Direitos Humanos e as Liberdades Fundamentais Universalmente Reconhecidos" (Daqui por diante a "Declaração da ONU sobre os defensores dos Direitos Humanos"). Em outras palavras, cinqüenta anos depois da Declaração Universal dos Direitos Humanos, e depois de vinte anos de negociações sobre um ante-projeto da declaração sobre os defensores dos 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.

A Representante Especial do Secretário-Geral da ONU para os defensores dos direitos humanos tem a função de "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."

Front Line define o defensor dos direitos humanos como "uma pessoa que trabalha, de forma pacífica, para todos e qualquer dos direitos consagrados na Declaração Universal dos Direitos Humanos." Front Line busca promover a Declaração sobre os defensores dos Direitos Humanos da ONU.

(Veja abaixo fontes para mais informações sobre a Declaração da ONU sobre os defensores de direitos humanos)

Quem é responsável por proteger os defensores dos direitos humanos?

A Declaração sobre os defensores dos direitos humanos sublinha que o Estado é o principal responsável por proteger os defensores dos direitos humanos. Mesmo assim 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"*.

Mas, segundo Hina Jiani, a atual Representante Especial do Secretário-Geral da ONU para os defensores dos 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 dos direitos humanos".[1] Todos os relatórios sobre os defensores dos 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.

[1] Relatório sobre os defensores dos direitos humanos, 10 de setembro de 2001 (A/56/341).

Leitura sugerida

📖 Para mais informação sobre os defensores dos direitos humanos, veja:

- www.unhchr.ch/defender/about1.htm (Alto Comissariado da ONU para os Direitos Humanos).
- www.frontlinedefenders.org (Front Line, Fundação Internacional para os defensores dos Direitos Humanos)
- www.peacebrigades.org/beo.html (Escritório Europeu da Peace Brigades International, em Bruxelas)
- Observatório para a Proteção de os defensores dos direitos humanos, criado pela Federação Internacional dos Direitos Humanos (FIDH; www.fidireitos humanos.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 dos Direitos Humanos do Serviço Internacional para os Direitos Humanos em Genebra)

📖 Para mais informação sobre os instrumentos legais internacionais existentes e a Declaração da ONU sobre os defensores dos Direitos Humanos, visite :

- 📖 www.unhchr.ch : esta é a página web do Alto Comissariado da ONU para os Direitos Humanos.
- 📖 www.frontlinedefenders.org/manual/en/index.htm (Front Line, Irlanda), para um manual sobre os instrumentos internacionais dos defensores dos direitos humanos. Sua página de links também é de grande utilidade: http://www.frontlinedefenders.org/links/
- 📖 www.ishr.ch/index.htm (Serviço Internacional dos Direitos Humanos, Genebra) para uma compilação de instrumentos internacionais e regionais para a proteção dos defensores dos direitos humanos.

CAPÍTULO I

CENÁRIOS DE TRABALHO: CONTEXTUALIZANDO AS DECISÕES SOBRE SEGURANÇA E PROTEÇÃO

Objetivos:
Tomar consciência da importância de analisar nossos cenários de trabalho e os diferentes atores que intervêm.
Aprender diferentes métodos para isto.

O ambiente de trabalho dos defensores dos direitos humanos

Os defensores dos direitos humanos acabam por trabalhar 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. 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 influencia 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 que medidas e que procedimentos de segurança por 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 um **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, seguindo a análise 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. Portanto, estes cenários devem 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 se encontre simplesmente um remédio para o sintoma, isto é, a perseguição. Mas se a pergunta é formulada *orientando-a para uma solução*, ficam mais fáceis de verificar os processos reais. Por exemplo, se a pergunta for: "É nosso ambiente sócio-político suficientemente seguro para que possamos dar conta do nosso trabalho?", resultaria 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-chaves 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", que nosso ambiente não é seguro o bastante, a partir deste ponto podemos seguir analisando por que não é seguro, e assim sucessivamente.

☞ *Uso do método de* Formular Perguntas*:*

- Busque perguntas que te ajudem a delimitar e compreender devidamente os pontos-chaves 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-chaves em jogo nos cenários sócio-político e econômico?
- Quem são os atores mais importantes relacionados com estas questões-chaves?
- Em que medida poderia nosso trabalho afetar de forma negativa ou positiva os interesses destes atores-chaves?
- Como poderíamos reagir na hipótese de nos convertermos em alvo destes atores, por conta do nosso trabalho?
- É nosso entorno sócio-político suficientemente seguro para executarmos nosso trabalho?

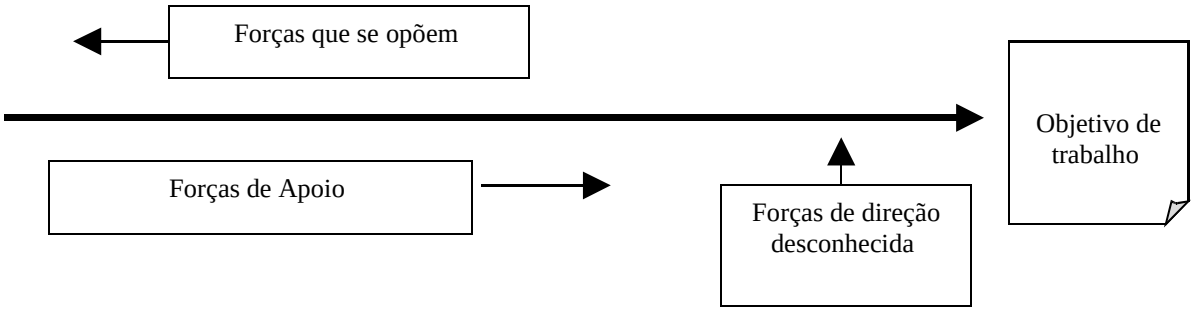
- Como responderam as autoridades locais/nacionais ao trabalho anterior dos defensores de direitos em relação a esta questão?
- Como responderam os atores-chaves a atuações similares de defensores de direitos, ou outros, em relação a estas questões?
- Como responderam os meios de comunicação e a comunidade 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, enquanto 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.

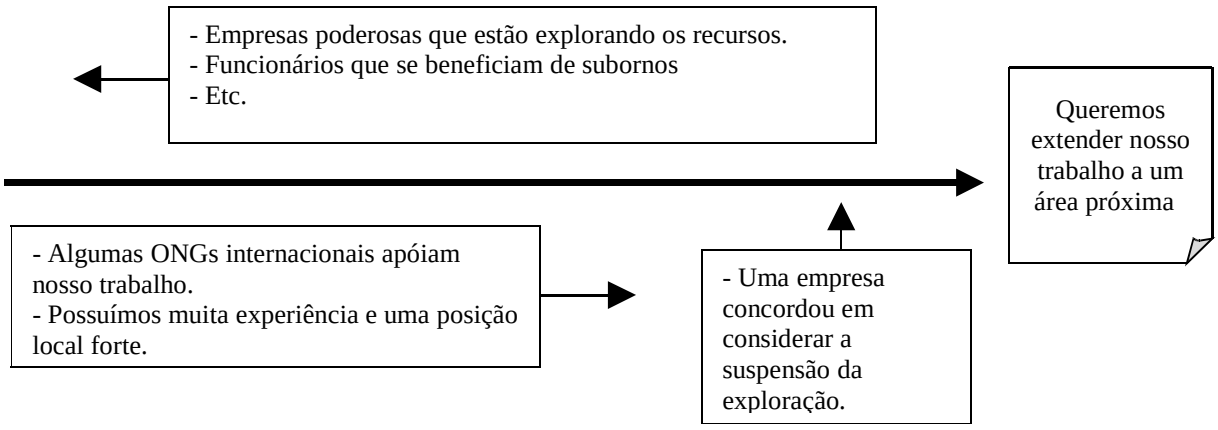
Comece desenhando uma flecha horizontal num quadro. Escreva um pequeno resumo de seu objetivo de trabalho nesse quadro. Isto proporcionará um foco para identificar as forças a favor e contra. Desenhe outro quadro sobre a flecha central: enumere aqui todas as possíveis forças que poderiam se opor ao alcance 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 um 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].**

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,** que têm obrigação de proteger os defensores, isto é:

- Instituições governamentais e estatais (incluindo as forças de segurança, os juízes, os legisladores, etc.)

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

- 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-chaves** que 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-chaves em proteção incluiria:

- Organismos da ONU (exceto os que têm mandato em proteção);
- O Comitê Internacional da Cruz Vermelha (CICR);
- Outros governos e instituições multilaterais (tanto doadores como responsáveis políticos, os "*policy-makers*");
- Outros atores armados;
- ONGs (tanto nacionais como internacionais);
- Igrejas e instituições religiosas;
- Empresas privadas;
- Os meios de comunicação.

Em outras palavras, a análise de atores é fundamental para compreender:

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

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 a aqueles inerentes às situações de conflito, projetam uma visão complexa do cenário em seu conjunto.

Análise de estruturas e processos variáveis

Os atores de proteção 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. Para isto, temos de falar de **estruturas e processos.**

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 se criar uma comissão inter-setorial (membros do governo, ONGs, a ONU e corpos diplomáticos) para fazer um seguimento da situação de proteção de uma organização específica de defensores dos direitos humanos.

Os **processos de proteção são** as séries 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.

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

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.

Um 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? 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 2). Copie a mesma lista de atores na primeira coluna e ao longo da primeira linha. Uma vez copiada, você pode realizar dois tipos de análise:

- Para analisar 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 (UNHCR), 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 da ONU**	**ONGs Internacional**
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 Internacio-nais									(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).

CAPÍTULO 2

VALORAÇÃO DO RISCO: AMEAÇAS, VULNERABILIDADES E CAPACIDADES

Objetivo:
Compreender os conceitos de ameaça, vulnerabilidade e capacidade de segurança.
Aprender como realizar uma valoração do risco.

Análise do risco e necessidades de proteção

O trabalho dos defensores dos 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 nos seguintes passos:

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 de segurança.

Não existe uma definição amplamente aceita do risco, mas podemos dizer que o risco faz referência às possíveis situações , por mais incertos que sejam, que poderiam causar um dano.

Numa dada situação, todos aqueles que trabalhem 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 os 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 enfrentar melhor os problemas 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]:

Risco = **ameaças** x **vulnerabilidades**

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 por defensores em questão, assim como aos interesses e às necessidades das pessoas que se opõem ao trabalho de tais defensores.

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 indiretas** surgem do possível dano causado por combates em conflitos armados, tais como "estar no lugar errado na hora errada. " Deste modo, estas ameaças concernem especialmente aos defensores que trabalham em zonas de conflito armado.

As ameaças tipo *targeting* (ameaças concretas) podem também ser consideradas de forma complementar: os defensores de direitos humanos poderiam sofrer ameaças **declaradas** ao receber, por exemplo, uma ameaça de morte (veja o Capítulo 3, sobre como avaliar as ameaças declaradas). Existem também casos de **possíveis** ameaças, quando um defensor recebe ameaças por conta de seu trabalho 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.

<u>Vulnerabilidades</u>

[1] Van Brabant (2000) e REDR.
[2] Dworken (1999).

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 é raro que se realize um ataque.
>
> A vulnerabilidade pode incluir a falta de acesso a um telefone, a um transporte local seguro ou de 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.
>
> A 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.) existem grandes possibilidades de que ele/ela cometa erros ou tome decisões inadequadas que poderiam lhe criar ainda mais problemas de segurança.

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

Capacidades

As capacidades são os pontos fortes e os recursos que 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, boas redes de defensores, e um sistema efetivo para enfrentar o eventual medo, etc.

☞**Na maioria casos, a vulnerabilidade e as capacidades representam duas caras 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.

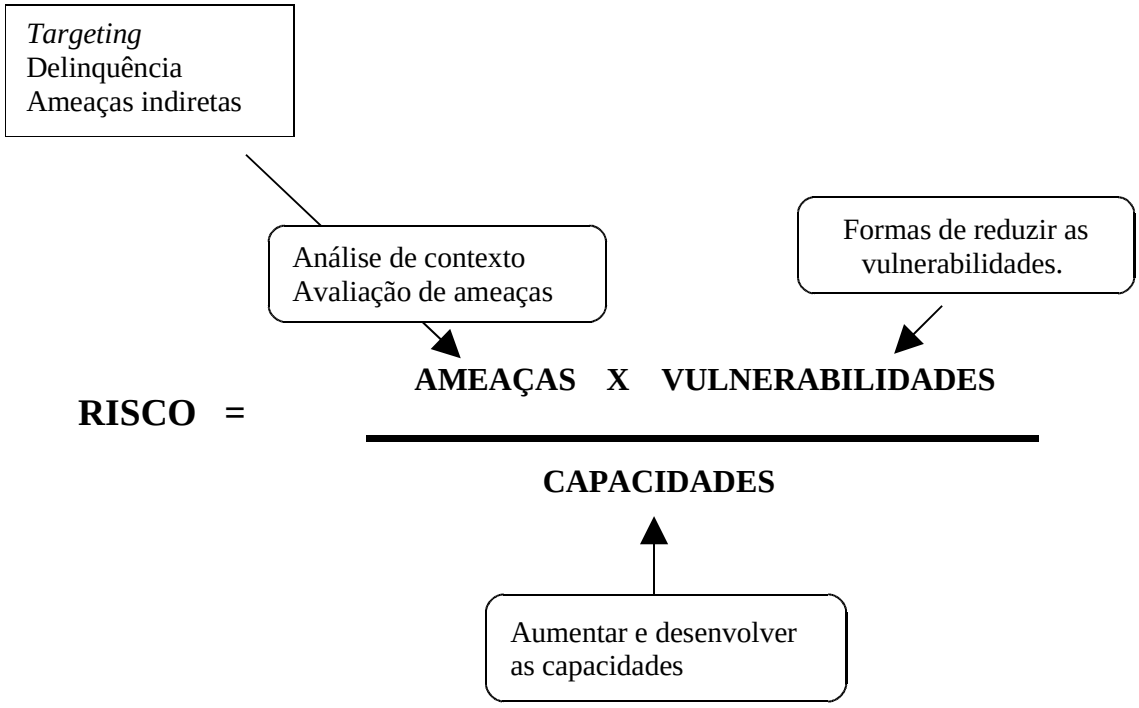
(Ao final do capítulo há uma lista completa de possíveis vulnerabilidades e capacidades)

O risco criado pelas ameaças e vulnerabilidades pode ser reduzido se os defensores dispõem de capacidades suficientes (quanto maior número de capacidades, menor o grau de risco).

$$\textbf{Risco} = \frac{\textbf{ameaças} \times \textbf{vulnerabilidade}}{\textbf{capacidades}}$$

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, quer dizer, as ameaças, nem tampouco à vontade de perpetrá-las, sobretudo em situações onde 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.

> Um 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).

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 a avaliação das vulnerabilidades e capacidades, utilizando como guia a tabela **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 ao invés de enumerar aquelas potenciais ou desejáveis.

Estratégias de enfrentamento e estratégias de resposta

Os defensores e os grupos sob ameaça podem usar diferentes **estratégias de enfrentamento** para tratar com os riscos que suspeitam que deverão enfrentar. Estas estratégias variam muito de acordo com seu ambiente (rural, urbano), o tipo de ameaça, os recursos sociais, econômicos e jurídicos disponíveis, etc.

A maioria das estratégias de enfrentamento podem ser implementadas de forma imediata e em resposta a objetivos de curto prazo. Portanto, funcionarão mais como táticas do que como estratégias de resposta mais elaborada. A maioria das estratégias de enfrentamento responde também a percepções subjetivas de risco pessoal, e em algumas ocasiões poderiam afetar o grupo, sobretudo se as estratégias utilizadas não podem ser alteradas posteriormente. .

As estratégias de enfrentamento estão muito relacionadas com a severidade e o tipo de ameaça, e também com as capacidades e vulnerabilidades do grupo.

Quando pensamos na segurança, é necessário ter em conta tanto nossas próprias estratégias de enfrentamento como as dos demais. É importante reforçar as estratégias efetivas, tentar limitar as que possam afetar negativamente, e procurar respeitar as restantes (em particular as estratégias de enfrentamento vinculadas a crenças culturais ou religiosas).

Algumas estratégias de enfrentamento:

- Reforçar barreiras protetoras, esconder objetos de valor.
- Evitar comportamentos que possam ser questionados por outro ator, sobretudo se o controle do território onde se está localizado se encontra em disputa militar.
- Esconder-se em situações de alto risco (incluindo lugares de difícil acesso, como montanhas ou a selva), mudar de casas, etc. Às vezes, escondem-se famílias inteiras e outras vezes apenas os defensores. Esconder-se pode ser necessário tão somente durante a noite ou pode se estender por várias semanas, e pode ainda implicar num isolamento total.
- Buscar a proteção militar ou política de um dos atores armados.
- Suspender o trabalho, fechar o escritório, evacuar. Mover-se para outra região ou sair do país.
- Confiar na "boa sorte" ou recorrer a crenças "mágicas".
- Ser mais reservado, inclusive com os companheiros, negar as ameaças, evitando falar sobre elas, beber em excesso, trabalhar demasiado, comportamentos erráticos, etc.

Os defensores também têm acesso a estratégias de resposta elaborada. Estas incluem: realizar relatórios ou comunicados para trazer à tona um assunto concreto, apresentar queixa, organizar manifestações, etc. Em muitos casos, estas estratégias não representam uma estratégia de longo prazo, mas respondem a necessidades de curto prazo. Em alguns casos, as estratégias de resposta podem criar problemas de segurança maiores que aqueles que pretendiam abordar inicialmente.

Ao analisar as estratégias de enfrentamento e de resposta, é preciso ter em conta o seguinte:

- **Sensibilidade**: Trarão uma resposta rápida às necessidades de segurança individuais ou do grupo?

- **Adaptabilidade**: estas estratégias se adaptarão rapidamente às novas circunstâncias, uma vez que o perigo de ataque tenha passado? Um defensor pode dispor de várias opções, como por exemplo, esconder-se ou ir viver na casa de outras pessoas por um tempo. Estas estratégias poderiam parecer fracas ou simples, mas resultam ser muito efetivas.

- **Sustentabilidade**: estas estratégias servirão no longo prazo, apesar de ameaças ou de ataques não letais?

- **Efetividade**: Protegerão adequadamente às pessoas ou ao grupo em questão?

- **Reversibilidade**: Se as estratégias não funcionam ou a situação muda, é possível voltar atrás?

<u>Após valorar o risco, o que podemos fazer com os resultados?</u>

Uma vez valorado o risco, é necessário prestar atenção aos resultados. Como é impossível medir a "quantidade" de risco que uma pessoa enfrenta, é necessário compreender e estimar qual é o **nível** de risco existente.

Os diferentes defensores e organizações podem estimar diferentes graus de risco. O que resulta inaceitável para alguns defensores pode ser aceitável para outros, e o mesmo sucede com diferentes pessoas dentro de uma mesma organização. Mais que debater sobre o que "se deveria fazer" ou sobre se é possível seguir adiante ou não, é importante valorar os diferentes limites de risco de cada pessoa: trata-se de encontrar um limite aceitável para todos os membros do grupo.

Dito isto, existem diferentes formas de enfrentar o risco:

- Você pode **aceitar o** risco tal e como se encontra hoje, porque se sente capacitado para “viver com ele”;
- Você pode **reduzir o** risco, concentrando-se nas ameaças, vulnerabilidades e capacidades;
- Você pode **compartilhar** o risco, realizando ações conjuntas com outros defensores para que as ameaças dirigidas somente a um defensor ou organização sejam menos efetivas;
- Você pode decidir **evitar o** risco, mudando ou paralisando suas atividades ou mudando a forma de trabalho para reduzir as ameaças potenciais;
- Você pode **ignorar o** risco, olhando para o outro lado. Não é preciso dizer que esta não é a melhor opção.

É preciso ter em conta que os níveis de risco geralmente são diferentes para cada uma das organizações e indivíduos envolvidos num caso de direitos humanos, e que os agressores visam atacar os pontos mais fracos, por isso, é preciso prestar atenção a estes

diferentes níveis de risco e tomar medidas correspondentes. Tomemos como exemplo o caso de um trabalhador rural assassinado por pistoleiros de um proprietário de terra. Poderia haver várias organizações e indivíduos envolvidos no caso, como um grupo de advogados da capital mais próxima, um sindicato de trabalhadores rurais e três testemunhas (alguns trabalhadores rurais que vivem numa localidade próxima). É imprescindível avaliar os diferentes níveis de risco de cada um destes atores para planejar-se devidamente a segurança de cada um deles.

Tabela 3: Informação necessária para avaliar as vulnerabilidades e as capacidades de um grupo (Nota: no geral, a informação da coluna da direita deve demonstrar um componente em concreto – da coluna da esquerda – é uma vulnerabilidade ou uma capacidade de um defensor ou grupo de defensores específico)

Componentes de vulnerabilidades e capacidades	**Informação necessária para avaliar as vulnerabilidades o capacidades destes componentes**
Componentes geográficos, físicos e técnicos	
Exposição	A necessidade de cruzar ou ficar em zonas perigosas para realizar atividades rotineiras ou ocasionais , com atores ameaçadores nessas zonas.
Estruturas físicas	As características de vida (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? Existem áreas reservadas unicamente ao pessoal? Você trata com desconhecidos que vem a seus escritórios?
Lugares de esconderijo, rotas de escape	Existe algum lugar para 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 o conflito	
Vínculos com as partes em conflito	Existe algum vínculo entre os defensores e as partes em conflito (parentes, vem da mesma zona, interesses comuns) que possa ser utilizado injustamente contra os defensores?
Atividades dos defensores	O trabalho dos defensores afeta de forma direta aos interesses de algum ator? (Como por exemplo no

que afetam a uma parte no conflito	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 com o 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 direito a reclamar seus direitos? Ou estão sujeitos a leis internas repressivas? Podem adquirir suficiente poder/influência para fazer que as autoridades registrem suas reclamações?
Registro, capacidade de manter a contabilidade e os critérios legais	Se é negado aos defensores 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 pirateados?
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 "piratas" de computação? Você pode enviar e receber informação de forma segura?
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 numa blitz ou numa entrevista)
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 inefetivas, 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 8)
Gestão da segurança fora do âmbito laboral (família e tempo livre)	Como manejam os defensores 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).
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 gente 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 dos testemunhos 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)
Capacidade de mobilização	Podem os defensores mobilizar a população em atividades públicas?

Componentes psicológicos (grupo/indivíduos)	
Capacidade para manejar 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 inter-pessoais?
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)?
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 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 das fontes que utilizar? Existe acesso a organizações específicas ou status de membro de alguma organização (por exemplo da ONU ou da OEA) que signifique apoio à capacidade de proteção?
Pessoal e quantidade 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.)
Acesso 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, embaixadas, outros governos, etc, visitantes? Com líderes da comunidade, líderes religiosos, ou outros personagens influentes? Podem realizar ações urgentes através de outros grupos?
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 (meios independentes)? Sabem os defensores como se relacionar com os meios de comunicação corretamente?

Uma balança para medir 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 capacidades no outro prato, veremos como nosso risco aumenta ou se reduz.

Quanto mais vulnerabilidades e ameaças temos, mais risco enfrentamos.

Quanto mais capacidades tenhamos, menos risco enfrentaremos. E para reduzir o risco, também podemos reduzir nossas ameaças e vulnerabilidades, assim como aumentar nossas capacidades.

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

CAPÍTULO 3

CONHECIMENTO E AVALIAÇÃO DAS 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 quebrar 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 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 (quando um defensor próximo a seu trabalho é ameaçado e existem suspeitas críveis de que você poderia ser o próximo), e ameaças **declaradas** (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 que tem seu trabalho, e a maioria das ameaças têm como objetivo ou paralisar o que estejam fazendo o defensor ou ainda forçá-lo a que faça alguma 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 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 a 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.

Sabemos que a ameaça está com freqüência relacionada com o impacto de nosso trabalho. Portanto, a ameaça representa um indicador de como o trabalho 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 dos 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, representam 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 mínimo nível 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 distinguí-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 dois 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.

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 a pessoas-chaves, e até mesmo por meio de relatórios relevantes.

2. **Determinar se existe uma pauta de ameaças ao longo do tempo.** Se foram recebidas várias ameaças sucessivas (como é o caso habitual), é importante examinar as pautas ou 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 de que a ameaça frequentemente 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 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. 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.

Os defensores não são “adivinhadores” e não podem fingir 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 a pior das situações.

Por exemplo: Um defensor dos 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 número1) a um raciocínio cada vez mais especulativo; o segundo passo 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 gera alarme no grupo de defensores, mas geralmente é difícil manter esta percepção de alarme até que ceda realmente a ameaça. 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 “acender a luz vermelha”, ou acionar o alarme, de um grupo quando existirem evidências inequívocas e este estado 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 o seguimento necessário da ameaça e reforçar a confiança do grupo quando for necessário.

Para finalizar, caso a ameaça não se materialize, é necessário proporcionar algum tipo de explicação do porquê, 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 4.
- Após a avaliação de ameaças declaradas, se você avalia que ainda corre o risco de ser atacado, veja o Capítulo 5, sobre a prevenção de ataques.

CAPÍTULO 4

INCIDENTES DE SEGURANÇA: DEFINIÇÃO E ANÁLISE

Objetivo:
Aprender a reconhecer e responder aos incidentes de segurança.

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 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** face 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 → análise → estabelece se se trata de um incidente de segurança → reação como melhor convenha.

Ainda que o tempo apresse este processo, você deve seguir igualmente esta seqüência, apenas de modo mais rápido do que o habitual para evitar atrasos (veja mais informação abaixo).

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. Lembre-se: as ameaças têm um objetivo (veja o Capítulo 2), e os incidentes simplesmente ocorrem.

- ***Todas as ameaças são incidentes de segurança, mas nem todos os incidentes de segurança são ameaças.***

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, estes tipos de incidentes o 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. 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 óbvio 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 é consciente de que ocorreu um incidente de segurança;
- o defensor é consciente deste fato, mas o descarta por sua pouca importância;
- o defensor não informou a organização (ou ainda 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!

<u>Como fazer frente aos incidentes de segurança</u>

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 ou risco de passar por cima de algo. Deve ser designado, ainda, alguém com a responsabilidade de 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 seus colegas e outras pessoas com quem trabalho? Não existe uma única regra 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 como realizamos nosso trabalho no dia-a-dia, sobre nossos **planos** de trabalho, e sobre nossas estratégias mais amplas de trabalho.

*Exemplo de um incidente que proporciona **retro-alimentação** sobre como trabalhar com mais segurança no dia-a-dia:*

É a terceira vez que alguém de sua organização tem problemas ao passar um controle policial, porque, com freqüência, esquece os documentos necessários. Portanto, se decide 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 está 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 supervisionar a situação.

*Exemplo de um incidente que proporciona retro-alimentação sobre as **estratégias mais amplas** de segurança:*
Pouco tempo depois de começar a trabalhar como defensor numa nova zona, 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 zona 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 concluído.

☞ *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 ou 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 re-estabelecer os procedimentos organizativos internos e melhorar as reações posteriores em relação aos incidentes de segurança.

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).

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

  Por exemplo, se um grupo de defensores descobrem 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.

CAPÍTULO 5

PREVENIR E REAGIR AOS 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

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.* 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.

2. *Antecedentes e fatores desencadeadores que levam o atacante a considerar a violência como uma opção.* A maioria dos indivíduos que atacam os defensores consideram a ação de atacar como uma forma de "conseguir um objetivo" ou de "resolver um problema".

3. O *contexto e circunstâncias* que facilitam a violência, ou seja, que permitem que seja implementada ou que não a detém.

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 atacante em potencial. A ameaça aumenta se quem considera o ataque também possui, ou ainda pode desenvolver, a **capacidade de atacar** um defensor.

Alguns ataques vêm precedidos por ameaças, e 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.

- ***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 castigado/a.***

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 3);
- Identificar e analisar os incidentes de segurança (veja o capítulo 4).

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 4).

O objetivo de vigiar os trabalhadores ou seus escritórios é obter informação que possa destinar-se a vários fins como:

- 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, ou pressionar-nos para que deixemos de ver essas pessoas ou de fazer algo ("vigilância demonstrativa").

É importante recordar que a vigilância pode ser necessária para se poder realizar 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 nestes casos tenha havido 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 dispor de 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 são dirigidos a defensores muito envolvidos em temas que

[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.

afetam os agressores. Isto quer dizer que os ataques frequentemente não são casuais ou sem objetivo, mas respondem aos interesses dos atacantes.

- *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 meio 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.

- *Antes de atacar devem ser tomadas certas decisões e optar por diferentes possibilidades.* 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 probabilidade de um ataque

Para poder averiguar a probabilidade de que um ataque seja levado a termo 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]

Quadro 1: Determinar ou grau de ameaça 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	Interesse parcial – nosso trabalho limita seus objetivos	Nosso trabalho obstaculiza claramente seus objetivos,

[2] Esta classificação de ataques inclui as mesmas categorias de ameaças: veja o capítulo sobre ameaças para um esclarecimento.

	objetivos	políticos ou militares	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 influencia 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 possuem nenhum meio 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 o grau de probabilidade de um crime por delinqüência comum

(C = criminosos)

PROBABILIDADE DE ATAQUE POR DELINQUÊNCIA COMUM			
FATORES	**PROBABILIDADE BAIXA**	**PROBABILIDADE MEIA**	**PROBABILIDADE ALTA**
Mobilidade e localização dos C	Os C geralmente permanecem em suas próprias áreas, diferentes das nossas áreas de trabalho	Os C frequentemente 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	Operam	2-4 pessoas operam	Operam em grupos

organização	individualmente ou em pares	juntas	
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 da polícia	Bem formadas e profissionais (podem ter falta de recursos)	Formação regular, salário baixo, recursos limitados	A polícia é ou 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 lenta e ineficazmente, 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 indireto

(AP = Agressores Potenciais)

PROBABILIDADE DE UM ATAQUE INDIRETO			
FATORES	**PROBABILIDADE BAIXA**	**PROBABILIDADE MÉDIA**	**PROBABILIDADE ALTA**
Nosso conhecimento das regiões de combate	Bom	Médio	Temos muito pouco conhecimento sobre a localização das áreas de combate
Proximidade das zonas de combate	Nosso trabalho está longe destas zonas	Nosso trabalho está próximo destas zonas e ocasionalmente se entra nelas	Nosso trabalho se realiza nas áreas de combate
Mobilidade das zonas de combate	As zonas 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 zonas de combate, que variam de forma lenta e previsível. Você trabalha próximo das zonas onde ocorrem enfrentamentos e, ocasionalmente, visita ou fica nas zonas 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 um ataque indireto.

Prevenir um possível ataque direto

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 um ataque ou nas probabilidades de ser capturado e punido.

Assim, para prevenir um ataque é necessário:

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

Este raciocínio para prevenir ataques é paralelo à análise do Capítulo 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.

Quadro 4: Prevenir um ataque direto: resultados esperados das ações de proteção

PREVENIR UM ATAQUE DIRETO: RESULTADOS ESPERADOS DAS AÇÕES DE PROTEÇÃO	
1. Mudanças no comportamento do atacante: dissuadir os atacantes mediante o incremento do custo potencial de um ataque. **2**. **Mudanças no cumprimento da Declaração da ONU sobre os defensores por parte das autoridades responsáveis[3]:** dissuadir os atacantes, aumentando a probabilidade de ação por parte das autoridades para proteger os defensores ou punir os autores de um ataque.	**Confrontar e reduzir as ameaças** (atuando diretamente contra a origem da ameaça, ou contra qualquer ação que parte desta origem)
3. Reduzir a possibilidade de ataque: Reduzir a exposição do defensor, melhorar seu ambiente de trabalho, lidar com estresse ou medo adequadamente, desenvolver planos de segurança, etc.	Reduzir **vulnerabilidades**, 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 requer tempo. Se o risco é muito elevado (quando um ataque direto e severo é iminente) apenas é possível evitá-lo de três modos:

[3] Veja o Capítulo 1. Por exemplo, uma vez que o defensor denunciou as ameaças; a polícia ou algum outro organismo investigará o que ocorreu e esta investigação levará a uma ação contra aqueles que ameaçaram o defensor. Ao menos este poderia ser o objetivo de uma reação para prevenir um ataque.

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[4]).

c) Outra opção seria a de solicitar uma proteção armada, assumindo, para tanto, que haja uma 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 decidiu 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 possibilidade declarar-se isento de suas obrigações. As empresas privadas de segurança podem representar um risco maior se estiverem vinculadas informalmente às forças de Estado (veja o Capítulo 9). No que se refere ao posse de armas por parte dos defensores, devemos mencionar que elas geralmente serão inefetivas 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 anti-terrorista ou de insurgência.

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 frequentemente 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 estar vigiando 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.

[4] Há também situações nas quais viajar representa uma situação de risco maior.

[5] Para mais informação sobre como se assegurar das comunicações veja o Capítulo 13.

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, 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 velhos 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 extremadamente cuidadoso e manter uma distância quando suspeitar que alguém está vigiando-o. Uma vez detectada a vigilância, pode ser colocada em funcionamento a ação recomendada neste manual (veja o Capítulo 9).

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: existem situações que poderiam resultar em vantagem ao relacionar com as forças de segurança que o controlam – 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 comprovar se você está sendo vigiado.
É recomendável comprovar 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 imaginar um maior risco para uma testemunha ou um familiar de uma vítima que o 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 única regra 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 4.

Em todo tipo de ataque há dois pontos primordiais a lembrar:

- 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.

CAPÍTULO 6

PREPARAÇÃO DE UMA ESTRATÉGIA E DE UM PLANO DE SEGURANÇA

Objetivo:
Aprender a elaborar uma estratégia de segurança.
Aprender a traçar um plano de segurança.

Os defensores dos direitos humanos que trabalham em ambientes hostis

São muitos os motivos pelos quais os defensores em geral trabalham muito em ambientes hostis. A maioria dos casos são devidos 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, quanto grupos armados de oposição ou milícias armadas privadas. Estes atores podem realizar todo tipo de represálias para tentar 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 pode depender do trabalho do defensor - algumas atividades podem ser consideradas aceitáveis, outras não.

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 às medidas para melhorar esta segurança. Existem também outras ações sócio-políticas que podem ser aplicadas para melhorar o respeito aos direitos humanos e o ambiente dos defensores dos 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 que não podemos 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 meio tempo, suas capacidades de segurança.

A noção do risco "aceitável" pode mudar com o tempo e varia enormemente para os 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 além disso, é muito sensível a mudanças do ambiente político nacional que o 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 poucos 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, então, atuarem contra eles.

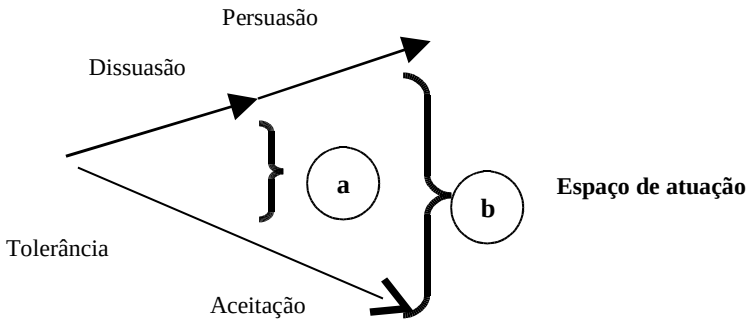
Esta tolerância pode ser **explícita**, como uma permissão formal das autoridades, ou **implícita**, como por exemplo, no caso dos grupos armados. A tolerância será mais alta se o ator vê que o trabalho do defensor pode trazer algum benefício, e será mais baixa se o ator detecta custos relacionados com 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.

---

[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 de trabalho dos defensores com seu acompanhamento protetor.

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, e que aumenta 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 conseguir, por meio de uma estratégia de persuasão, a aceitação do trabalho do defensor, 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 pela 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".

<u>Expandir o espaço de atuação mediante o aumento do contínuo 'tolerância-aceitação'.</u>

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 ao máximo 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 se realiza este trabalho. 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, se reduzirão 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, ele 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 imagem". 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 for 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 agressoes potenciais (veja mais informação abaixo).

Expandir o espaço de atuação mediante a dissuasão e a 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 a 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 obter-se a persuasão. Os defensores utilizam todas estas táticas no âmbito nacional ou internacionalmente em diferentes situações. Evidentemente, os defensores não podem utilizar as "ameaças" diretas: a estratégia se baseia, sobretudo, em recordar aos demais que as decisões que tomam **podem** gerar uma série de conseqüências.

Colocando a dissuasão em marcha

Para poder dissuadir os atores de realizarem ataques, é necessário cumprir com uma série de requisitos:

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 a almejada 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, portanto, 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 fração 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: isto acontece quando a comunidade internacional pode punir os governos, mas eles 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 o 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 dos defensores devem, portanto, desenvolver planos de emergência muito flexíveis e ainda a habilidade de responder com rapidez a acontecimentos inesperados.

Elaborar um plano de segurança

Não é difícil elaborar um plano de segurança. Aqui está o processo representado em somente alguns passos:

1. **Os componentes do plano.** A finalidade do plano de segurança é reduzir seu risco. Portanto, terá, 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.

    Resultaria útil que seu plano incluísse também:

    - Planos preventivos ou protocolos de ação, para assegurar que o trabalho cotidiano se realize sob normas de segurança (por exemplo, como preparar uma denúncia pública ou a visita a uma região remota).
    - Planos de emergência para tratar de problemas específicos, como por exemplo, uma detenção ou um desaparecimento.

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 pela segurança;
    - 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 correria um maior risco com essa ameaça específica.

    - **Faça uma lista das vulnerabilidades correspondentes à lista de ameaças.** Você deve concentrar-se, primeiro, nestas vulnerabilidades, e lembre que nem todas as vulnerabilidades estão relacionadas com todas as ameaças. Por exemplo, se você recebe uma ameaça de morte, não resultará muito prático começar a melhorar as portas do escritório do centro da cidade (a não ser que possam atacá-lo facilmente no escritório, o que não costuma ser o caso). Poderia ser mais prático reduzir sua exposição durante seus deslocamentos de casa ao escritório ou durante os fins de semana. Não é que melhorar as portas não tenha importância, mas esta ação em concreto, seguramente, não reduzirá sua vulnerabilidade ante uma ameaça de morte.

    - **Faça uma lista das capacidades que você possui que se correspondam com a lista de ameaças.**

Agora você está em posição de concentrar-se nas ameaças, nas vulnerabilidades e nas capacidades selecionadas em seu plano de segurança, e pode estar medianamente convencido de poder reduzir seu risco, começando por um lugar adequado.

Não se esqueça de que este é um sistema *ad hoc* para elaborar um plano de segurança. Existem outros métodos "formais" para o fazer, 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 "real"; 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.)*

Enfrentar os desafios de segurança: a gestão de segurança passo a passo

A gestão da segurança não acaba nunca e é sempre parcial e seletiva. Isto é devido aos seguintes fatores:

- A quantidade de informação que se pode absorver tem um limite – não se pode agrupar e lidar simultaneamente com todos os fatores que afetam sua segurança;

- É um processo complexo – é necessário investir tempo e esforço para poder criar uma consciência, desenvolver um consenso, formar as pessoas, administrar a renovação do pessoal, realizar atividades, etc.

A administração da segurança é, sobretudo, prática.

O manejo da segurança raramente consegue um olhar detalhado e de longo prazo. Seu valor se baseia na capacidade de prevenir ataques e de desenvolver estratégias organizativas para confrontá-los. Talvez isto não pareça muito ambicioso, mas é preciso recordar que, de fato, destinamos muito poucos recursos à segurança.

Quando se examinam as práticas de segurança de um defensor ou de uma organização se encontram vários tipos de diretrizes, planos, medidas ou pautas de conduta já estabelecidos. Haverá muitas discrepâncias sobre a segurança, desde idéias estereotipadas sobre as práticas de segurança até resistências em incorporar novas atividades de segurança por temor de incrementar o volume de trabalho existente.

A prática da segurança costuma ser um trabalho fragmentado e intuitivo, sempre em processo de elaboração. O objetivo da administração da segurança é o de ir implantando, gradualmente, diferentes mudanças para melhorar a ação. As normas e procedimentos de segurança costumam originar de diferentes partes da organização que cobrem certas áreas específicas de trabalho, tais como logística, ou uma equipe de campo especialmente preocupada com sua segurança, um diretor sob pressão em função das preocupações dos financiadores sobre a segurança, etc.

Pouco a pouco, o manejo da segurança vai abrindo portas para processos informais e abre também um espaço para a prática de novos métodos. Os eventos inesperados, assim como os incidentes de segurança, requererão decisões urgentes de curto prazo que, se forem realizadas corretamente, podem converter-se em práticas de segurança a longo prazo para toda a organização.

Implementar 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 outra 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 dispõem 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 reclamem mais!"
- "Devemos nos concentrar mais nas pessoas a quem queremos ajudar, não em nós mesmos."

Formas de melhorar a implementação de um plano de segurança

- **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 sempre.
- **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.

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.

- O mandato, a missão e os objetivos gerais da organização.

- 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 que e em que situações.

- Como atuar numa crise de segurança: organizar um comitê ou grupo de crise, delegar um responsável para se responsabilizar pelos meios de comunicação, 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;
  - Incidentes sérios, tais como rapto, desaparecimento, lesão pessoal, etc.;
  - A segurança das testemunhas;
  - A prevenção sanitária e 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 esconderijos (visitantes incluídos).

- Planos de prevenção e protocolos sobre:
  - Preparação de viagens ao campo;
  - Manejo de dinheiro vivo ou de objetos valiosos;
  - Sistemas e protocolos de comunicação;
  - Manutenção de veículos;
  - Minas;
  - Reduzir o risco de ser afetado por crimes comuns, incidentes armados ou ataques sexuais;
  - Reduzir o risco de acidentes em deslocamentos por zonas de risco.

- Planos e protocolos para reagir a crises de segurança, como:
  - 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;
  - Incêndio e outros acidentes;
  - Evacuação;
  - Desastres naturais;
  - Buscas legais ou ilegais ou invasões ilegais em escritórios ou residências;
  - Incidentes armados (se alguém se vê sob disparos, por exemplo, ou num bombardeio);
  - Se matam alguém;
  - Se há um golpe de estado.

CAPÍTULO 7

AVALIAR O RENDIMENTO DA SEGURANÇA DE SUA ORGANIZAÇÃO: A RODA DA SEGURANÇA

Objetivo:
Examinar a forma como lidam com sua segurança.
Avaliar em que grau a segurança está integrada no trabalho de um grupo de defensores dos direitos humanos.

A roda da segurança

Comecemos pelo mais simples: para que uma roda gire corretamente, esta deve ser totalmente redonda. Este ponto é evidente. Mas o que ocorre se ela tem raios mais longos que outros? A roda não será totalmente redonda e, portanto, não girará corretamente.

O mesmo ocorre com a administração da segurança de um grupo ou organização. Se não desenvolvemos, ao mesmo tempo, os principais componentes de segurança, não podemos achar que a estratégia global de segurança funcione corretamente. Partindo desta constatação, podemos elaborar a denominada "roda da segurança", que nos ajudará a analisar como manejamos a segurança, e a avaliar em que grau ela está integrada ao trabalho de um grupo específico de defensores.

Esta avaliação pode ser feita em grupo. Você pode fazer uma lista com as possíveis razões pelas quais certos componentes da roda não foram desenvolvidos suficientemente, e propor diferentes soluções para estes problemas. Uma vez que você tenha enumerado as possíveis soluções, pode iniciar escolhendo as que mais o interessa e colocá-las em prática.

Uma vez completada a avaliação de sua roda da segurança, conserve o resultado e o diagrama. Quando vier a repetir o exercício meses mais tarde, você poderá comparar seu novo diagrama com o anterior e comprovar, ponto por ponto, se a situação melhorou ou não.

Os componentes da roda da segurança

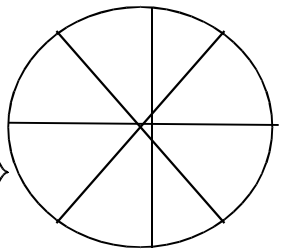
A roda da segurança está composta por 8 raios, ou componentes

Experiência prática: conhecimento prático da segurança e da proteção. Seu ponto de partida e seus objetivos.

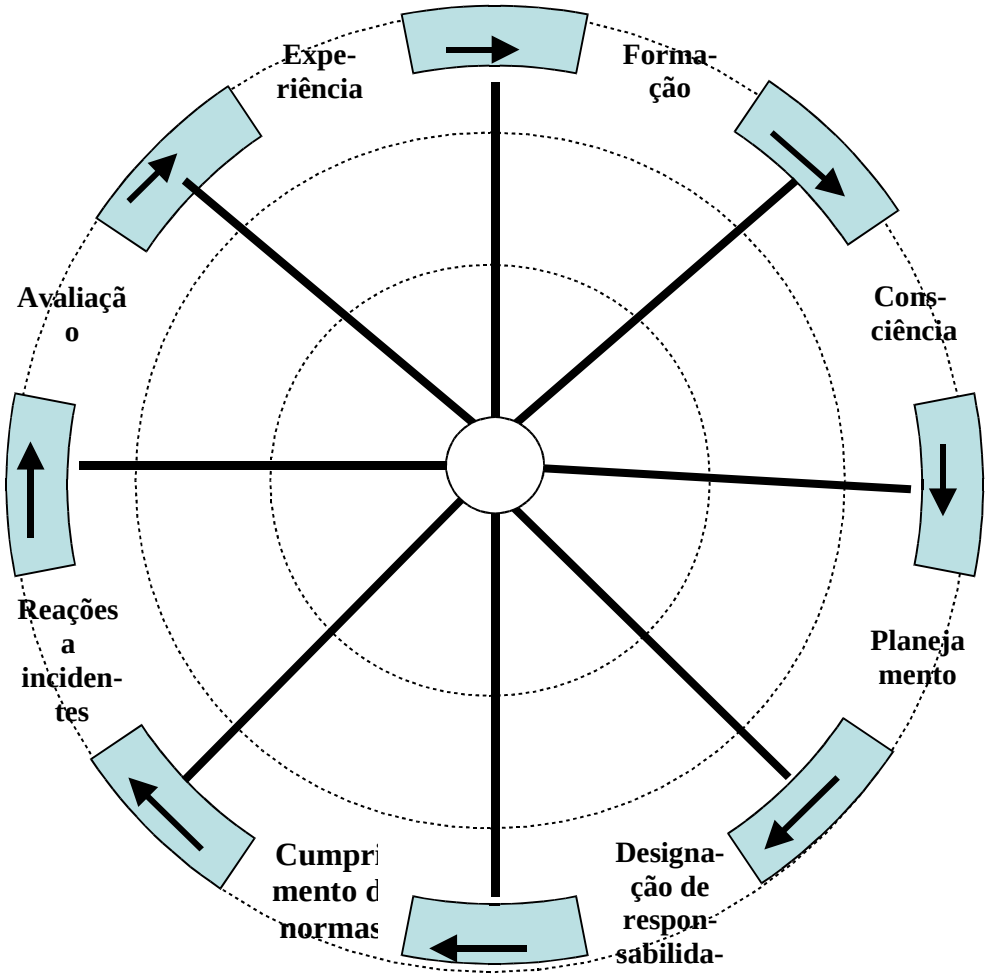
Formação: pode obter formação em segurança com um cursinho ou por iniciativa própria durante seu trabalho diário.

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 garantí-las.

- **Planejamento:** 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 cumprimento 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:** a avaliação da segurança em seu trabalho diário, assim como a de suas reações aos incidentes de segurança, trarão maior conhecimento e experiência às pessoas e organizações.

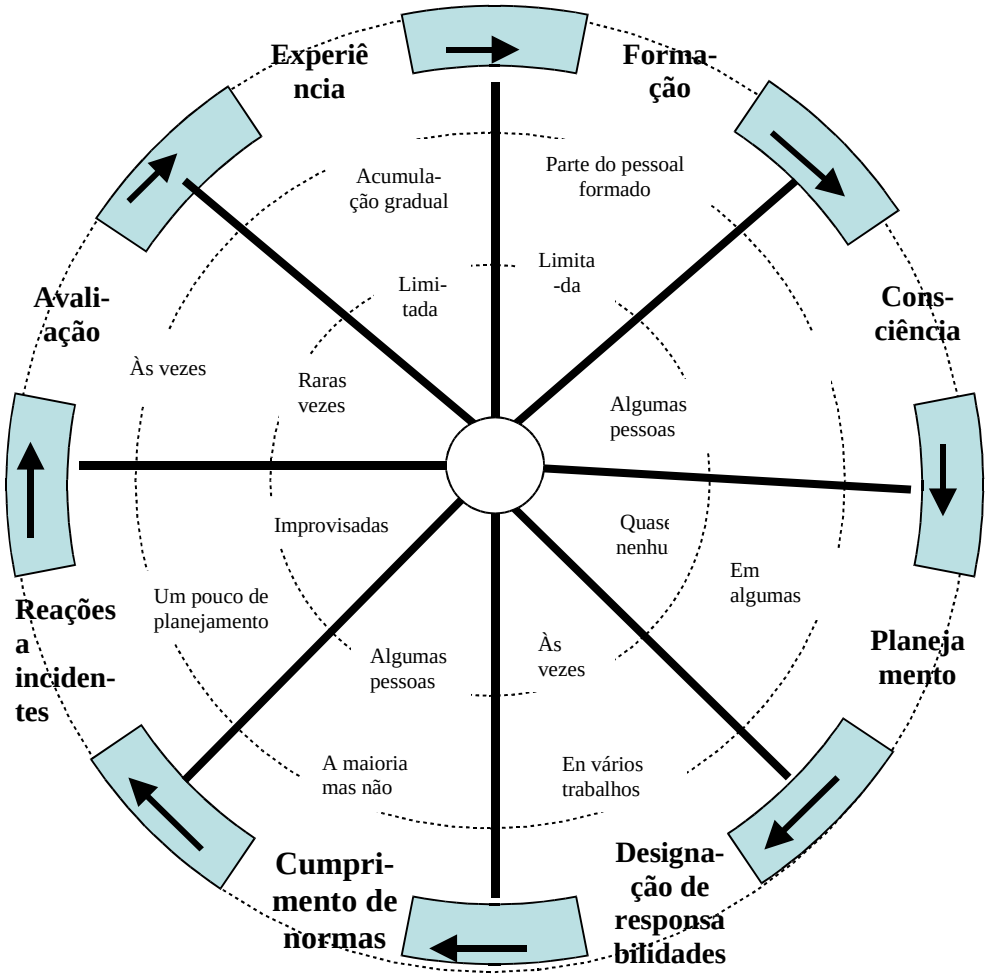


Agora que você está mais familiarizado com os componentes da roda da segurança, tente construir um diagrama adicionando mais informação. Poderia ser assim como este:



A RODA DA SEGURANÇA
E SEUS OITO COMPONENTES, OU RAIOS

A roda da segurança nunca é perfeita: alguns de seus componentes costumam estar 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.

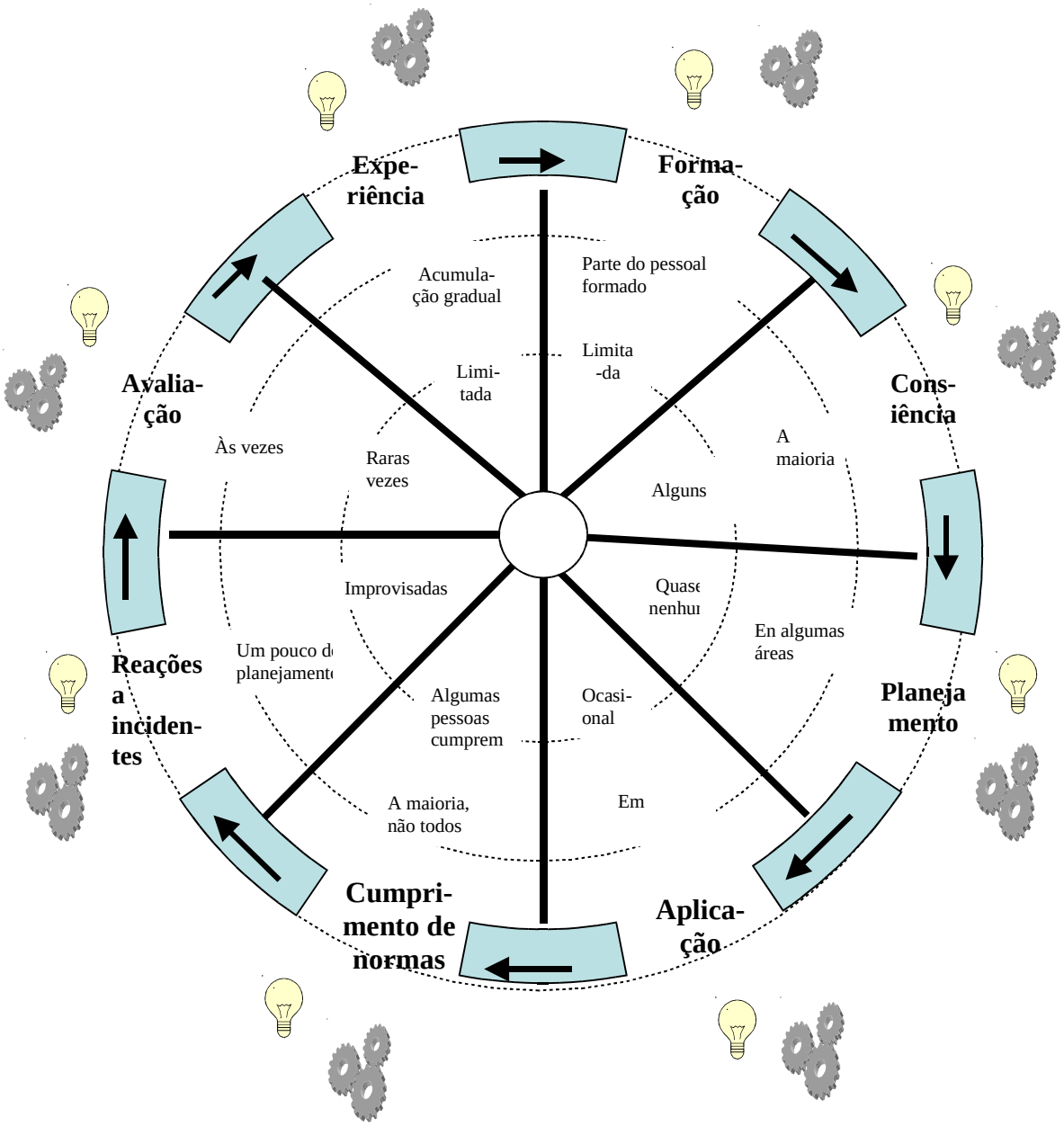


Faça cópia da roda e pinte com cores os espaços entre os raios. Assim, você obterá a estrutura da roda de seu grupo ou sua organização, e isso o ajudará a comprovar que algumas partes estão mais ou menos desenvolvidas.

Se qualquer um dos oito componentes da roda não funcionar você deverá estabelecer:

Quais são os problemas deste componente da roda…

…e quais são as soluções para estes problemas.



CAPÍTULO 8

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 concerne a 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 continuam sem observar as normas de segurança da organização.

Isto poderia parecer incrível, tendo em conta que os defensores dos 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. Poderia suceder também que se ataque uma pessoa cuidadosa, se a pessoa descuidada deixar a porta aberta... Isto vem demonstrar que uma pessoa descuidada pode colocar a todos numa situação de maior risco.

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.

> ☞ ***A segurança é um assunto que concerne a toda a organização, e aos indivíduos que a compõem.***

Um bom plano de segurança não tem sentido se não se cumpre. Sejamos realistas: muita gente não observa as normas ou procedimentos. 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 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 recebido 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 em 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 (porque coincidimos com seu propósito/necessidade, para poder ajudar a proteger aos nossos companheiros e às 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 devem 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 as normas, 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 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 são as normas na prática.

Por que não se observam as normas e procedimentos de segurança?

Não existe um protótipo do defensor dos 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 inefetivas, 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 discordância 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;
- O pessoal tem um grande volume de trabalho e um tempo limitado, e não prioriza nenhuma ou algumas das normas;
- Uma falta de motivação generalizada por causa do estresse, as disputas de trabalho, etc.

A cultura organizacional é tão formal como informal, e deve ser desenvolvida não apenas no todo da organização, mas também nas equipes de trabalho. Uma boa cultura organizacional se reconhece por suas conversas informais, piadas, brincadeiras, festas, etc.

<u>Seguimento do cumprimento das normas e procedimentos de segurança</u>

Seguimento direto:
Podemos incluir as normas e procedimentos nas valorações 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 pode 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 ("Possíveis razões para o descumprimento das normas") pode servir como guia.

2. Se o problema é intencional e está relacionado com 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 seja totalmente conscientizada 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.

Em 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, convidamo-lo 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…

CAPÍTULO 9

MELHORAR A SEGURANÇA NO TRABALHO E NAS RESIDÊNCIAS PARTICULARES

Objetivo:
Avaliar a segurança em escritórios e nas 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 com relação ao trabalho dos defensores dos 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.** Em casos excepcionais, também é necessário proteger o escritório de um possível ataque (um atentado à bomba, por exemplo).

Isto nos leva à primeira consideração geral sobre 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 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 como convenha.

☞ ***A segurança de um escritório é igual a de seu ponto mais fraco.***

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

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 o também "pontos a considerar para uma boa localização" mais abaixo)

É conveniente revisar as medidas de segurança adotadas na vizinhança. 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 se adotem 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 um 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, é perigoso o trajeto que vai do escritório às residências dos trabalhadores, ou a zonas 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.

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 que 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); 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.

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 representa um **filtro** pelo qual deve passar todo indivíduo que deseje 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;
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 valas altas ou baixas, preferivelmente sólidas e o suficientemente

altas 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.

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 todo os possíveis acessos ao telhado, desde o solo ou desde os edifícios vizinhos.

Em lugares com risco de ataque armado, é importante estabelecer zonas de segurança no interior do escritório (veja o Capítulo 11 sobre a 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.

Uma observação sobre as chaves

- Nenhuma chave deve estar visível ou acessível a visitas. Mantenha todas as chaves num armário ou caixa 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 caixa correspondentes, já que isto facilitaria o roubo. É melhor que utilize um código de números, letras ou cores.

Medidas técnicas: iluminação e alarmes

As medidas técnicas como olho mágico, interfones, câmeras de vídeo, apenas **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 se limitarão 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 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 **pilhas,** 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 ativá-lo 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).

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, pode instalar microfones ou permitir o acesso de outras pessoas.

Se decidirem usar os serviços de uma empresa de segurança, vocês devem 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 armas de curto alcance, 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 sócio-político mínimo necessário para poder realizar seu trabalho.

Filtros do procedimento de acesso.
As barreiras físicas devem ser acompanhadas por um "filtro" de um **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 ou 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 por quê 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 dize representar. Lembre que nem um uniforme 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 de sua visita, 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 deveria ser anotado 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 que deixem uma mensagem, que venham, que 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 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 esta gente, 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 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 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.

- *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.

- *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 que?** 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 **detalhe 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 como mínimo todos os miolos da fechadura 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 urgências 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 ondas visitas possam ter acesso a elas. Nunca "esconda" as chaves fora da entrada do escritório – isto as torna acessíveis, não as esconda.

- **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 supervisados em todo momento, enquanto permaneçam no interior do escritório.

- Se você se encontrar com um visitante não autorizado no escritório:
  - Nunca confronte a 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 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 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?

CAPÍTULO 10

A SEGURANÇA E AS MULHERES DEFENSORAS DOS DIREITOS HUMANOS

Objetivo:
Estudar as necessidades de segurança específicas das mulheres defensoras dos direitos humanos.

Na seqüência, trataremos de cobrir alguns aspectos básicos sobre as necessidades específicas das mulheres defensoras dos direitos humanos. Este é um tema que requererá uma análise mais profunda baseada nas experiências de mulheres defensoras dos direitos humanos. Esperamos que sejam produzidos conteúdos mais detalhados sobre este tema no contexto da Conferencia Internacional de Mulheres Defensoras dos Direitos Humanos em 2005.

Mulheres defensoras dos direitos humanos

As mulheres sempre tiveram um papel importante na promoção e proteção dos direitos humanos, ainda que este papel nem sempre tenha sido reconhecido positivamente. As mulheres trabalham sozinhas ou junto a homens na defesa dos direitos humanos.[1] Muitas mulheres pertencem a organizações que trabalham para os desaparecidos e os presos. Outras defendem os direitos dos grupos minoritários ou das vítimas da violência sexual, e outras são sindicalistas, advogadas ou fazem campanha pelo direito à propriedade da terra .

Ataques a mulheres defensoras dos direitos humanos

Em seu Informe anual de 2002 à Comissão de Direitos Humanos Hina Jilani, 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.
>
> 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

[1] Você encontrareá um guia muito prático sobre mulheres defensores dos 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 dos Direitos Humanos, 4-6 abril de 2003*, Publicado por Asia Pacific Forum on Women, Law and Development, e *Atores Esenciáis de Nosso Tempo: os defensores dos direitos humanos nas Américas*, Anistia Internacional.

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 ou 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.

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

Qualquer ato de violência com base no gênero, sexo, que resulta 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)

Se entenderá que a violência contra a mulher abarca os seguintes atos, ainda que sem limitar-se a eles:

a) A violência física, sexual e psicológica que se produza na familia, 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 familia 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 ocurra. (Artigo 2)

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 segurança das mulheres defensoras dos direitos humanos.

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

- *As mulheres podem atrair uma atenção não desejada.*

As mulheres defensoras podem provocar hostilidade porque ser mulher e defensora dos direitos humanos pode desafiar as normas locais culturais, religiosas ou sociais sobre a feminilidade e o papel da mulher.

- *As mulheres defensoras podem ter que infringir leis patriarcais e tabus sociais.*

Em alguns países, a defesa dos direitos das mulheres à vida e a liberdade resultou na violação de vidas e liberdades das próprias defensoras. Em muitas culturas, a exigência de que a mulher mostre respeito ao homem em público pode supor um obstáculo para as mulheres que questionam publicamente atos cometidos por homens que violam os direitos humanos. Certas interpretações discriminatórias ou sexistas de textos religiosos também são utilizadas ao formularem-se leis ou estabelecerem-se práticas que terão uma importante influência nos direitos da mulher.

- *Existem formas de ataque específicas contra mulheres defensoras.*

A hostilidade, assédio e repressão enfrentadas pelas mulheres defensoras podem ser específicas ao gênero, e representam desde abusos verbais dirigidos exclusivamente a elas até o assédio sexual e o estupro. As conseqüências de tais ataques podem ser também específicas ao gênero, tais como a gravidez e o rechaço social.

- *As mulheres defensoras podem sentir-se forçadas a "demonstrar" sua integridade.*

O profissionalismo e a posição social das mulheres podem ser ameaçadas e desacreditadas de formas que são específicas a elas, tais como se colocar em dúvida sua integridade.

- *Os homens defensores poderiam não compreender, ou inclusive rechaçar o trabalho das mulheres defensoras.*

Os colegas masculinos das mulheres defensoras dos direitos humanos podem ter os mesmos preconceitos sociais que os mesmos homens que atacam as mulheres defensoras. Os homens também podem sentir-se ameaçados pela competência profissional de uma mulher. Isto pode levar a tentativas de marginalização ou enfraquecimento das mulheres defensoras dos direitos humanos e, em alguns casos, pode transcender a situações de assédio e violência contra as defensoras, perpetradas por seus colegas.

- *As mulheres defensoras podem ser vítimas da violência doméstica.*

A violência doméstica pode estar vinculada à mudança das estruturas de poder numa família. A ascensão do papel profissional e da atribuição de poder de uma defensora pode fazer com que seu marido, companheiro ou outros familiares se sintam ameaçados e tentem frear suas atividades ou atuar de forma violenta. A violência doméstica contra mulheres inclui todo dano físico, sexual e psicológico que ocorra no seio familiar, como espancamento, estupro marital, mutilação genital feminina e outras práticas tradicionais que sejam danosas para as mulheres (veja abaixo).

- *Obrigações familiares adicionais.*

Muitas mulheres defensoras, aparte de seu trabalho, têm também a responsabilidade de cuidar dos filhos e de outros parentes. Tais responsabilidades, especialmente se inclui filhos pequenos, influirá em muitas das decisões de segurança que a defensora deverá tomar numa situação de alto risco.

- *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 dos direitos humanos

É importante reconhecer que as mulheres defensoras constituem uma grande variedade de mulheres, enfrentando a diferentes problemas, com diferentes antecedentes e que requerem diferentes soluções. O ponto mais importante a se ter em conta é que, em qualquer situação determinada, as mulheres são defensoras dos direitos humanos que podem identificar problemas e encontrar soluções apropriadas. Para que assim seja, é necessária uma maior participação das mulheres, um adequado enfoque de questões de segurança específicas para o gênero e uma formação adequada quando for necessário.

- *Uma participação majoritária de 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 tratar as necessidades de segurança e proteção específicas de gênero.*

Assim como outras necessidades de segurança, é muito importante, em toda organização, que o grupo de defensores determine responsabilidades para tratar 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.

Em resumo, as diferenças nas necessidades de segurança das mulheres estão relacionadas aos diferentes papeis, 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.

Como 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

A prevenção da agressão sexual é similar a dos demais ataques, principalmente aqueles associados com crimes comuns. Os ataques sexuais podem ser usados para reprimir o defensor ou defensora, e as vítimas podem ser escolhidas ou agredidas aproveitando uma situação oportunista.

Todas as pessoas – homens ou mulheres - são vítimas potenciais de uma agressão sexual, mas as mulheres costumam ser um alvo mais freqüente. A agressão sexual é um crime de **poder e** violência, e o contato sexual é um método de o agressor demonstrar seu poder sobre a vítima.

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

Reação frente a uma agressão sexual[2]

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, diarréia, provocar vômito, etc.

[2] 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.

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

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 e sua reação será a apropriada para você e sua situação em concreto.

Após uma agressão sexual

Todas as organizações e grupos defensores dos direitos humanos devem dispor de planos de prevenção e reação para casos de agressões sexuais. O plano de reação deve incluir, no mínimo, a administração de **assistência médica efetiva**, que inclua assistência psicológica, exames de análise imediatos e regulares de doenças sexualmente transmissíveis, a pílula do dia seguinte, etc., e **assistência jurídica.**

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 5.

CAPÍTULO 11

A SEGURANÇA EM ZONAS DE CONFLITO ARMADO

Objetivo:
Reduzir os riscos inerentes às zonas de conflito armado.

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.

É difícil exercer algum tipo de controle sobre uma ação militar em curso, mas se 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, seguramente já estabeleceu 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 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 dos disparos de um ataque com morteiros ou de franco-tiradores.

O risco de entrar na linha de fogo

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 se encontrar na linha de fogo, resulta 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 vidros 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 com cores ou sinais nas paredes ou 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 projéteis sem detonar (*Unexploded ordnance*, UXO)[1]

As minas e projéteis sem detonar 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 estão enterradas 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 sem detonar:**
  - Qualquer tipo de munição que foi disparada mas que não explodiu.

Prevenção contra as minas e os projéteis não detonados.

A única forma de evitar as zonas minadas é sabendo onde estão . Se você não está ou não vive na zona, a única forma de determinar a localização dos campos minados é perguntando de forma continua e ativa aos moradores locais, ou aos especialistas, 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.

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

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

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 longe dos edifícios abandonados.

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

Existem duas regras de ouro:

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

Se precisa se retirar, volte seus passos se eles ainda forem visíveis. Se você viaja num veículo e suspeita que pode haver minas anti-tanques, abandone o veículo e retire-se seguindo 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 pau fino de madeira ou de metal (*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, não corte.

Tudo isso, evidentemente, requer uma quantidade de tempo considerável.[2]

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

CAPÍTULO 12

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.

Manual 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. Você necessita a informação que esta pessoa lhe está dando?
3. Você está num ambiente seguro? É possível que se coloquem microfones escondidos ou outros dispositivos de escuta em áreas que a gente considera seguros, tais como escritórios particulares, ruas com muita circulação, quartos da casa e carros.

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

[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 dos direitos humanos oferecendo cursos e informação. Atualmente a Privaterra está elaborando um manual mais detalhado sobre as comunicações electrônicas e segurança para Front Line, que será publicado em 2005 (este texto foi ligeiramente adaptado em alguns parágrafos por Enrique Eguren).

de grande distância. As cortinas grossas, assim como instalar 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, podem ser encontrados alguns "descartáveis" (microfones ocultos muito baratos, e 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 deve ser examinado cuidadosa e regularmente por algum dispositivo de segurança, já que podem 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 pin, 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 frequentemente, 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. 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.

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.

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 às pessoas que você quis proteger.

A segurança do material de informação do escritório

Mantenha o escritório fechado 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 na calçada.

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. Separe 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.

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

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 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, re-formate 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.

Problemas de segurança com a Internet

Seu e-mail 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!).**

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 e-mail. 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 surfam. O ISP de seu destinatário também pode ser vulnerável, ou ainda sua rede interna ou seu escritório.

Segurança de Internet básica
Os vírus e outros problemas, tais como os "Cavalos de Tróia" ou os "Trojan", podem vir de qualquer parte; inclusive seus amigos podem propagar um vírus sem saber. Utilize um bom programa anti-vírus 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 e-mail (veja abaixo). Os vírus são programas únicos, construídos para replicar e podem ou não ser nocivos. Os "Trojan" são programas construídos para oferecer o acesso de seu computador a terceiros (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 "Trojan" 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 anti-vírus, 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 (cachê). 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 (cachê); 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 devem 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 re-envie um mensagem de um desconhecido, ou originada por um desconhecido. Todas estas mensagens tipo “Tenha pensamentos felizes”, que a gente fica enviando, 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 contem e se é seguro. Desconecte as opções de “download” automático de seu programa de e-mail. Muitos vírus ou “Trojan” se auto-propagam em forma de “vermes” e os vermes modernos costumam ser enviados por um conhecido. Os vermes inteligentes escaneiam 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 o 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 encriptados. 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 que escaneiam e 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.

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, todos 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 declarada 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;
- Disco de encriptação;
- 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 funcionarão se não as utilizarem todo o tempo!

Mas não é necessário apenas dispor do software correto. **As pessoas costumam ser a conexão mais problemática, 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 tiroteio 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 não aumenta ou risco de que se adotem medidas severas contra mim?

R: Ninguém saberá que 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

[3] Por exemplo, PGP – "*Pretty Good Privacy*" (Privacidade Realmente Boa) – é um método conhecido e seguro. Pode ser baixado em http://www.pgpi.org.

ponto de vista militar – 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 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 ocorre?

R: Talvez haja um espião dentro da organização ou alguém sensivelmente 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 descobrí-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 encriptado 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 re-confirmar.

- **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 positivos 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 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 normas:

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" ou programas

O uso de "software" (programa ou aplicativo) pirateado pode expor uma organização à denominada "polícia de software". Os policias 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 anti-vírus 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 como 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 e-mail

A encriptação do e-mail deve converter-se 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 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 e outros

Os correios eletrônicos enviados num texto legível ou decodificados pela Internet, podem ser lidos por muitas partes diferentes. Uma delas é seu Provedor de Internet local (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:

- Proteger um arquivo com uma senha protege tão pouco o arquivo que não merece 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 Washington ou enviá-lo desde um café Internet da África do Sul a um computador do escritório do México.

- 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 anti-vírus. 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. 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.

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[1]

A Assembléia Geral,

Reafirmando a importância da observância dos propósitos e princípios da Carta das Nações Unidas para a promoção e proteção de todos os direitos humanos e as liberdades fundamentais de todos os seres humanos em todos os países do mundo,

Reafirmando também a importância da Declaração Universal de Direitos Humanos e dos Pactos internacionais de direitos humanos como elementos fundamentais dos esforços internacionais para promover o respeito universal e a observância dos direitos humanos e das liberdades fundamentais, assim como a importância dos demais instrumentos de direitos humanos adotados no âmbito do sistema das Nações Unidas e em nível regional,

Destacando que todos os membros da comunidade internacional devem cumprir, conjunta e separadamente, sua obrigação solene de promover e fomentar o respeito dos direitos humanos e das liberdades fundamentais de todos, sem distinção alguma, em particular sem distinção por motivos de raça, cor, sexo, idioma, religião, opinião política ou outra índole, origem nacional ou social, posição econômica, nascimento ou qualquer outra condição social, e reafirmando a importância particular de lograr a cooperação internacional para o cumprimento desta obrigação, de conformidade com a Carta,

Reconhecendo o importante papel que desempenha a cooperação internacional e a valiosa tarefa que levam a cabo os indivíduos, os grupos e as instituições ao contribuir para a eliminação efetiva de todas as violações dos direitos humanos e das liberdades fundamentais dos povos e dos indivíduos, inclusive em relação às violações massivas, flagrantes ou sistemáticas como as que resultam do *apartheid*, de todas as formas de discriminação racial, colonialismo, dominação ou ocupação estrangeira, agressão ou ameaças contra a soberania nacional, a unidade nacional ou a integridade territorial, e a negativa de reconhecer o direito dos povos, a livre determinação e o direito de todos os povos de exercer plena soberania sobre sua riqueza e seus recursos naturais,

Reconhecendo a relação entre a paz e a segurança internacional e o desfrute dos direitos humanos e das liberdades fundamentais, e consciente de que a ausência de paz e segurança internacional não isenta a observância desses direitos,
Reiterando que todos os direitos humanos e as liberdades fundamentais são universalmente indivisíveis e interdependentes e que estão relacionados entre si, devendo-se promover e aplicar de uma maneira justa e eqüitativa, sem prejuízo da aplicação de cada um desses direitos e liberdades,

Destacando que a responsabilidade primordial e o dever de promover e proteger os direitos humanos, e as liberdades fundamentais incumbem ao Estado,

Reconhecendo o direito e o dever dos indivíduos, dos grupos e das instituições de promover o respeito e o conhecimento dos direitos humanos e das liberdades fundamentais no plano nacional e internacional,

[1] Tradução Não Oficial

Declara:

Artigo 1

Toda pessoa tem direito, individual ou coletivamente, de promover e procurar a proteção e a realização dos direitos humanos e das liberdades fundamentais nos planos nacional e internacional.

Artigo 2

1. Os Estados têm a responsabilidade primordial e o dever de proteger, promover e tornar efetivos todos os direitos humanos, e as liberdades fundamentais, entre outras coisas, adotando as medidas necessárias para criar as condições sociais, econômicas, políticas e de outra índole, assim como as garantias jurídicas requeridas para que toda pessoa submetida a sua jurisdição, individual ou coletivamente, possa desfrutar na prática de todos esses direitos e liberdades.

2. Os Estados adotarão as medidas legislativas, administrativas e de outra índole que sejam necessárias para assegurar que os direitos e liberdades referidos nesta presente Declaração estejam efetivamente garantidos.

Artigo 3

O direito interno, enquanto concorda com a Carta das Nações Unidas e outras obrigações internacionais do Estado na esfera dos direitos humanos e das liberdades fundamentais, é o marco jurídico no qual devem se materializar e exercer os direitos humanos e as liberdades fundamentais e no qual devem ser levadas a cabo todas as atividades a que se faz referência nesta presente Declaração para a promoção, proteção e realização efetiva desses direitos e liberdades.

Artigo 4

Nada do que for disposto nesta presente Declaração será interpretado no sentido de que menospreze ou contradiga os propósitos e princípios da Carta das Nações Unidas nem que limite às disposições da Declaração Universal de Direitos Humanos, dos Pactos internacionais de direitos humanos ou de outros instrumentos e compromissos internacionais aplicáveis nesta esfera, ou constitua exceção a elas.

Artigo 5

Com fins de promover e proteger os direitos humanos e as liberdades fundamentais, toda pessoa tem como direito, individual ou coletivamente, no plano nacional e internacional:

a) A reunir-se ou manifestar-se pacificamente;

b) A formar organizações, associações ou grupos não governamentais, e a afiliar-se a esses ou participar em esses;

c) A comunicar-se com as organizações não-governamentais e intergovernamentais.

Artigo 6

Toda pessoa tem direito, individualmente e com outras:

a) A conhecer, buscar, obter, receber e possuir informações sobre todos os direitos humanos e liberdades fundamentais, com a inclusão do acesso à informação sobre os médios pelos quais se dá efeito a tais direitos e liberdades nos sistemas legislativo, judicial e administrativo internos;

b) Conforme o disposto nos instrumentos de direitos humanos e outros instrumentos internacionais aplicáveis, a publicar, distribuir ou difundir livremente à terceiros opiniões, informações e conhecimentos relativos a todos os direitos humanos e as liberdades fundamentais;

c) A estudar e debater se esses direitos e liberdades fundamentais são observados, tanto na lei como na prática, e a formar-se e manter uma opinião a respeito, assim como a chamar a atenção do público para essas questões por conduto desses meios e de outros meios adequados.

Artigo 7

Toda pessoa tem direito, individual ou coletivamente, a desenvolver e debater idéias e princípios novos relacionados com os direitos humanos, e a preconizar sua aceitação.

Artigo 8

1. Toda pessoa tem direito, individual ou coletivamente, a ter a oportunidade efetiva, sobre uma base não discriminatória, de participar no governo de seu país e na gestão dos assuntos públicos.

2. Esse direito compreende, entre outras coisas, o que tem toda pessoa, individual ou coletivamente, a apresentar aos órgãos e organismos governamentais e organizações que se ocupam de assuntos públicos, críticas e propostas para melhorar seu funcionamento, e chamar a atenção sobre qualquer aspecto de seu trabalho que possa obstruir ou impedir a promoção, proteção e realização dos direitos humanos e das liberdades fundamentais.

Artigo 9

1. No exercício dos direitos humanos e das liberdades fundamentais, incluídas na promoção e na proteção dos direitos humanos a que se refere a presente Declaração, toda pessoa tem direito, individual ou coletivamente, a dispor de recursos eficazes e a ser protegida em caso de violação desses direitos.

2. Para tais efeitos, toda pessoa cujos direitos ou liberdades tenham sido violados anteriormente tem o direito, por si mesma ou por conduto de um representante legalmente autorizado, a apresentar uma denúncia ante uma autoridade judicial independente, imparcial e competente ou qualquer outra autoridade estabelecida pela lei e que essa denúncia seja examinada rapidamente em audiência pública, e a obter dessa autoridade uma decisão, de conformidade com a lei, que disponha a reparação,

incluída a indenização correspondente, quando se tenham violado os direitos ou liberdades dessa pessoa, assim como a obter a execução da eventual decisão e sentença, tudo isso sem demoras indevidas.

3. Para os mesmos efeitos, cada um tem o direito, individual ou em associação, a:

a) Denunciar as políticas e ações dos funcionários e órgãos governamentais em relação às violações dos direitos humanos e as liberdades fundamentais mediante petições ou outros meios adequados ante as autoridades judiciais, administrativas ou legislativas internas ou ante qualquer outra autoridade competente prevista no sistema jurídico do Estado, as quais devem emitir sua decisão sobre a denúncia sem demora indevida;

b) Assistir as audiências, os procedimentos ou as audiências públicas para formar uma opinião sobre o cumprimento das normas nacionais e das obrigações dos compromissos internacionais aplicáveis;

c) Oferecer e prestar assistência letrada profissional ou outro assessoramento e assistência, pertinentes para defender os direitos humanos, e as liberdades fundamentais.

4. Para mesmos efeitos, toda pessoa tem o direito, individual ou coletivamente, de conformidade com os instrumentos e procedimentos internacionais aplicáveis, a dirigir-se sem entraves aos organismos internacionais que tenham competência geral ou especial para receber e examinar comunicações sobre questões de direitos humanos e liberdades fundamentais, e a comunicar-se sem impedimentos com eles.

5. O Estado realizará uma investigação rápida e imparcial ou adotará as medidas necessárias para que se leve a cabo uma apuração rigorosa quando existam motivos razoáveis para crer que se produziu uma violação dos direitos humanos e das liberdades fundamentais em qualquer território submetido a sua jurisdição.

Artigo 10

Ninguém participará, por ação ou por descumprimento do dever de atuar, na violação dos direitos humanos e das liberdades fundamentais, e ninguém será punido nem perseguido por negar-se a fazê-lo.

Artigo 11

Toda pessoa, individual ou coletivamente, tem direito ao legítimo exercício de sua ocupação ou profissão. Toda pessoa que, devido a sua profissão, possa afetar a dignidade humana, os direitos humanos, e as liberdades fundamentais de outras pessoas deverá respeitar esses direitos e liberdades e cumprir com as normas nacionais e internacionais de conduta ou ética profissional ou ocupacional que sejam pertinentes.

Artigo 12

1. Toda pessoa tem direito, individual ou coletivamente, a participar em atividades

pacíficas contra as violações dos direitos humanos e das liberdades fundamentais.

2. O Estado garantirá a proteção pelas autoridades competentes de toda pessoa, individual ou coletivamente, frente a toda violência, ameaça, represália, discriminação de fato ou de direito, pressão ou qualquer outra ação arbitrária resultante do exercício legítimo dos direitos mencionados na presente Declaração.

3. Sobre este aspecto, toda pessoa tem direito, individual ou coletivamente, a uma proteção eficaz sob as leis nacionais a resistir ou opor-se, por meios pacíficos à atividades e atos, com inclusão das omissões, imputáveis aos Estados que causem violações dos direitos humanos e das liberdades fundamentais, assim como a atos de violência proferidos por grupos ou particulares que afetem o desfrute dos direitos humanos e das liberdades fundamentais.

Artigo 13

Toda pessoa tem direito, individual ou coletivamente, a solicitar, receber e utilizar recursos com o objetivo expresso de promover e proteger, por meios pacíficos, os direitos humanos e as liberdades fundamentais, em concordância com o Artigo 3 desta presente Declaração.

Artigo 14

1. Incumbe ao Estado a responsabilidade de adotar medidas legislativas, judiciais, administrativas ou de outra índole apropriadas para promover em todas as pessoas submetidas a sua jurisdição a compreensão de seus direitos civis, políticos, econômicos, sociais e culturais.

2. Entre essas medidas figuram as seguintes:

a) A publicação e ampla disponibilidade das leis e regulamentos nacionais e dos instrumentos internacionais básicos de direitos humanos;

b) O pleno acesso em condições de igualdade aos documentos internacionais na esfera dos direitos humanos, inclusive os informes periódicos dos Estados aos órgãos estabelecidos por tratados internacionais sobre direitos humanos nos quais seja Parte, assim como as atas resumidas dos debates e dos informes oficiais desses órgãos.

3. O Estado garantirá e apoiará, quando corresponda, a criação e o desenvolvimento de outras instituições nacionais independentes destinadas a promoção e a proteção dos direitos humanos e das liberdades fundamentais em todo o território submetido a sua jurisdição, como, por exemplo, mediadores, comissões de direitos humanos ou qualquer outro tipo de instituições nacionais.

Artigo 15

Incumbe o Estado a responsabilidade de promover e facilitar o ensino dos direitos humanos e das liberdades fundamentais em todos os níveis de ensino, e de garantir que os que tenham a seu cargo a formação de advogados, funcionários encarregados do cumprimento da lei, pessoal das forças armadas e funcionários públicos incluam

em seus programas de formação elementos apropriados do ensino dos direitos humanos.

Artigo 16

Os particulares, as organizações não-governamentais e as instituições pertinentes têm a importante missão de contribuir na sensibilização do público sobre as questões relativas a todos os direitos humanos e as liberdades fundamentais mediante atividades educativas, capacitação e investigação nessas esferas com o objetivo de fortalecer, entre outras coisas, a compreensão, a tolerância, a paz e as relações de amizade entre as nações e entre todos os grupos raciais e religiosos, tendo em conta as diferentes mentalidades das sociedades e comunidades em que levam a cabo suas atividades.

Artigo 17

No exercício dos direitos e liberdades enunciados na presente Declaração, nenhuma pessoa, individual ou coletivamente, estará sujeita a mais limitações que as que se impõe em conformidade com as obrigações e compromissos internacionais aplicáveis e determine na lei, com o único objetivo de garantir o devido reconhecimento e respeito dos direitos e liberdades alheios e responder às justas exigências da moral, da ordem pública e do bem estar geral de uma sociedade democrática.

Artigo 18

1. Toda pessoa tem deveres para com a comunidade e dentro dela, posto que somente nela pode desenvolver livre e plenamente sua personalidade.

2. Aos indivíduos, grupos, instituições e organizações não-governamentais corresponde uma grande função e uma responsabilidade na proteção da democracia, a promoção dos direitos humanos e às liberdade fundamentais e a contribuição ao fomento e progresso das sociedades, instituições e processos democráticos.

3. Analogamente, lhes corresponde o importante papel e responsabilidade de contribuir, como seja pertinente, na promoção do direito de toda pessoa e uma ordem social e internacional em que os direitos e liberdades enunciados na Declaração Universal dos Direitos Humanos e outros instrumentos de direitos humanos podem ter uma plena aplicação.

Artigo 19

Nada do disposto na presente Declaração será interpretado com o sentido que confira a um indivíduo, grupo ou órgão da sociedade ou qualquer Estado o direito a desenvolver atividades ou realizar atos que tenham como objetivo suprimir os direitos e liberdades, enunciados na presente Declaração.

Artigo 20

Nada do disposto na presente Declaração será interpretado com o sentido que permita aos Estados apoiar e promover atividades de indivíduos, grupos de indivíduos, instituições ou organizações não-governamentais, que estejam em contradição com as

disposições da Carta das Nações Unidas.

Bibliografia selecionada e outros recursos.

Bibliografia selecionada.

• Anistia Internacional (2003): “Atores Essenciais do Nosso Tempo: defensores dos direitos humanos nas Américas”. Seccretariado Internacional AI(Index AI: AMR 01/009/2003/s)
• AVRE and ENS (2002): “Afrontar la amenaza por persecución sindical”. Escuela de Liderazgo Sindical Democrático. Publicado pela 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”. Série de módulos para OFDA/InterAction PVO Security Task Force (Mimeo, incluído em 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”, Luc Reychler e Thania Paffenholz (editores). Lynne Rienner Publishers (London).
• Eguren, E. (2000), “The Protection Gap: Policies and Strategies” *in* 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
• ICRC (1983): Normas Fundamentais das Convenções de Genebra e seus Protocolos Adicionais. Genebra.
• International Council on Human Rights Policy (2002): “Ends and means: Human Rights Approaches to Armed Groups”. Versoix (Suíça). www.international-council.org
• Jacobsen, K. (1999) “A ‘Safety-First’ Approach to Physical Protection in Refugee Camps”. Working Paper # 4 (mimeo).
• Jamal, A. (2000): “Acces to safety? Negotiating protection in a Central Asia emergency. Evaluation and Policy Analysis Unit, UNHCR. Genebra.
• 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): “Afirmacion 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.
• Slim, H. and Eguren, E. (2003): "Humanitarian Protection: An ALNAP guidance booklet". ALNAP. www.alnap.org.uk. London.
• Sustainable Livelihoods Guidance Sheets (2000). DFID. London, February 2000
• Sutton, R. (1999) The policy process: An overview. Working Paper 118. ODI. London.
• UNHCHR (2004): "About Human Rights Defenders": http://www.unhchr.ch/defenders/about1.htm
• UNHCHR (2004): "Human Rights Defenders: Protecting the Right to Defend Human Rights". Fact Sheet no. 29. Genebra.
• UNHCHR (2004): On women defenders: www.unhchr.ch/defenders/tiwomen.htm
• UNHCR (1999): Protecting Refugees: A Field Guide for NGO. Genebra.
• UNHCR (2001): Complementary forms of protection. Global Consultations on International Protection. EC/GC/01/18 4 September 2001
• UNHCR (2002) Strengthening protection capacities in host countries. Global Consultations on International Protection. EC/GC/01/19 * / 19 April 2002
• UNHCR-Department of Field Protection (2002) Designing protection strategies and measuring progress: Checklist for UNHCR staff. Mimeo. Geneva.
• Van Brabant, Koenraad (2000): "Operational Security Managment in Violent Environments". Good Practice Review 8. Humanitarian Practice Network. Overseas Development Institute, London.
• Vincent, M. and Sorensen, B. (eds) (2001) "Caught between borders. Response strategies of the internally displaced". Pluto Press. London.

Outros recursos.

O Escritório Europeu das Brigadas da Paz Internacional (Peace Brigades International) oferece desde o ano 2000 formação e assessoria sobre proteção e segurança para para defensores de direitos humanos, dependendo da disponibilidade de tempo e recursos para isto.
Por favor contate-nos em pbibeo@protectionline.org ou pbibeo@biz.tiscali.be, ou escreva para PBI- European Office, 38, Rue Saint-Christophe, 1000 Bruxelles (Bélgica)
Tel./fax + 32 (0)2 511 14 98
Veja também www.protectionline.org ou www.peacebrigades.org/beo.html

Ver também uma página web com recursos sobre proteção e segurança de defensores de direitos humanos em www.protectionline.org

Front Line apóia a formação e criação de capacidades em segurança e proteção para defensores e publica manuais e materiais em relação a este tema.
Para mais informação acesse www.frontlinedefenders.org ou contate-nos info@frontlinedefenders.org, ou ainda escreva para Front Line, 16 Idrone lane, Off Bath Place, Blackrock, County Dublin, Irlanda

tel.: +353 1212 3750 fax: +353 1212 1001