SEGURANÇA HOLÍSTICA

Um Manual de Estratégias para Defensores de Direitos Humanos

Segurança Holística

Um Manual de Estratégias
para Defensores de
Direitos Humanos

Publicado em inglês em 2016
Traduzido pelo Coletivo Mar1sc0tron
https://mariscotron.libertar.org

1ª impressão: outono de 2018

Editora Subta

Créditos

Autores
Craig Higson Smith do Center for Victims of Torture
Daniel Ó Cluanaigh do Coletivo Tactical Technology
Ali G. Ravi do Front Line Defenders
Peter Steudtner do Coletivo Tactical Technology

Escritos adicionais
Magdalena Freudenschuss do Coletivo Tactical Technology
Sandra Ljubinkovic do Coletivo Tactical Technology
Nora Rehmer do Protection International
Anne Rimmer do Front Line Defenders

Coordenação
Chefe do Projeto - Daniel Ó Cluanaigh
Coordenadora - Hannah Smith
Arte e projeto gráfico - La Loma GbR
Revisão - Johanna Whelehan

Um projeto do
Coletivo Tactical Technology

Em colaboração com
Center for Victims of Torture
Front Line Defenders

Com agradecimento especial a
Wojtek Bogusz, Emilie De Wolf, Jelena Djordjevic, Enrique Eguren, Andrea Figari, Ricardo Gonzalez, Stephanie Hankey, Oktavía Jonsdottir, Becky Kazansky, Tom Longley, Chris Michael, Eleanor Saitta, Bobby Soriano, Niels Ten Oever, Marek Tuszynski, Arjan van der Waal, Pablo Zavala;

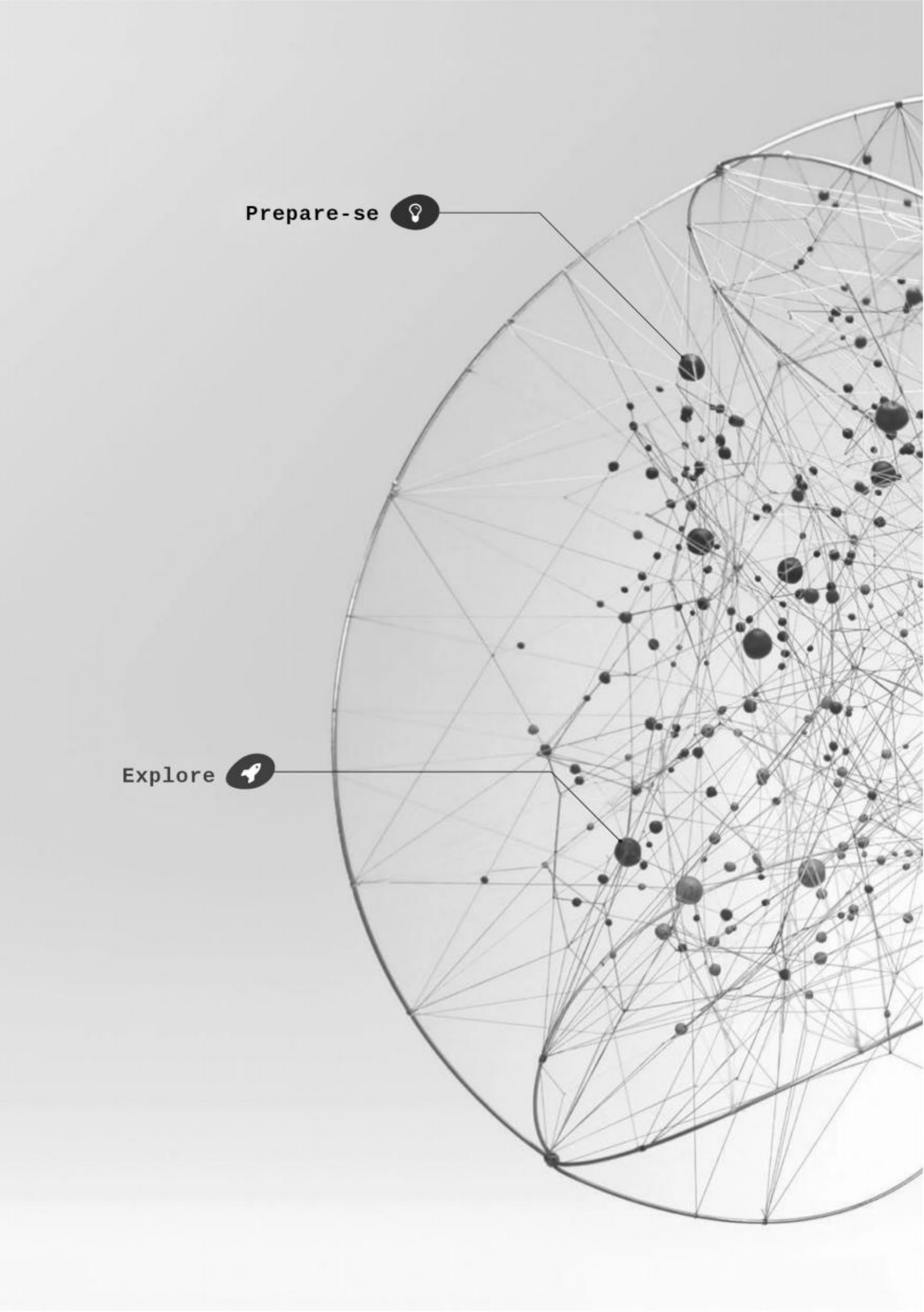
e aos nossos amigos e colegas do
Article 19
Centre for Training and Networking in Nonviolent Action

“Kurve Wustrow”
IREX S.A.F.E Initiative
Protection International
Coletivo Tactical Technology

e à comunidade de treinadores e especialistas em segurança e defensores de direitos humanos com os quais colaboramos e aprendemos durante o processo de criação deste manual.

Patrocinadores
Esta publicação foi produzida com a assistência da União Europeia e o apoio adicional de Hivos.*

* N.T.: a presente tradução não conta com nenhum apoio financeiro institucional, apenas o que tiramos dos nossos próprios bolsos. Distribuímos o livro sob contribuição voluntária (financeira ou não), incluindo a opção gratuita.


Prepare-se
Explore


Ação
Monte Estratégias

Conteúdo

Prefácio

Há poucos dias recebi a notícia de que os 23 ativistas envolvidos nas jornadas de junho de 2013 que haviam sido perseguidos pela polícia do Rio de Janeiro foram sentenciados a 7 anos de prisão. Isso lembrou-me novamente por que o nosso coletivo existe e da importância do que fazemos.

O ano de 2013 foi um aprendizado político para muita gente no Brasil. Porém, na verdade, o que havia começado com uma tradicional manifestação do MPL contra o aumento da passagem logo se transformou em nossa versão local da falência da democracia. Foi algo semelhante ao que estava ocorrendo em outros lugares do mundo como no Movimento de Ocupações de Praças na Espanha e Grécia, o movimento Occupy nos EUA e a Primavera Árabe. Centenas de milhares de pessoas nas ruas tentando desesperadamente ser atores políticos (mesmo que momentaneamente, para em seguida abdicar do poder que conquistaram). Dentro do nosso escopo enquanto coletivo, um dos desdobramentos mais importantes daquele momento aconteceu no que chamamos de tecnopolítica.

Recentemente, foi muito fácil notar a influência recíproca entre tecnologia e política. Em 2018, vimos a manipulação do eleitorado através da influência psicológica massiva usando dados do Facebook. A empresa Cambridge Analytica virou escândalo mundial após a revelação de que os partidários da saída da Inglaterra da União Europeia e da entrada de Trump no governo dos EUA usaram seus serviços para obter a vitória. Esses acontecimentos chamaram atenção para algo que por 40 anos Chomsky vinha tentando denunciar, o Consenso Fabricado. Hoje, alegando temer esse tipo de manipulação e a circulação de notícias falsas nas primeiras eleições pós-golpe, o Supremo Tribunal Eleitoral brasileiro disse que irá recrudescer a “ronda eletrônica” e não cansa de alardear que cancelará as eleições caso for necessário.

Entretanto, nas jornadas de junho de 2013, a interseção entre tecnologia e política seguia outro algoritmo: a vigilância. Foi justamente naquele ano que Snowden revelou o escandaloso uso que a agência de inteligência gringa faz da rede mundial de computadores: uma captura massiva de dados. Descobrimos a *vigilância de arrasto*: não eram mais as pessoas suspeitas ou terroristas em potencial que estavam na mira do Estado, mas absolutamente todos os cidadãos.

A situação é muito mais perturbadora aqui nos países dependentes de infraestrutura tecnológica do que os gringos em geral e Snowden, com seu nacionalismo inocente, pensam: todas as nossas comunicações (serviços como Gmail, Facebook, pagamentos online, etc.) passam pelo território estadunidense – logo, podem ser vigiadas melhor. Através do vazamento que saiu no portal do Wikileaks em 2015, tivemos finalmente a evidência de que a então presidenta Dilma Rousseff estava sendo grampeada pelos tecnocratas da gringolândia desde 2013. Depois dessa, o governo brasileiro anunciou a construção de um cabo submarino dedicado à internet ligando o Brasil diretamente à Europa.

Foi essa a mesma presidenta que, durante sua campanha para a reeleição no final de 2014, afirmava com muita pompa que o mais importante legado da Copa do Mundo realizado nesse mesmo ano no Brasil havia sido a integração dos sistemas de inteligência da Polícia Civil, Polícia Militar, Abin, Departamento Penitenciário Federal, etc. Ou seja, um aparato de vigilância total que estava sendo montado desde 2011 com a desculpa dos megaeventos, Copa e Olimpíadas (2016). Que oportunidade para a democracia mostrar sua função social!

É no meio dessa sequência sinistra de eventos que minam nossa liberdade que surge, então, o coletivo Mariscotron. No final de 2014, nos reunimos e decidimos montar uma oficina sobre *comunicação segura* no hackerspaço local. Tínhamos em vista o uso desleixado e perigoso que ativistas vinham fazendo da internet. Por exemplo, houve chamadas para vandalismo na página de Facebook "oficial" do *black bloc* da cidade do Rio de Janeiro. Nessa época, já

havíamos entendido a necessidade da criptografia, mas ainda estávamos presos na ideia de "qual software vai nos salvar?". Claro, isso é um exagero: nossas oficinas eram longas conversas carregadas de críticas à tecnologia e à "mentalidade de consumidor", essa forma acrítica e "intuitiva" de usar computadores, espertofones e a internet. Conhecimento livre e direitos autorais, código aberto e proprietário, protocolos federados e privados, exposição e anonimato. Em poucos meses, uma compreensão mais aprofundada sobre a diferença entre paranoia e anonimato foi, na minha opinião, o que transformou nosso enfoque. Como a galera do coletivo Saravá dizia, segurança é aquilo que nos protege para agir, enquanto a paranoia é o que nos impede qualquer ação. Eis o salto qualitativo: como os softwares estão sempre nascendo e morrendo (e se transformando, como o caso do Signal que nasceu do protocolo federado OTR, se fechou impedindo a federalização com o LibreSignal, que não usava os serviços da Google, e acabou se "vendendo" para o WhatsApp), a parte prática de nossas oficinas, para além das maravilhosas análises críticas sobre tecnopolítica, passaram a focar em ações que aumentassem a autonomia dos grupos ativistas. Os movimentos por transformação política não podiam ficar reféns de softwares, corporações ou especialistas, nem se paralisar na paranoia da ignorância tecnológica. Era preciso que criassem as condições para tomarem suas próprias boas decisões visando o contexto específico de suas ações.

É aqui que este livro, Segurança Holística, aparece em nosso caminho. Olhar para o conceito de *risco* como aquilo que restringe nosso espaço de trabalho ou de *segurança* como bem-estar em ação foram mudanças cruciais em nossa compreensão de mundo e forma de atuação. Passamos a ter mais confiança em nossa abordagem, assim como manter um foco claro sobre nosso objetivo: promover uma cultura de segurança.

Como toda cultura, essa é um conjunto de ações e compreensões que visa especificamente nossa capacidade de agir bem e manter nossa energia para transformação política. É algo que parte

de cada pessoa, mas que só ganha sentido em coletivo. Sua força se manifesta no campo social.

Os coletivos ambientalistas de ação direta dos anos 1980 resumiram sua cultura de segurança em três frases: não fale o que não precisa ser dito, não pergunte o que não precisa saber e o "não" é uma resposta válida para uma pergunta desnecessária. A segurança holística, entretanto, adicionalmente à infiltração e repressão, traz à nossa atenção o cuidado psicológico, tanto individual como socialmente, para podermos fazer nosso ativismo e mantê-lo operando.

A segurança holística também nos ajudou a pensar contextualmente. Em muitas oficinas durante o início do coletivo, apresentávamos o cenário tecnológico desde uma perspectiva global, onde era preciso atuar em todas as frentes imagináveis. Tínhamos "boas soluções" para senhas, comunicação, aplicativos, reuniões, infiltração, etc. Mesmo sabendo que não existe segurança total, naquela época, a medida do sucesso para nós era o quão perto estávamos do uso absoluto da criptografia e da prática do sigilo. Esse é um enfoque que avalia o inimigo como sendo extremamente poderoso e onipresente. Obviamente, sabíamos das dificuldades de causar uma mudança pública e manter o anonimato ao mesmo tempo. Porém, estando imerso nos desdobramentos dos anos de 2013 e 2014 e frente a violência do Estado e das empresas, isso pareceu o mais sensato. A perseguição política também é parte do jogo democrático. Não existe democracia sem prisões, polícia, fronteiras ou guerra. Qualquer pessoa ou grupo que se posicione contra ou questione o *status quo* mais cedo ou mais tarde sofrerá represálias. A situação recente da Nicarágua é exemplar: uma população que rejeita a perda de direitos é recebida com franco-atiradores. Já são mais de 400 mortos e 260 desaparecidos.

Olhar os riscos contextualmente, então, mudou completamente essa visão. A análise em grupo de nossas capacidades e medidas de segurança atuais, assim como do risco presente em nossas ações deixa mais claro como podemos atuar melhor e trabalhar sobre nossas vulnerabilidades. Quem são nossos aliados e inimi-

gos declarados? Quais atores podem mudar de lado? De onde brota nosso medo quando atuamos? Temos nos alimentado bem? Algo mudou na "normalidade" do dia a dia? Como está nossa comunicação interna, as tensões dentro do grupo? Precisamos de ajuda externa? Temos planos de emergência para eventos chave? Enfim, é uma série de questões que melhora nossa compreensão do que fazemos e estimula nossa criatividade para encontrar saídas não pensadas antes.

Porém, não precisamos descartar nosso acúmulo anterior. Percebi que, no fundo, o que visávamos com uma segurança digital "total" era a preservação de valores muito importantes para a manutenção da liberdade na internet. Ou seja, basicamente defendíamos a circulação livre de informação e não-militarização do espaço virtual. Sabendo que nosso primeiro enfoque era a comunicação segura, usar softwares de código livre e aberto assim como incentivar e defender nossa privacidade (dos de baixo) eram temas recorrentes que continuam fazendo sentido.

Esta tradução é, então, parte de nosso aprendizado. Não somos todas especialistas nem temos diplomas. Durante este trabalho, dividi meu tempo entre escrever, plantar e cozinhar comida, construir uma casa, trabalhar e fortalecer relações, programar software, viajar, tomar banhos de rio, CryptoRaves e tudo o mais que compõe uma vida que busca reduzir as inter-mediações criadas pelo Estado e pelo consumo. Sou grato a minhas amizades, que me acolheram e ajudaram no dia a dia durante a tradução, mesmo não tendo nada a ver com a produção do livro. Este foi meu "financiamento".

Desde o lançamento de Segurança Holística em português na CryptoRave 2018 em São Paulo, começamos a organizar um treinamento para coletivos e grupos de esquerda pela transformação social. Esperamos que o livro contribua para manter nosso ativismo forte e nossas vidas cheias de energia.

Coletivo Mariscotron, inverno de 2018

Introdução

> "Cuidar de mim mesma não é uma indulgência, é autopreservação, e isso é um ato político de guerra."
>
> Audre Lorde

Há duas décadas, a Declaração de Direitos Humanos das Nações Unidas[1] foi adotada pela Assembleia Geral das Nações Unidas, reconhecendo o direito de indivíduos e organizações de (voluntariamente ou profissionalmente) lutar para preservar, promover ou propor direitos humanos, tanto relacionados a elas próprias, quanto a suas comunidades ou causas.

Assim, o termo "defensores de direitos humanos" (DDH) se refere a qualquer pessoa que promova ou defenda qualquer dos diversos direitos, que podem incluir direitos civis e políticos (como liberdade de expressão ou justiça para sobreviventes de abuso); transparência e luta contra a corrupção ou por maior participação política; direitos ambientais, justiça social e direitos culturais; direitos relacionados à orientação sexual e identidade de gênero ou defender o reconhecimento de novos direitos humanos. Independente de suas profissões ou dos direitos humanos que promovem, o reconhecimento do trabalho de defensores de direitos humanos pela lei internacional, assim como pelas leis de vários Estados, dá a DDHs uma camada adicional de proteção para seguirem fazendo seu trabalho.

Infelizmente, defensores de direitos humanos continuam sofrendo ataques tanto do Estado como de atores não estatais. Esses ataques causam impacto em sua integridade física e psicológica, e, além disso, frequentemente também afetam suas amizades e familiares. Aqueles que se opõem ao trabalho de DDHs procuram fechar o espaço para associação livre e pacífica, comunicação, expressão, organização e apoio de sobreviventes de violações de direitos humanos.

1 http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Declaration.aspx

Por exemplo, defensoras de direitos humanos das mulheres frequentemente são alvo (geralmente, de formas sexualizadas) de violência já que seu trabalho desafia discursos, leis e tradições patriarcais. As pessoas que trabalham com os direitos de Lésbicas, Gays, Bissexuais, Transgênero e Intersex (LGBTI) e outras questões relacionadas à orientação sexual e identidade de gênero normalmente são, de maneira similar, atacadas e marginalizadas pelas estruturas existentes de poder. Defensores de direitos ambientais, assim como pessoas que lutam contra corrupção, são alvo de ataques pessoais, econômicos e sociais de companhias privadas que agem através do Estado ou de agentes não estatais. Além de tudo isso, nos últimos anos tem ocorrido um desenvolvimento cada vez maior de mecanismos complexos de vigilância eletrônica que invadiram nossas vidas pessoais e atividades diárias, comunicações e formas de trabalhar. Esse fator é uma ameaça muito grande para defensores de direitos humanos, que podem acabar expostos, ter suas fontes e trabalho ameaçados como resultado de suas atividades *online*.

No vácuo criado pela falta de assistência adequada do Estado, segurança e proteção tornam-se fatores chave para defensores de direitos humanos: em casa, no trabalho e enquanto realizam suas atividades para promover ou defender direitos humanos. O objetivo deste guia é ajudar DDHs a adquirir uma abordagem organizada, construir estratégias para manter seu bem-estar e criar espaços para o ativismo e a resistência, seja quando estiverem trabalhando sozinhos, em pequenos grupos, em coletivos ou em organizações.

Sobre a abordagem holística

Este guia é o primeiro a adotar explicitamente uma abordagem "holística" com relação a segurança e estratégias de proteção para defensores de direitos humanos. Resumidamente, isso significa que ao invés de olhar separadamente para a importância de nossa **segurança digital**, nosso **bem-estar psicossocial** e dos **processos organizaci-**

onais de segurança, essa abordagem tenta integrar tudo isso e destacar suas inter-relações.

Antes, os vários aspectos da segurança de defensores de direitos humanos tendiam a ser tratados separadamente, como se eles existissem isolados um do outro. Entretanto, essa "compartimentalização" de aspectos profundamente inter-relacionados da nossa segurança acaba limitando muito e de várias maneiras nossa capacidade de adotar uma abordagem abrangente, o que inclui:

- A falta de atenção adequada aos aspectos emocionais e psicossociais de segurança frequentemente nos cega para potenciais ameaças, como os efeitos de longo prazo do estresse na nossa saúde. Além disso, promover o bem-estar mental e físico beneficia nossa habilidade de entender nossa situação de segurança e de tomar decisões importantes.
- Com o aumento da vigilância sobre ativistas, a falta de um entendimento adequado das tecnologias digitais que usamos no curso do nosso trabalho pode também limitar enormemente nossa habilidade de perceber com clareza as ameaças que nos cercam. Alcançar esse entendimento e tomar decisões proativas para proteger nossos dados contra acessos não desejados ou contra a vigilância não apenas significa ter uma abordagem mais abrangente da nossa segurança como um todo, mas também nos fornece uma certeza relativa com respeito à fonte das ameaças, que pode ser altamente secreta ou difícil de perceber.
- Adotar medidas de segurança de forma improvisada ou baseada na "tradição" ou no que dizem por aí, sem realizar uma análise do nosso contexto e das ameaças que enfrentamos frequentemente no faz tomar decisões que nos dão uma falsa sensação de segurança. Por isso, é vital que mapeemos regularmente o contexto sociopolítico no qual estamos agindo, identificando o mais precisamente possível as ameaças que enfrentamos e atualizando as estratégias, ferramentas e táticas que podemos usar para defender nosso espaço e continuar trabalhando de maneira empoderadora.

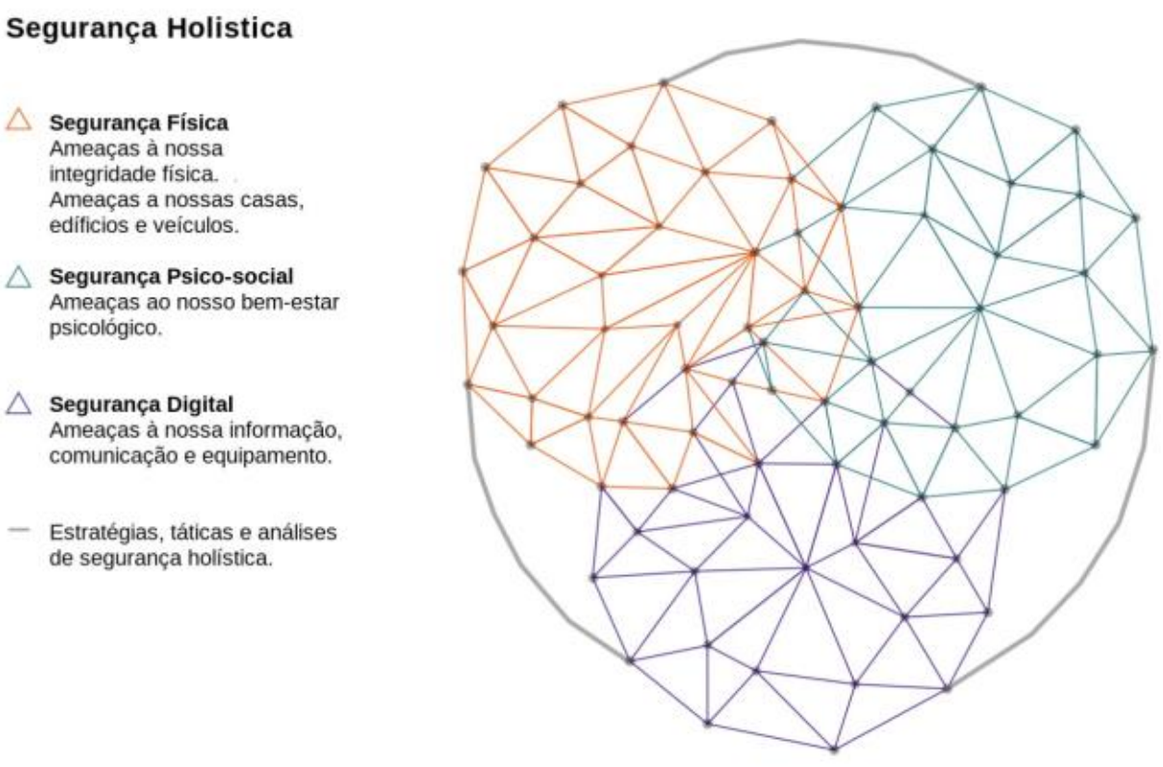
Seguindo o importante trabalho de outras pessoas para estabelecer a abordagem da "Segurança Integrada", a abordagem holística deste manual está fundamentada no entendimento de que "segurança" é um conceito profundamente pessoal, subjetivo e com viés de gênero. De fato, segurança possui um significado especial quando nos encontramos realmente em perigo como resultado de lutarmos por nossos direitos e os direitos daqueles ao nosso redor. Assim, nossa abordagem precisa levar em conta a natureza subjetiva e pessoal de nossa jornada em defesa dos direitos humanos. Qualquer tentativa de realizar uma compreensão "racional" da nossa situação de segurança deve considerar, aceitar e abraçar nossa própria e inerente irracionalidade.

Nossa abordagem de segurança e proteção deve levar em conta os efeitos não apenas da violência física, mas também da violência estrutural, econômica, de gênero e institucional, do assédio e da marginalização. Isso pode ser realizado pelo Estado, mas também por empresas privadas, grupos armados não-estatais ou mesmo pelas nossas próprias comunidades e pessoas próximas. Esses efeitos podem afetar profundamente nosso bem-estar psicológico, nossa saúde física e nossas relações com amizades, família e colegas. Ter consciência e tomar atitudes em relação a essas ameaças é vital para que nosso ativismo e resistência sejam sustentáveis, e para tornar mais fácil que identifiquemos e implementemos estratégias para nossa segurança e proteção. Assim, entendemos e apontamos o autocuidado – muitas vezes considerado como "egoísta" entre ativistas – como um ato político subversivo de autopreservação e fundamental para que tenhamos estratégias e uma cultura de segurança eficientes.

Nossas estratégias de segurança também precisam ser atualizadas regularmente. À medida que o contexto em volta muda, também muda as tarefas e os desafios para integrar a segurança em nosso trabalho. Isso é particularmente verdade numa era na qual nos tornamos cada vez mais dependentes de ferramentas e plataformas digitais para nosso ativismo: computadores, telefones celulares, mí-

dias sociais, câmeras digitais e outras soluções tecnológicas tornaram-se indispensáveis para nosso trabalho, mas elas também trabalham contra nós pois servem como ferramentas de vigilância, identificação e assédio por parte do Estado, de grupos armados, empresas, comunidades e famílias.

Portanto, uma segurança abrangente deve não apenas incluir nossos corpos, emoções e estados mentais, como também as informações eletrônicas contidas nos dispositivos em nossas mãos, bolsos, mochilas, casas, escritórios, ruas e veículos. Não podemos compreender totalmente nossa segurança ou bem-estar sem levar seriamente em conta o papel da dimensão digital em nossas vidas e em nosso ativismo. Portanto, este manual integra explicitamente a necessidade de entender nosso entorno técnico e suas relações com nosso trabalho e nossa segurança.



Prepare-se, Explore e Monte estratégias

O conteúdo desta edição do manual é dividido em três Seções: **Prepare-se**, **Explore**, **Monte Estratégias**. A quarta seção, **Ação**, está disponível *online*. Estes passos foram pensados como um processo **cíclico** e sempre em evolução, que deve ser regularmente revisitado como parte do seu plano estratégico existente.

Em **Prepare-se**, começaremos reconhecendo que cada uma de nós possui e toma medidas de segurança: nossas estratégias para saúde e bem-estar, nossas crenças pessoais e fontes de resiliência e nossas respostas intuitivas a ameaças e perigos. Encorajamos você a considerá-las e também os seus efeitos nas dinâmicas do grupo. Isso deve ser reconhecido para que possamos nos envolver de forma mais produtiva em estratégias de segurança.

Em **Explore**, seguiremos uma série de passos para analisar nosso contexto sociopolítico e chegar a algumas conclusões sobre as ameaças concretas que podem surgir em nosso trabalho e sobre as pessoas que são contra o que fazemos.

Em **Monte Estratégias**, começaremos com as ameaças que identificamos e veremos como criar estratégias de segurança para lidar com essas ameaças, assim como desenvolveremos planos e acordos concretos para manter nosso bem-estar durante a ação.

Ao nos empenharmos nesses três passos, estaremos nos preparando para o quarto: aprender novas ferramentes e táticas para nossa segurança em ação – **Seção IV | Ação**. Para alcançar esse fim, este manual é acompanhado por pequenos guias *online* que analisam cenários específicos focando em ferramentas e táticas concretas – do aspecto tecnológico ao psicossocial e para além disso também – de segurança para atividades particularmente muito arriscadas, algo comum para muitos defensores de direitos humanos.

Como usar este manual

Este manual foi pensado como um guia para o processo de estabelecimento ou melhoria de estratégias de segurança para indivíduos, coletivos ou organizações. Usamos o termo *defensores de direitos humanos* para ser o mais inclusivo possível e esperamos que o manual seja útil para pessoas que trabalham em diversos contextos, de ativistas de base e organizadores comunitários a advogadas, jornalistas e ativistas. Embora seja escrito num formato de narrativa linear, com uma sugestão de estrutura (particularmente para grupos que sejam principiantes na implementação de medidas de segurança como parte de sua estratégia), sinta-se à vontade para focar em qualquer parte do conteúdo que considere útil.

Cada uma das Seções está dividida em alguns pequenos capítulos. A maioria deles está acompanhada por um ou mais exercícios de reflexão que poderão lhe ajudar a conhecer os pontos relevantes do seu próprio contexto. Esses exercícios podem frequentemente ser usados para reflexão individual, mas foram escritos de maneira a também serem realizados por grandes grupos. Dicas foram incluídas para lhe ajudar a facilitar a aplicação dos exercícios em grupo.

Para implementá-los efetivamente em um coletivo ou uma organização, será preciso dedicar de forma regular e consistente tempo e espaço exclusivos para trabalhar na sua segurança e bem-estar como um grupo no contexto do seu ativismo.

O manual foi escrito por um coletivo editorial de treinadores em segurança e estratégia, com a colaboração de um vasto grupo de especialistas e defensores de direitos humanos. Como resultado, a estrutura do manual reflete aquilo que seria utilizado num cenário de treinamento. Os exercícios de cada Seção fornecem um momento de reflexão como indivíduos ou grupos, de maneira a facilitar uma caminhada autônoma em direção à prática da segurança holística sem a necessidade de treinamento e especialistas externos. Convidamos você a usar este manual como um guia e uma base para a sua prática de segurança holística seguindo o ritmo mais adequado a você e/ou sua organização.

A intenção e a motivação por trás da criação e a construção de uma abordagem de segurança holística clara, no sentido de "bem-estar em ação"", é a de tratá-la como um processo iterativo e sempre em evolução onde este manual pode ser visto apenas como um ponto de partida. Assim, priorizamos ser o mais completo possível ao invés de montar um pequeno guia de bolso. Esperamos que um texto longo possa mais tarde ser contextualizado para servir a diferentes audiências com diferentes prioridades e formas de aprendizado. Por essa razão, encorajamos de todo o coração que você nos dê algum retorno, contextualize, copie, melhore e distribua mais amplamente essa versão desse sistema inicial.

O manual tem como base conceitos previamente estabelecidos em diversas fontes existentes incluindo o "***New Protection Manual for Human Rights Defenders***"[2] de Protection International, o "***Workbook on Security for Human Rights Defenders***"[3] de Front Line Defenders, o "***Security in a Box***"[4] dos coletivos Front Line Defenders and Tactical Technology, e o "***Integrated Security Manual***'[5] de Kvinna till Kvinna. Assim, queremos agradecer os autores dos guias citados, a comunidade de defensores de direitos humanos e as pessoas que trabalham pela sua proteção e empoderamento. Esperamos que esse manual contribua positivamente para esse campo de atuação.

Por fim, seremos profundamente gratos por qualquer retorno ou sugestões com respeito a melhorias neste manual e sua metodologia, particularmente daquelas pessoas defensoras de direitos humanos e treinadoras que estejam tentando implementá-lo no curso do seu trabalho. Por favor, não hesite em contatar-nos em ttc@-tacticaltech.org para comentar e sugerir. Poderemos usar suas opiniões nas futuras edições.

---

2 http://protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/

3 https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk

4 https://securityinabox.org

5 http://integratedsecuritymanual.org

PREPARE-SE

Entendendo a
Segurança Holística

I Prepare-se

Entendendo a Segurança Holística

Conteúdo

Introdução

Nesta Seção, daremos os primeiros passos para adotar uma abordagem holística organizada em relação à nossa segurança como defensores de direitos humanos. Para isso, exploraremos primeiro o que de fato a noção de "segurança" significa para nós como defensores de direitos humanos e consideraremos os aspectos dessa noção que podem não ter nos ocorrido antes. O que é "segurança" e o que ela significa quando nos colocamos regularmente em perigo para lutar pacificamente por aquilo que acreditamos?

Embora queiramos organizar melhor nossa abordagem de segurança, não faremos isso começando do zero. Ao invés disso, iremos construí-la com base no que já existe: nossos bem-estar, atitudes, habilidades, conhecimentos e recursos. Exploraremos esses

aspectos nesta Seção. Nela, consideraremos as crenças pessoais que colorem nossa percepção do mundo e que podem ser recursos importantes quando estamos sob ameaças, assim como as respostas instintivas que nossos corpos desenvolveram para responder a elas. Precisamos reconhecer essas crenças para podermos entender melhor a nós mesmas.

Quando sofremos ameaças à nossa segurança, as dinâmicas dos grupos e das organizações em que operamos podem variar de muitas maneiras. Nesse contexto, exploraremos aqui algumas boas práticas para conversar sobre segurança enquanto colegas, grupos, ou organizações.

Em Prepare-se, iremos:

- definir o que significa **segurança** para nós
- explorar o que queremos dizer com **segurança holística**
- refletir sobre nossas **práticas existentes de segurança**
- aprender sobre **reações naturais** ao perigo, suas vantagens e limitações
- explorar algumas respostas a ameaças entre **colegas e dentro de grupos e organizações**
- destacar boas práticas para **conversar sobre segurança** dentro de grupos e organizações.

1
O que é Segurança Holística para Defensores de Direitos Humanos?

Todas as pessoas desejam e precisam de um senso de segurança, de ter a sensação de que estão protegidas. Quando nos sentimos seguras, podemos relaxar nossos corpos, acalmar nossas mentes, descansar e recuperar-nos. Se não conseguimos nos sentir seguras por longos períodos de tempo, é possível que rapidamente nos cansemos,

esgotemos nossa energia e até adoeçamos fisicamente. Como defensores de direitos humanos, às vezes escolhemos sacrificar nosso senso de segurança (pelo menos temporariamente) para lutar por uma sociedade melhor, livre de opressão e exploração. Infelizmente, no curso do nosso trabalho como defensores de direitos humanos, ocasionalmente nos confrontamos com pessoas que irão tentar, talvez através de violência, intimidação e assédio, ou por métodos mais sutis de opressão, evitar que atinjamos nossos objetivos.

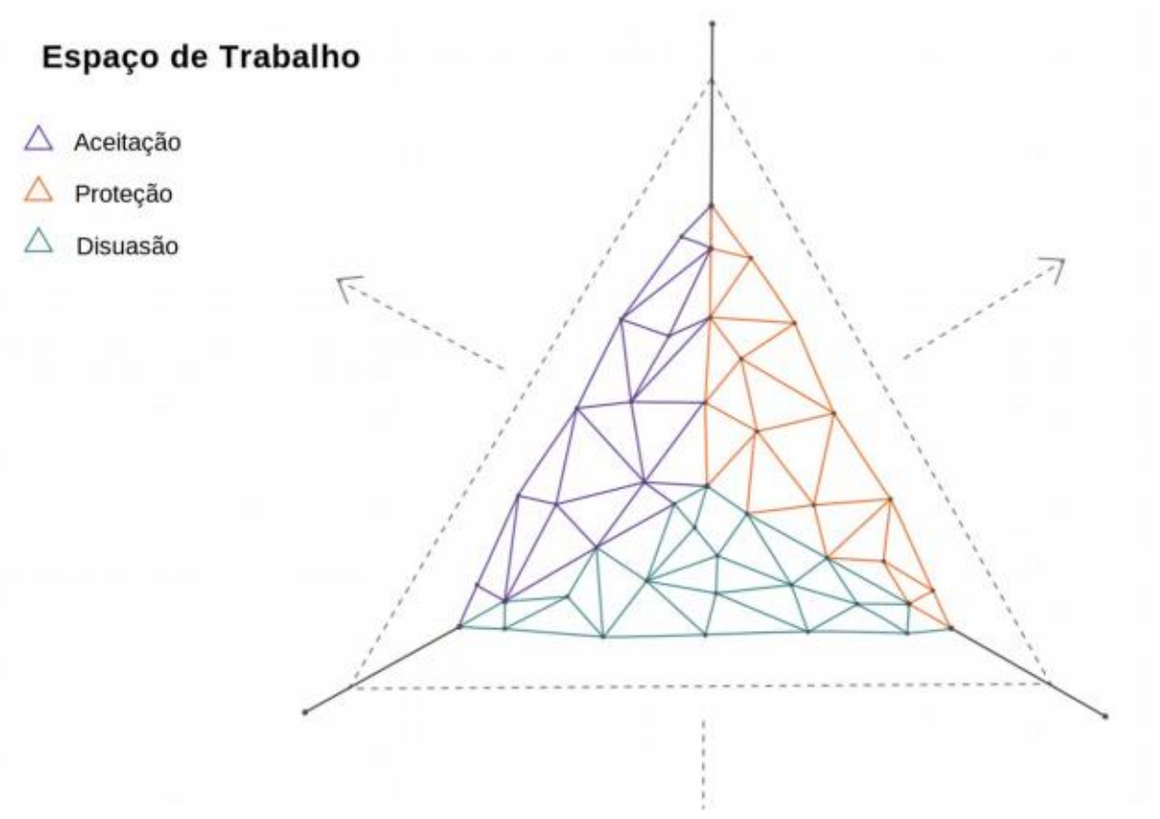
Mantendo e expandindo nosso espaço

Incidentes que vão de prisões, intimidação e ataques violentos, a assédio, calúnia, vigilância e exclusão social, podem ser vistos como tentativas feitas por nossos adversários (aqueles que não compartilham nossos objetivos ou que ativamente se opõem a eles) de limitar ou fechar os espaços nos quais trabalhamos e vivemos. Esses "espaços" podem significar literalmente espaços físicos, incluindo praças e áreas públicas onde grupos podem protestar ou se manifestar, nossos escritórios ou casas, assim como nosso espaço econômico (ao limitar nosso acesso a recursos), nosso espaço social (ao limitar nossa liberdade de expressão ou de associação pacífica), nosso espaço tecnológico (através de censura, vigilância e acesso aos nossos dados), nosso espaço legal (através de assédio judicial, administrativo ou burocrático), nosso espaço ambiental (através da promoção de modelos de "desenvolvimento" que não são sustentáveis), apenas para nomear alguns.

Ao adotar uma abordagem organizada de segurança, nosso objetivo último é defender nosso espaço para trabalhar e, idealmente, expandi-lo para que as sociedades e Estados nos quais operamos mudem em direção ao respeito e à proteção dos direitos humanos.

Para fazer isso, podemos adotar várias táticas e utilizar ferramentas e tecê-las na forma de planos para nossas atividades de direitos humanos. Essas ferramentas e táticas frequentemente correspondem a uma ou mais estratégias para manter e expandir nosso espaço de trabalho: aquelas que encorajam outras pessoas a **aceitar**

nosso trabalho; aquelas que procuram **dissuadir** ataques contra nós, e aquelas com as quais nos **protegemos**.



Essas estratégias abrangentes são explicadas em mais detalhes na **Seção III | Monte Estratégias**.

Bem-estar como subversão e ato político

As ameaças que defensores de direitos humanos enfrentam são variadas e complexas. Talvez estejamos acostumados a pensar sobre segurança em termos estreitos como nos proteger de ataques violentos, invasão de nosso escritório, assédios judiciais ou ameaças de grupos armados.

Embora uma abordagem organizada a esses tipos de ameaças seja muito necessária, uma abordagem holística de segurança vai além disso. Ameaças podem incluir formas estruturais de violência e assédio: marginalização econômica, cargas de trabalho extremamente pesadas, falta de segurança financeira, estresse e expe-

riências traumáticas, entre outros diversos fatores. Tais ameaças não apenas nos afetam, como também têm implicações para as pessoas que estão à nossa volta, incluindo amizades e familiares. Além disso, precisamos reconhecer que ameaças externas afetam não apenas nossa segurança física mas também o espaço entre nós, nossos corpos e nossas mentes, os quais, quando ameaçados, inibem nossa capacidade de realizar nosso trabalho e de sermos felizes fazendo-o. Bem-estar é central não apenas para realizar nosso ativismo de forma eficiente mas também para nossa habilidade de pensar o mais "objetivamente" possível, de analisar e montar estratégias.

Uma abordagem holística de segurança entende que o autocuidado não é egoísmo, mas um ato subversivo e político de autopreservação. A maneira como definimos nosso bem-estar no contexto do ativismo é subjetiva e profundamente pessoal. Ela é influenciada por diferentes necessidades do nosso corpo e de nossa mente, desafios que enfrentamos, nossas crenças (religiosas, espirituais ou seculares), nossas identidades de gênero, interesses e relacionamentos. Como ativistas e defensores de direitos humanos, precisamos definir segurança para nós mesmas e construir nesses termos solidariedade e apoio entre nós dentro de nossos grupos, organizações e movimentos.

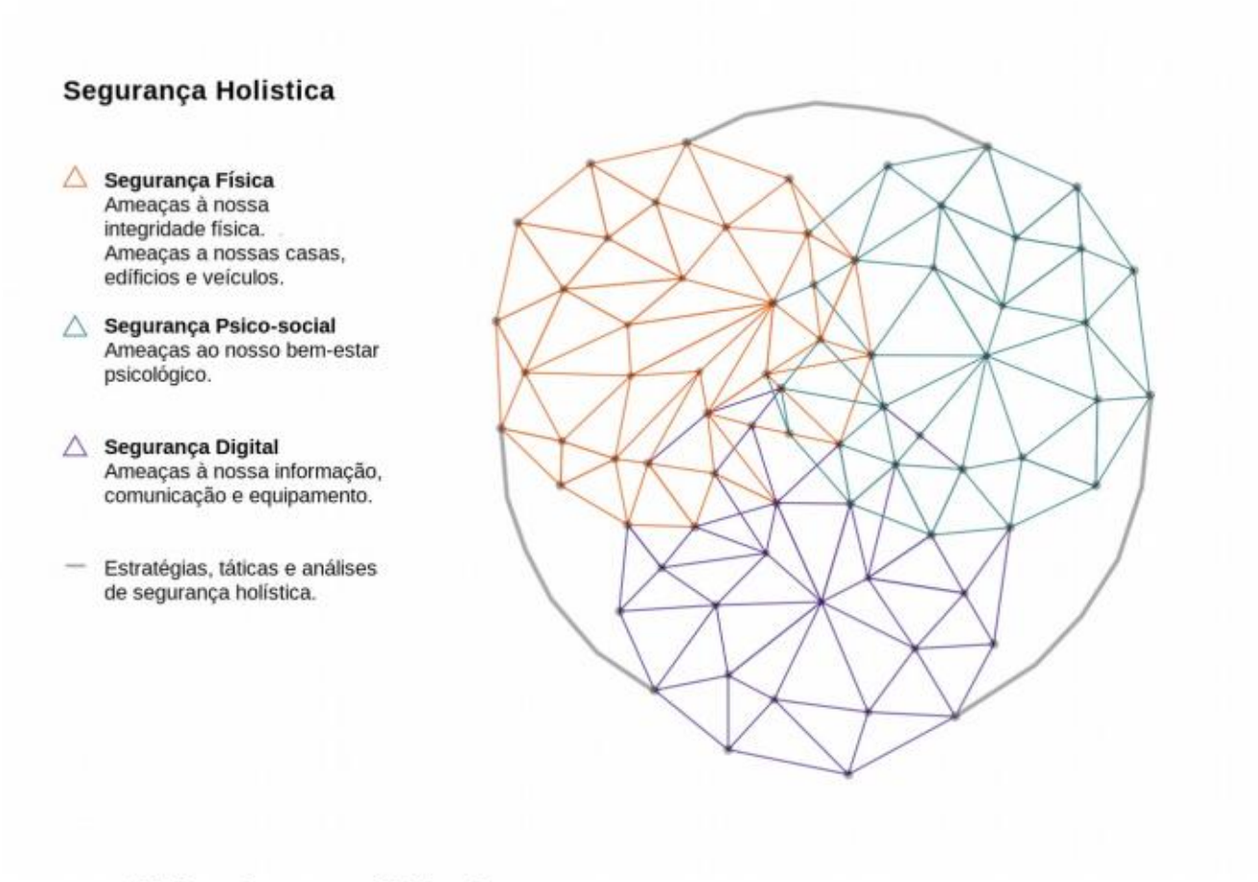
Mesmo com as ameaças ao nosso espaço de trabalho e à nossa expressão pessoal, nós não desistimos: decidimos continuar desafiando as injustiças que vemos no mundo. Por essa razão, **podemos pensar segurança para defensores de direitos humanos como bem-estar em ação**: estar física e emocionalmente saudáveis e sustentar a nós mesmas ao mesmo tempo que continuamos o trabalho que acreditamos ser importante, e realizando a análise e o planejamento necessários para nos mantermos seguras em nossos próprios termos.

Tendo controle sobre nossa informação

Nenhuma abordagem organizada de segurança está completa sem uma abordagem organizada sobre informação e gerenciamento de dados. As ferramentas que dependemos para gerenciar nossas informações – digitais e analógicas – também fazem parte do nosso espaço de trabalho e estão sujeitas a muitas das mesmas ameaças que enfrentamos em outras áreas.

Amplamente despercebida e operando a portas fechadas, a vigilância industrial passou por um enorme crescimento desde a virada do século. O acesso aos nossos dados sensíveis (os arquivos que gerenciamos, nossos emails e comunicações via celular, etc.) é mais importante que nunca para aqueles que procuram impedir o trabalho de defensores de direitos humanos. Igualmente, agora a dimensão digital constitui uma enorme parte de nossas vidas, e ainda assim muitos de nós acham que ela não está sob nosso controle ou tratam-na como algo que não possui um impacto "real" em nossa segurança. Devemos desafiar essas percepções; precisamos identificar nossos dados que são sensíveis, entender onde estão guardados e quem tem acesso a eles antes de levar a cabo um processo de implementação de formas de protegê-los. Isso não é apenas uma medida de segurança, mas também um ato político de auto-empoderamento.

Assim, a prática da segurança holística se refere à conservação do nosso bem-estar e da nossa capacidade de ação (nossa agência) como defensores de direitos humanos, de nossas famílias e comunidades. Buscaremos isso através do uso consistente de ferramentas psicossociais, físicas, digitais e outras táticas para que possamos nos reforçar (ao invés de nos contradizer) umas às outras. Essas táticas nos permitem aumentar nossa segurança geral, mitigar as ameaças que enfrentamos e expandir as escolhas que somos capazes de fazer no dia a dia.



Resiliência e agilidade

É bom ter em mente que as ameaças e os desafios do mundo ao nosso redor estão sempre mudando. Isso é particularmente verdade para defensores de direitos humanos. Precisamos evitar cair na armadilha de pensar que podemos ter um único plano para tudo. Infelizmente, devido ao nosso trabalho, eventos “inesperados” são quase uma norma para muitas de nós e as comunidades ativistas precisam ser capazes de desenvolver a flexibilidade emocional e mental necessárias para lidar com isso. Cultivar um forte senso de bem-estar e se sentir mental e emocionalmente centrada é crítico num contexto onde os riscos e ameaças que encontramos são na maioria das vezes imprevisíveis.

Dado que as necessidades e demandas do ativismo podem frustrar até os melhores planos de segurança, uma abordagem mais realista não significa ignorar o inesperado, mas incorporá-lo em nossas respostas. Neste sentido, não é suficiente apenas desenvolver um plano de segurança e segui-lo ao pé da letra. Pelo contrário, é melhor trabalhar com o inesperado e desenvolver outros atributos

como presença de espírito ou centramento para aguçar nossa habilidade de lidar com ele.

Normalmente continuamos a fazer nosso trabalho mesmo sabendo dos riscos inerentes a ele. De fato, é a nossa vulnerabilidade que nos mantêm conectadas com as experiências das pessoas cujos direitos estão sendo violados. Não é possível tornar-nos completamente "seguras" e talvez isso nem seja desejável. Com isso em mente, também precisamos construir **resiliência** e **agilidade**. Resiliência é a habilidade de se recuperar rapidamente de complicações ou danos. Agilidade é a habilidade de adotar rapidamente novas práticas de segurança em resposta a novas ou emergentes ameaças. O objetivo não é estar segura não fazendo nada, mas enfrentar conscientemente as ameaças e proteger a nós mesmas e a nossas comunidades o máximo possível para que possamos continuar a nos engajar e sermos ativas.

Para a maioria dos defensores de direitos humanos em risco, as noções de resiliência e agilidade não são novas, nem a ideia de ter ferramentas e táticas para manter-se seguro durante um trabalho perigoso. Neste primeiro exercício, iremos explorar algumas das práticas existentes que temos para estarmos seguros.

Nota: os exercícios ao longo deste manual podem ser feitos tanto sozinha quanto em grupo. Em alguns tipos de grupos, os assuntos levantados podem ser delicados ou causar divisão. Assim, é importante que você crie um espaço "seguro" onde cada pessoa do grupo se sinta confortável para falar e compartilhar suas próprias opiniões e que haja uma atmosfera geral de confiança. Algumas dicas sobre como criar um espaço seguro incluem estabelecer acordos compartilhados no início de uma conversa, estar ciente de que é OK ter opiniões diferentes, assegurar que todos os membros do grupo sejam ouvidos e que cada contribuição seja tratada como igualmente válida.

1.1 Exercício

Refletindo sobre as práticas de segurança existentes

Propósito & Resultado

Este exercício nos ajudará a refletir sobre o que significa segurança para você e a explorar as táticas, planos e estratégias de segurança que você consciente ou inconscientemente já tem.

Teremos uma "fotografia" das nossas práticas existentes, de como elas interagem entre si e de como podemos usá-las como uma base para os próximos passos.

Informações de entrada & Materiais

Se você deseja documentar os resultados do exercício, escreva as respostas num cartão ou em notas para colar na parede.

Formato & Passos

Reflexão individual ou discussão em grupo

Pergunte a si mesma ou ao grupo as seguintes questões:

1. Pense sobre a palavra "segurança" ou "proteção". O que isso significa para você? O que você precisa para se sentir segura ou protegida?
1. O que você faz todos os dias para evitar perigos e proteger a si mesma, sua propriedade, suas amizades ou família?
2. Quando foi a última vez que você fez algo que lhe deu a sensação de estar segura e forte?
3. Lembre de uma atividade perigosa que você participou. O que você fez para se manter segura?
4. Quais outras pessoas são importantes para lhe ajudar a se sentir segura ou protegida?
5. Quais recursos ou atividades são importantes para lhe ajudar a se sentir segura ou protegida?

Anote suas respostas pois elas serão úteis nos próximos exercícios e lhe ajudarão a lembrar que você não constrói novas práticas do zero.

Lembretes & Dicas

Seus colegas podem se sentir estranhos falando sobre "segurança" se não existe nenhuma cultura organizacional preexistente para falar sobre esses assuntos. Mesmo assim, este exercício pode se usado para iniciar esse processo de conscientização.

O exercício em si pode dar início ao processo de gerar ideias sobre o que precisa melhorar ou ser adicionado às suas práticas de segurança. Pode ser que você queria tomar notas sobre isso para se preparar para a **Seção III | Monte Estratégias** que está focada em planejamento.

Como ativistas, pode ser que tenhamos pouca atenção consciente sobre segurança e apenas notemos passivamente a falta de perigo ou a sensação de insegurança. Aos nos referirmos à segurança holística como "bem-estar em ação", nos propomos a ser mais conscientes sobre segurança desde uma perspectiva empoderadora e criar uma experiência integrada ao colocar a segurança como parte da nossa percepção diária, estando atentas a ameaças, nossos sentimentos, reflexões e práticas influenciadas pelas comunidades onde vivemos e trabalhamos.

No restante da **Seção I | Prepare-se**, começaremos os preparativos para uma abordagem mais abrangente e organizada de segurança. Partiremos de um exame de como as pessoas reagem psicologicamente a perigos e ameaças e de que maneiras isso afeta nossa percepção, nossa visão de mundo e, consequentemente, nossas ações. Em seguida, exploraremos como é trabalhar em grupos sob estresse e perigo e como dinâmicas positivas (e negativas) emergem nesse contexto, e como influenciarão nossa segurança.

2
Respostas Individuais a Ameaças

Organizar uma abordagem de segurança significa, em sua maior parte, desenvolver uma maior precisão para perceber e analisar ameaças e escolher meios de evitá-las. Entretanto, não precisamos desenvolver essa percepção do zero: já temos respostas psicológicas para ameaças que devem ser compreendidas e reconhecidas. Além disso, nossa percepção e habilidade de analisar podem ser desafiadas por alguns aspectos do nosso trabalho. Se ao menos estamos conscientes deles, isso nos ajudará a fazer planos mais realistas.

As pessoas possuem mecanismos de defesas naturais, desenvolvidos durante nosso processo evolutivo. Possuímos caminhos neurais e estruturas inatas com a função primária de nos manter vivas quando estamos sob ameaça. Essas funções estão frequentemente abaixo do nível da nossa atenção consciente; ou seja, nossos processos de segurança estão operando mesmo que não estejamos atentas a eles. Isso se aplica tanto para quando estamos sob ameaça quanto, indiretamente, quando alguém perto de nós está ameaçada.

Um dos nossos mecanismos de sobrevivência é geralmente chamado de intuição. São aquelas sensações poderosas mas aparentemente irracionais que às vezes temos sobre uma pessoa, lugar ou atividade específicas. Quando nossa intuição nos avisa sobre algo não confiável ou um perigo, geralmente é porque conseguimos reconhecer múltiplos e sutis **indicadores** que sozinhos não servem para identificar um perigo em particular, mas que juntos, sugerem fortemente que estamos na presença de uma ameaça. Muitos defensores de direitos humanos já se salvaram por terem prestado atenção à sua intuição ou por terem "confiado no seu estômago", mesmo quando não conseguiram explicar como sabiam que estavam em perigo.

Intuições sobre perigo produzem uma sensação de **ansiedade**. Embora ansiedade seja um sentimento desconfortável, ela é extremamente útil. Ansiedade nos provoca a agir para reduzir nosso desconforto. Quando nos sentimos ansiosas, procuramos ativamente informações que possam confirmar ou desafiar a possibilidade de que estamos em uma situação potencialmente nociva ou perigosa. Dependendo do que aprendemos no passado, nossa ansiedade pode se transformar em medo.

Quando sentimos medo, mostramos poderosas **respostas de sobrevivência**. Estas respostas são movidas pelas mesmas estruturas cerebrais e impulsionadas por mudanças biológicas. Quando isso acontece, muito do nosso comportamento se torna automático, no sentido de que temos menos consciência de escolher agir de uma forma específica. Respostas comuns de sobrevivência incluem as seguintes reações:

1. **"Paralisia"** é quando uma pessoa fica completamente imóvel ao mesmo tempo em que está altamente alerta e preparada para ação. Essa reação se baseia na possibilidade de fuga até que o perigo tenha passado. Por exemplo, pode ser que paremos de trabalhar, de nos comunicar pelos meios que geralmente usamos, ou diminuir a comunicação com alguém com quem temos um conflito. Em cada caso, esperamos que a atenção indesejada passará se ficarmos inativas.

2. **"Fuga"** é quando uma pessoa tenta rapidamente ir para o mais longe possível do perigo. Podemos mover nossas operações para um local mais seguro, abandonar certas atividades ou formas de comunicação ou nos separar de pessoas que podem nos machucar.

3. **A reação de "obediência"** envolve fazer o que um agressor diz na esperança de que a cooperação resultará no término do ata-

que de maneira rápida e com menos danos. Podemos concordar em suspender ou abandonar certos objetivos ou atividades, ou ceder senhas que protegem informações sensíveis.

4. A reação de "cuidar" acontece quando uma pessoa tenta proteger outra mais vulnerável que também está sofrendo. Muitos defensores de direitos humanos são motivados a ajudar as outras pessoas por causa das suas próprias experiências de opressão e exploração.

5. A reação de "tornar-se amigo" envolve tentar construir algum tipo de relação com o agressor na esperança de que isso limitará o dano causado contra si ou outras pessoas. Ao contar sobre nossas famílias a agressores fisicamente presentes, estamos tentando nos humanizar para eles, uma estratégia que às vezes é útil para reduzir a violência.

6. "Pose" é uma tentativa de distanciar o perigo fingindo ter maior poder do que na verdade se tem. Como defensores de direitos humanos, frequentemente ameaçamos expor e tornar públicas as ameaças de violência que recebemos como forma de constranger publicamente nossos adversários.

7. A reação de "luta" é quando uma pessoa ataca com a intenção de distanciar ou destruir o agressor. É claro que existem muitos jeitos diferentes de lutar e cada uma de nós faz suas escolhas quanto a isso.

O que é importante notar é que quando nos envolvemos numa resposta de sobrevivência, nos tornamos mais rápidas, fortes, focadas e mais resilientes do que normalmente somos. Como resultado, essas estratégias de sobrevivência são extremamente eficientes em muitas circunstâncias. Elas nos ajudam a lembrar que mesmo que você

possa estar apenas começando a desenvolver sua própria abordagem organizada de segurança, seus mecanismos naturais de sobrevivência já estão funcionando fortemente.

Mas por mais poderosas que nossas repostas sejam, elas não são perfeitas. Embora nossos cérebros sejam capazes de processar quantidades enormes de informação e de reagir muito rápido, eles não fazem isso de maneira sistemática e lógica. Existem algumas situações nas quais nossos cérebros não são particularmente confiáveis e devemos prestar uma atenção especial a elas.

Ameaças na esfera digital

Uma das formas que podemos ficar na mão devido a nossas reações psicológicas, como discutido acima, diz respeito à segurança digital e da informação. Estamos muito bem adaptadas para responder a ameaças físicas (tais como nos defender contra um ataque), ou ameaças interpessoais (tais como enfrentar o distanciamento de nossos familiares) e como resultado, temos fortes reações intuitivas e emocionais a esses tipos de perigo.

Entretanto, apesar dos mundos físico e digital estarem intimamente entrelaçados, podemos ter dificuldades em identificar ou responder apropriadamente a ataques digitais; um estranho que esteja parado de forma suspeita em frente à nossa casa pode nos causar uma forte ansiedade e nos impulsionar para agir de forma a nos sentirmos mais seguras, mas claros avisos de vírus num computador são geralmente experienciados como irritantes e ignorados, apesar de terem implicações muito reais.

Além disso, a prevalência da tecnologia proprietária e da vigilância eletrônica secreta por toda parte torna difícil identificarmos aquilo que nos ameaça. Frequentemente, não conseguimos reconhecer esses perigos ou, pelo contrário, percebemos ameaças que na verdade podem não ser relevantes para nós.

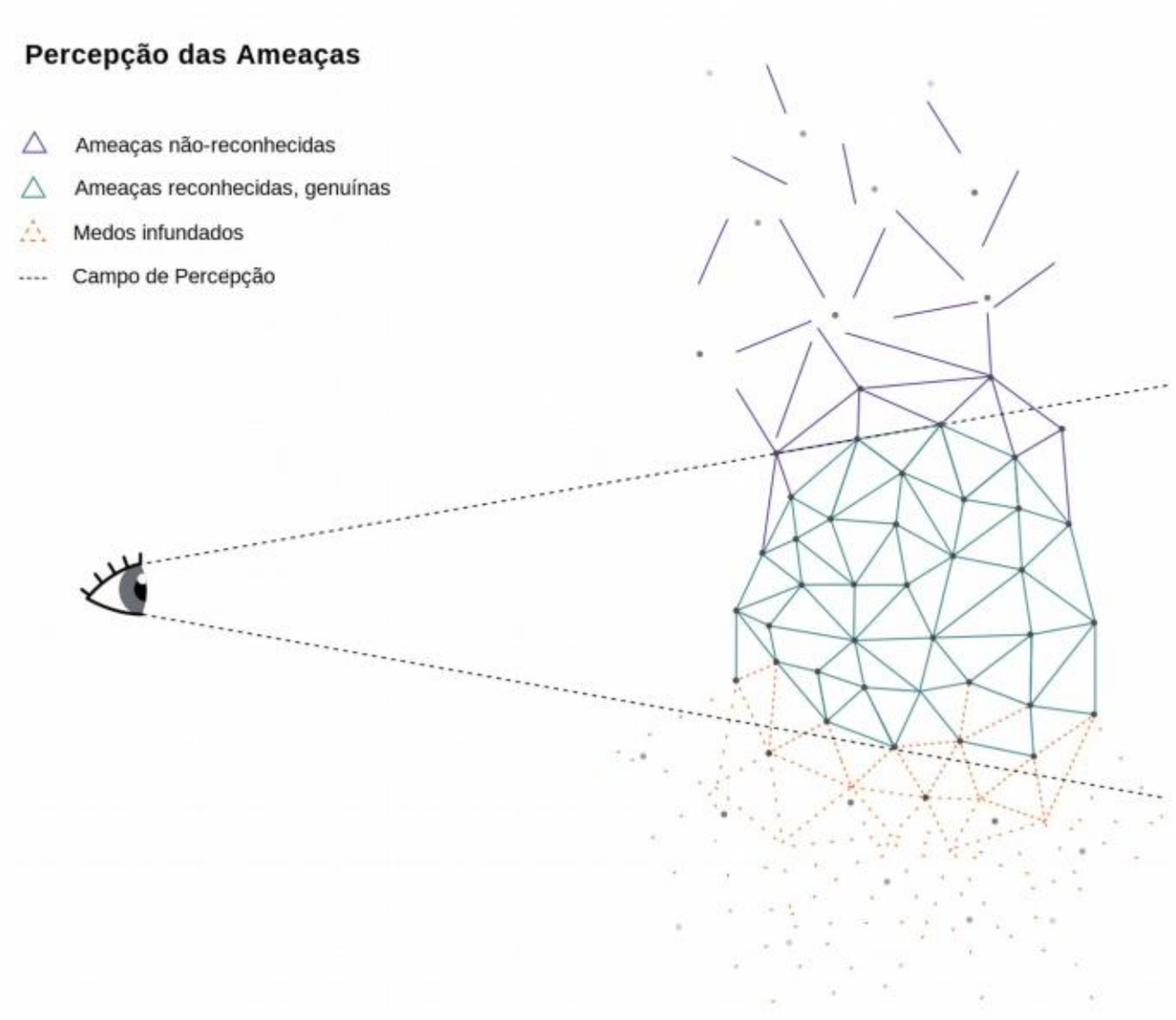
Já que defensoras de direitos humanos estão sujeitas a meios cada vez mais sofisticados de vigilância eletrônica e dependem

cada vez mais de ferramentas digitais, precisamos aprender a compensar a falta desse instinto de proteção. Ao levar em conta que nossa informação é muito importante para o nosso trabalho e optar proteger nossos dados contra acesso indesejado ou vigilância onde consideramos necessário, podemos aumentar nossos níveis de certeza e reduzir o estresse e o medo que esse assunto pode nos causar.

Trauma, estresse e fadiga

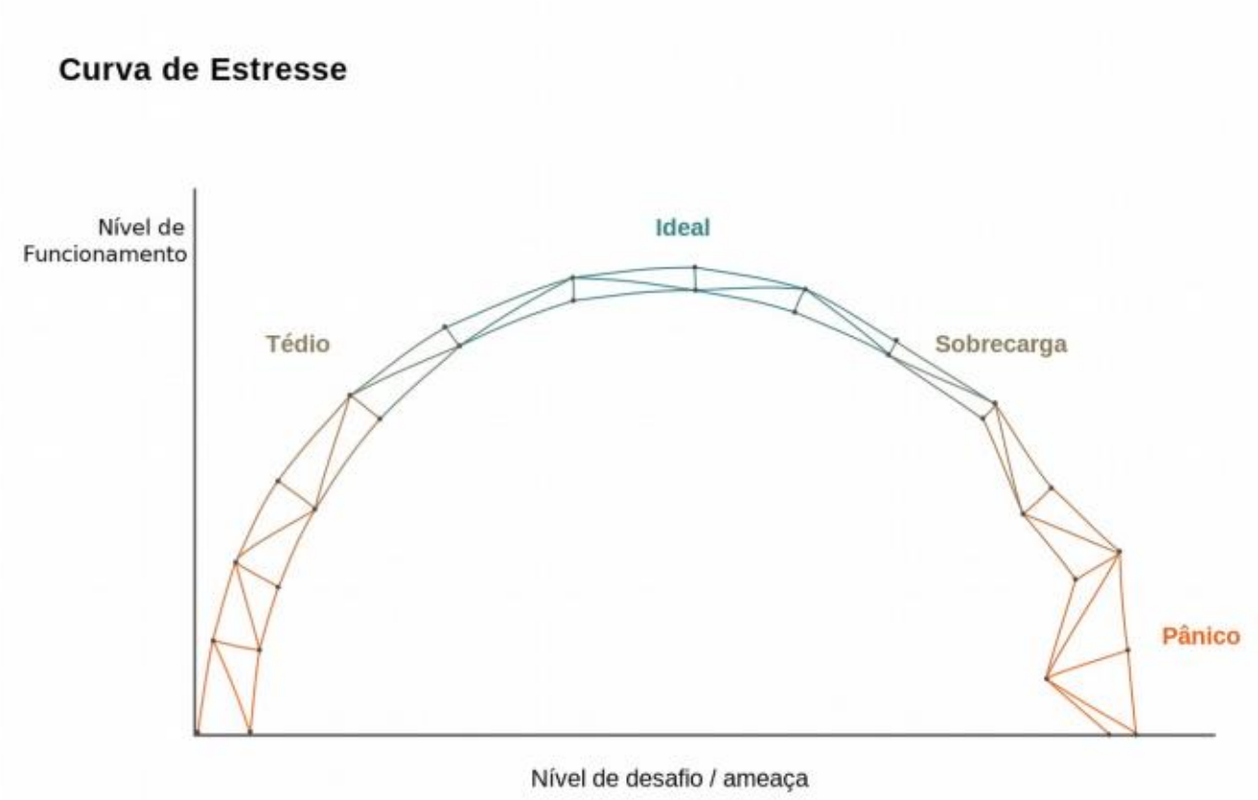
Experiências traumáticas passadas ou muito perturbadoras podem distorcer desnecessariamente a forma como respondemos aos indicadores de perigo. Isso é particularmente verdade para aquelas experiências traumáticas que continuam conosco de um jeito poderoso e desconfortável, mesmo anos depois do evento ter acontecido. Esses tipos de experiências traumáticas levam a duas reações comuns. Para muitas pessoas, experiências traumáticas passadas contribuem para nossos **medos infundados**. Essas pessoas tornam-se muito sensível a coisas que possam lembrá-las dessas experiências. Quando isso acontece, situações completamente inofensivas ganham uma aparência sinistra e nossa intuição começa a nos dizer que estamos em perigo quando na verdade não estamos. Isso pode levar-nos a reagir de forma inapropriada tendo consequências em nossas relações com as pessoas e organizações ao nosso redor.

Outras pessoas reconhecem seu problema ou ficam exaustas por terem que lidar constantemente, com seus cérebros e corpos, com esses alarmes falsos. À medida que o tempo passa, essas pessoas às vezes começam a reprimir ou ignorar o seu sistema saudável de alarme interno. Embora ajude as pessoas a viver de forma mais eficiente no mundo, isso também reduz sua atenção aos potenciais perigos do ambiente. Nesse sentido, experiências traumáticas passadas, podem contribuir para a percepção de **ameaças não reconhecidas**.



Estresse e **fadiga** podem também resultar na identificação e resposta imprecisas aos indicadores de perigo no nosso ambiente. Quando nos sentimos sobrecarregadas pelos desafios de nosso trabalho e de nossas vidas em casa, ou quando estivemos trabalhando muito duro, por muito tempo e sem descanso suficiente, começamos a nos comportar de forma diferente.

Cada pessoa tem um nível diferente de desafio ou ameaça que a estimula a um ponto de máxima produtividade e bem-estar. Se não há estímulo ou desafio o suficiente em nossas vidas, nos sentimos entediadas e acabamos improdutivas, ou até mesmo deprimidas. Se existe desafio ou ameaças demais, começamos a ficar sobrecarregadas. Sentimos que não conseguimos lidar com nada que nossa vida exige e mais uma vez ficamos improdutivas, ansiosas e deprimidas.



Muitos defensores de direitos humanos podem estar acostumados com altos níveis de desafio em suas vidas e alguns podem até desfrutar deles, mas isso não significa que somos imunes ao estresse. Cada uma de nós possui um limite que além do qual não conseguimos mais lidar. Quando atingimos esse limite, nos tornamos infelizes e nossa produtividade diminui. Além disso, o nível de cuidado e atenção que podemos ter com nossa segurança cai.

Quando estamos sobrecarregadas, os indicadores de segurança podem às vezes ser vistos simplesmente como mais um problema que temos que lidar. Se nossos recursos já estão completamente comprometidos, pode ser que escolhamos ignorar o indicador ou reagir de formas que não ajudem a nós, nossos colegas ou nosso trabalho. Outro motivo de falha em lidar adequadamente com ameaças reais é que acabamos nos acostumando com certo (e às vezes crescente) nível de ameaça em nossa vida pessoal ou profissional. Esse nível de ameaça começa a parecer “normal” ou confortável. Quando isso acontece, temos menos chance de fazer o que é preciso para melhorar nossa segurança.

Como resultado, é fundamental desenvolver uma cultura (tanto para si como para o grupo, organização ou movimento) de gerenciamento de estresse e autocuidado visando uma abordagem holística de segurança. Isso não apenas ajudará a prevenir ameaças devido à exposição de longo prazo a estresse e fadiga, como será crucial para pensar na segurança em geral.

Nos exercícios a seguir, refletiremos sobre algumas de nossas experiências passadas e sobre como elas podem continuar afetando nossa percepção sobre como vemos o perigo. Uma vez que estivermos mais conscientes disso, será mais fácil de construir táticas para mantermos nossa percepção "viva" quando planejarmos nossa segurança.

1.2a Exercício

Exercício de auto-consciência: reconhecendo e reagindo a ameaças

Propósito & Resultado	O propósito deste exercício é ajudar a reconhecer as áreas em que sua percepção é mais apurada e as áreas onde ela é menos clara. Você deverá entender melhor: • suas reações a ameaças no passado que tiveram bons e não tão bons resultados • as falhas no seu reconhecimento de ameaças • coisas que você talvez queria mudar • coisas que te fazem mais confiante frente novas ameaças e que devem continuar.
Informações de entrada & Materiais	Cópias impressas das perguntas

Formato & Passos	Reflexão individual Lembre de uma experiência passada onde você se sentiu particularmente insegura e em seguida fez algo para cuidar de si. Embora a experiência possa ter sido primeiramente física, emocional ou relacionada à segurança da informação, ela também pode ter tido impactos adicionais em outros aspectos da sua segurança. Use a tabela a seguir para manter o registro de suas ideias.
Lembretes & Dicas	É recomendável separar um tempo para este exercício e escrever suas respostas claramente, para que, depois, você possa voltar a elas à medida que você aprofunda sua autoconsciência. Se você fizer isso, preste atenção para manter suas anotações em um local privado. Compartilhe seus pensamentos e questões somente com as pessoas que você confia.

Escolha um momento em que você se sentiu ameaçada ou em perigo e então agiu para se proteger. Pense nas experiências de perigo físico (como um assalto), experiências emocionalmente danosas (como ser ameaçada ou traída) ou ameaças a suas informações e comunicações (como celulares confiscados ou telefones grampeados).

Como você percebeu a ameaça?

Já haviam indicadores da ameaça que você notou, ou talvez você não conseguiu percebê-la? Considere os indicadores no ambiente sociopolítico, no seu meio físico, nos seus dispositivos e no seu corpo e mente.

Já haviam indicadores da ameaça que você notou, mas descartou como não sendo importantes? Considere os indicadores no ambiente sociopolítico, no seu meio físico, nos seus dispositivos e no seu corpo e mente.

Quais foram as suas reações iniciais quando percebeu a ameaça e quão efetivas elas foram?

Quais foram as suas ações subsequentes e quão efetivas elas foram?

O que você mudaria se pudesse voltar no tempo? O que você teria feito?

O que você pode aprender dessa experiência que pode lhe ajudar a se sentir mais confiante na sua habilidade de lidar com futuras dificuldades?

1.2b Exercício

Nota: se você, os membros do seu grupo, colegas ou ativistas parceiras passaram por experiências traumáticas e você quer saber como elas podem impactar na percepção delas sobre ameaças, você pode realizar esse aprofundamento. Este exercício pode ser emocionalmente desafiador. Caso você não se sinta preparada neste momento, considere fazê-lo em outra ocasião.

Exercício de auto-consciência: Como experiências traumáticas afetam nossa percepção

Propósito & Resultado	O propósito deste exercício é ajudar a reconhecer áreas nas quais suas percepções são mais acuradas e áreas onde você pode ter menos discernimento devido a experiências traumáticas.
Informações de entrada & Materiais	É recomendável separar um tempo para este exercício e escrever suas respostas claramente, para que, depois, você possa voltar a elas à medida que você aprofunda sua autoconsciência. Se você fizer isso, preste atenção para manter suas anotações em um local privado. Compartilhe seus pensamentos e questões somente com as pessoas que você confia.

Formato & Passos

Pense em qualquer experiência traumática passada que pode não ter sido completamente resolvida. Serão experiências que você pensa com frequência e que ainda têm o poder de te fazer sentir assustada, com raiva, culpada, envergonhada ou triste. Não mergulhe na situação em si, mas foque no que você fez para se ajudar, para ajudar os outros e o que os outros fizeram ou poderiam ter feito para lhe ajudar.

Considere as seguintes questões:

- Quais tipos de situações perigosas são particularmente carregadas emocionalmente para você como resultado de suas experiências passadas?
- Quando você se depara com ambientes potencialmente perigosos, existem quaisquer situações que fazem você se sentir ansiosa ou amedrontada com facilidade?
- Existe alguém que você confia que poderia te ajudar a identificar quaisquer medos infundados que você tenha?
- Que tipos de ameaças você imagina que falha em reconhecer com facilidade?
- Como poderia verificar se você está falhando em reconhecer algum indicador de perigo?
- Com quem você se sente confortável para discutir seus medos e possíveis pontos cegos?

Lembretes & Dicas

Por esse exercício poder ser emocionalmente desafiante, comunique isso claramente aos seus colegas. É importante que ninguém se sinta coagido a participar do exercício, e se alguém começar a ficar desconfortável, essa pessoa deve parar imediatamente. Pode ser também uma boa ideia relacionar o exercício a outras atividades que cubram áreas do bem-estar psicossocial.

Exercício Opcional: Uso do Tempo[6]

Como defensores de direitos humanos, um aspecto muito importante de nossas vidas que frequentemente perdemos a noção é o nosso uso do tempo. Nossas cargas de trabalho são geralmente extremamente difíceis de gerenciar e nossa luta para nos mantermos de acordo com elas podem vir ao custo de nosso bem-estar físico e emocional. Também pode ter um efeito negativo em nossa habilidade de perceber perigos. Você pode explorar isso por si mesma no exercício abaixo. O desenvolvimento de práticas de segurança bem-sucedidas demanda o comprometimento de recursos, especialmente o tempo. Como indivíduos, precisamos de tempo para refletir sobre os efeitos que nosso trabalho está tendo em nós, para fazer perguntas e buscar respostas, para identificar boas táticas e ferramentas, para planejar e coordenar e para integrar novas práticas em nossas vidas e trabalhos.

A sensação de segurança emocional é frequentemente relacionada ao nosso uso e percepção do tempo. Qual é a razão entre nossas horas de trabalho ou engajamento e o tempo que usamos com as pessoas queridas ou para atividades recreativas? Como ativistas, quase sempre encaramos o dilema de que nossa carga de trabalho nunca acaba, mas nossa energia sim. Então, onde colocamos o limite? O exercício do "Uso do Tempo", do Manual de Segurança Integrada, ajuda a nos encaminharmos em direção a um uso do tempo mais saudável e seguro em termos emocionais. Veja o **Apêndice E**.

6 Reproduzido de Barry, J. (2011) Integrated Security: The Manual, Kvinna till Kvinna Foundation, Stockholm.

3
Crenças e Valores Próprios

Nossas respostas psicológicas instintivas não são o único recurso que temos à disposição para nos ajudar a construir a resiliência para encarar ameaças. Entender a si mesma e nossa segurança nesse contexto também demanda que reflitamos sobre as crenças e valores que trazemos para nosso ativismo: elas embasam a forma como percebemos o mundo e a sociedade ao nosso redor, nosso papel lá dentro, e, além disso, nossa compreensão sobre segurança e bem-estar. A partir dessa perspectiva, nos ajuda muito reconhecer as crenças e valores próprios que nos inspiram, que motivam nosso trabalho e constroem nossa resiliência. Também é igualmente importante que respeitemos as crenças e valores de nossos colegas e companheiros defensores de direitos humanos para evitarmos divisões, tensões e desconfiança em nossos coletivos, organizações e movimentos.

As crenças e valores próprios que sustentam nosso trabalho variam enormemente. Para algumas pessoas, eles podem ter raízes em crenças da cultura tradicional, religiosa ou espiritual; para outras, eles podem ser totalmente humanistas ou ateus. De qualquer forma, para muitos defensores de direitos humanos, crenças e valores próprios são lentes fundamentais através das quais percebemos o mundo: elas oferecem a muitas de nós um senso de propósito; elas podem nos ajudar a encontrar paz interior em tempos complicados, força face à adversidade e cura quando estamos machucadas.

Entretanto, esses valores são profundamente significantes e pessoais, e pode ser que hesitemos antes de falarmos deles para outras pessoas. Trazer nossos valores para nosso trabalho geralmente é pensado como um processo pessoal, mas como seria explicitá-los enquanto indivíduos, ou tornar claros nossos valores comuns como um coletivo ou movimento? Se falarmos de nosso *ethos*, crenças e seus rituais associados, e reconhecermos o papel que esses valores têm em inspirar nosso ativismo e em manter nossa resiliência, esta-

remos mais inclinadas a criar, respeitar e defender espaços para eles dentro do nosso trabalho.

Por outro lado, pode também ser o caso de assumir (corretamente ou não) que nossos colegas ou companheiros defensores de direitos humanos compartilham os mesmos valores ou crenças que nós. Ao agir com base nessa pressuposição, podemos inadvertidamente limitar o espaço para os valores e crenças diferentes de outras pessoas durante nosso trabalho conjunto. Independente de quais valores e crenças fundamentam nosso trabalho, é muito benéfico para formar um ambiente de grupo onde podemos ser confiantes que os valores que nos motivam sejam respeitados e até mesmo celebrados.

Um primeiro passo em direção a uma visão mais abrangente de nossos valores - sejam ateus, espirituais, religiosos ou de outro tipo - é criar um espaço seguro onde podemos compartilhá-los com as pessoas à nossa volta. Isso pode vir a ser uma fonte comunal de entendimento mútuo, inspiração, crescimento e apoio, abrindo caminho para entendermos melhor por que, como ativistas, nos arriscamos do jeito que nos arriscamos, e nos permite cuidar melhor de nós mesmas durante nosso trabalho.

Além disso, tal espaço precisa ser aberto e respeitoso, onde cada pessoa ali dentro se sinta capaz de compartilhar os valores que a inspiram, de forma a não cair em julgamentos, discussões ou dogmatismos, mas ao invés disso, criar solidariedade, respeito mútuo e aprendizado.

Fé e práticas culturais como fonte de conexão ou divisão

Práticas culturais ou de fé podem ser um fator unificador ou de conexão dentro do seu grupo, mas elas também podem ter o efeito oposto. Se as práticas de grupos minoritários são desencorajadas – por exemplo, não levar necessidades dietéticas em consideração (as quais podem ser culturais, éticas ou religiosas) quando estiverem organizando refeições ou, inversamente, criando uma atmosfera de “eles e

nós" –, elas podem se tornar uma força que separa o grupo. Isso tem um impacto negativo não apenas nas pessoas marginalizadas, mas no grupo como um todo.

Olhando para a sociedade, práticas culturais e de fé podem ser uma conexão unificadora (e talvez até estrategicamente útil) entre vocês e a sociedade que vocês querem transformar. Entretanto, elas também podem se tornar um fator de divisão, algo que separa você das "outras pessoas", e podem ser usadas para te estigmatizar ou te colocar como alvo.

Para ter uma visão mais detalhada sobre esses fatores de conexão e divisão, e de que forma você pode lidar com eles, veja a **Seção III | Monte Estratégias. A Abordagem Não-Cause-Dano**.

Até agora, viemos discutindo a segurança holística em termos de pessoas individualmente. Porém, como defensores de direitos humanos, raramente trabalhamos sozinhas e a maioria de nós possui familiares e comunidades que podem também ser afetadas direta ou indiretamente pelo nosso trabalho. Comumente, trabalhamos em pares e grupos. Enquanto grupos, precisamos construir confiança o suficiente para falarmos entre nós de forma significativa sobre nossas motivações e medos, para desenvolver uma compreensão compartilhada dos riscos e ameaças contra nós, para entrar em acordo sobre um conjunto integrado de práticas de segurança, para construir solidariedade, resiliência e agilidade juntas e para poder responsabilizarmo-nos por uma implementação consistente dessas práticas. Exploraremos as dinâmicas dessas relações no contexto de nosso trabalho no próximo capítulo.

4
Respostas do Grupo e de Colegas a Ameaças

As pessoas se organizam em grupos como famílias, círculos de amizades ou grupos – tanto dentro quanto fora de nosso ativismo por direitos humanos. Quando as pessoas se sentem ansiosas ou amedrontadas, esses grupos podem mudar de maneiras que são pelo menos parcialmente previsíveis. Já que alcançar uma segurança holística envolve quase sempre outras pessoas, é útil pensar em como os grupos mudam em momentos em que o perigo aumenta: isso irá nos ajudar no processo de planejamento. Abaixo, exploraremos alguns exemplos de como as dinâmicas nos grupos podem ser afetadas por ameaças tais como assédio, marginalização, violência física e de outros tipos (como econômica, de gênero, institucional ou estrutural).

Enrijecimento das fronteiras do grupo

Uma mudança previsível que ocorre em grupos sob ameaça é que as fronteiras que definem o grupo se solidificam: as pessoas de dentro do grupo ficam mais proximamente conectadas entre si e aquelas de fora do grupo acabam ficando mais distantes. Também acaba sendo mais difícil para as pessoas entrarem ou saírem do grupo. Embora a função de proteção de tais mudanças seja importante, também existem algumas dificuldades nisso. Fronteiras mais duras podem distanciar o grupo de aliados existentes ou potenciais, deixando-o mais isolado. Elas também reduzem o fluxo de informação para dentro e para fora do grupo, resultando em alguns membros do grupo ficando menos informados e tendo menos oportunidades de verificar suas percepções sobre o mundo em relação às das outras pessoas. Fronteiras endurecidas também dificultam a saída de pessoas do grupo. Membros que desejam sair

podem ser taxados de traidores ou vendidos de maneira bem danosa tanto para aquela pessoa quanto para as outras que são vistas como suas aliadas. É bastante útil para grupos discutir regularmente sobre as formas com as quais as pessoas e as informações entram e saem do grupo, e como lidar com isso de uma maneira holística para de fato promover nossa segurança.

Padrões fixos

Uma segunda mudança previsível é que os padrões de comportamento se tornam mais fixos ou difíceis de mudar. Isso torna mais difícil para um membro do grupo questionar crenças supostamente compartilhadas, ou desafiar o comportamento de outros membros. Quando perdemos a habilidade de questionar entre si nossas suposições ou apontar comportamentos potencialmente insalubres, nossa habilidade de construir positivamente e compassivamente a segurança do grupo fica enormemente comprometida. Por esta razão, é importante que os grupos revisitem regularmente e discutam seus valores compartilhados de forma honesta.

Autoritarismo

Uma terceira mudança previsível está relacionada com liderança e dinâmicas de poder dentro dos grupos. Quando grupos se sentem inseguros, os membros do grupo toleram um maior autoritarismo das lideranças ou de pessoas mais poderosas do grupo. Isso resulta em menos troca de informações dentro do grupo e menos oportunidades para os membros do grupo de verificar suas percepções de mundo em relação a outros membros. Em casos extremos, membros poderosos do grupo podem se tornar abusivos, e uma rigidez aumentada das fronteiras do grupo pode impedir vítimas de sair dele. Novamente, é importante que os grupos falem sobre dinâmicas de poder e estilos de liderança regularmente, e deixem claro que cada pessoa tem a oportunidade de contribuir. Observando as ligações entre tomada de decisão e segurança, não devemos subestimar os efeitos positivos de ter processos justos e transparentes de tomada

de decisão. O perigo de as lideranças do grupo serem atacadas por adversários é menor se o grupo compartilha responsabilidades e conhecimento entre si.

Diferentes grupos podem, entretanto, responder de formas diferentes: é uma boa ideia considerar como o seu grupo ou organização responde às pressões de trabalhar sobre ameaça e o impacto que isso tem no bem-estar de cada indivíduo no grupo. Isso demanda uma abertura à possibilidade de conversar sobre segurança no grupo, o que iremos explorar em mais detalhes no próximo Capítulo.

Desconfiança e infiltração[7]

Suspeita e desconfiança dentro e entre grupos de defensores de direitos humanos é comum e pode ou não ser justificado dependendo das circunstâncias. Geralmente, as raízes disso estão nas táticas de infiltração e espionagem que são frequentemente usadas contra defensores de direitos humanos, embora, simplesmente criar suspeita e desconfiança também pode ser um objetivo primário de nossos oponentes.

Num contexto de opressão, as pessoas viram informantes por muitas razões: elas mesmas com frequência são vítimas também. Assim, enquanto fazemos nosso trabalho, pode ser que levantemos suspeitas contra outras pessoas em nosso movimento ou organização. Existem muitas razões culturais, subculturais e interpessoais para a desconfiança, incluindo comportamentos "suspeitos" de uma tal pessoa, ou nossas próprias percepções e critérios subjetivos sobre em quem confiamos.

Essa suspeita vem a um preço pago em desconfiança e medo. O benefício potencial de talvez expulsar um informante de um grupo pode não nos proteger de outros informantes presentes. Além disso, a atmosfera criada por uma mentalidade de "caça às

7 Baseado em: Jessica Bell e Dan Spalding Cultura de Segurança para Ativistas. The Ruckus Society, www.ruckus.org/downloads/RuckusSecurityCulture-ForActivists.pdf

bruxas" pode sugar a energia e a motivação de todo o grupo. Pode ser que devido a essa atmosfera, acusemos falsamente um colega de espionagem, o que em seguida pode se provar mais danoso do que de fato ter um informante no grupo. Também costuma ser útil criar uma discussão aberta dentro do grupo e chegar num acordo sobre um processo transparente para decidir sobre como as informações sensíveis devem ser tratadas e como lidar com membros do grupo que podem causar problemas. Talvez possa ser útil rever suas decisões secretas ou a transparência de suas atividades levando em conta a possibilidade de que existam informantes no grupo. A criação de espaços para falar de nossos medos ligados à possibilidade de informantes no grupo ou de membros do grupo estarem sendo pressionados para se tornarem informantes pode evitar situações de caça às bruxas ou a demonização de informantes.

A infiltração em organizações de direitos humanos e movimentos sociais geralmente tem por objetivo final ou a documentação ou – o que é mais comum – a provocação de atividades ilegais. Com respeito a esse ponto, é importante garantir que as atividades da organização ou do grupo em defesa e na promoção de direitos humanos sejam explicitamente de natureza não-violenta, protegidas pela lei e por padrões internacionais, tais como a Declaração Universal dos Direitos Humanos, a Convenção Internacional de Direitos Civis e Políticos, a Convenção Internacional sobre Direitos Econômicos, Sociais e Culturais, entre outras. Nesse caso, aquelas pessoas no grupo que pressionam por métodos ilegais ou violentos de protesto ou de desobediência civil devem ser tratadas com cautela e sua afiliação no grupo reconsiderada.

A questão da infiltração é complexa e envolve muitas diferentes variáveis e muita incerteza. Muitas das ferramentas descritas na **Seção II | Explore** deste manual são úteis para ajudar defensores de direitos humanos a pensar cuidadosamente sobre os problemas de uma possível infiltração.

No próximo capítulo, aprenderemos algumas estratégias interessantes para criar e implementar um espaço habitual para falar sobre segurança dentro de organizações.

5
Conversando sobre Segurança dentro de Grupos e Organizações

Uma vez que entendamos como indivíduos e grupos reagem a estresse e ameaças, torna-se importante refletir sobre como práticas saudáveis sobre isso podem ser cultivadas em nossos grupos e organizações.

Criar um ambiente seguro e regular para conversar sobre segurança dentro de grupos e organizações é um dos mais importantes passos preparatórios para uma estratégia bem-sucedida de segurança e bem-estar organizacional. Todas as ferramentas que nos ajudam a construir nossa segurança listadas neste e em outros materiais demandam tempo e a criação de um espaço para falar, trocar, refletir e aprender sobre segurança. Fora essa clara necessidade prática, criar um espaço para falar sobre segurança com nossos pares e colegas nos ajuda a:

- perceber mais precisamente as ameaças de nosso trabalho, reduzindo o número de ameaças não reconhecidas e medos infundados.
- entender por que membros do grupo reagem de maneira diferente ao estresse e às ameaças (respostas individuais a ameaças)
- designar funções e responsabilidades devido a medidas de segurança
- aumentar a apropriação das medidas de segurança pelo grupo
- construir solidariedade e cuidado para com colegas que estejam sofrendo ameaças.

Entretanto, pode haver barreiras que nos impeçam de discutir segurança abertamente dentro de nossa organização. Algumas delas podem ser:

- cargas de trabalho pesadas e falta de tempo

- simplesmente ter medo de discutir isso
- temer que nossas observações sobre segurança possam ser percebidas como medo, paranoia ou fraqueza
- não querer confrontar nossos colegas sobre suas práticas
- não querer ser a primeira pessoa a trazer o assunto para discussão
- questões de gênero e/ou dinâmicas de poder.

Para criar um espaço para discussão, podemos fazer o seguinte:

a. construir confiança dentro do grupo

b. marcar regularmente conversas sobre segurança

c. nutrir uma cultura saudável de comunicação interpessoal

À medida que exploramos cada um desses pontos, discutiremos formas de estabelecê-los e alguns benefícios (assim como desvantagens) associados a cada um.

a. Construir confiança dentro do grupo

Ter um grupo que funciona baseado em confiança é ótimo para produtividade assim como para questões de segurança. A confiança facilita a implementação de novas medidas de segurança, especialmente entre membros que não podem estar ou não estavam envolvidos na hora de decidir sobre elas. Isso cria uma atmosfera de abertura na qual os membros compartilharão mais prontamente seus incidentes de segurança e as informações que eles acham que são importantes, e até os seus erros. Isso dá confiança aos membros para saberem com quem falar sobre aspectos de segurança.

Existem várias formas de aumentarmos a confiança dentro do grupo. Abaixo, temos alguns exemplos do que fazer:

- Conhecer as pessoas fora do contexto profissional ou ativista; por exemplo, através de atividades fora do trabalho, socialização e momentos de diversão.
- Verificar regularmente o bem-estar dos membros do grupo (talvez no começo das reuniões), para ter uma ideia sobre o nível de estresse de cada pessoa, o humor geral e o que elas estão trazendo para seu ativismo de suas vidas pessoais.
- transparência sobre hierarquias e estruturas de decisão de poder.
- Protocolos claros para como lidar com assuntos pessoais ou sensíveis que podem surgir, como incidentes de segurança, ameaças, entre outros.
- Ter acesso a uma conselheira ou psicóloga de confiança.

Construir confiança dentro de um grupo não é uma tarefa trivial – ela envolve esforço e riscos, dado o potencial de infiltração mencionado acima. Porém, a esse respeito, tirando confiar umas nas outras, podemos também construir confiança em nossas estratégias para lidar com informações sensíveis, ter canais de comunicação abertos e criar formas de falar sobre essas informações.

Uma atmosfera de confiança também depende de cada pessoa ser capaz de fazer e receber críticas construtivas e trazer *feedbacks*, o que iremos explorar na parte sobre comunicação interpessoal mais abaixo.

b. Encorajando o agendamento regular de conversas sobre segurança

Como explorado no **Capítulo 1.4 Respostas do Grupo e de Colegas a Ameaças**, é essencial criar espaços regulares e seguros para falar sobre os diferentes aspectos de segurança. Quando um grupo separa tempo de forma regular para falar sobre segurança, ele eleva a importância do assunto e da conversa. Dessa forma, se os membros de um grupo têm dúvidas e preocupações sobre segurança, eles se sentirão menos agoniados caso pareçam paranoicos ou desperdiçando o tempo dos outros.

Marcar conversas regulares sobre segurança também normaliza a frequência das interações e reflexões sobre questões de segurança. Assim, os assuntos não são esquecidos e os membros do grupo têm mais chance de desenvolver pelo menos uma consciência passiva sobre a segurança dos seus trabalhos em andamento.

É também importante incorporar elementos de segurança no funcionamento normal do grupo. Dessa forma, evitamos que a segurança vire um elemento estranho, mas sim uma parte integral de nossa estratégia e operações. Por exemplo, isso pode ser alcançado com a adição da segurança na pauta de uma reunião ordinária. Outra forma é rotacionar a responsabilidade por organizar e facilitar uma discussão sobre segurança no grupo, para trazer a noção de que segurança é responsabilidade de todo mundo e não apenas de algumas pessoas.

Em situações de alto risco, é importante aumentar o número de conversas sobre nosso bem-estar atual (*check-ins*) em reuniões e espaços informais, como também elevar a receptividade geral para conversar sobre segurança numa atmosfera acolhedora. No próximo exercício, haverá algumas perguntas para lhe ajudar a explorar a cultura de conversar sobre segurança dentro do seu grupo, identificando barreiras e pensando em formas de lidar com elas.

1.5a Exercício

Conversando sobre segurança em grupos

Propósito & Resultado

O objetivo deste exercício é refletir sobre como e quando falamos sobre segurança com nossos pares, colegas ou em grupo. O exercício acontece melhor se for facilitado pelo menos por duas pessoas, mas também pode servir como uma reflexão individual útil sobre suas interações com seus colegas. Ele ajuda a começar um

processo de conversa e discussão construtiva sobre segurança no seu grupo.

Informações de entrada & Materiais

Para fazer este exercício de uma maneira participativa e de forma a documentá-la, pode ser interessante ter materiais para escrever (cartões ou papeizinhos com adesivo e canetinhas).

Uma boa parede, uma *flip-chart* ou um moral de cortiça também podem ser úteis.

Formato & Passos

Trabalho individual & discussão em grupo

Passo 1: divida o grupo em pares. Peça para cada par pensar nas seguintes questões sobre dinâmicas de grupo e anote suas respostas.

- Quais tópicos tomam a maior parte do tempo nas conversas do grupo?
- Quais tópicos parece que nunca temos tempo para conversar?
- Quais aspectos das interações no nosso grupo consideramos empolgantes?
- Quais aspectos das interações no nosso grupo consideramos cansativas?
- O que acontece no grupo que as pessoas discordam?
- Vocês criaram algum espaço para desenvolver e refinar suas práticas de segurança (como indivíduos)? Descreva-o: onde e quando esse espaço existe? Ele é suficiente, e como será que vocês expandiriam esse espaço, se fosse necessário?
- Vocês têm espaço o suficiente para falar sobre questões de segurança com as outras pessoas (com colegas que trabalham junto com você) e como será que esse espaço pode ser criado ou expandido caso necessário?

Passo 2: junte todas as respostas a essas questões em um quadro ou num caderno.

Passo 3: como um grupo, pensem nas seguintes questões.

- Onde e como queremos definir nossas prioridades com respeito à segurança?
- Quais são os problemas comuns que aparecem quando falamos sobre segurança em grupo?
- O que pode evitar que falemos sobre segurança? Como podemos lidar com isso?
- Como podemos criar e manter espaço suficiente e adequado para conversar sobre segurança? O que isso significará em termos de tempo e recursos?
- Como será que podemos aumentar a efetividade de nossa interação de grupo com respeito à segurança?
- Quais problemas surgem quando nos comprometemos a mudar nossas práticas de segurança? Resistimos a mudar, individual ou coletivamente, e por quê?

Passo 4: convide cada pessoa a refletir sobre:

- Se você deveria ter uma atenção semelhante para com sua família e as pessoas que ama?
- Quais são as diferenças nas dinâmicas e formas pelas quais família e pessoas amadas são afetadas?
- De que formas você comunica as ameaças que está enfrentando para sua família, comunidade, amizades e outras pessoas que não estão no seu círculo de trabalho?

Passo 5: Agora no grupo, compartilhem os pontos que as pessoas se sentem à vontade para compartilhar. Com isso, vocês devem montar um acordo sobre o que pode ser falado para as pessoas de "fora" do grupo, por razões de confidencialidade, intimidade e segurança. Faça o acordo sobre esses princípios com todo o grupo.

Lembretes & Dicas

Considerem também discutir os passos e requisitos necessários para colocarem suas ideias de como falar sobre segurança no futuro em prática.

Perguntas importantes para se levar em consideração seriam:

- O que acontece se vocês não avançam na "conversa sobre segurança"?
- O que acontece se alguém não segue os princípios sobre o que pode ser falado para pessoas de fora?

---

c. Nutrir uma cultura saudável de comunicação interpessoal

A capacidade e a vontade individuais de se colocar numa comunicação aberta com as outras pessoas é fundamental para criar um espaço onde a segurança pode ser discutida de maneira franca e efetiva.

Precisamos ter certeza que a comunicação entre os membros de um grupo se mantenha saudável e aberta, para que tenhamos acesso ao máximo de informação possível e para poder tomar decisões informadas, como um grupo, sobre segurança.

Falar sobre segurança pode, entretanto, ser desafiador por diversas razões, devido à sua natureza bastante pessoal e ao fato de que nossas vulnerabilidades e mesmo nossos erros são, geralmente, informações muito relevantes. Encontrar uma forma construtiva de falar sobre segurança em grupos ou organizações ajuda a evitar interpretações erradas que podem levar a um conflito entre as pessoas envolvidas. Abaixo estão alguns aspectos que valem à pena ser considerados durante a criação de uma cultura saudável de comunicação:

A atmosfera atual sobre segurança

Isso ajuda a descobrir qual é a forma de pensar da organização sobre segurança. Por exemplo, podemos refletir sobre se o tempo dis-

pendido para conversar sobre segurança é tão valorizado e cuidado quanto outros tempos em uma reunião; ou podemos prestar atenção a se os membros do grupo apresentam um tom de despreocupação quando discutem questões de segurança; ou se estamos genuinamente interessadas e pessoalmente conectadas quando nossas colegas estão pontuando suas preocupações.

Hierarquias existentes

É também importante criar mecanismos para tal comunicação entre as hierarquias dentro de uma organização, para que os membros sejam capazes de discutir as coisas numa atmosfera livre de dinâmicas de poder.

Comunicação

Prestar atenção ao nosso estilo de comunicação dentro de grupos torna-se particularmente importante durante períodos de estresse elevado. Em momentos em que estamos sob ameaça e estresse, tendemos a não focar em nossa linguagem e tom devido a outras circunstâncias extenuantes. Podemos até não estar atentas à nossa impaciência, ou pode ser que esperemos que as outras pessoas entendam as razões por trás da nossa mudança de comportamento.

Situações interculturais

Também temos que ter em mente que a comunicação é um aspecto fundamental da cultura e da diversidade cultural. Devemos prestar atenção à nossa comunicação verbal e não-verbal em situações interculturais.

Modos formais de comunicação

Alguns grupos tendem a ser mais formais em sua comunicação e seu processo de tomada de decisão em reuniões. Embora estabele-

cer formalmente práticas de segurança e para bem-estar seja útil em muitos contextos, essa forma de comunicação pode ocasionalmente impedir uma troca aberta, especialmente relacionada aos aspectos emocionais da segurança. Pensar sobre facilitação e formatos para essas discussões pode ajudar a chegar numa estrutura efetiva que forneça espaço para trocas abertas sobre esperanças e medos, assim como para discussões mais técnicas. É importante incorporar todos esses aspectos quando tomamos decisões sobre segurança.

Um exemplo de uma prática útil nas comunicações interpessoais é o método da **comunicação não-violenta**. A comunicação não-violenta é um método de comunicação baseado na pressuposição de que todas as pessoas são compassivas por natureza, que todas as pessoas compartilham as mesmas necessidades básicas humanas e que cada uma das nossas ações é uma estratégia para satisfazer uma ou mais dessas necessidades.

Embora esse método seja certamente enviesado culturalmente pelo "Ocidente", ele permite uma comunicação que inclui formas de refletir confortavelmente sobre como a comunicação está afetando todas as pessoas envolvidas. Isso pode ser especialmente efetivo em dar e receber *feedback* sobre segurança e em discutir o impacto de ataques, acidentes, ameaças e outros eventos relacionados com segurança que acontecem conosco como indivíduos e grupos. A maior vantagem de usar essa forma particular de estruturar conversas e *feedbacks* é que ela ajuda a evitar maneiras acusatórias de expressar pontos de vista e encoraja a deixar as coisas mais claras onde existe confusão. No exercício a seguir, você pode praticar os seguintes passos para dar um *feedback* construtivo sobre segurança de acordo com os princípios básicos da comunicação não-violenta.

1.5b Exercício

Feedback não-violento

Propósito & Resultado

O objetivo deste exercício é praticar a comunicação não-violenta como forma de melhorar a efetividade da comunicação sobre segurança dentro de grupos. Ele oferece uma reflexão sobre como podemos dar nosso *feedback* de uma forma compreensível e clara e evitar algumas das dificuldades que podem levar a discussões/brigas ou a uma comunicação não efetiva.

O exercício é melhor realizado, num primeiro momento, em pares, embora possa ser adaptado para grandes grupos.

Informações de entrada & Materiais

Pode ser útil escrever os princípios para um *feedback* não-violento em algum lugar visível, como um quadro.

Formato & Passos

Bole um cenário para conduzir uma discussão para dar *feedbacks* (isso pode ser feito em pares, ou com observadores, fazendo turnos). Os participantes devem escolher um assunto (real ou imaginário) sobre o qual eles querem dar um *feedback*. Pode ser um tópico relacionado à segurança, como um incidente que aconteceu, ou alguma outra coisa completamente diferente.

Peça à pessoa que vai dar o *feedback* para seguir os princípios abaixo. Para cada princípio, há um pequeno exemplo ilustrativo. Aqui, estamos imaginando um cenário no qual dois colegas estão falando: uma das pessoas costuma trabalhar tarde e uma vez esqueceu de fechar a porta do escritório depois de sair; a outra pessoa quer falar sobre o incidente.

Quem recebe o *feedback* deverá apenas fazer perguntas por clareza, mas não comentar, responder, justificar ou questionar o conteúdo do *feedback*.

Princípios para o *feedback* não-violento:

Eu falo por mim mesma: você só pode fazer desde sua própria experiência subjetiva – não sobro o "senso comum", "meu grupo", "nós", ou "alguém", mas somente "eu".

- Por exemplo: "Me sinto insegura quando encontro o escritório aberto pela manhã".
- Prática desaconselhável: "O que você fez ontem me deixa furiosa!"

O que você observa? Você deve falar apenas dos fatos da forma como experimentou-os para que o interlocutor saiba a que o seu *feedback* se refere (o que você viu, ouviu, etc.).

- Por exemplo: "Quando cheguei no escritório esta manhã, a porta da frente estava destrancada e pude abri-la sem a chave".
- Prática desaconselhável: "Você esqueceu de fechar a porta ontem!"

Qual foi a sua reação? Quais foram os seus sentimentos internos e reações físicas durante o que você experienciou? Tente não julgar, mas novamente, simplesmente fale desde a sua experiência como você a entende.

- Por exemplo: "Eu estava muito preocupada, pois pensei que talvez tivéssemos sido roubadas. Quando descobri que estava tudo OK, eu ainda estava com bastante raiva."

Como você interpreta o que aconteceu? O que as suas interpretações pessoais [BRING TO THE FACTS]? Embora sua interpretação pessoal seja de fato subjetiva, ain-

da assim ela tem valor e colore sua experiência.

- Por exemplo, “Acho que isso aconteceu porque você esteve trabalhando até bem tarde e estava cansada e simplesmente esqueceu de fechá-la.”

Formato & Passos

Quais são seus desejos, conselhos ou interesses? Quais são suas sugestões para mudança baseadas nesta experiência? Elas devem ser oferecidas sem exigências, mas ao invés disso, como pedidos em consideração pelo grupo.

- Por exemplo: “Me sentiria melhor se soubesse que todos estamos tendo descanso suficiente e não trabalhando demais para que possamos cuidar melhor de coisas como essa, e seria melhor se você não trabalhasse até tão tarde”.

Peça aos pares para compartilharem suas ideias sobre esse processo e maneira de dar um *feedback* - não sobre o conteúdo. Experimentaram sensações diferentes de quando normalmente recebem um *feedback*?

Esse exercício pode também ser usado para tornar mais claro o conteúdo e o tom do seu *feedback* como uma preparação para uma seção real de *feedbacks* ou uma discussão potencialmente difícil.

Lembretes & Dicas

É importante receber um *feedback* com os ouvidos e não com sua boca, e entendê-lo como uma reflexão pessoal do seu parceiro, não como “a verdade” ou um convite para você justificar ou defender suas ações. Você é quem irá decidir se isso tem valor para você e como reagir a isso. Seguir essa abordagem pode ser um passo preventivo para conflitos dentro de um grupo. Dessa forma, isso pode contribuir para o bem-estar de todo mundo.

Se você tem interesse em se aprofundar em modos de comunicação que tratam conflitos com sensibilidade,

talvez lhe interesse dar uma olhada nas abordagens da comunicação não-violenta.

Lembre-se de que “falar apenas por mim mesma” não é apropriado em muitas regiões do planeta. Faça adaptações da metodologia para que ela se encaixe em suas necessidades e contextos.

Conclusão

Esperamos que esses exercícios tenham lhe ajudado a ter um senso mais elaborado sobre o que segurança significa, assim como um entendimento melhor de como você e as pessoas ao seu redor reagem a ameaças contra vocês e os seus trabalhos. Estabelecer uma cultura saudável de comunicação como explorado acima pode representar uma das mais difíceis mudanças de se fazer ao adotar uma abordagem mais positiva e organizada de nossa segurança e bem-estar. Entretanto, entender isso e todos os tópicos abordados nesta Seção é vital para criar um espaço para o processo de análise de contexto. Esta análise é chave e consta de uma série de atividades para melhorar e manter uma abordagem organizada sobre segurança. Este será o assunto da **Seção II | Explore**.

EXPLORE

Análise de Contexto e de Ameaças

II Explore

Análise de Contexto e de Ameaças

Conteúdo

Introdução

1. Estrutura Abrangente para Análise de Contexto
2. Monitoramento e Análise da Situação
3. Visão, Estratégia e Atores
4. Compreendendo e Catalogando nossas Informações
5. Indicadores de Segurança
6. Identificando e Analisando Ameaças

Conclusão

Introdução

Nesta seção, analisaremos o contexto no qual realizamos nosso trabalho pela defesa de direitos humanos. Criar e manter uma análise sistemática de nosso contexto político, econômico, social, tecnológico, legal e ambiental nos permite entender melhor as ameaças que enfrentamos, preparar-nos para lidar com elas e manter nosso bem-estar enquanto perseguimos nossos objetivos.

Ameaças, nesse caso, se referem a **qualquer evento ou ocorrência em potencial que poderia causar dano a nós ou ao nosso trabalho**.

Às vezes, esse processo leva o nome de modelo de ameaças ou análise de risco. Quanto mais tempo pudermos dispender nessa análise de contexto, melhor será o nosso entendimento a respeito do

nosso entorno e estaremos melhor preparadas para perceber e reagir às ameaças contra nossa segurança e bem-estar.

Logo, as ferramentas para análise de contexto exploradas nesta Seção podem e devem ser entrelaçadas em nossos processos de montar estratégias e planejamento que já fazemos em nosso trabalho de defesa de direitos humanos. Pode ser que você já esteja familiarizada com várias dessas ferramentas e use-as de forma não tão explícita ou organizada. Entretanto, ser mais sistemáticas sobre elas pode lhes ajudar a construir um "diagnóstico" mais completo sobre sua situação de segurança e talvez desafiar algumas suposições que você possa ter sobre ela.

Em Explore, iremos:

- propor uma série de passos para realizar uma **análise de contexto**
- fazer um exercício simples para entender as **tendências sociopolíticas** ao nosso redor
- mapear nossa **visão** e os **atores** próximos em nosso contexto
- criar um **inventário de nossas informações** tomando-as como um recurso para nosso trabalho e compreender as ameaças a elas
- **reconhecer e analisar os indicadores** que podem nos dizer mais sobre nossa situação de segurança
- identificar e analisar **as ameaças mais significativas** à nossa segurança.

1
Estrutura Abrangente para Análise de Contexto

Uma prática de segurança efetiva está baseada em um bom conhecimento dos tipos de ameaças que encaramos como resultado de nosso trabalho e os possíveis danos que essas ameaças representam. Porém, será que é fácil identificar com precisão todas as ameaças que podem impactar negativamente nosso bem-estar e nossa capacidade de atingir nossos objetivos? Para responder essa questão, temos que considerar dois fatores importantes.

Ameaças mutáveis

É importante reconhecer que as ameaças estão constantemente mudando, às vezes muito rapidamente. Assim como nossa vida e nosso trabalho vão acontecendo, assim também nossos aliados e oponentes vão se transformando. Enfraquecendo ou se tornando piores, a gama de ameaças que enfrentamos evolui e muda, assim como os contextos político, econômico, social, tecnológico, legal e ambiental no qual trabalhamos. As ameaças para as quais nos preparamos hoje podem ser irrelevantes em um mês, e o melhor é se manter ágil e estar sempre revisando e refinando nossas práticas de segurança de forma constante.

Na realidade, esse não é necessariamente um conceito muito estranho para nós. Regularmente fazemos análise de contexto para tomar decisões sobre nossa segurança no dia a dia. A única diferença aqui é que estamos sendo mais conscientes e organizados sobre esse processo. Isso nos ajuda a evitar tomar precauções de segurança só por hábito ou baseado em boatos, pois pode ser que descubramos que mudanças nas circunstâncias tornaram essas medidas ineficazes.

Uma análise de contexto nos ajuda a entender de forma mais clara as ameaças que enfrentamos como resultado de nosso trabalho. Ela é composta de uma série de passos familiares e talvez outros que sejam novos. Os passos que iremos seguir estão resumidos abaixo – pode ser que você já realiza alguns deles.

1. **Monitoramento e Análise da Situação**

   Observar as tendências gerais (políticas, econômicas, sociais, tecnológicas, legais ou ambientais) relevantes para o nosso trabalho e anotar quaisquer mudanças relacionadas à nossa segurança. Um exemplo simples seria ler os jornais diariamente, embora exista várias outras fontes específicas de informação de segurança.

2. **Definir nossa visão e nossas atividades**

   Baseado no que foi feito acima, refletimos sobre quais mudanças desejamos para nossa sociedade e quais estratégias nos ajudarão a implementar essas mudanças. Muitos defensores de direitos humanos estarão familiarizados com o exercício de identificar um problema que queremos resolver em nossa sociedade e uma estratégia para alcançar isso.

3. **Mapear atores e relações**

   Criar e manter um inventário de todas as pessoas, grupos e instituições que serão ou poderão ser afetadas por nossas ações, incluindo nós mesmas, nossas aliadas e oponentes.

4. **Mapear informações**

   Conhecer nossas informações pessoais e profissionais, e ter certeza de que elas não vão cair nas mãos dos oponentes que identificamos. Um exemplo simples seria distinguir nossos documentos financeiros de outros documentos em casa, e decidir guardá-los em um local seguro.

5. **Indicadores de segurança**

   Tomar nota das ocorrências que saem do ordinário e que podem indicar uma mudança em nossa situação de segurança, e analisar qualquer tendência visível que possa impactar sua estratégia. Um exemplo simples seria perceber um aumento nos roubos na área onde você vive e reconhecer que isso pode também afetar a sua segurança.

6. **Identificação e análise de ameaças**

   Tentar desviar ou diminuir um perigo fingindo ter maior poder do que se tem. Como defensores de direitos humanos, frequentemente ameaçamos expor e tornar públicas as ameaças de violência que recebemos como forma de constranger publicamente nossos adversários.

7. **Planejamento e táticas de segurança**

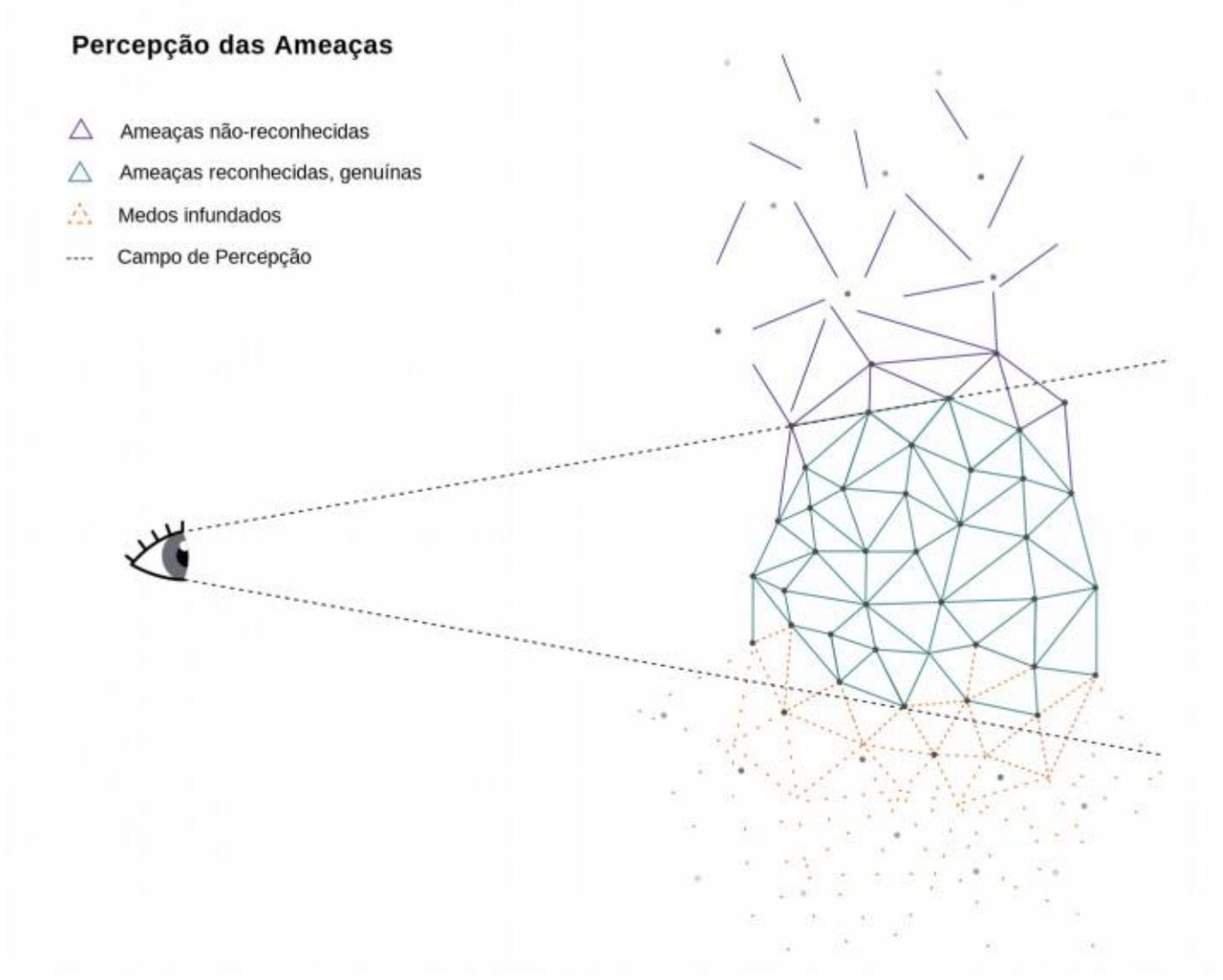
   Baseado nessa análise, você irá identificar e tomar medidas concretas para melhorar a sua segurança, tais como comprar novas fechaduras para as portas ou instalar câmeras. Olharemos mais profundamente para isso na **Seção III | Monte Estratégias** e na **Seção IV | Ação**.

Esses passos não representam uma atividade que se faz uma vez e pronto. Para que sejam efetivos, eles precisam ser repetidos regularmente e tecidos dentro de nosso planejamento estratégico em andamento.

Análise e percepção

Pode ser tentador considerar esse tipo de análise como científica e objetiva. Porém, a esta altura é importante lembrar o que aprendemos na **Seção I | Prepare-se**. Por definição, nossa **percepção** de ameaças muitas vezes é desafiada, limitada ou errônea. Embora possam haver diversas ameaças de que estamos conscientes, tam-

bém podem haver outras que não estamos percebendo. Essas **ameaças não percebidas** são particularmente prováveis quando trabalhamos em novos ambientes com uma compreensão limitada do que está à nossa volta, ou onde nossos oponentes estão ativamente escondendo ameaças, tais como a vigilância eletrônica. Reações emocionais de ansiedade tais como negação, fatalismo ou diminuição de efeitos podem também fazer com que falhemos em reconhecer ameaças em potencial.



Também é possível que escorreguemos para a outra direção e foquemos em ameaças que, na verdade, provavelmente não nos causarão danos ou ao nosso trabalho. Tais **medos infundados** podem ser o resultado de informação confusa de nossos oponentes ou de reações emocionais de ansiedade, possivelmente relacionadas com

experiências traumáticas passadas. Ainda assim, é possível e útil tomar decisões adequadas de segurança baseadas na informação limitada disponível. A experiência nos dá ideias e nossa intuição, na maioria das vezes, nos leva na direção certa. Embora nossos oponentes desenvolvam novas táticas e trabalhem para confundir nossas práticas de segurança, o desafio que nós e nossos aliados enfrentamos é **reduzir o número de ameaças não reconhecidas e medos infundados** para assim construir um quadro mais preciso sobre o qual basear nossas práticas de segurança.

Começando pelo reconhecimento de que nossa percepção de ameaças pode estar errada, é uma boa ideia pensar com antecedência sobre onde podem estar nossos pontos cegos e visualizar estratégias para verificar nossas percepções com pessoas que confiamos. Voltaremos a isso no **Exercício 2.6b**, onde levantaremos algumas questões que podem ajudar nisso.

Nossa percepção pode se tornar mais precisa se fizermos pesquisas e análises. No restante desta Seção, mapearemos um caminho para a auto-exploração, começando com nossa própria visão de mudança sociopolítica, continuando com uma pesquisa sobre o universo onde operamos ao lado de nossos oponentes, aliados e outros grupos; um inventário de nossos recursos, bens e comportamentos existentes, e o registro do que percebemos como indicadores de segurança em nosso contexto (ou seja, o que vem antes das ameaças).

O conhecimento adquirido com a exploração acima é útil para criar e manter uma lista prioritária de ameaças potenciais (e reais), a sua probabilidade e intensidade, os agressores potenciais (e reais) e suas capacidades e motivações, qualquer forma de mitigação que nós (ou nossos aliados) possamos ter à mão, assim como os possíveis passos futuros para minimizar essas ameaças ao nosso bem-estar e sucesso.

Ao iniciarmos essa exploração pela identificação e mitigação de ameaças que enfrentamos, é importante estar plenamente atenta para não criar ou alimentar medos infundados. Isso pode ser

evitado se tivermos em mente qual o papel de nossa percepção e nosso comportamento, e trabalharmos para criar um espaço saudável para lidar com esses desafios. Em outras palavras, precisamos fomentar uma forma de pensamento individual autoconsciente e uma comunicação saudável em nossos grupos e organizações, como explorado na **Seção I | Prepare-se**.

É igualmente importante lembrar de nossas limitações em termos de tempo, estresse e recursos. Isso nos ajudará a determinar tarefas realistas, tangíveis e gerenciáveis para identificar, priorizar e analisar ameaças.

Neste Capítulo, começaremos olhando para a paisagem política, econômica, social e tecnológica na qual operamos como defensores de direitos humanos, e como ela pode impactar em nossa segurança.

2
Monitoramento e Análise da Situação

Começaremos esse processo com uma análise bem ampla de nosso contexto: observar os desenvolvimentos políticos, econômicos, sociais, tecnológicos, legais e ambientais na sociedade que sejam relevantes para o nosso trabalho e que possam impactar em nossa situação de segurança.

Em geral, durante nosso ativismo, é provável que façamos, seja formal ou informalmente, algum tipo de monitoramento e análise de contexto: ou seja, analisar quaisquer que sejam as fontes disponíveis de informação com respeito a **mudanças políticas, econômicas, sociais, tecnológicas, legais e ambientais** em nossa sociedade. Podemos fazer isso simplesmente lendo os jornais toda manhã ou falando com amizades ou colegas de confiança sobre suas observações. Também pode englobar tarefas mais complicadas ou sensíveis, como fazer nossas próprias investigações e pesquisas. Através desse processo, a informação que obtivermos naturalmente

embasará nossas decisões e as estratégias, os planos e as ações que realizaremos como ativistas.

Entretanto, ao fazer e manter um monitoramento situacional constante, é importante considerar as nossas **fontes** de informação: será que a mídia é uma fonte confiável de informação objetiva, ou temos que diversificar nossas fontes? Colegas, amizades e organizações parceiras, assim como acadêmicas, especialistas, autoridades e embaixadas amigas, listas de email sobre segurança, agentes de viagem, entre outras, também podem ser ricas fontes de informação, muitas vezes relevantes para montar nossas estratégias e para nossa segurança.

Fazer um monitoramento e uma análise deliberados e mais profundos de nossa situação, de maneira regular, também é uma ótima forma de refletir sobre nossa situação de segurança. Isso nos ajuda a situar nosso trabalho e nossas estratégias dentro dos acontecimentos locais, regionais, nacionais e globais que estejam acontecendo, e identificar aqueles que possam apontar para uma mudança em nossa situação de segurança.

Monitoramento e análise situacional podem ser pensados como o "motor" de nosso planejamento de segurança, a partir do qual podemos identificar os **acontecimentos chave** que irão impactar nossa estratégia. Exemplos de acontecimentos chave podem incluir:

- o aparecimento de novos atores (tais como novos políticos eleitos)
- a emergência de novas formas de vigilância eletrônica ou formas de evitá-la
- uma mudança no discurso de atores chave com respeito a como eles vêm o nosso trabalho.

Analisar com regularidade os acontecimentos tais como os citados acima com parcerias confiáveis é uma importante prática de segurança, e também pode nos ajudar a **verificar nossas percepções**

para que sejamos menos suscetíveis a sofrer de **medos infundados** e **ameaças não reconhecidas**.

Existem várias estruturas que podem ser usadas para análise de contexto. Duas são comumente usadas no contexto de planejamento estratégico: a análise PESTLA (política, econômica, social, tecnológica, legal e ambiental)*, e a FFOA (Forças, Fraquezas, Oportunidades e Ameaças)**. No próximo exercício, faremos uma breve análise do tipo PESTLA e tentaremos identificar os acontecimentos mais importantes do último ano que devemos estar atentas.

2.2 Exercício

Monitoramento da situação: uma análise rápida tipo PESTLA

Propósito & Resultado	Este exercício nos ajuda a pensar as formas em que nós já fazemos análise da situação, e considerar rapidamente algumas tendências e acontecimentos dominantes nos últimos 12 meses que podem impactar nossa segurança.
Informações de entrada & Materiais	Materiais para escrita
Formato & Passos	Sozinha ou em grupo, pense e anote suas respostas para as seguintes questões: 1. Como você faz hoje um monitoramento e uma análise situacional? Quais espaços você tem para discutir os acontecimentos em andamento na sociedade? 2. Quais são suas fontes de informação? Faça uma lista das fontes e, para cada uma, anote

* N.T.: do inglês *PESTLE, Political, Economic, Social, Technological, Legal and Environmental.*

** N.T.: do inglês *SWOT, Strengths, Weaknesses, Opportunities and Threats.*

suas forças e fraquezas em termos de qualidade da informação que elas oferecem. Elas são objetivas ou enviesadas?

3. Pense o que aconteceu localmente, regionalmente e internacionalmente nos últimos 12 meses e faça uma lista de 5 a 10 acontecimentos que você considera importantes. Pode ser que seja necessário categorizá-los, porém tenha certeza de considerar:
    - acontecimentos políticos
    - acontecimentos econômicos
    - acontecimentos sociais
    - acontecimentos tecnológicos
    - acontecimentos legais
    - acontecimentos ambientais.

Nota: se você não consegue lembrar dos acontecimentos em si, pense em características mais visíveis das transformações.

4. Algum desses acontecimentos pode impactar a sua segurança, direta ou indiretamente? Se sim, como? Você sofreu algum ataque ou acidente no último ano? Como eles se relacionam com esses acontecimentos?

3
Visão, Estratégia e Atores

Fazer uma análise da situação, como sugerido acima, frequentemente destaca as tendências em nossa sociedade que vemos como negativas ou injustas. Nesse contexto, lutamos para fazer mudanças em nossa sociedade que incluam direitos civis e políticos, assim como justiça econômica, ambiental, de gênero e social, entre outras formas de justiça. Como defensores de direitos humanos, estamos acostumadas a identificar injustiças e a responder a elas. Entretanto, é importante ter uma visão definida da mudança que queremos engendrar e uma estratégia para alcançá-la. Baseadas nessa estratégia e num entendimento de como iremos implementá-la, podemos identificar as ameaças que enfrentamos e construir um plano de segurança completo e apropriado.

Pensar criticamente sobre nossas estratégias torna-se ainda mais importante se e quando agimos como um grupo ou uma organização. Ser internamente transparentes e abertas sobre as mudanças que queremos alcançar e as estratégias que usamos também pode evitar dificuldades e conflitos dentro do grupo e com as pessoas de fora.

Definir nossa visão e atividades

Identificar um problema que queremos resolver é geralmente nosso primeiro passo como defensores de direitos humanos e felizmente isso é acompanhado ou seguido pela visão do resultado bem sucedido de nosso trabalho. Se vocês ainda não têm uma visão definida, responder às seguintes questões pode ajudar:

- Qual é o problema, ou os problemas, que vocês esperam lidar?
- Quais mudanças vocês gostariam de ver acontecer?

- De que formas sua comunidade seria diferente depois disso?
- O que seria diferente nas relações entre as pessoas, caso dê certo?
- Quem são as outras pessoas, grupos, instituições, etc. envolvidas nesse assunto e como elas reagem às suas atividades?

Mapear atividades

Uma vez que tenhamos estabelecido nossa visão, precisamos considerar os métodos que empregaremos para realizá-la. Podemos fazer diversas atividades como indivíduos ou organizações para alcançar nossos objetivos. Quais são as suas "áreas de trabalho" ou as atividades que você faz?

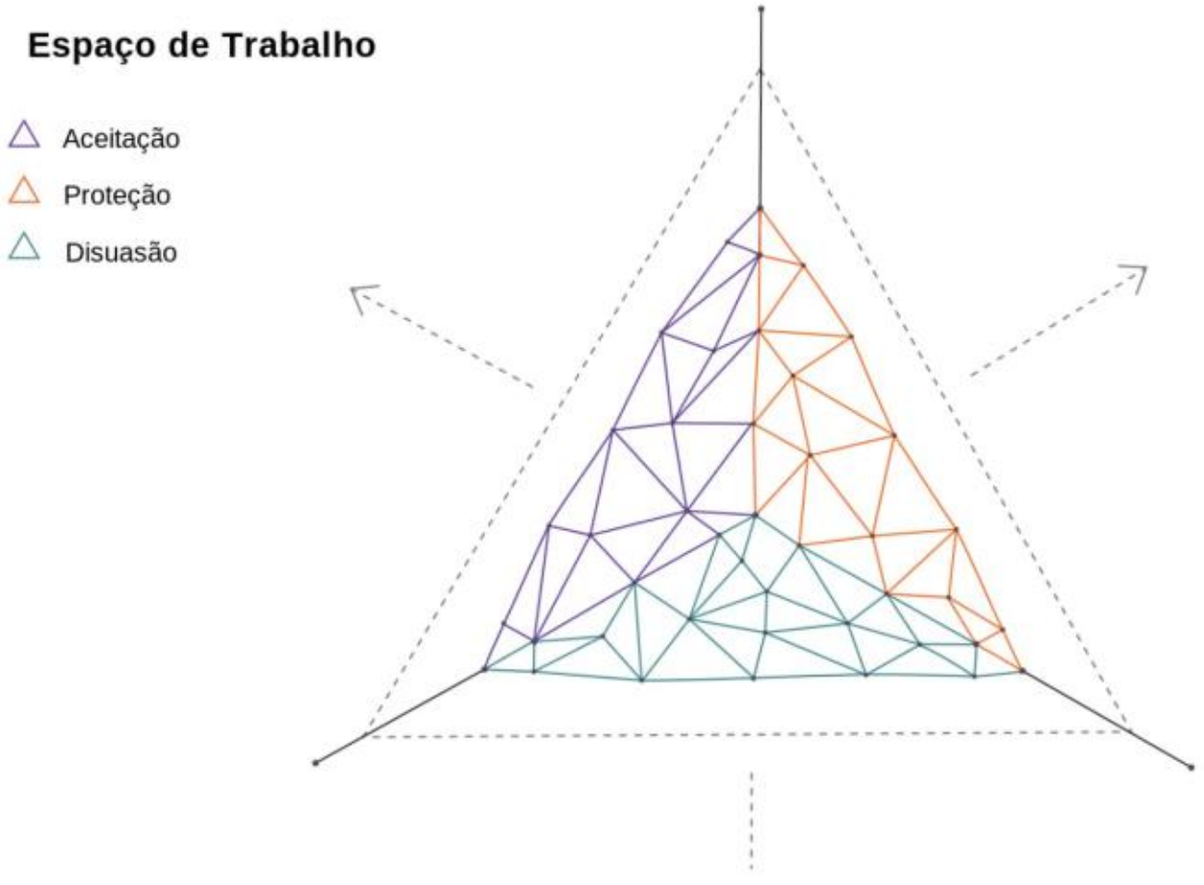
É importante listar explicitamente cada uma delas e considerar, num primeiro momento, se elas são apropriadas ou não para alcançar o objetivo que escolhemos. Nosso trabalho não acontece no vácuo, mas ao invés disso, num contexto rico e variado, geralmente com algumas características de conflito. Nossas atividades são a nossa "interface" com esse conflito, com o Estado e com a sociedade que estamos tentando influenciar; elas são nossos meios de tentar mudar as situações, as percepções e os comportamentos de um variado conjunto de atores (pessoas, instituições e organizações) à nossa volta. Alguns desses atores irão se beneficiar com, acreditar e apoiar nossas atividades. Outros, porém, irão perceber que essas atividades não são do seu interesse e tentarão fechar o nosso espaço de trabalho.

Mapear os atores

Construir nossas estratégias nos ajuda a identificar toda a gama de atores (pessoas, instituições, organizações, etc.) que são quem tem poder de ação na presente situação. Eles podem estar trabalhando para sustentar ou desafiar o *status quo*, ou nenhum dos dois, ou eventualmente ambos. Identificar todos os atores significa que você

pode priorizar ações de engajamento com cada tipo de ator; por exemplo, como mudar suas opiniões sobre o nosso trabalho, como mudar seus hábitos ou impedi-los de se comportarem de uma dada maneira. Tenha em mente que seus oponentes, assim como seus aliados, desenvolvem suas próprias estratégias e ações baseadas na percepção que eles têm das suas posições e atividades. Essa percepção pode ser diferente da sua.

Por isso, entender quais atores estão envolvidos e dedicar tempo coletando informações e refletindo sobre suas dinâmicas é crucial para seu planejamento de segurança. Ter conhecimento profundo de nossos aliados e oponentes também nos ajuda a decidir quais estratégias de aceitação, dissuasão e proteção serão empregadas para manter nosso espaço sociopolítico de trabalho. Discutiremos mais sobre isso na **Seção III | Monte Estratégias**.



Um jeito útil de começar esse processo de mapear os atores é fazer uma chuva de ideias visual de todos os atores no campo e a natureza das relações entre eles, como demonstrado nos exercícios a seguir.

2.3a Exercício

Mapa visual dos atores - parte 1

Propósito & Resultado

A ideia deste exercício é começar o processo de visualizar a si mesma, seu grupo ou organização, e suas relações com os atores ao seu redor, incluindo conexões diretas, indiretas e potencialmente futuras.

Nesta parte, sugerimos que você foque nos atores ao seu redor e na intensidade da sua relação com eles (direta, indireta ou potencial).

No próximo passo do exercício, você ampliará a visualização ou o mapa de forma a incluir os tipos de relacionamentos que você tem com eles.

Informações de entrada & Materiais

Se você deseja fazer essa atividade num grupo, será preciso:

- papel pardo ou cartolina
- canetinhas coloridas ou canetas
- notas adesivas.

Formato & Passos

Visualização escrita/desenhada

Neste exercício, sugerimos que você use as notas adesivas, cada uma com o nome de um ator do seu contexto, para mapear visualmente eles e suas relações.

1. Comece consigo mesma ou com sua organização como uma entidade e faça uma chuva de ideias identificando o maior número possível de atores relacionados com seu trabalho. Isso pode incluir indi-

víduos, grupos, organizações ou instituições. Considere atores locais, regionais, nacionais e internacionais onde for necessário.

2. Uma vez identificado tantos atores quanto você conseguir, coloque-os na parede ou numa cartolina, com você (e/ou seu grupo, caso seja identificável) no centro.
3. Pense na seguinte categorização para esses atores:

- **Direta**: Pessoas, grupos, organizações, instituições que têm contato direto com você com respeito à questão que você está tentando causar impacto. Por exemplo, provavelmente você tem uma relação direta com o grupo-alvo para o qual trabalha e com algumas entidades que se opõem diretamente ao seu trabalho. Você pode querer incluir membros da comunidade ao seu redor, seja sua família e amizades, pessoas que apoiam ou se opõem ao seu trabalho de uma forma ou de outra.
- **Indireta**: Aqui podem entrar pessoas, grupos, organizações ou instituições que estão um passo afastadas de você. No exemplo acima, se o grupo-alvo tem uma relação direta com você, ele pode estar em relação direta com outros. Estes se tornam indiretamente conectados a você.
- **Potencial/Periférica**: pessoas, grupos, organizações e instituições que têm relação com o assunto, mas com as quais você (ainda) não tem uma conexão ou relação. Exemplos disso incluem corpos internacionais que podem ser simpáticos à sua causa, mas (ainda) não estão ativos no seu contexto.

Nota: Atores e informações

Embora possa não ter lhe ocorrido, você pode querer incluir atores nos quais você confia para o cuidado da sua informação e comunicação. Podemos incluir aqui:

- sua companhia telefônica
- seu provedor de serviço de internet

- provedores de contas de mídias sociais
- provedores de contas de email

Exploraremos esses atores em mais detalhes no próximo exercício.

Lembretes & Dicas

No próximos capítulos, expandiremos nosso conhecimento desses atores e usaremos eles para construir nossa análise de ameaças. Assim que tiver terminado esse exercício, é uma boa ideia manter uma lista desses atores para ter uma referência e para elaborações futuras.

Expandir nosso conhecimento sobre os atores

Uma vez que tenhamos estabelecido os atores em nosso ambiente, pode ser útil categorizá-los, o melhor que soubermos e conseguirmos, segundo a natureza das relações entre nós e esses atores, especialmente suas posições com respeito à nossa visão, seus interesses e a quantidade de recursos que possuem.

Podemos categorizá-los grosseiramente em três grupos:

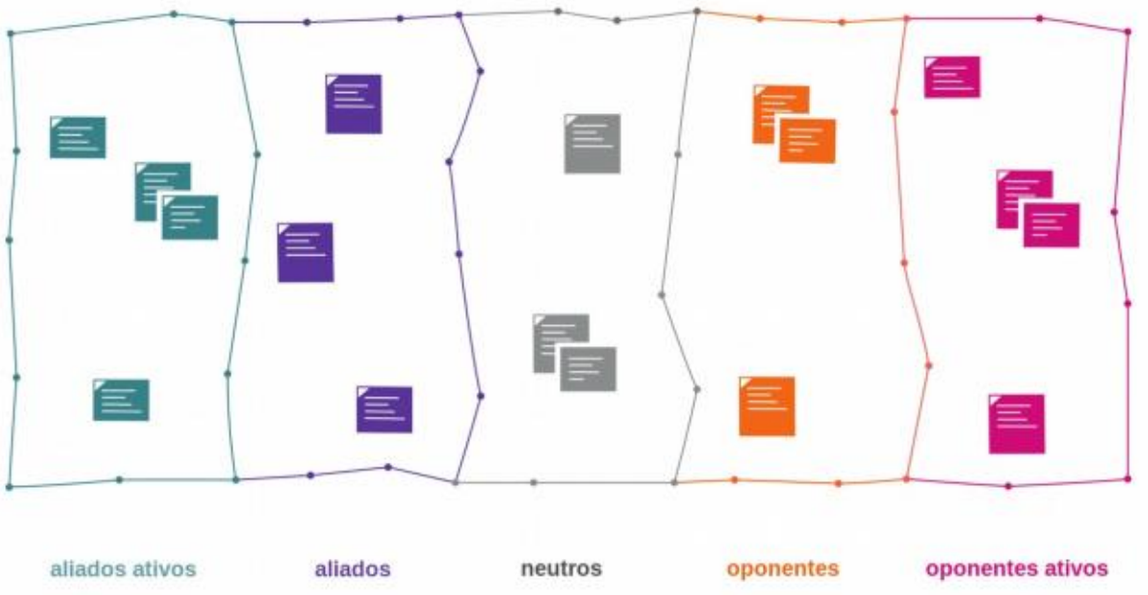
- **Aliados**: são os atores com alinhamento estratégico com nossos objetivos. A força e a duração do seu apoio podem flutuar com o tempo. Aqui podem entrar defensores de direitos humanos e organizações companheiras, a comunidade onde trabalhamos, elementos amigáveis do Estado, embaixadas e nossas amizades.
- **Adversários ou oponentes**: esses são os atores cujos interesses estratégicos são opostos aos nossos, ou se opõem de alguma forma aos nossos objetivos por diversas razões. A intensidade da oposição pode variar com a mudança das circunstâncias. Para algumas pessoas defensoras de direitos humanos, especialmente aquelas que trabalham com

gênero e direitos sexuais, aqui também podem entrar os membros da família.

- **Neutros**: são aqueles que nem apoiam nem se opõem à nossa causa. Entretanto, o seu papel pode mudar dependendo das mudanças na situação.

Pode ser útil imaginar ou visualizar esses atores como um **espectro**:

Espectro de Aliados



O "espectro de aliados" [8] ilustrado acima é comumente usado na organização de uma campanha de ação, para poder identificar os setores importantes da sociedade que queremos influenciar para que eles se mexam na direção contrária da de nossos oponentes e se enquadrem na posição de alianças ativas. Também pode ser

8 Baseado no exercício "Espectro de Aliados" do "Treinando para a Mudança". Um bom aprofundamento sobre o engajamento com os atores dessas categorias pode ser encontrado aqui: https://organizingforpower.files.wordpress.com/2009/05/allies-chart-new1.jpghttp://www.trainingforchange.org/tools/spectrum-allies-0

usada no planejamento de segurança e na promoção de aceitação e tolerância de nosso trabalho entre diferentes elementos do Estado e da sociedade.

Mapear as relações entre os atores

O próximo passo no nosso exercício de mapeamento visual de atores inclui analisar, identificar e especificar a natureza das relações entre os atores. Esse passo é particularmente útil para identificar os atores cujas motivações podem levá-los a nos ameaçar ou o nosso trabalho, assim como os aliados em quem podemos confiar para nos ajudar a trabalhar com mais segurança

2.3b Exercício

Mapa visual dos atores - parte 2

Propósito & Resultado

Este exercício é baseado no **Exercício 2.3a** e busca encontrar no mapa as relações entre os atores, identificando os aliados, oponentes e neutros.

O mapa resultante pode então ser usado para identificar e analisar atores específicos no nosso contexto que podem representar fontes intencionais (ou não intencionais) de ameaças.

Informações de entrada & Materiais

- Um mapa básico de atores (do exercício anterior)
- Papel e canetinhas ou canetas
- Alfinetes coloridos

Formato & Passos

Visualização escrita/desenhada

Considerando todos os atores que você conseguiu anotar até agora:

1. Marque os atores com base na natureza das suas relações com o seu trabalho (aliados, adversários,

neutros, desconhecido). Isso pode ser feito pela assinação de pontos coloridos para cada tipo de ator, diferentes cores de notas adesivas, ou diferentes posições (aliados na esquerda, oponentes na direita, neutros no meio, etc.)

2. Desenhe um círculo ao redor de cada ator no mapa. O seu tamanho corresponde a **seu poder e seus recursos** no contexto sociopolítico (veja a legenda).
3. Começando consigo mesma no mapa, você pode fazer conexões com qualquer ator com o qual tem uma relação.

Use a legenda na próxima página para representar os diferentes tipos de relações que existem entre os atores no mapa.

Exemplos de relações a incluir aqui são:

- **Relações próximas**: onde os atores têm uma relação positiva entre si.
- **Alianças**: onde os atores coordenam suas atividades entre si e agem juntos.
- **Relação fraca ou desconhecida**: relações com pouco contato, ou onde a natureza do contato é desconhecida.
- **Conflito**: onde dois atores possuem uma relação antagônica entre si.
- **Conflito violento**: onde a relação é caracterizada pela violência física (potencialmente armada) de uma ou mais partes.
- **Compulsória**: onde um ator possui poder sobre outro e pode obrigá-lo a fazer algo por exemplo, um grupo paramilitar que é controlado pelas forças armadas).
- **Interdependência**: onde duas entidades estão liga-

das entre si de alguma maneira.

Lembretes & Dicas	É útil revisitar e refletir periodicamente sobre o mapa que você criou e fazer qualquer adição, subtração ou mudança que lhe ocorrer. Lembre-se, é importante que ele seja reavaliado e atualizado com frequência, especialmente antes de uma nova ação.

Planilha adicional de informações de atores

Para cada aliado ou oponente (mas priorizando os que estão ativos), pode-se trabalhar mais sobre a natureza das relações deles com seu trabalho e criar uma planilha de informações que forneça mais dados sobre suas motivações, interesses, a história de suas relações com você e seus recursos (materiais, financeiros, relacionais e outros).

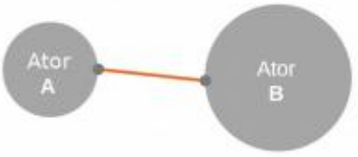
Essa planilha de informações será útil para:

- identificar os interesses e relações subjacentes que motivam suas posturas. Por que eles estão "com" ou "contra" você?
- identificar os recursos e estratégias que possuem e empregam e que podem usar para ajudar ou atrapalhar o seu trabalho. Pense também sobre suas posições dentro do contexto sociopolítico mais amplo e quais privilégios e recursos eles podem usar dessa posição.

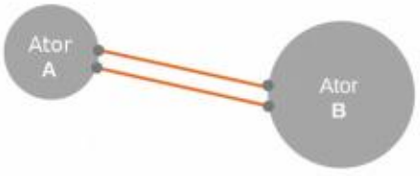
É importante notar que essas motivações e recursos podem mudar com o tempo. Essa análise deve ser atualizada regularmente sempre que novas informações aparecerem. Além disso, é muito importante considerar a confiabilidade das fontes de informação: se foram conseguidas através de contatos pessoais, redes informais, mídia local, ou outros.

Legenda[9]

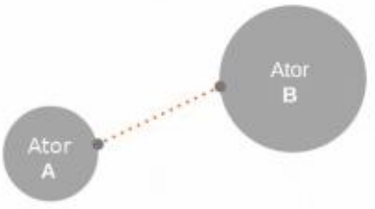
Círculos de tamanhos diferentes representam diferenças em poder.



Uma linha cheia representa uma relação próxima. Você também pode "interromper" a linha (cruzando-a pelo meio) se existe uma relação rompida.



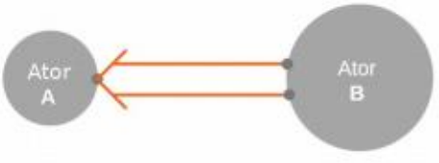
Uma linha dupla representa uma aliança.



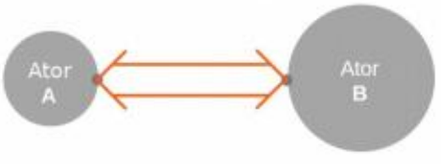
Uma linha pontilhada representa uma relação fraca ou desconhecida.

Uma linha em zig-zag representa um conflito ou uma relação ruim.

Uma linha dupla em zig-zag representa um conflito violento.



Uma linha dupla com uma seta representa dominação, controle ou compulsão (onde um ator age sob as ordens de outro).



Uma linha dupla com setas dos dois lados representa uma interdependência.

9 Adaptado do KURVE Wustrow (2006) Transformação Não-Violenta de Conflitos Um Manual de Treinamento para um Curso de Treinamento de Treinadores. Centro de Treinamento e Rede em Ação Não-Violenta KURVE Wustrow e.V., Wustrow. (pdf: http://www.trainingoftrainers.org/), pp.45-46.

Uma vez tendo completado o mapa visual de atores pela primeira vez, pode ser útil transferir essa informação para outro formato onde possa ser atualizado com frequência de acordo com seu monitoramento e análise da situação, e com as mudanças nas suas atividades.

No próximo segmento, veremos a importância da informação e como ela se move entre nós e os atores no mapa. Além de explorar por que devemos prestar atenção à nossa própria informação, como ela é gerada, usada, compartilhada, guardada, etc, também exploraremos quais medidas tomar para proteger nossa comunicação e nossas informações.

4
Compreendendo e Catalogando nossas Informações

Este capítulo busca desenvolver um entendimento sobre o que "informação" de fato significa em relação a nossas atividades e objetivos como ativistas. A importância do gerenciamento da informação não deve ser subestimada, especialmente dado o crescimento do uso de tecnologias digitais no contexto da defesa e promoção de direitos humanos. Embora essas ferramentas forneçam a você um grande potencial para comunicação, pesquisa, organização e campanha, elas também são um dos alvos principais para os nossos adversários que buscam nos colocar sob vigilância, reunir informações ou atrapalhar nosso trabalho.

Quando falamos de "informação" no contexto do nosso trabalho, estamos dizendo muitas coisas, como:

- O resultado do trabalho que estamos fazendo; como relatórios, bases de dados de violações de direitos humanos, imagens, gravações de voz e vídeo.
- Informação operacional que nos ajuda a realizar nosso trabalho; como nossas mensagens de textos durante uma ação, nossos ar-

quivos e relatórios e outras informações e comunicação de escritório, incluindo documentos financeiros, documentos sobre recursos humanos e organização estratégica.

- Informação pessoal que identifique quem somos, tanto como membros de uma organização como outras afiliações pessoais ou profissionais.
- Dados gerados pelo nosso uso de dispositivos digitais durante nosso trabalho, ou "metadados", que podem ser usados para rastrear nossos movimentos ou monitorar nossas relações.

Essa informação pode ser guardada e comunicada de muitas formas: em papel, nos nossos computadores, telefones celulares, pela internet, em servidores de arquivos, serviços diversos da internet e redes sociais. Tomadas como um conjunto, essas informações compreendem um dos bens mais importantes que qualquer uma de nós (ou qualquer organização) tem. Assim como qualquer outro bem, eles nos servem melhor quando temos garantias de que são devidamente cuidados para que, de forma acidental ou maliciosamente, não se percam, se corrompam, se comprometam, sejam roubados ou usados de forma incorreta.

Quando estamos cuidando de nossa segurança, precisamos cuidar da segurança de nossa informação. Informações sobre nós, nossas atividades e nossos planos podem ser muito úteis para nossos oponentes e, com o aumento do uso de dispositivos digitais e mídias sociais, é crucial que tenhamos certeza de que somos nós que estamos no comando de quem tem e controla nossa informação. A vigilância e a coleta de informações sempre têm sido usadas para planejar ataques contra defensores de direitos humanos e esse tipo de invasão do direito à privacidade pode, por si mesmo, ser considerado uma forma (geralmente baseada em gênero) de violência.

Ameaças comuns à informação de DDH

Perda de dados

Devido à uma higiene pobre do computador, infecções de *malwares*, cortes de luz ou hardware velho, computadores e outros dispositivos ocasionalmente param de funcionar causando a perda de nossos dados.

Contas comprometidas

Às vezes, nossas senhas ou "perguntas secretas" não são muito difíceis de quebrar, ou estamos sujeitas a fraudes virtuais (*phishing*) (que podem ser aleatórias ou direcionadas especialmente para nós) e, sem que saibamos, caem na mão de terceiros, que ganham acesso às nossas contas de email ou redes sociais.

Apreensão ou roubo de dispositivo

Computadores e telefones celulares são alvos comuns de ladrões. Além disso, se estamos sob um risco muito grande, nossos escritórios e casas podem sofrer invasões por parte do Estado ou de atores não estatais, e computadores, telefones celulares, discos rígidos, pendrives e servidores podem ser "confiscados" ou roubados para análise.

Inspeção de dispositivos em *checkpoints*

Às vezes, pode ser que nosso dispositivo seja temporariamente confiscado enquanto cruzamos uma fronteira ou *checkpoints* militares, onde nossos dados podem ser copiados ou nosso computador pode ser infectado com um *spyware* ou voltar com um *keylogger* em *hardware* acoplado.

Entrega de informações

Provedores de serviços de internet e os provedores de email e sites de redes sociais que usamos também podem entregar nossos dados para certas autoridades se existir um pedido legal para isso. Enquanto eles protegem nossos dados de algumas, estão muito interessados em dar a outras, e essa situação está em constante mudança de acordo com seus interesses políticos e de negócios.

Vigilância e monitoramento

Investidores que negociam dados, provedores de internet, provedores de email e muitas outras companhias sujeitam a população em geral à vigilância através da coleta e do armazenamento de detalhes de nossas atividades *online*. Enquanto em alguns casos isso tem o simples objetivo de compulsoriamente nos direcionar propagandas, também pode ser usado para identificar minorias específicas, às quais podemos pertencer, e tê-las como alvo de uma vigilância profunda.

Malware direcionado

A indústria de *malwares* direcionados vem crescimento muito: algumas autoridades estatais e outros grupos investem em *softwares* projetados para nos enganar e nos fazer baixar algum *malware* e assim dar acesso futuro a um atacante a todos os dados em nossos dispositivos.

A segurança de nossa informação é criticamente importante e por isso, protegê-la torna-se uma fonte de ansiedade. Uma estratégia de segurança da informação efetiva e atualizada pode nos dar a paz de espírito necessária para focar em nossos objetivos e realizar nosso trabalho de maneira saudável.

O primeiro passo envolve um processo de catalogação, o melhor possível, de todas as instâncias e versões de nossa informação. Criar uma compreensão mental de quais elementos existem em

nosso próprio “ecossistema” informacional irá nos ajudar a afastar-nos de perceber a “informação” como uma massa vaga de dados, e nos levar em direção a um melhor entendimento dela como um recurso tangível e importante.

Ao catalogar nossa informação em vários componentes e tipo, podemos identificar qualquer potencial situação e áreas onde nossa informação pode estar ou pode vir a estar vulnerável, assim como áreas onde precisamos melhorar a sua guarda.

Esse processo se baseia no que tiramos dos exercícios anteriores onde identificamos os “atores” em nosso contexto, incluindo nós mesmas, nossos aliados, oponentes e grupos neutros. Pode ser que voltemos e aumentemos o mapa de atores com os potenciais novos atores identificados através do processo de mapeamento da informação. O mapa também deixará mais fácil de entendermos as relações entre os elementos de nossas informações e nossos aliados e oponentes e suas intensões e capacidades.

Em seguida, olharemos para alguns conceitos chave para compreender como catalogar nossa informação, seguido pelo exercício do “ecossistema informacional”, que nos ajudará a gerar um mapa de nossos bens informacionais mais importantes.

Categorias de informações

O primeiro passo para criar uma estratégia de segurança da informação é conhecer quais informações temos, onde elas estão e como elas se deslocam de um lugar para outro.

Uma maneira simples de começar esse processo de catalogação é pensar na informação em termos daquela que está, num primeiro momento, parada (em descanso) e da que viaja (em movimento). Exemplos poderiam ser a informação financeira guardada num armário de arquivos (informação em descanso) e, por outro lado, trocas de mensagens via telefone celular antes de um evento (informação em movimento).

Essa distinção é usada primariamente como um princípio organizativo, para ajudar com o processo de catalogação. É importante lembrar que hoje muita da nossa informação está na forma digital e, com o aumento do uso da internet e dos serviços de armazenamento remoto (a "Nuvem"), muita da informação que possuímos está num momento ou em outro em movimento. De forma similar, devido ao aumento da popularidade de dispositivos portáteis (tais como *smartphones* e *tablets*), ao aumento da capacidade de armazenamento e da mobilidade desses aparelhos, qualquer informação guardada neles, embora possa estar digitalmente "em descanso", está na verdade movendo-se no espaço físico.

Vale repetir que usando a categorização acima, nossa comunicação – tais como emails, bate-papos, mensagens de texto e chamadas telefônicas são "informação em movimento", e que elas são extremamente comuns, especialmente no contexto de estar quase constantemente conectada à internet. Esse princípio organizativo pode se tornar útil quando decidimos quais táticas empregar para manter nossa informação mais segura, pois existem formas distintas de cuidar da informação em descanso e daquela em movimento.

Informação em descanso

Uma vez que tenhamos estabelecido nossa visão, precisamos considerar os métodos que empregaremos para realizá-la. Podemos fazer diversas atividades como indivíduos ou organizações para alcançar nossos objetivos. Quais são as suas "áreas de trabalho" ou as atividades que você faz?

É importante listar explicitamente cada uma delas e considerar, num primeiro momento, se elas são apropriadas ou não para alcançar o objetivo que escolhemos. Nosso trabalho não acontece no vácuo, mas ao invés disso, num contexto rico e variado, geralmente com algumas características de conflito. Nossas atividades são a nossa "interface" com esse conflito, com o Estado e com a sociedade que estamos tentando influenciar; elas são nossos meios de tentar mudar as situações, as percepções e os comportamentos

de um variado conjunto de atores (pessoas, instituições e organizações) à nossa volta. Alguns desses atores irão se beneficiar com, acreditar e apoiar nossas atividades. Outros, porém, irão perceber que essas atividades não são do seu interesse e tentarão fechar o nosso espaço de trabalho.

Tudo isso frequentemente pode fornecer informações sobre uma pessoa, um projeto, um movimento ou uma organização, e por essa razão, roubo e apreensão de computadores, telefones, e dispositivos de armazenamento de dados são táticas comuns dos oponentes de defensores de direitos humanos.

Quando fizerem uma lista com a chuva de ideias sobre a "informação em descanso", é útil considerar alguns atributos, como:

- onde elas estão
- quem tem acesso a elas
- quão sensíveis são os seus conteúdos para você, sua organização ou para as pessoas mencionadas no documento (por exemplo, depoimentos de testemunhas ou vítimas)
- quão importante é mantê-las guardadas
- por quanto tempo deverão ficar guardadas.

Informação em movimento

Como mencionado anteriormente, muitos dos nossos bens informacionais(especialmente na forma digital) são, em algum momento, transportados de um lugar para outro. Considere todas as formas que suas informações podem se mover:

- a caixa lotada de documentos que você mandou para os arquivos via entregador
- a chamada telefônica que você faz usando a rede de telefonia celular
- vídeos de um evento que você sobe num servidor *online*

- a informação dos contatos no seu telefone celular quando participa de um protesto.

Nos exemplos acima, podemos ver várias formas de como nossa informação se move: partes físicas de informação viajando no espaço físico, ou informação digital viajando pela internet, ou informação digital (guardada em dispositivos físicos) movendo-se pelo espaço físico.

Devemos também prestar atenção para as diferentes maneiras que nossa informação pode viajar:

- **Transferência**: seja movê-la quando mudamos de escritório, ou quando um anexo é enviado para um colega pela internet, ou o a cópia de segurança (*backup*) de arquivos sensíveis em um servidor em outro local, nossa informação está sendo transferida de um ponto para outro.
- **Comunicações**: quando interagimos com nossos colegas, aliados, com o público e mesmo com nossos oponentes, existe uma troca de informações acontecendo. A comunicação pode tomar a forma de instruções sendo anunciadas por um alto-falante num evento, ou uma troca confidencial de informação durante uma conversa telefônica, uma chamada de vídeo, uma reunião ao vivo, por email, mensagens de texto e muitas outras. Nossa comunicação contém montanhas de informações sobre nossas intensões, a situação atual de nossa ação, e nossos planos e atividades futuras.

Para catalogar tais informações, além dos atributos mencionados para “informações em descanso”, você também pode pensar em:

- como a informação é transferida
- qual rota física ou virtual ela segue
- quem pode ter acesso durante o caminho, ou quem pode estar interessado em capturá-la (considere o seu mapa de atores)?

Informação em formato digital

Existem alguns atributos únicos relacionados à informação que está em forma digital que vale a pena considerar:

- **Replicação**: informação na forma digital é constantemente replicada. Durante uma transferência de arquivos, trocas de emails, cargas e descargas de arquivos pela internet, e mesmo quando a movemos de um dispositivo para outro, cópias da informação são criadas, o que para todos os casos e propósitos são idênticas ao original. Essa é uma diferença importante com relação à era pré-digital onde era possível (embora em certos momentos, muito difícil) distinguir entre uma informação original (por exemplo, atas de uma reunião batidas à máquina numa folha de papel) e suas cópias subsequentes.
- **A "permanência" da informação**: como colocado acima, uma vez que se sobe uma informação na internet, o processo de subida (*upload*), transferência e descarga (*download*) engendra múltiplas ocasiões onde a informação é copiada. A consequência é que nossa informação pode ser retida em algum lugar enquanto trafega por partes da internet que não temos controle (como geralmente é o caso). A cópia e o translado entre os nós da rede acontece quando servidores de email, roteadores e pontos intermediários fazem cópias da informação para ajudar o processo de transferência, ou para outros propósitos, dependendo das intenções de quem quer que controle os aparelhos. Logo, é importante entender que é possível que uma informação fique armazenada de forma intencional ou não por um (ou mais) desses atores por um longo período. Um exemplo que muitas pessoas podem atestar são as mensagens de texto. Essas mensagens foram enviadas de um celular par ao outro, mas durante o envio, elas passam por várias torres de celular e outras infraestruturas que pertencem à companhia telefônica. A

companhia tem acesso a essas mensagens e irá, em muitos casos, retê-las por um período de tempo, independentemente de você tê-las deletado de seu celular ou não.

- **Metadados**: Quando os computadores e dispositivos digitais realizam suas operações, uma camada de "metadados" é criada. Metadado é uma informação criada sobre e para esses processos computacionais. Essa informação acompanha o próprio dado enviado, e algumas vezes não pode ser removido dele. Exemplos de metadados incluem:
  - O seu **endereço de IP** que serve para localizar onde você está conectando na internet, e o endereço de IP dos sites que você visita.
  - os **dados de localização** do seu telefone celular enquanto ele se move de um ponto a outro, **os números identificadores únicos do seu cartão SIM e do seu telefone** (conhecido como número IMEI). Em geral, não é possível mudar o IMEI do seu telefone.
  - **remetente, destinatários, registro de data e hora e assunto de email, e se eles possuem algum arquivo anexado.** Essa informação não pode ser apagada, pois o servidor precisa saber para quem enviar os emails e seus anexos. Entretanto, alguns deles podem ser alterados ou ofuscados (disfarçados).
  - **as propriedades de um arquivo de imagem**, ou seja, a informação sobre a localização onde a foto foi tirada, seu tamanho e o equipamento usado para produzir a imagem (marca da câmera e das lentes, o software usado para editá-la). Algumas dessas informações podem ser apagadas usando um software de processamento de imagem.
  - **propriedades de um documento**, ou seja, a informação sobre autoria, data de criação ou modificação do documento. Algumas dessas informações podem ser apagadas ao mudar as configurações pessoais de privacidade

do processador de texto ou planilha, ou usando um software para remoção de metadados como o MAT (*Metadata Anonymization Toolkit*).[10]

Os metadados geralmente passam despercebidos porque não são alguma coisa que nós criamos ou que estejamos inteirados da existência. Porém, devemos manter em mente sua existência e tomar os passos apropriados para entender seu escopo e as possíveis ramificações que aparecerão ao considerarmos os diferentes elementos de nosso ecossistema informacional.

Entendendo a informação em movimento através de canais digitais

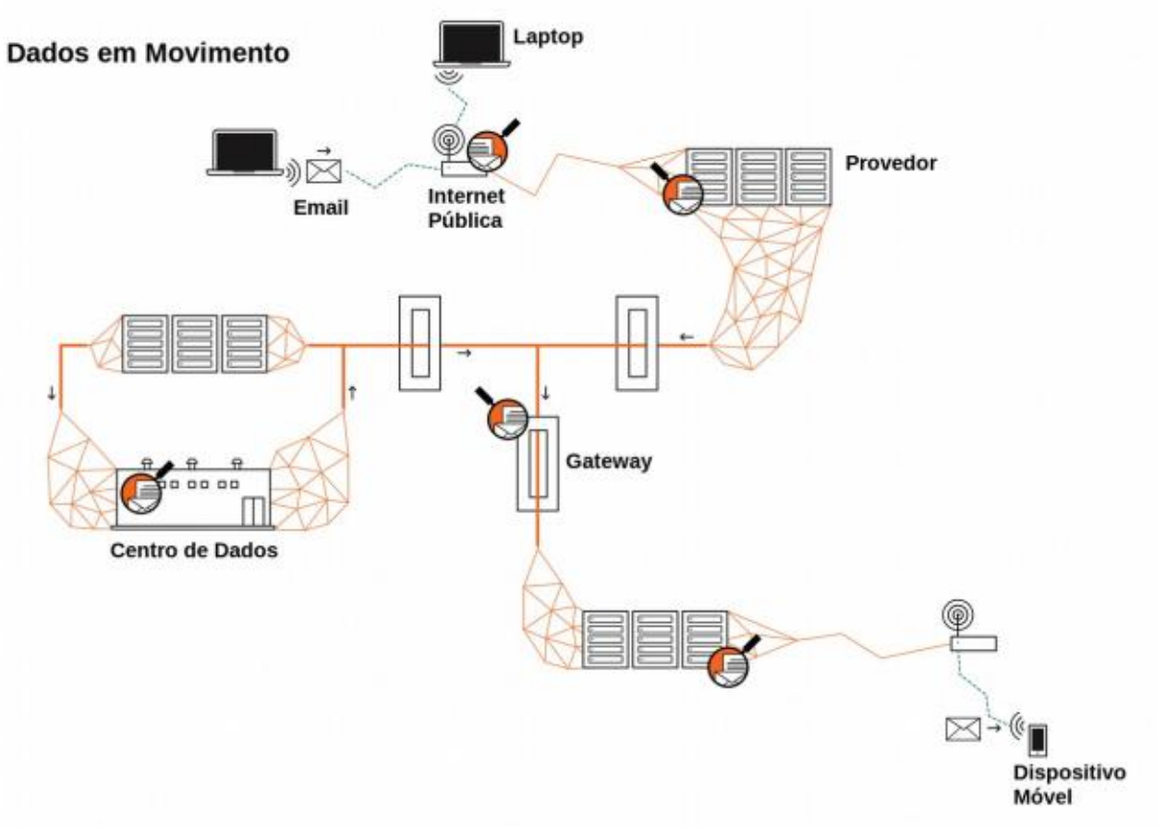
Os atributos das formas digitais de informação expostos acima têm um papel importante quando pensamos na nossa informação em movimento através de canais digitais, uma vez que a informação pode ser tão prontamente duplicada e armazenada. A informação está em movimento através de canais digitais quando nós:

- nos comunicamos usando nossos dispositivos: fazer chamadas usando telefone celular, enviar emails, fazer chamadas usando *voice-over-IP*, teleconferências, mensageria instantânea ou enviar mensagens de texto.
- transferimos dados: subir vídeos para um site, acessar uma página *web* no seu computador, fazer *backup* dos seus documentos em um servidor localizado em outro lugar, postar uma atualização em rede social.

A informação que viaja através de canais digitais está quase sempre se movendo pelo espaço físico, por exemplo, uma atualização de status que começa no seu telefone celular viajará para o site da sua rede social, que está fisicamente num servidor hospedado num de-

10 Veja https://mat.boum.org

terminado lugar, talvez no outro lado do mundo. Ela pode passar através de vários países pelo caminho. Para que possamos saber as formas pelas quais podemos garantir a segurança de nossa informação em movimento, é útil considerar sua origem, destino e o caminho por onde ela vai passar.



Embora possamos saber onde nossa informação se originou (por exemplo, escrevemos um email no nosso laptop), precisamos prestar atenção em onde ela irá chegar (por exemplo, a caixa de entrada de nossa colega, via o seu provedor de email), assim como todas as paradas ao longo do caminho, que podem incluir:

- Provedor(es) de serviço de internet
- as companhias de telecomunicação que operam a infraestrutura de internet e transferem seus dados
- entidades do Estado que realizam captura ativa e vigilância de dados e metadados enquanto são transferidos pela internet

- qualquer outra entidade que tenha controle sobre as paradas dos dados e possa ou não estar interessada em capturá-los
- terceiros como companhias de propaganda que podem coletar dados sobre suas atividades *online*.

O processo de movimentação da informação digital é relativamente simples. Tirar um tempo para aprender ou dar uma olhada no básico de como a internet e a comunicação de telefonia funciona pode nos ajudar a entender melhor esse processo. Fazendo isso, podemos reduzir nossa ansiedade ou nossos medos infundados que possam surgir devido à falta de informação, mitos e mistérios associados com as tecnologias digitais e a vigilância eletrônica.

Busque incluir também o tipo de criptografia (se houver alguma) usada para proteger dados. Criptografia é uma medida técnica para reduzir o número de pessoas que podem acessar certas informações. Às vezes, ela é fornecida pelor provedores de serviços (por exemplo, sites de bancos ou alguns aplicativos de comunicação[11]), embora frequentemente tenhamos que aprender a criptografar nossa informação ou comunicação usando certos softwares para ter mais certeza de que eles não serão acessados indevidamente.

Dedicar atenção ao que foi dito acima é também importante pois pode sugerir novos elementos no nosso mapa de atores. Podemos descobrir que precisamos investigar se existe alguma relação entre esses atores e nossos aliados ou oponentes. Tendo refletido sobre isso, você pode querer voltar ao seu mapa de atores e incluir outros como:

- seu provedor de serviços de internet ou de hospedagem de sites
- sua companhia telefônica
- provedores dos serviços de email e redes sociais
- qualquer entidade relevante (por exemplo, agências do governo) que podem ter alguma relação com o que descrevemos acima.

11 Para mais informação sobre como proteger suas comunicações, veja Security in a Box https://securityinabox.org/en/guide/secure-communication

Essas adições criam um quadro mais claro do que existe no nosso ecossistema informacional, assim como ajuda a listar qualquer novo ator que possa estar envolvido em nosso trabalho como consequência de como nossa informação é manuseada. Esse conhecimento nos ajudará a proteger nossa informação de forma mais eficiente. Pode ser através da implementação de políticas sobre quem pode acessar qual informação, ou usar softwares que protejam nossa informação, tais como aqueles que deletam de forma segura os dados de nossos dispositivos ou criptografam nossas conversas e emails.

No próximo segmento, iremos realizar um exercício para mapear nossa informação "em descanso" e nossa informação "em movimento". Isso será útil para identificarmos as brechas em nossas práticas de gerenciamento de informação assim como os caminhos para cobrir essas falhas.

Mapeando nosso ecossistema informacional

Considerando tudo o que foi exposto acima, este exercício ajudará a criar e manter um mapa sobre sua informação, ou da sua organização, que categoriza seus documentos e as informações relacionadas ao seu trabalho. Ele ajudará a entender o estado atual de suas informações sensíveis e quem pode ter acesso a elas, com o objetivo de tomar medidas para protegê-las. Isso pode incluir políticas sobre quem pode acessar quais dados, assim como métodos técnicos como criptografia.

Esse "mapa da informação" pode adquirir a forma de um documento de texto ou planilha que possa ser atualizada regularmente. No exercício a seguir, seguiremos os passos para criar tal documento, e assim teremos um modelo que pode ser bem útil.

Quando criamos um mapa da informação, é útil considerar as seguintes questões:

O que é informação?

Um princípio organizativo aqui é agrupar os tipos similares de informação. Por exemplo, você pode decidir que todos os documentos financeiros pertencem à mesma categoria, mas nem todos os emails ficarão juntos. Agrupar "o quê" de acordo com o tipo de informação depende enormemente do jeito que você e sua organização funcionam. Inclua também aqui os softwares que você usa, pois eles podem ser vistos como um conjunto de informações, e alguns podem ser considerados sensíveis.

Como foi mencionado previamente, um tipo de informação do meio digital e das comunicações que geralmente não consideramos são os metadados. Especialmente para a informação "em movimento", é uma boa ideia incluir os metadados de certos documentos e comunicações (tais como arquivos de imagens e emails) e considerar se eles precisam ser removidos ou distorcidos para proteger sua privacidade.[12]

Onde ela fica?

Quais são os lugares ou entidades físicas onde seus bens informacionais são mantidos? Podem ser: servidores de arquivos no escritório, servidores *web* nos provedores de serviço, servidores de email, *laptops*/computadores, discos rígidos externos, pendrives, cartões de memória e telefones celulares.

Quem tem acesso a ela?

Considere aqui a situação como ela de fato é, ao invés de algo que você aspira alcançar. Por exemplo, no caso de uma pasta pessoal de relatórios no computador de um escritório, as pessoas que têm acesso a ela podem incluir: a própria autora dos relatórios, qualquer técnico de TI que cuida do servidor, pessoas de confiança, etc.

12 Para mais informações sobre como remover os metadados de arquivos, veja https://securityinabox.org/en/lgbti-mena/remove-metadata e para permanecer anônima *online*, veja https://securityinabox.org/en/guide/anonymity-and-circumvention

Quão sensível ela é?

Existem muitas maneiras de classificar o quão sensível é um documento. É uma boa ideia estabelecer uma categorização explícita para informações sensíveis com instruções claras sobre como elas devem ser protegidas. O objetivo aqui é que você tenha uma escala que seja aplicada consistentemente à sua informação e que irá lhe ajudar a identificar os dados que são mais prováveis de estarem sob risco e os meios pelos quais eles devem ser protegidos.

Abaixo temos um exemplo de uma escala de três marcações:

- **Secreto**: somente pessoas específicas devem ter acesso à essa informação. Existe uma cadeia clara de responsabilidade para esse tipo de informação (por exemplo: arquivos de pacientes numa clínica).
- **Confidencial**: esse tipo de informação não é para uso público, mas não existe nenhuma necessidade específica que impeça os membros do grupo de apoio da organização de acessá-los.
- **Público**: esse tipo de informação não representa nenhum risco caso seja exposto ao público. Entretanto, ainda é necessário políticas gerais para manter sua integridade e salvaguarda.

É importante notar que, durante um projeto, a confidencialidade dos dados envolvidos pode mudar. Por exemplo, se estamos investigando um caso de tortura para depois lançar um relatório público sobre ele, muitos dos detalhes envolvidos serão inicialmente secretos ou confidenciais. Mais tarde no projeto, uma vez que os dados foram reunidos, aquilo que continuará sendo confidencial deverá estar separado do que deve ir a público como parte de um relatório.

Considerando nossa informação sob a luz dessas questões, podemos criar um documento que represente um mapa da nossa informação como ela atualmente é. Entretanto, como foi mencionado

acima, é importante lembrar que esse é um documento vivo e que deve ser atualizado regularmente.

2.4 Exercício

Ecossistema informacional

Propósito & Resultado	O objetivo desse exercício é fazer um inventário dos bens informacionais mais importantes que você lida, para criar políticas para melhor guardá-los em seguida.
Informações de entrada & Materiais	Pode ser útil reproduzir a tabela-exemplo abaixo, seja imprimindo-a ou desenhando-a numa cartolina ou outros materiais.
Formato & Passos	Chuva de ideias e documentação Para começar o exercício - especialmente em grupo - pode ser útil usar uma planilha, ou uma grande folha e notas adesivas, ou alguma outra maneira que lhe permita realizar facilmente uma chuva de ideias e juntar as informações coletadas. Faça a chuva de ideias e monte uma lista com todos os dados que você gerencia. Se você não tem muito claro por onde começar, pense em: • dados relacionados a cada uma das suas atividades por direitos humanos • dados e arquivos pessoais, especialmente se estiverem armazenados no seu computador de trabalho • atividades de navegação online, especialmente dados sensíveis • emails, mensagens de texto e outras comunicações relacionadas às suas atividades por direitos humanos.

Imagine uma planilha que tenha diversas colunas enumerando categorias como descrito abaixo. Sua tarefa é preencher as colunas com informação.

Comece com suas informações em descanso e, para cada tipo de informação, elabore em cima do seguinte

- qual é essa informação?
- onde ela está?
- quem tem acesso a ela?
- quão confidencial ela é?
  - secreta
  - confidencial
  - pública
- quão importante é mantê-la?
- quem tem acesso a ela?
- como ela deve ser protegida?
- quanto tempo ela deve ser mantida antes de ser destruída?

Caracterize e qualifique a informação que você mapeou. Você pode repetir o mesmo processo e expandir a planilha com categorias adicionais para sua informação em movimento; por exemplo: dados sendo transferidos (fisicamente, eletronicamente), comunicações pela internet ou redes de telecomunicações.

As perguntas e o exemplo abaixo na **Tabela 2** pode lhe servir de ajuda.

Lembretes & Dicas

Esse processo é iterativo. Uma vez tendo feito a primeira rodada, pode ser que você detecte padrões e agrupamentos. Por exemplo, pode ser que você decida que uma vez que toda a informação financeira (independente do tipo) possui confidencialidade e longevidade similares, você pode agrupá-la e pensá-la como uma catego-

ria de informação financeira.

Por outro lado, você pode perceber que precisará expandir uma coluna em diversas colunas. Por exemplo, uma coluna contendo “email” precisa ser expandida para diversas colunas para levar em conta subcategorias de emails – e formas de guardá-las - que são sensíveis.

Esse documento deve ser algo vivo e irá mudar à medida que aconteçam mudanças e avanços na sua situação. Assim, você irá se beneficiar se atualizar regularmente esse documento anotando qualquer das mudanças que ocorrer.

Tabela 1.

Informação em descanso

O quê (exemplos)	**Atributos**			
	Onde ela fica?	Quem pode/tem acesso a ela?	Quão sensível ela é?	Como ela deve ser protegida?
Documentos financeiros em formato eletrônico	Pasta compartilhada - servidor de arquivos seguros	Equipe executiva	Secreta	Salva em uma partição escondida criptografada. Cópia de backup diário em discos rígidos criptografados
Relatórios para campanha contra censura	Pasta de documentos – servidor de arquivos	Membros da equipe, diretor do programa	Confidencial	Salva em uma partição criptografada
Adobe InDesign para desenvolvedor web	Conteúdo web no laptop do gerente	Administrador de conteúdo *web*	Confidencial	Com licença, protegido com senha

Tabela 2.

Informação em movimento

O quê (exemplos)	**Atributos**				
	Qual método de transferência você está usando?	Quem tem (ou quer) acesso a ela?	Quais caminhos físicos ou virtuais ela percorre (origem, caminho, destino)?	Quão sensível ela é?	Como ela deve ser protegida?
Emails em geral entre membros da equipe	Email (gmail)	Membros da equipe, provedor de email	Origem: computador da equipe técnica Caminho: internet (via servidores do Google) Destino: computadores da equipe técnica	Confidencial	Criptografia GPG
Verificações de rotina durante as missões	Mensagens de texto (SMS)	Membros da equipe, companhia de telecomunicação	Origem: telefone celular Caminho: rede de telefonia celular Destino: telefone celular	Secreta	Palavras em código

A essa altura, você já terá um documento inicial que descreve o ecossistema informacional da sua organização. Junto com o mapa de atores, ele será muito valioso à medida que você começa o processo de compreensão da sua força e resiliência, assim como das áreas de fraqueza ou vulnerabilidade.

Em seguida, você pode começar a desenhar um caminho que vai dos indicadores de segurança identificados, para cenários de

ameaças específicas, para planejamento de estratégias, planos, ferramentas e táticas que podem lhe ajudar a evitar esses tipos de cenários ou minimizar seus efeitos.

Até agora, nós:

- mapeamos quem são nossos aliados e oponentes, e os atores neutros que podem se tornar aliados ou oponentes dependendo da situação
- listamos algumas das relações que nós, nossos aliados e oponentes temos
- criamos nosso próprio documento do ecossistema informacional que irá nos ajudar a entender e priorizar nossa informação enquanto ela está parada em algum lugar, ou enquanto ela está viajando por diversos canais.

No próximo capítulo, mudaremos o foco de nossa análise para os indicadores que encontramos ao longo do nosso trabalho que podem nos alertar para potenciais ameaças e como sistematizar nosso conhecimento sobre eles para que possamos agir.

5
Indicadores de Segurança

Ao realizar análises regulares sobre a situação, mapeando nossa visão e os atores que estão operando conosco e contra nós, e entendendo nossa informação e o seu papel, a essa altura já devemos ter uma compreensão mais ampla do nosso contexto.

Desse ponto, podemos começar a buscar indicadores concretos de segurança. Eles são os elementos que observamos em nosso contexto que podem indicar ameaças com as quais nos deparamos ou uma mudança em nossa situação de segurança, como a emergência de novas ameaças ao nosso trabalho. Neste capítulo, exploraremos formas de procurar por esses indicadores em

nossa vida cotidiana, nossos dispositivos eletrônicos e nossos arredores. Eles podem nos alertar para um perigo iminente para nós ou para nossas amizades, colegas e pessoas com quem trabalhamos ou para nossa organização. Veremos também como e onde procurar por esses sinais.

Um indicador de segurança é qualquer coisa que notamos fora do comum que possa ter um impacto em nossa segurança. Indicadores de segurança podem incluir incidentes concretos como receber ameaças diretas, ataques contra organizações parceiras, ou comportamentos suspeitos de certas pessoas. Entretanto, também podem incluir acontecimentos mais sutis como mudanças no comportamento de nossos dispositivos ou em nossa saúde e bem-estar. O que eles têm em comum é que podem indicar uma mudança em nossa situação de segurança. Podemos identificar indicadores de segurança em vários diferentes momentos de nossa vida cotidiana e trabalho. Alguns exemplos seriam:

- receber uma carta das autoridades sobre uma busca iminente no escritório
- alguém tirar uma foto sua sem sua permissão, ou notar alguém fotografando as instalações de sua organização sem autorização
- não ser capaz de se concentrar e esquecer de fechar a porta do escritório
- abrir inesperadamente muitas janelas *pop-up* quando está navegando pela internet
- sentir-se exausta mesmo depois de uma boa noite de sono.

Como muitos dos passos anteriores, observar indicadores de segurança e utilizá-los como base para agir buscando evitar danos não é algo necessariamente novo para nós. No dia a dia, as pessoas geralmente fazem isso informalmente: por exemplo, uma série de assaltos acontecendo de noite num determinado bairro provavelmente irá, quando observado por outras pessoas, levar muitas delas a evitar aquela área ou a tomar precauções quando estiverem passando por ali.

Por enfrentarem maiores ameaças como resultado do seu trabalho, defensores de direitos humanos acabam frequentemente estando mais organizados sobre esse processo. É importante desenvolver o hábito de notar, gravar, compartilhar e analisar regularmente os indicadores de segurança com colegas e aliados. Essa prática ajuda de diversas maneiras.

1. Nos permite corroborar nossas observações com outras pessoas e entender se a noção de perigo que percebemos é compartilhada e irá nos mover para a ação.
2. Cria um catálogo desses itens, com os quais mais tarde podemos entender padrões de ameaças.
3. Alerta nossas aliadas para uma situação que possivelmente pode impactar sua própria segurança.

Identificando indicadores de segurança

Nós já temos um instinto (nossa intuição) para notar peculiaridades que podem afetar nosso bem-estar no dia a dia, tal como alguém nos seguindo, um veículo desconhecido estacionado em frente ao nosso escritório ou sentir insegurança num bairro desconhecido. Lembre-se que esses instintos são valiosos, mas não são de nenhuma forma precisos e podem nos deixar na mão de vez em quando.

Quanto a isso, os indicadores de segurança são mais facilmente notados uma vez que passarmos por um processo de estabelecer explicitamente uma linha-base: analisar e conhecer nosso meio sociopolítico, nossa vida cotidiana (incluindo nossas casas, escritórios, veículos e entre outros), nossos dispositivos eletrônicos e também nosso estado de saúde física e bem-estar emocional. Uma vez que tivermos estabelecido a "normalidade" para essa questão, será fácil perceber qualquer coisa que seja "anormal".

É bom estabelecer certar práticas com as quais podemos identificar regularmente e compartilhar potenciais incidentes de segurança. Abaixo, exploraremos algumas boas práticas que você pode realizar com regularidade para poder identificar indicadores e compartilhá-los e analisá-los mais eficientemente.

Monitorando nosso meio sociopolítico em busca de mudanças em segurança

Ao observar as tendências gerais e os acontecimentos particulares na situação política, econômica, social, tecnológica, legal e ambiental na qual operamos, como no monitoramento e análise situacional (veja o Capítulo 2, no início desta Seção), isso pode nos ajudar a identificar certos indicadores de segurança. Existem diversas atividades que podem ser úteis para alcançar esse objetivo, como:

Conversar com amizades e colegas confiáveis e organizações parceiras

Uma boa ideia é verificar regularmente com colegas, amizades e parcerias quem está engajada no mesmo tipo de atividade, ou atividade similar, para ver se essas pessoas notaram ou experimentaram alguma coisa fora do comum. Isso pode lhe ajudar a identificar padrões ou ficar atenta a indicadores similares.

Seguindo e documentando as notícias

Alguns indicadores podem ser retirados de fontes da mídia, onde podemos saber sobre as mudanças nos interesses e nos recursos disponíveis de nossos aliados ou oponentes (como identificados em nosso mapa de atores), ou ataques contra defensores de direitos humanos parceiros, o que podem ser importantes indicadores. Pode ser útil analisar com regularidade as grandes notícias sobre eventos com suas amizades ou colegas, de maneira informal ou durante reuniões marcadas para isso, para poder identificar tendências que podem indicar uma mudança na situação de segurança na qual vocês trabalham.

Encontrando-se com especialistas

Se você está entrando numa atividade ou começando a trabalhar sobre uma questão ou área que é novidade para você, pode ser útil en-

contrar-se com uma pessoa experiente e confiável que possa lhe dar informações com respeito a questões de segurança para tal trabalho.

Indicadores nas atividades cotidianas

Na vida cotidiana, existem muitas oportunidades para verificar e procurar por coisas que podem indicar uma mudança na sua situação de segurança. Como foi mencionado acima, algumas vezes isso vem instintivamente. Entretanto, dado que a intuição pode às vezes ser confusa e o cansaço ou o estresse podem afetar negativamente nossa atenção, pode ser útil considerar algumas das táticas apontadas no exercício abaixo.

Nota: esta lista é apenas um conjunto de exemplos e não pretende ser exaustiva. Busque tirar um tempo para sentar com seus colegas e amizades confiáveis para realizar ou discutir a atividade abaixo.

2.5a Exercício

Indicadores de segurança em nossa vida cotidiana

Propósito & Resultado	O propósito deste exercício é nos ajudar a ter uma visão geral de nossas rotinas e outras atividades diárias, tentando olhar claramente para elas e notando os pontos através dos quais podemos buscar indicadores de mudanças em nossa situação de segurança. Podemos usar essa visão geral de nossas rotinas para fazer uma lista de checagem dos momentos do dia onde podemos estabelecer uma linha-base e, em seguida, verificar se existem potenciais incidentes de segurança.
Informações de entrada & Materiais	Use qualquer material para desenhar, seja caderno, documento eletrônico, quadro, etc., para criar sua lista de checagem.

Formato & Passos

Visualização: desenho, escrita

Neste exercício, sugerimos que você use o desenho como uma forma de visualizar suas rotinas. Embora desenhar possa parecer estranho num primeiro momento, será um bom jeito de externalizar suas rotinas para ter uma perspectiva diferente sobre as atividades que você normalmente não considera do ponto de vista da segurança.

Desenhe um típico dia de trabalho, ou um dia no qual você realiza uma atividade considerada perigosa.

Não se preocupe em desenhar bonito ou de forma artística: apenas o suficiente para que você mesma possa entender. Comece simples: onde você está quando acorda. Considere coisas como:

- Onde você está quando toma o café da manhã (se é que toma)?
- Se trabalha fora de casa, como chega lá? Em qual veículo, com quem, e através de quais áreas?
- Quando chega no trabalho, quais dispositivos eletrônicos carrega consigo? Quais outras coisas está trazendo (chaves, carteira, etc.)?
- Onde você trabalha, e quem mais está lá? Como você trabalha e quais dispositivos usa para isso?
- Se você almoça ou janta durante o trabalho, inclua isso também. Quanto tempo você usa para comer e onde?
- A que horas para de trabalhar? Se trabalha longe de casa, de que maneira retorna? Qual caminho usa?
- O que você faz antes de dormir? A que horas geralmente você dorme?
- Onde você normalmente gasta seu tempo tirando trabalho e casa?

Uma vez que você tenha feito essa imagem do seu dia, tente olhar para os momentos onde você queira parar e

estabelecer uma linha-base, ou seja, como é um dia normal, para depois buscar por sinais, caso haja, de coisas fora do comum que estão acontecendo no seu arredor físico. Algumas sugestões poderiam ser:

- O veículo que você usa: existe algum sinal de alteração (rodas, freios, direção, etc.)?
- O caminho que você faz para o trabalho: tem alguma área perigosa? Vale a pena verificar se alguém está te seguindo?
- Seu escritório ou local de trabalho: está tudo no seu lugar quando você chega e antes de sair? As portas e janelas estão trancadas?
- O espaço imediatamente em volta de sua casa e seu escritório: existe alguém ou alguma coisa (por exemplo, estranhos, polícia ou veículos) fora do comum por ali?

Anote os momentos em que você irá procurar por sinais de perigo no seu entorno físico, e considere compartilhá-los com suas amizades, vizinhança e colegas confiáveis. Se você considera que está sob alto risco, pode ser que você queira incluir as rotinas de seus familiares ou outras pessoas próximas.

Crie uma lista de checagem a partir desses resultados: o que você irá verificar, e quando?

Lembretes & Dicas

Este processo foi criado visando ajudar tanto a identificar os momentos quando realizamos uma ação ou tomamos uma precaução baseada em nosso próprio sentido de segurança, mas também perceber momentos quando pode ser que sintamos que precisamos prestar mais atenção ou tomar precauções.

Se você está envolvida em muitas atividades em seu trabalho de defesa de direitos humanos, tente repetir esse exercício para os diferentes caminhos do seu trabalho.

O objetivo de compartilhar isso com amizades ou colegas confiáveis é garantir a certeza ou confirmar nossas observações e/ou olhar para áreas potenciais que talvez tenhamos deixado passar.

Importante: como monitorar os indicadores durante atividades perigosas?

Durante atividades mais perigosas, tais como um protesto ou uma ação de resistência, ou uma missão de monitoramento e documentação, temos que estar particularmente atentas aos indicadores de segurança, especialmente dado que a situação ao nosso redor pode mudar rápido. Considere realizar o exercício acima para essas atividades particulares e tome nota de quaisquer outros diferentes momentos nos quais você deve se assegurar de verificar possíveis sinais de perigo nos seus arredores físicos. Faça a sua própria lista de checagem!

Indicadores digitais de segurança

Pode ser que estejamos de alguma forma acostumadas a olhar para os indicadores de segurança em nosso ambiente sociopolítico ou no mundo físico, ou mesmo em nossa vida cotidiana. Entretanto, as ameaças que surgem no meio digital são cada vez mais relevantes para defensores de direitos humanos: censura de *websites*, apreensão de computadores e outros dispositivos e vigilância eletrônica são comumente usados para reunir informações, intimidar e/ou atacar defensores de direitos humanos.

Pode requerer um pouco mais de tempo e habilidade para perceber indicadores de segurança no mundo digital. Quando falamos de segurança digital, ainda não desenvolvemos um instinto

evolutivo para identificar ou reagir a ameaças, perigos ou mesmo perceber sinais que possam indicar risco à nossa informação. Além disso, devido ao acesso variado e frequentemente limitado à tecnologia, pode ser que não tenhamos muito conhecimento sobre dispositivos digitais e o conceito de insegurança digital em si pode parecer que está além das nossas capacidades. É possível desenvolver esse conhecimento e essa familiaridade com as tecnologias digitais, porém, geralmente, temos que começar do início e aprender a quais sinais prestar atenção em nossos dispositivos eletrônicos e sistemas que possam nos alertar para alguma irregularidade. Irregularidades incluem qualquer interrupção do funcionamento normal de nossos dispositivos e podem incluir problemas como:

- demora para ligar, funcionar e desligar nosso aparelho
- movimentos estranhos do cursor do mouse na tela
- emails ou mensagens de texto estranhas vindas de contatos conhecidos
- pessoas desconhecidas entrando em contato contigo usando informações que elas não deveriam ter
- tentativas de fraude (*phishing*): emails alegando vir de contatos conhecidos, do seu provedor de email, de redes sociais ou outras fontes buscando lhe convencer a baixar um arquivo anexo ou clicar em um *link* para obter detalhes de sua conta ou infectar seu computador
- emails não lidos aparecendo como “lidos”
- emails ou outras notificações sobre tentativas fracassadas de entrar em uma conta de suas contas
- a bateria do seu telefone ou *notebook* está descarregando muito rápido para o seu funcionamento normal.

Identificando indicadores de segurança digitais

Existem algumas práticas úteis que, se realizadas com regularidade, podem lhe ajudar a estabelecer uma linha-base (isto é, um funcionamento "normal") e depois identificar indicadores que de outra forma passariam despercebidos. Você pode monitorar o resultado de suas atividades abaixo e, através de documentação e revisão, identificar quaisquer mudanças para ver se elas correspondem a um indicador de segurança relacionado a uma possível ameaça.

- Escaneie seus dispositivos com um programa anti-vírus para ver se existe algum *malware* ou *spyware*.
- Verifique sua *firewall* para ver quais informações saem do seu dispositivo e entram nele.
- Verifique quais processos e programas estão rodando no seu computador e telefone celular, para ver se existe algum não autorizado.
- Utilize autenticação em duas etapas para os seus serviços *online* quando possível, para que você possa detectar se outras pessoas tentaram se passar por você.
- Faça marcas físicas (usando, por exemplo, uma caneta UV) ou use um lacre (como uma fita adesiva) nos seus dispositivos e tire fotos deles para lhe ajudar a verificar se eles foram adulterados.[13]

Para informações mais detalhadas sobre procura de indicadores de segurança, veja o **Apêndice B**.

Indicadores em nossa saúde e bem-estar

Outro espaço onde explorar indicadores de segurança é dentro de nós mesmas, nossa experiência física e nossas emoções. Nossa situação emocional pode dar uma pista tanto sobre ameaças externas quanto sobre uma condição interna que pode se provar problemática

13 Para mais informação sobre proteção física de dispositivos, veja Security in a Box: "Protect your data from physical threats" https://securityinabox.org/ en/ guide/physical

para nossa situação de segurança como um todo. É improvável que alguém que esteja exausta, estafada ou deprimida seja tão segura ou efetiva quanto se ela estivesse saudável ou mais descansada. Ter atenção a nós mesmas e cuidar de nossas vulnerabilidades físicas e emocionais pode contribuir para nossa segurança da mesma forma que pode se provar uma fonte de inspiração e força.

Alguns indicadores comuns de segurança sobre esse aspecto incluem:

- mudança nos padrões de sono
- está sempre se sentindo cansada
- está tendo dificuldades de trabalhar de forma motivada e focada
- mudanças bruscas de humor
- fica irritada ou furiosa com coisas pequenas
- se sente triste ou deprimida a maior parte do tempo
- não consegue parar de pensar nas coisas ruins que viveu ou testemunhou
- mudanças no seu apetite ou padrões de alimentação
- aumento do seu consumo de álcool, drogas ou remédios
- pensamentos sobre acabar com sua vida.

Muitas pessoas estão acostumadas a perceber esses indicadores ao longo de suas vidas cotidianas e a agir para melhorar a situação. Entretanto, como ativistas, às vezes continuamos a nos forçar e nos arriscamos a nos machucar seriamente. Às vezes, podemos estar tão imersas em nosso trabalho que nem nos damos conta do que estamos sentindo em nossas mentes e corpos. Por isso, como com tudo o que cobrimos até agora, é uma boa ideia tentar ser metódica sobre como tomar cuidado de nós mesmas física, emocional e psicologicamente. Uma forma de fazer isso é construir uma tabela de estresse.

2.5b Exercício

Tabela de estresse

Propósito & Resultado

Este exercício pode lhe ajudar a identificar seus limites com respeito a diferentes tipos de estresse, como reconhecer esses limites e tomar medidas para ficar bem. Tire um tempo, idealmente quando você não está sob pressão, e tente criar sua própria tabela de estresse.

Informações de entrada & Materiais

Para este exercício, separamos três níveis de estresse, como um semáforo:

Verde = estresse suportável e motivante. Este tipo de estresse pode nos manter ativas, mas talvez fiquemos cansadas mais facilmente, precisando fazer mais pausas e não queremos nos sentir assim por um longo período de tempo.

Amarelo = estresse desagradável. Neste nível, pode ser que sintamos cansaço e ao mesmo tempo estejamos alerta. Podemos manifestar sinais de estresse (que podem variar de uma pessoa para outra). Normalmente, temos uma grande vontade de mudar a situação que está nos causando essa sensação.

Vermelho = estresse insuportável, profundo e duradouro. Este tipo de estresse afeta diferentes esferas de nossas vidas incluindo nossas relações no trabalho, com nossas amizades e familiares, assim como nossas relações pessoais. Ele também reduz o prazer e o relaxamento que conseguimos com atividades recreativas, e nos sentimos ansiosas e/ou péssimas. Nossos corpos mostram claras reações físicas, e pode ser que nos sintamos perto do colapso, recorrendo, assim, a medidas não saudáveis para nos manter alertas, tais como tomar estimulantes.

Formato &

Passo 1: Baseando-se no exemplo abaixo, monte uma

Passos

tabela de estresse inicial e reflita sobre ela com alguém que você confia.

Passo 2: Decida, com uma regularidade marcada na sua agenda, quando você irá revisar sua situação de estresse e tente realizá-la como você estipulou.

Passo 3: Se você experimenta com frequência altos níveis de estresse num período de tempo, revise sua tabela de estresse para determinar se ela continua adequada.

Lembretes & Dicas

Verificar essa tabela pode ser um ponto das suas diretrizes de segurança pessoal e deve ser feito com regularidade. Certifique-se de verificar suas definições para ver se os diferentes níveis de estresse continuam precisos, ou se você acabou se acostumando com altos níveis de estresse!

	Indicadores (Como reconhecer que você está num tal nível de estresse? O que torna esta fase qualitativamente diferente da do nível anterior?)	**O que você pode fazer para reduzir o nível de estresse, ou aumentar sua capacidade de segurar o tranco?**	**Recursos necessários**
Verde			
Amarelo			
Vermelho			

Tenha em mente que perigos emocionais são muitas vezes sutis e podem nos assustar. Eles crescem devagar ao longo do tempo e talvez não consigamos perceber o quanto mudaram. Algumas estratégias para buscar regularmente por indicadores de perigo emocional incluem:

- prestar atenção quando amizades ou familiares comentam sobre seu humor, sua aparência ou seu comportamento interpessoal.
- procurar ativamente a opinião de amizades e colegas confiáveis que se importam com você o suficiente para serem sinceras sobre isso
- manter um diário privado de seus pensamentos e suas emoções a cada dia
- prestar atenção às formas pelas quais seu nível de estresse pode estar lhe tornando menos consciente de indicadores de segurança (físicos, informacionais ou emocionais) no seu entorno;
- caso necessário, procurar a opinião e o apoio de uma profissional de saúde mental.

Compartilhando e analisando indicadores de segurança

É muito importante que compartilhemos e analisemos os indicadores de segurança com amizades ou colegas confiáveis para que possamos estabelecer se vale a pena tomar alguma providência. Também pode ser o caso de que uma ou mais pessoas envolvidas em suas atividades tenha notado sinais semelhantes, observando os mesmos indicadores ou outros parecidos.

Se você trabalha para uma organização ou um grupo que realiza reuniões regulares, incluir os indicadores de segurança como um item comum de discussão na pauta é uma forma de garantir que eles serão analisados. Quando compartilhar incidentes e notar indicadores de segurança é visto como uma atividade valiosa, ela naturalmente acontece com mais frequência e também de maneira informal.

Passos para se fazer uma análise dos indicadores de segurança[14]

No caso de indicadores de segurança particularmente importante, tais como incidentes concretos, pode ser muito útil perguntar as seguintes questões como uma base para a análise.

1. **O que aconteceu?**
2. **Quando isso aconteceu?**
3. **Onde aconteceu?**
4. **Quem foi afetada?**
5. **Houve violência de gênero?** Isso é especialmente importante no caso de incidentes concretos envolvendo terceiros. Pondere os fatores físicos e psicológicos.
6. **No caso de uma agressão, quem foi o responsável?**
7. **Na nossa percepção, por que isso aconteceu?** Tente estabelecer os fatos e não começar a fazer acusações.
8. **Como se originou?** Ele tinha relação com vandalismo comum, fatores ambientais ou com nosso trabalho e ativismo?

Já que incidentes de segurança geralmente são informações "sensíveis", é bom discuti-los e analisá-los num espaço digital, emocional e fisicamente "seguro". Mantenha os seguintes fatores em mente:

- Se você está compartilhando indicadores remotamente (por exemplo, de um trabalho em campo), leve em consideração o canal que você está usando para comunicá-los. Para dissipar temores, pode ajudar falar com alguém pelo telefone, mas lembre-se que isso pode não ser seguro. Talvez fosse melhor usar um canal digitalmente mais seguro, como enviar mensagens de texto ou emails criptografados.
- Perceber e compartilhar indicadores dentro de um grupo é um serviço para si mesma e para seus colegas e deve ser tratado como tal. Os indicadores, mesmo quando aconte-

14 Baseado no Peace Brigades International Mexico Project (MEP, 2014) Programa de Asesorías en Seguridad y Protección para Personas Defensoras de Derechos Humanos, p.82

cem dentro do grupo, não necessariamente são "culpa" de alguém. Acima de tudo, deve-se considerar quais significados eles podem ter para a segurança de todo mundo. Compartilhar um indicador é um momento de agradecimento e não de vergonha.

- Quando for compartilhar indicadores de segurança relacionados ao comportamento de uma pessoa, é útil incluir indicadores positivos de segurança (quando uma pessoa toma uma precaução de segurança apropriada, ou quando a situação política muda em nosso favor) assim como indicadores críticos (quando uma ação ou inação foi percebida). Compartilhar esses indicadores num ambiente positivo e sem julgamentos é crucial para você e seus colegas, beneficiando-se de uma discussão aberta, para que se busque soluções coletivas ao invés de culpar e marginalizar as pessoas.

Mantendo um registro dos indicadores de segurança

Seja trabalhando como um indivíduo, um grupo ou uma organização formal, é importante criar um espaço onde você possa registrar os indicadores de segurança com tantos detalhes quanto possível, para poder compartilhá-los e analisá-los depois. Pode ser através de um documento ou uma planilha que deve ser periodicamente analisada (a cada semana ou mês) para que qualquer tendência nos indicadores possa ser notada.

Num grupo ou organização, é útil designar alguém para manter o registro dos indicadores e guardá-los de maneira segura. Independente da escolha, o registro dos indicadores de segurança deve ser considerado informação altamente sensível e deverá somente ser compartilhada com pessoas confiáveis. Obviamente, em algumas ações de alto risco como um protesto, o único espaço que você pode usar para registrar incidentes é a sua mente. Nesses casos, o melhor é encontrar uma amiga ou colega com a qual você possa compartilhar detalhes do incidente o mais cedo possível.

Exemplo: Registro de indicadores de segurança

Quando?

Onde?

Quem?

O que aconteceu?

Análise (Violência de gênero? Responsável? Por quê? Origem?)

Nota: Algumas pessoas podem não se sentir confortáveis tendo seus indicadores pessoais ou emocionais de segurança registrados nesse documento. Como uma regra geral, é sempre melhor perguntar se as pessoas estão confortáveis com isso e respeitar os desejos das que não estão. Nesses casos, é importante que mesmo assim elas tenham um espaço social ou profissional seguro e confortável para compartilhar essas sensações com a confidencialidade que seja necessária.

6
Identificando e Analisando Ameaças

Neste capítulo, construiremos nossa análise para identificar ameaças concretas ao nosso bem-estar. Ameaças, da forma como estamos vendo neste exercício, referem-se a qualquer evento potencial que possa causar dano a nós ou ao nosso trabalho.

O processo de identificar e analisar ameaças não é novo para nós. Na vida cotidiana, ele é algo que muitas de nós fazem naturalmente e quase sem nenhum esforço consciente. Cruzar uma rua movimentada é algo cheio de possíveis perigos mas aquelas de nós que vivem em áreas urbanas estamos geralmente acostumas a fazê-lo de maneira bastante segura, empregando nossa habilidade de identificar ameaças, tais como a aproximação de um ônibus ou de um motorista em um carro em alta velocidade, e tomar as medidas necessárias para minimizar a capacidade deles de nos causar danos.

Para isso, confiamos em nosso conhecimento anterior assim como no processamento de novas informações. Levamos em conta fatores ambientais (a rua está molhada devido à chuva?), normas sociais (cruzar em qualquer lugar em algumas culturas ou apenas usando a faixa de pedestres em outras), e quem são os possíveis aliados e oponentes (um policial, a pessoa que dirige o ônibus). Algumas de nossas experiências anteriores nos permitem cruzar uma rua em lugares não familiares, mas talvez precisemos de mais informação em uma nova situação, tal como as normas e leis de numa outra cidade. Por exemplo, em algumas cidades da Europa, ciclofaixas podem ser um perigo surpreendente para alguém que está acostumada a interagir somente com veículos motorizados ao cruzar uma rua. De forma similar, em nosso trabalho e ativismo, normalmente somos capazes de identificar algumas das ameaças que enfrentamos e tomamos medidas para reduzi-las ou evitá-las. Entretanto, à medida que o contexto à nossa volta muda, podemos nos deparar com ameaças que não havíamos percebido ou não conhecíamos. Nossa

preparação irá nos ajudar a ter um quadro mais completo das ameaças que podemos enfrentar.

Através dos exercícios dos capítulos anteriores, você pode ter acumulado um corpo de conhecimento sobre sua situação, incluindo sua visão, o ambiente onde você atua, seus aliados e oponentes, assim como seus respectivos recursos e limitações, quais seriam seus recursos informacionais e ter identificado os indicadores de segurança que lhe ajudam a se manter atenta a sua situação de segurança.

Essa informação deve nos deixar bem preparadas para identificar ameaças contra nós, nosso grupo ou nossa organização. Podemos ter provas das ameaças que percebemos através da percepção dos recursos e capacidades de nossos oponentes, da identificação prévia de ameaças não percebidas ao nosso ecossistema informacional e do uso dos indicadores na nossa preparação para evitar, nos defender, responder ou resolver tais eventualidades.

Nota: é importante, porém, ter em mente que nem todas as ameaças ao nosso bem-estar e segurança são políticas ou relacionadas ao nosso trabalho. Temos também que estar atentas a ameaças que podem surgir da delinquência, pequenos crimes, violência de gênero, danos ambientais, etc. Embora essas ameaças não representem necessariamente uma resposta política ao nosso trabalho, elas podem estar entre as mais importantes ameaças aos defensores de direitos humanos.

Neste capítulo, podemos começar com o que sentimos que são as ameaças contra nós e avaliá-las uma a uma. Usaremos também os passos anteriores desta Seção como um ponto de partida para identificar as ameaças potenciais subjacentes. Usando as descobertas anteriores, estaremos então numa boa posição para avaliar essas ameaças baseado no que consideramos ser a **probabilidade** de que elas venham a acontecer, e o tamanho do **impacto** ou o dano causado caso aconteçam.

Nossa resposta a elas também serão categorizadas segundo os dois conceitos acima e podem ser pensadas como uma combinação de táticas de **prevenção** e **resposta**. Nos próximos capítulos, chegaremos às preparações e ações para minimizar a possibilidade dessas ameaças, assim como os passos e ações que iremos realizar para reduzir o dano das ameaças que vierem a acontecer.

2.6a Exercício

Ameças: chuva de ideias

Propósito & Resultado

Este exercício é uma primeira tentativa de identificar as ameaças a você, seu grupo ou organização e seu trabalho na defesa de direitos humanos. Esta lista inicial de ameaças pode depois ser refinada para poder focar nas ameaças que possuem mais chance de acontecer ou que sejam potencialmente mais nocivas.

Informações de entrada & Materiais

Este exercício será mais fácil se você começar com:

- sua análise das tendências políticas, econômicas, sociais e tecnológicas atuais no seu contexto
- uma lista das atividades ou tipos de trabalhos que você realiza para alcançar seus objetivos
- um mapa de atores, em particular, de seus oponentes
- uma lista de indicadores de segurança que você observou no seu trabalho anterior.

Materiais sugeridos:

- **Caso esteja sozinha**: uma folha de papel ou algum outro material para escrever.
- **Caso esteja em grupo**: uma folha grande ou cartolina e materiais para escrever.

Formato & Passos

Pense e escreva todas as potenciais ameaças contra você, sua organização e seu trabalho. Pode ser útil categorizá-las começando por cada uma de suas atividades ou áreas de trabalho. Lembre-se: uma ameaça é qualquer evento potencial que pode causar dano a nós ou ao nosso trabalho. Não esqueça de considerar ameaças potenciais à segurança da sua informação e ameaças ao seu bem-estar (políticas ou não).

Crie uma lista dessas ameaças. Se você achar isso difícil, pense nos seus oponentes e nas formas como eles agiram contra outros defensores de direitos humanos no passado. Analise seus indicadores de segurança e veja se eles representam uma ameaça concreta. Observe qualquer padrão que emerge das ameaças que você identificou: elas se relacionam primeiramente com certas atividades suas, ou se originam de certos oponentes? Isso será útil quando chegarmos no planejamento de segurança (isto é, um planejamento particular para certas atividades, ou planos dedicados para engajar com alguns atores). Mantenha essa lista para poder analisá-la nos próximos exercícios.

Lembretes & Dicas

Se a lista for um tanto longa, pode ser desgastante pensar em cada uma dessas ameaças potenciais. Pode também ser um exercício desafiador caso não saibamos o quão realista estamos sendo.

É importante lembrar que ameaças políticas sempre se originam de um certo ator ou grupo de atores que vê seus interesses potencialmente ameaçados por você e seu trabalho. Nesse sentido, ameaças são um sinal de que o seu trabalho está sendo efetivo e que seus oponentes têm medo dele. Embora possa ser um momento que inspire medo, reconhecer claramente as ameaças que você enfrenta pode também ser um momento de empoderamento. Reconhecer essas ameaças e a possibilidade que elas venham a acontecer permite que você se planeje melhor e possivelmente mitigue o dano causado a você ou ao seu trabalho, caso alguma delas aconteça.

Percebendo ameaças

Como mencionado anteriormente, nossa percepção de ameaças às vezes é dificultada por diversas razões: talvez a informação disponível seja limitada; talvez o medo, o estresse ou as experiências traumáticas anteriores tenham um impacto em nossa percepção e possam nos levar a experimentar medos infundados ("paranoia") ou errar em reconhecer ameaças. Ambas ocorrências são muito naturais, embora não sejam desejáveis. Portanto, é uma boa ideia estar atenta a isso e encontrar mecanismos para verificar nossa percepção – seja através de pesquisas ou de conversas com pessoas que confiamos.

No próximo exercício, levantamos algumas questões que podem lhe ajudar a pensar criticamente sobre sua percepção de ameaças e enxergar táticas para tornar sua percepção mais acurada.

2.6b Exercício

Reflexão sobre a percepção de ameaças

Propósito & Resultado

Melhorar o reconhecimento e a análise de ameaças para poder responder adequadamente.

Você irá aprender a reconhecer seus próprios pontos cegos e processos falhos para identificar ameaças assim como criar processos para preencher essas brechas.

Informações de entrada & Materiais

Use a lista de ameaças da chuva de ideias anterior (**Exercício 2.6a**) para este exercício.

Formato & Passos

Reflexão individual ou discussão em grupo

Pergunte a si mesma ou ao grupo as seguintes questões:

1. Houve algumxa ameaça que você descobriu ou que foi mencionada por outras pessoas, que você não tinha percebido antes?
2. Se você fez o exercício em grupo, alguém ficou surpresa com as ameaças que você mencionou? Por quê?

3. Desde quando você acha que as ameaças que você identificou existiam antes de você ter se percebido delas?
4. Como será que você poderia tê-las percebido antes?
5. Como você comunicou sobre elas no seu grupo ou com suas colegas?
6. O que as faz parecer mais ou menos sérias?
7. Você identificaria alguma ameaça como sendo mais séria do que de fato poderia ser?
8. Se você está trabalhando em grupo: quais são as diferenças nas suas respostas em relação às acima? O que te faz pensar na mesma ameaça de formas diferentes?

Lembretes & Dicas

Pode ser muito desgastante listar todas as ameaças que você enfrenta. Assegure-se de não ir rápido demais neste exercício e de abrir espaço para as pessoas expressarem seus sentimentos à medida que vai sendo feito. Se você considerar este exercício útil, pense em fazê-lo de forma regular (a cada semana ou mês).

Priorizando ameaças: análise de risco

Ao começar o processo de identificação de todas as ameaças ou obstáculos que possam nos afetar ou nosso trabalho, é importante evitar se sobrecarregar. Se fazemos uma chuva de ideias de ameaças, pode ser que de fato montemos uma grande lista e não saibamos por onde começar. Além disso, esse processo pode ser agravado por medos infundados ou exagerados. É por isso que pode ser útil analisarmos cada ameaça, como no exercício anterior. Ameaças podem ser vistas e categorizadas sob a seguinte luz:

- a probabilidade de que a ameaça aconteça
- o impacto dela caso aconteça e quando.

A probabilidade e o impacto são conceitos que podem nos ajudar a determinar o risco: quanto maior a probabilidade ou o impacto de uma ameaça, maior o risco. Se uma ameaça tem menos chance de acontecer ou um impacto menor, o risco é menor.

Claro, ao realizar tal exercício, precisamos estar conscientes de que estamos confiando em nossa própria percepção. Como explorado nos capítulos anteriores, nossa percepção pode sofrer diversos desafios quando estamos cansadas ou sob estresse, ou quando conversamos sobre ameaças fora de nossas áreas de conhecimento (por exemplo, ameaças à informação digital, para defensores de direitos humanos que são menos confortáveis com tecnologia). É importante ter isso em mente, comparando nossas percepções com as percepções de outras pessoas, e realizando pesquisas quando necessário para verificá-las.

Probabilidade

Para avaliar a probabilidade de ocorrência de uma ameaça, podemos usar diversas fontes de informação, como: o mapa de atores que criamos, nossa análise de indicadores passados de segurança, e a experiência de nossas aliadas em situações semelhantes. Esse processo não busca encontrar a probabilidade exata de uma ameaça vir a acontecer, mas, pelo contrário, nos ajuda a priorizar aquelas ameaças que consideramos iminentes. Em geral, elas podem ser agrupadas nas seguintes categorias.

Improvável de acontecer

Essas são as ameaças que possuem poucos precedentes e poucas condições favoráveis. Embora possamos escolher “diminuir” sua prioridade, temos que mantê-las em mente, especialmente se o seu impacto pode ser substancial (veja abaixo). Além disso, é importante registrá-las, pois à medida que o contexto sociopolítico muda, sua probabilidade também pode mudar.

Provável que aconteça

Essa são as ameaças com claros precedentes e/ou condições muito favoráveis. Essas ameaças são prioridade para os próximos passos.

Indefinida, ou sem informações

Em alguns casos, pode ser que nossa informação e intuição não cheguem à mesma resposta, ou talvez não haja informação suficiente para categorizar confortavelmente uma ameaça potencial entre provável e improvável. Nesse caso, é importante errar para o lado do cuidado:

- investigue mais a respeito da ameaça potencial com a ajuda de nossas aliadas e suas experiências, de especialistas no assunto que sejam confiáveis, ou de deliberações dentro de nosso grupo, até que possamos, de forma segura, colocá-la dentre de uma das categorias acima, ou:
- coloque-a logo na categoria “provável”.

Impacto

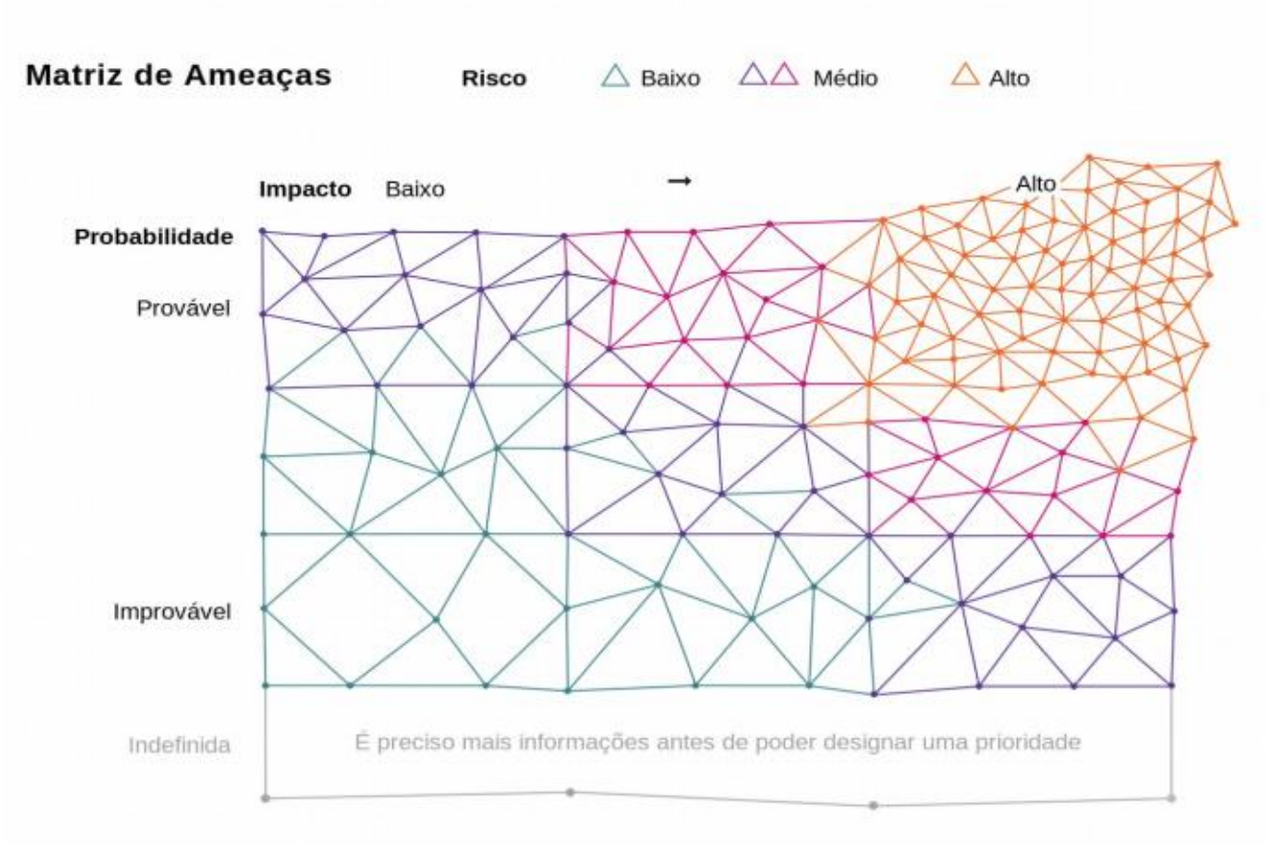
Quando analisamos qual o potencial impacto que um evento nocivo pode ter, é útil imaginar um cenário onde a ameaça já aconteceu. Nesse cenário, como a ameaça nos causou dano? Examine a situação e reflita sobre questões como:

- Quantas pessoas foram afetadas?
- Quanto dura o efeito da ameaça?
- Em que medida isso dificulta nossa operação normal?
- Quais outras situações nocivas ela torna possível?
- Existe um perigo imediato para outras pessoas que ainda não foram afetadas?

De acordo com seus próprios padrões, você pode considerar as ameaças como sendo de baixo, médio ou alto impacto. Ameaças de baixo impacto devem ter apenas impactos negativos limitados

em nossa habilidade de continuar nosso trabalho, e, de maneira geral, ameaças devem ser consideradas de alto impacto se elas impedirem você ou sua organização de continuar realizando suas atividades no médio ou longo prazo.

Pode ser que lhe ajude visualizar a probabilidade e o impacto das ameaças que você identificou através de um gráfico de matriz como exemplificado abaixo, notando que, grosso modo, as ameaças prioritárias – aquelas de "alto risco" – tenderão a ficar no canto direito superior.



Considerando as ameaças que identificamos sob a luz da sua probabilidade e do seu impacto, podemos avançar para uma análise mais profunda delas, das condições necessárias para que elas aconteçam e suas potenciais consequências. Isso irá nos ajudar a planejar formas de reagir a elas.

Ameaças declaradas

Pense na possibilidade de estarmos enfrentando uma declaração explícita de uma intenção de nos machucar, por exemplo, uma mensagem de uma pessoa, grupo ou organização que expressa abertamente sua vontade de nos causar dano. Com frequência, isso é chamado de "ameaças declaradas" e são muito comuns a defensores de direitos humanos na forma de textos, telefonemas, emails, abuso verbal ou cartas. Elas também podem estar implicadas nas declarações públicas de nossos oponentes ou através de assédio judicial, propostas de leis ou muitos outros métodos. A intenção deles é infligir dano ao nosso trabalho, nos punir ou machucar e dissuadir outras pessoas. Tais mensagens constituem um tipo especial de indicador de segurança porque elas já têm um impacto (psicológico), e podem muito bem corresponder a uma ameaça real. Elas merecem nossa atenção pois precisamos estabelecer sua veracidade e severidade.

Em geral, "ameaças declaradas" são:

Intencionais	são feitas com o claro propósito de nos intimidar e desencorajar nosso trabalho
Estratégicas	são parte de um plano maior para evitar ou dificultar nosso trabalho
Pessoais	são direcionadas especificamente a nós e ao nosso trabalho
Baseadas em medo	são feitas para nos assustar e assim pararmos nosso trabalho.[15]

É importante ter em mente que enquanto algumas ameaças podem ser reais, outras buscam criar novos medos infundados enquanto não há nenhuma ação planejada para nos atacar por parte da pessoa ou grupo que realizou a ameaça. Quando analisamos esse tipo de

15 Veja o *Workbook on Security for Human Rights Defenders* do Front Line Defenders e o *New Protection Manual for Human Rights Defenders* do Protection International, http://protectioninternational.org/publication-page/manuals/

indicador, pode ser útil voltar ao mapa de atores e pensar sobre os recursos e interesses do adversário em questão.

Tais ameaças são muito "econômicas", pois elas podem alcançar o mesmo resultado que um ataque, porém sem o esforço ou os custos de realizá-lo de fato. (Como foi mencionado anteriormente, identificar medos infundados é uma parte importante do desenvolvimento de um plano efetivo de segurança holística). Mesmo assim, receber tal mensagem pode, por si mesma, ser uma experiência muito chocante e pode inspirar muito medo em nós. É importante, o máximo possível, criar um espaço seguro para nós ou para nosso grupo (emocional, digital e físico) para poder perguntar, discutir, analisar e responder. Para uma sugestão de passos a seguir com respeito à análise de ameaças declaradas, veja o **Apêndice C**.

Infelizmente, nem todas as ameaças que enfrentamos são diretamente ou explicitamente evidentes. Os resultados de nossa preparação nos capítulos anteriores são um recurso inestimável para identificar, analisar e encontrar formas de responder às ameaças que percebemos. Neste capítulo, empregaremos nossos indicadores de segurança, nossos documentos sobre o ecossistema informacional, assim como nossos mapas de atores e de relações e a análise situacional.

No próximo exercício, começaremos com a lista de ameaças que identificamos através da chuva de ideias, designaremos a elas níveis de prioridade e expandiremos nossa compreensão da sua natureza. É importante notar também que com relação a muitas das ameaças, o estado de nossa mente e de nosso corpo tem um papel importante na determinação da probabilidade assim como do impacto de qualquer ameaça dada.

2.6c Exercício

Inventário de ameaças

Propósito & Resultado

Este exercício nos ajudará a designar prioridades às ameaças e descobrir suas causas, ramificações e fontes, assim como os recursos necessários, as ações existentes e os possíveis próximos passos.

O resultado deste exercício será um inventário detalhado de suas ameças divididas em prioridades, que será usado no próximo capítulo para ajudá-la a criar planos de ação.

Informações de entrada & Materiais

- Mapas de atores e de relações
- Ecossistema informacional
- Indicadores de segurança
- Matriz de impacto/probabilidade

- Canetas e papel
- Cartolina
- Canetinhas

Formato & Passos

Primeiro, começando com a chuva de ideias de ameaças do exercício anterior, pense nas ameaças listadas em termos de sua probabilidade e impacto. Selecione aquelas que você considera como as mais prováveis e as que possuem o maior impacto para serem usadas no próximo exercício.

Novamente, pode ser útil separar e organizar as ameaças de acordo com atividades particulares (por exemplo, separar aquelas que aparecem no contexto de protestos daquelas relacionadas com as atividades cotidianas do escritório).

Comece com o que você considera como as ameaças de mais alta prioridade, baseado na matriz de impacto/probabilidade e, usando o exemplo-modelo fornecido, desenvolva (individualmente ou em grupo).

- Escreva o título e sumário das ameaças.
- Para cada ameaça, se for uma ameaça complexa, você pode optar por dividir e analisar sub-ameaças (por exemplo, uma invasão do escritório seguida de prisão pode ser facilmente analisada se separada segundo as diversas consequências que podem ter – prisões potenciais, apreensão de dispositivos, assédio judicial, etc.). Use as linhas para expandir cada uma delas em sub-ameaças.

Faça as seguintes perguntas para cada ameaça. É possível que algumas ameaças sejam complexas e que algumas respostas necessitem seu próprio espaço. Use quantas linhas forem necessárias. Se, por exemplo, uma ameaça constitui um ataque a uma pessoa, assim como à informação que ela esteja portando, você pode usar uma linha para descrever os aspectos informacionais e outra para a pessoa em questão.

- **O quê**: Descreva o que acontece se a ameaça vira realidade. Pense no impacto que ela pode ter sobre você, sua organização, seus aliados. Inclua dano ao espaço físico, estresse humano e trauma, comprometimento de informações, etc.
- **Quem**: identifique a pessoa, organização ou entidade por trás da ameaça: olhar o mapa de atores pode lhe dar informações específicas sobre esse adversário:
  - Qual sua capacidade de ação?
  - Quais são as limitações dele para levar a cabo essas ameças?
  - Existem elementos neutros ou aliados que podem influenciá-lo?

    - Existe alguma história parecida de tal ação contra você ou um aliado?
- **Quem/O quê**: identifique o alvo potencial da ameaça; uma informação específica sendo roubada, uma pessoa sob ataque (fisicamente, emocionalmente, financeiramente), materiais ou recursos sob ameaça (apreensão ou destruição de propriedade).
- **Como**: Qual informação é necessária?
    - Qual informação é necessária para o adversário ser capaz de levar a cabo a ameaça?
    - De onde ele pode tirar essa informação?
- **Onde**: descreva o lugar onde o ataque potencial pode acontecer.
    - Será que um agressor precisa de acesso ao mesmo local que você, como costuma ser o caso de um ataque físico?
    - Quais são as características do local em questão? O quão seguro ele é? O que tem de mais perigoso nele?

Formato & Passos

Desenvolva sobre os fatores psicológicos, emocionais e de saúde relacionados a essa ameaça, incluindo o do seu nível de estresse, cansaço, medo e outros fatores na ocorrência potencial dessa ameaça. Considere:

- Como o seu estado mental atual poderia afetar qualquer planejamento e medidas de contingência em andamento?
- Essa ameaça acontece no contexto de uma atividade em particular? Em que tipo de estado mental ou físico você se encontra durante tais atividades? Quais seriam as boas práticas que poderiam lhe proteger, ou o que lhe torna mais vulnerável?

- Quais elementos do seu comportamento ou estado mental pode de fato aumentar a probabilidade de isso acontecer, ou do seu impacto?

Se você quiser anotar os resultados do exercício, experimente usar um formato como o seguinte:

Ameaça	[Nome da ameaça]			
Resumo	[Breve descrição/resumo da ameaça]			
O quê	Alvo	Adversário	Como	Onde
Descreva o que acontece se a ameaça vira realidade (se necessário, subdivida abaixo a ameaça em seus componentes)	Especifique o quê/quem é o alvo.	Quem é a entidade por trás dessa ameaça?	Qual informação é necessária para levar a cabo a ameaça?	Quais são os espaços físicos onde a ameaça pode se manifestar?
1)				
2)				
3)				
Impactos psicológicos, emocionais e na saúde				

Agora que você identificou uma lista das ameaças que podem surgir no curso de suas atividades, junto com quem pode estar por trás de

cada uma, você pode começar a fazer planos e se preparar para dois objetivos inter-relacionados:

- reduzir a probabilidade de que a ameaça venha a acontecer
- minimizar seu impacto caso ela aconteça.

Lembre-se que a lista acima não é estática, e é muito importante revisitá-la. Reviravoltas e mudanças de contexto invariavelmente afetam a paisagem do seu trabalho. Podem surgir ameaças não previstas, ou a probabilidade de certas ameaças pode ser reduzida devido a fatores externos. Você pode determinar a frequência com a qual você deve revisitar essa lista e dedique um tempo para isso.

Conclusão

Na **Seção II | Explore**, seguimos uma série de passos com o objetivo de analisar nosso contexto, começando com o panorama geral (situação política, econômica, social, tecnológica, legal e ambiental) e nos movemos gradualmente para a identificação de ameaças específicas à nossa segurança.

Na próxima seção, iremos nos preparar para reduzir a probabilidade de que ameaças virem realidade assim como seu impacto, examinando nossas capacidades existentes e nossas relativas vulnerabilidades a essas ameaças. A partir daí, construiremos estratégias, planos e táticas de segurança.

Também temos que considerar como podemos integrar esses passos dentro de nossas rotinas existentes e no trabalho que já fazemos para manter uma análise atualizada de nosso contexto, e construir abordagens organizacionais consistentes para lidar com nossa segurança e nosso bem-estar.

MONTE ESTRATÉGIAS

Respondendo a Ameaças com
Estratégias, Planos e Acordos

III Monte estratégias

Respondendo a Ameaças com Estratégias, Planos e Acordos

Conteúdo

Introdução

Nesta seção, exploraremos o processo de como desenvolver e refinar nossas estratégias, planos e táticas de segurança baseados nas ameaças identificadas em nossa análise de contexto. Para tanto, devemos começar com as ameaças contra nós mesmas, nosso trabalho e nosso bem-estar, como identificamos na **Seção II | Explore**. Examinaremos essas ameaças sob a luz de nossas práticas atuais de segurança, assim como de nossas capacidades e vulnerabilidades para estabelecer as brechas que persistem em nossa habilidade de responder propriamente a elas.

Uma vez que tenhamos feito uma avaliação realista de nossa situação de segurança, podemos começar a pensar e construir nossas estratégias de segurança e formalizá-las em planos e acordos para diferentes aspectos de nosso trabalho.

Em paralelo a esse processo, consideraremos algumas dinâmicas particulares que surgem em nós quando estamos tentando construir planos de segurança como uma organização. Incluímos uma avaliação de práticas de segurança organizacional, e veremos o princípio "Não Cause Danos" para planejamento de segurança.

Em Monte Estratégias, iremos:

- examinar nossas **capacidades e vulnerabilidades** relativas às ameaças que identificamos
- identificar **novas** capacidades que queremos construir e explorar algumas questões chave sobre **construção de habilidades** de segurança
- olhar para os elementos chave que serão incluídos nos **planos de segurança** e para o processo de criá-los
- explorar questões chave sobre planejamento de segurança em grandes **grupos e organizações**
- conhecer e adotar o princípio **Não Cause Danos** e saber como ele pode ser aplicado em nossas práticas de segurança.

1
Analisando nossas Respostas a Ameaças

Começaremos analisando nossas práticas existentes de segurança e nossas respostas a ameaças que consideramos prioritárias. Quando falamos de planejamento de segurança, pouquíssimas de nós estão começando "do zero": como mencionado anteriormente, temos certos instintos que nos ajudam a evitar ou responder a ameaças em nossa vida cotidiana. Para além disso, é muito comum termos certas práticas socializadas – geralmente referidas como "senso comum" – que realizamos sem pensar para ficarmos longe de perigos.

Nesta Seção, iremos lançar mão de uma visão que reconhece o valor dessas práticas existentes, mas ao mesmo tempo busca ser crítica quanto a elas. Identificaremos os passos que devemos tomar para desenvolver estratégias, planos e táticas de segurança que correspondam à análise que fizemos acima na **Seção II | Explore**.

Estrutura geral: Ameaças, capacidades e vulnerabilidades

Neste processo, é útil trabalhar com os conceitos de capacidades e vulnerabilidades relativas a cada ameaça em particular que identificamos.

- Capacidades são os fatores que nos ajudam a manter-nos seguras contra uma ameaça em particular (por exemplo, reduzir sua probabilidade ou seu impacto).
- Vulnerabilidades são os fatores que nos tornam mais suscetíveis a uma ameaça (por exemplo, elas aumentam sua probabilidade ou seu impacto).

Capacidades e vulnerabilidades podem ser características próprias, de nossos aliados ou do ambiente onde estamos operando e que consideramos relevantes para nossa segurança.

Uma vez que identifiquemos nossas capacidades e vulnerabilidades, relativas a cada uma das ameaças que enfrentamos, podemos trabalhar para reduzir nossas vulnerabilidades e desenvolver nossas capacidades para reduzir a probabilidade ou o impacto dessas ameaças: desenvolver capacidades e reduzir vulnerabilidades ajuda a reduzir o risco de uma dada ameaça.

Nossas práticas e capacidades existentes

Usando a análise de ameaças que realizamos no final da última seção como um ponto de partida, começaremos analisando essas ameaças em termos de nossas práticas existentes e capacidades relacio-

nadas à segurança que identificarmos. Assim, poderemos tentar identificar as brechas ou vulnerabilidades em nossas práticas com vistas a melhorá-las.

Já consideramos algumas dessas práticas existentes para nosso bem-estar e segurança em geral nos capítulos anteriores, mas agora iremos examiná-las sob a luz das ameaças que identificamos. Mesmo que essa seja a primeira vez que você realiza uma análise crítica de sua segurança, algumas de suas práticas existentes de segurança e para seu bem-estar já podem ser efetivas em evitar que suas ameaças de mais alto nível venham a se concretizar. Segurança não precisa ser algo complicado: ela pode incluir ações simples como trancar a porta do seu escritório, ter senhas fortes para suas contas *online* ou ter um kit de primeiros socorros em casa.

Entretanto, é importante evitar de criar um falso senso de segurança. Devemos pensar criticamente sobre nossas práticas existentes e ver se elas são ou não efetivas em nosso contexto. A questão é: como suas práticas existentes se relacionam com as ameaças que identificamos?

Na **Seção II | Explore**, pensamos nossas ameaças prioritárias com bastante detalhe. Vimos:

- quais os efeitos que cada ameaça pode ter (caso se concretize)
- quem pode ser responsável por ela
- quem ou o quê seria o seu alvo
- como a ameaça se concretizaria
- quais informações nossos adversários necessitariam para isso
- onde o potencial ataque aconteceria, e
- como nosso estado mental e físico pode nos tornar mais fortes, mais resilientes ou, pelo contrário, mais suscetíveis e vulneráveis à ameaça.

No próximo exercício, consideraremos essas questões em termos de nossas boas práticas existentes.

3.1a Exercício

Práticas e capacidades existentes

Propósito & Resultado	Neste exercício, considere cada uma das ameaças que você já identificou e priorizou sob a luz de suas práticas existentes e capacidades relacionadas à segurança. Isso lhe dará uma "linha-base" sobre a qual poderá mais tarde desenvolver e melhorar.
Informações de entrada & Materiais	Para realizar este exercício, você precisa ter identificado e priorizado as ameaças no **Exercício 2.6b/c**. Pode ser útil escrever as capacidades que você identificou para que possa revisá-las mais tarde.
Formato & Passos	Volte às ameaças identificadas no **Exercício 2.6b**. Para cada uma das ameaças identificadas, existe uma série de questões. Aqui você pode relacionar suas práticas existentes e capacidades relacionadas à segurança com cada umas das seguintes questões: • **Quem/O que** está sob ameaça? Identifique aqui quais capacidades (se existe alguma) já estão protegendo essa pessoa ou coisa dessa ameaça. Exemplos de capacidades podem incluir ◦ em caso de assédio judicial: bons conhecimentos legais ◦ no caso de apreensão de computadores: ter os discos rígidos criptografados. • **Quem** está por trás da ameaça? Você já tem

algum tipo de tática para se relacionar com esse ator? Existe alguma tática ou recurso que você desenvolveu para prevenir que ele aja contra você? Se sim, o quê? Se já agiram contra você antes, você respondeu de alguma forma? Se sim, como? Se não o fez, tudo bem: isso será importante de lembrar quando você for identificar as brechas de segurança.

- **Como**: Quais informações são necessárias para realizarem o ataque? Você possui algum tipo de práticas de proteção de informação ou contra-vigilância em andamento que possa prevenir que informações caiam nas mãos deles?
- **Onde**: que acesso a você ou à sua propriedade eles precisam? Como você protege os espaços físicos à sua volta (por exemplo, prédios, veículos, propriedade privada)? Por exemplo, você tranca seu escritório e sua casa? Quais práticas do "senso comum" você tem para sua segurança pessoal em ambientes perigosos? Tudo isso é importante de tomar nota, para que você não comece do zero!
- **Táticas psicológicas, emocionais e de saúde**: Incluem quaisquer práticas de bem-estar que existam para lidar com essa ameaça – você tem alguma prática que lhe ajuda a reduzir estresse, cansaço, etc., e aumente sua concentração e atenção de forma a lhe ajudar a responder a essa ameaça?

Onde for possível, tente pensar nos aspectos relativos a cada uma das ameaças que você identificou. **Se não conseguir pensar numa resposta para uma ou mais questões, tudo bem**: você apenas identificou uma brecha a ser preenchida. Você irá trabalhar com as brechas no exercício seguinte. Elas também servirão como uma forma de identificar quais novos recursos e práticas são necessárias.

Lembretes & Dicas

Cuidado! Para cada resposta que der, avalie **se essa prática ou capacidade é positiva. Como saber?** Há um leve perigo de criar um falso senso de segurança se você erroneamente avaliar que uma prática existente ajuda a lhe manter segura. Se você não estiver segura de algo, vale a pena separar um tempo para pensar mais sobre isso e **falar com seus colegas ou amizades de confiança** para ter uma nova perspectiva.

Se você quiser anotar os resultados do exercício, experimente usar um formato como o seguinte:

Ameaça	[Nome da ameaça]			
Resumo	[Breve descrição/resumo da ameaça]			
O quê	Alvo	Adversário	Como	Onde
Descreva o que acontece se a ameaça vira realidade (se necessário, subdivida abaixo a ameaça em seus componentes)	Especifique o quê/quem é o alvo.	Quem é a entidade por trás dessa ameaça?	Qual informação é necessária para levar a cabo a ameaça?	Quais são os espaços físicos onde a ameaça pode se manifestar?
1)				
2)				
3)				
Impactos psicológicos, emocionais e na saúde				

Identificando brechas e vulnerabilidades

Agora que identificamos nossas boas práticas e a forma como elas podem se relacionar com as ameaças que priorizamos, devemos nos fazer uma pergunta um pouco mais difícil. **Quais brechas continuam abertas** que podem nos tornar mais vulneráveis a essas ameaças? Quais atitudes inúteis ou que insuficiência de conhecimento ou habilidade de nossa parte representam vulnerabilidades?

Ao tentar responder a essa pergunta, é importante lembrar que estresse, cansaço e medo (entre outros fatores) podem inspirar **medos infundados**. Além disso, nossa limitação de recursos (ou a sofisticação de nosso adversário) pode resultar tanto em imprecisão na avaliação das ameaças que reconhecemos quanto em **ameaças não reconhecidas**.

Reconhecer tais incertezas onde elas existem é um passo positivo que pode nos instigar a **investigar mais** as ameaças à nossa volta. Também podemos tomar medidas para **verificar nossas percepções** conversando com nosso grupo ou com nossos aliados, colegas e amizades de confiança.

Com isso em mente, será útil voltar agora para sua análise de ameaças e refletir sobre os detalhes que você sabe sobre elas e suas práticas existentes usadas para prevenir ou reagir a elas. Onde estão as brechas e vulnerabilidades em relação a cada um dos aspectos que você considerou?

3.1b Exercício

Vulnerabilidades e brechas em nossas práticas existentes

Propósito & Resultado

Neste exercício, pense em cada uma das ameaças que você identificou e priorizou na **Seção II | Explore**, agora sob a luz das brechas em suas práticas existentes de segurança e suas vulnerabilidades. Isso tornará muito mais claro o terreno onde você precisa começar a desenvolver novas capacidades.

Informações de entrada & Materiais

Para realizar este exercício, você precisa ter a) identificado e priorizado suas ameaças no **Exercício 2.6b**, e b) organizado o resultado do **Exercício 3.1a** acima.

Use canetas e papel ou outros materiais para escrita.

Formato & Passos

Volte às ameaças identificadas no **Exercício 2.6b** e às capacidades e práticas existentes identificadas no **Exercício 3.1a**.

Aqui, você pode tentar identificar as brechas nas suas práticas existentes e suas vulnerabilidades, relacionando isso com cada uma das questões que você respondeu anteriormente. Considere as seguintes questões:

- **Quem/O que** está sob ameaça? Identifique aqui quais brechas ou vulnerabilidades (caso existam) estão tornando essa pessoa ou coisa mais vulnerável à ameaça. Vulnerabilidades podem incluir:
  - no caso de um assédio judicial, uma pessoa tendo pouco conhecimento legal, ou
  - no caso de apreensão de computadores, os discos rígidos não terem senha ou criptografia.

- **Quem** está por trás da ameaça? Quais vulnerabilidades ou brechas existem na sua habilidade de influenciar esse ator? Por exemplo, se não há maneiras de se engajar diretamente com esse ator para criar aceitação do seu trabalho ou dissuasão de um ataque, isso pode ser considerado uma brecha.
- **Como**: Quais informações são necessárias para realizarem o ataque? É difícil controlar o fluxo de informação – existe alguma vulnerabilidade na forma como você lida com a informação relevante ao seu trabalho que possa facilitar essa ameaça ou torná-la mais nociva?
- **Onde**: Quais aspectos do espaço físico à nossa volta (por exemplo, prédios, veículos, propriedade privada) pode fazer com que essa ameaça seja mais provável ou mais nociva? No caso de invadirem e roubarem um escritório, por exemplo, ter fechaduras fracas nas portas pode ser uma vulnerabilidade.
- **Vulnerabilidades psicológicas, emocionais e na saúde**: no contexto dessa ameaça, como o estresse, o cansaço, etc., poderia lhe afetar?

  Quais brechas ou vulnerabilidades existem nas suas práticas de bem-estar que podem fazer com que a ameaça seja mais provável ou mais nociva?

Se você quiser anotar os resultados do exercício, experimente usar um formato como o seguinte:

Ameaça	[Nome da ameaça]			
Resumo	[Breve descrição/resumo da ameaça]			
O quê	Alvo	Adversário	Como	Onde
Descreva o que acontece se a ameaça vira realidade (se necessário, subdivida abaixo a ameaça em seus componentes)	Especifique o quê/quem é o alvo.	Quem é a entidade por trás dessa ameaça?	Qual informação é necessária para levar a cabo a ameaça?	Quais são os espaços físicos onde a ameaça pode se manifestar?
1)				
2)				
3)				
Impactos psicológicos, emocionais e na saúde				

Pode ser inquietante identificar as brechas em nossas práticas de segurança, mas é um passo importante no desenvolvimento da sabedoria que nos ajudará a construir melhores planos de segurança. Uma vez tendo identificado essas brechas, podemos pensar quais recursos e conhecimentos precisamos para construir e desenvolver planos e acordos com objetivos claros com respeito à segurança.

Identificando novas capacidades

Nesse momento, devemos ter um boa ideia das ameaças que enfrentamos, nossas capacidades relativas a cada uma delas (incluindo nossas práticas existentes) e nossas vulnerabilidades relativas a cada uma delas (o que também destaca onde existem brechas e espaço para melhorias em nossas práticas). Tendo como base essa análise, podemos agora identificar **novas capacidades a serem desenvolvidas** para podermos melhorar nosso bem-estar em ação.

Para tanto, será útil fazer uma chuva de ideias inicial sobre essas novas capacidades. Nos próximos capítulos, exploraremos algumas dinâmicas sobre como desenvolver e implementar essas capacidades.

3.1c Exercício

Chuva de ideias sobre novas capacidades

Propósito & Resultado	Neste exercício, você pode considerar cada uma das ameaças que você identificou e priorizou na **Seção II | Explore**, sob a luz das brechas em suas práticas existentes de segurança e suas vulnerabilidades.
Informações de entrada & Materiais	Para realizar este exercício, você precisa ter identificado e priorizado suas ameaças no **Exercício 2.6b**, e organizado os resultados do **Exercício 3.1a** e **3.1b** acima.
Formato & Passos	Reflita sobre as ameaças que você enfrenta e suas capacidades e vulnerabilidades existentes identificadas nos exercícios anteriores. Pode ser que você queria escrever suas respostas em um formato como aquele apresentado no **Apêndice D**. Aqui, você tentará fazer uma chuva de ideias sobre as novas capacidades que você quer construir. Para ajudar-lhe a identificá-las, considere as seguintes questões:

- **Quem/o que** está sob ameaça? Quais novas capacidades a pessoa ou as pessoas sob ameaça devem construir para poder reduzir a probabilidade ou o impacto da ameaça identificada?
- **Quem** está por trás da ameaça? Como você poderia influenciar a análise de custo-benefício da pessoa ou instituição que pode estar por trás da ameaça identificada? Existe alguma forma através da qual você pode melhorar a tolerância ou aceitação deles ao seu trabalho, ou dissuadi-los de agir contra você?
- **Como**: Quais informações são necessárias para realizarem o ataque? Como você pode proteger melhor as informações sensíveis sobre o seu trabalho e evitar que elas caiam em mãos erradas?
- **Onde**: Como podemos aumentar as capacidades de segurança do espaço ao nosso redor (por exemplo, prédios, veículos, propriedade privada) para tornar essa ameaça menos provável ou nociva?
- **Considerações psicológicas, emocionais e de saúde**: no contexto dessa ameaça, quais práticas você pode construir para reduzir o estresse e o cansaço para estar mais atenta e reagir mais criativamente a essa ameaça?

A essa altura, pode ser uma boa ideia juntar as anotações de todos os exercícios anteriores para ter uma ideia mais clara da sua atual situação de segurança e de algumas das novas capacidades necessárias para lidar com as ameaças que você enfrenta.

Nos próximos capítulos, consideraremos algumas dinâmicas sobre como construir essas novas capacidades e como desenvolvê-las como uma estratégia geral de segurança e montar planos de segurança

2
Construindo Novas Abordagens sobre Segurança

Agora que temos uma ideia clara de nossa atual situação e de algumas das novas capacidades que precisamos construir, já podemos começar o processo de construção de uma nova estratégia de segurança.

Ter uma estratégia é diferente de ter uma abordagem improvisada de segurança. Muitas das nossas reações iniciais e instintivas a ameaças, tais como aquelas que já identificamos, podem ser efetivas em nos manter seguras. Entretanto, algumas delas podem não fazer isso, e talvez até nos causem mal. Assim, à medida que começamos a construir novas táticas, devemos garantir que elas estejam relacionadas a uma estratégia geral para **manter o nosso "espaço"**, o que nos permite, assim, continuar nosso trabalho em defesa de direitos humanos. Abaixo, exploraremos três estratégias arquetípicas para manter nosso espaço de trabalho. Podemos recorrer a elas quando estivermos bolando nossa nova abordagem de segurança.

Estratégias de segurança: mantendo um espaço para nosso trabalho[16]

Quando pensamos em desenvolver uma ou mais estratégias (ou planos) de segurança, é útil lembrar que elas devem corresponder ao contexto político, econômico, social, tecnológico, legal e ambiental no qual estamos operando. Não existe uma estratégia para todas as situações.

Com respeito a isso, pode ser útil pensar em termos de quanto espaço temos à disposição para realizar nosso trabalho. Os atores que se opõem ao nosso trabalho têm o objetivo de encolher

16 Para informações em mais detalhes sobre estratégias de aceitação, dissuasão e proteção, veja Eguren, E. (2009). Protection International, *Novo Manual de Proteção para Defensores de Direitos Humanos*, Ch. 1.6

esse espaço, talvez até o ponto onde não possamos mais fazer nosso trabalho – por isso eles nos ameaçam.

O sentido de uma estratégia de segurança é nos ajudar a identificar táticas e fazer planos para manter ou expandir o espaço para o nosso trabalho na sociedade, e isso geralmente envolve engajar-nos com os atores que se opõem a nós, seja através do meio legal ou da conscientização.

Algumas pessoas consideram útil categorizar essas estratégias da seguinte forma:

Estratégias de aceitação

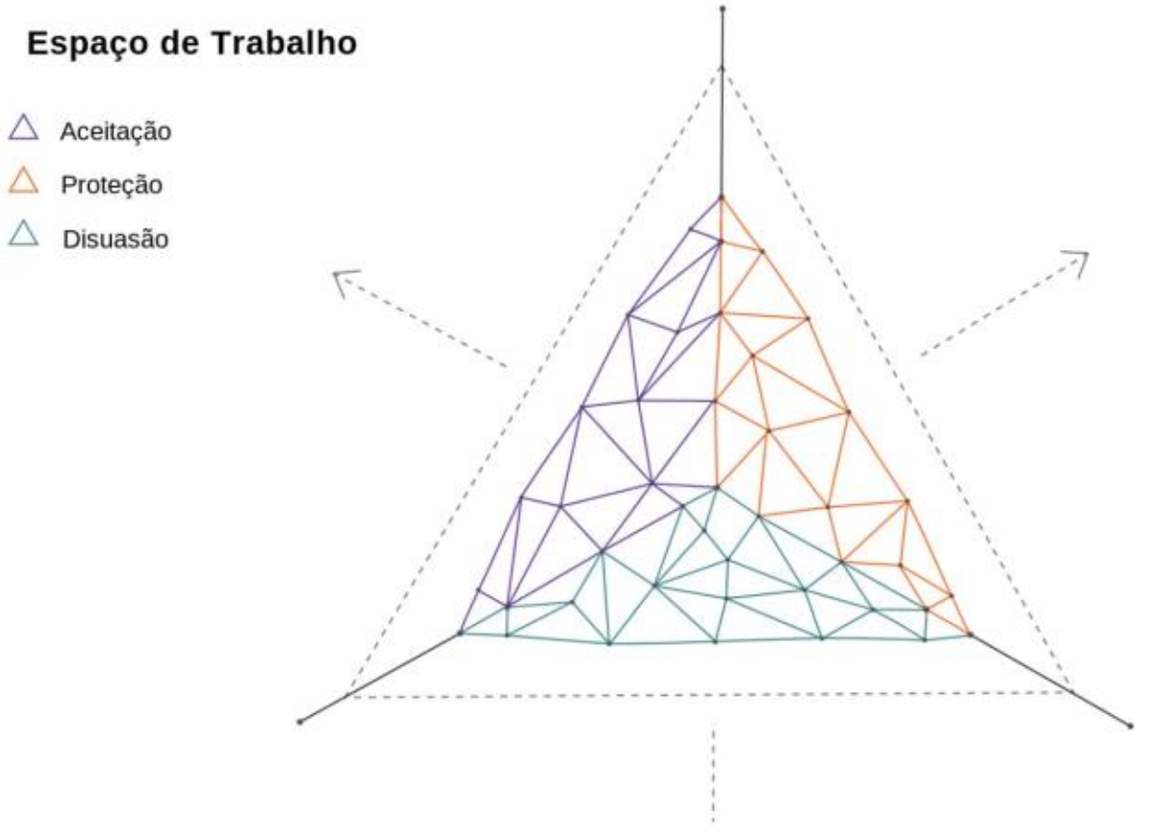
Uma estratégia de aceitação envolve engajar-nos com todos os atores – incluindo aliados, adversários e grupos neutros – para fomentar a tolerância, a aceitação e, por fim, o apoio às suas atividades pelos direitos humanos na sociedade. Estratégias de aceitação podem incluir fazer campanhas para construir apoio público para o seu trabalho ou para o de defensores de direitos humanos em geral, ou usar o meio legal para desenvolver relações positivas com as pessoas locais, o Estado, ou autoridades internacionais cujas obrigações correspondem a respeitar defensores de direitos humanos.

Estratégias de proteção

Uma estratégia de proteção ou autodefesa enfatiza o aprendizado de novos métodos e a implementação de novas práticas ou a potencialização da força dos seus aliados para proteger-se e cobrir as brechas nas suas práticas existentes. Exemplos de práticas que caem nessa categoria poderiam incluir a implementação do uso de criptografia de email ou práticas de gerenciamento de estresse dentro do grupo, ou então a organização de proteção acompanhada ou observância de direitos humanos durante suas atividades.

Estratégias de dissuasão

Uma estratégia de dissuasão foca no aumento do custo de seus adversários para realizar um ataque contra você ou seu trabalho Se voltarmos ao "espectro de aliados" mencionado na **Seção II | Explore**, essa estratégia pode incluir táticas que tragam seus oponentes ativos para a posição onde suas ações "saem pela culatra" de tal forma que oponentes passivos ou mesmo outros oponentes ativos possam (no âmbito moral) mudar de posição e tornarem-se neutros ou mesmo aliados passivos.[17] Exemplos de outras práticas que caem nessa categoria podem incluir emitir um apelo urgente denunciando violações a um Relator Especial das Nações Unidas ou realizando uma ação legal contra um adversário que está lhe ameaçando. Essas práticas são mais eficientes quando você possui um conhecimento extenso sobre o seu adversário e, idealmente, tem o apoio de aliados poderosos.



17 Martin, B. (2012) *Backfire Manual: tactics against injustice*. Irene Publishing, Sparsnäs, Sweden or Chenowith, E. & Stephan M.(2013) *Why Civil Resistance Works*. Columbia University Press.

É claro, essas categorias não são mutualmente exclusivas. A maioria dos defensores de direitos humanos utilizará todas as três estratégias durante o seu trabalho, sabendo disso ou não, e algumas táticas podem ser vistas como tendo a ver com duas ou todas as três estratégias simultaneamente. Entretanto, essa categorização ainda pode ser útil pois nos ajuda a pensar criticamente sobre os objetivos de nossas táticas de segurança.

No caso de organizações, é particularmente útil lembrar esses tipos de estratégias de segurança durante o processo de planejamento estratégico da organização e também para integrar a segurança como um aspecto fundamental desse processo.

Construindo capacidades

Agora que identificamos novas capacidades para melhorar nossa segurança, pode ser que tenhamos que passar por um processo de construção de capacidades, o que pode tomar várias formas: em nossa vida cotidiana, constantemente entramos nesse processo de aprendizado. Nesse caso, podemos simplesmente precisar identificar e dedicar-nos mais explicitamente à criação de um novo hábito ou montar um espaço em nosso trabalho e na nossa vida pessoal para desenvolver novas atitudes, conhecimentos e habilidades. De fato, ler este material é um exemplo desse processo. Na **Seção IV | Ação**, podemos aprender ferramentas e táticas específicas que podem ser úteis em certos cenários comuns para defensores de direitos humanos.

Quando pensamos em construir novas capacidades, pode ser útil considerar os cinco fatores a seguir que podem contribuir para essa mudança:

Bem-estar

Se queremos aprender qualquer coisa nova ou passar por qualquer processo de mudança, precisamos criar as condições em nosso corpo e em nossa mente para facilitar esse processo. Isso implica não

apenas ter autocuidado no sentido físico e psicológico, mas também significa criar o tempo e o espaço necessários em nossa agenda diária e incorporar conscientemente os processos de aprendizado em nossa rotina, ao invés de vê-los como mais um peso em nossa carga de trabalho existente.

Atitudes

são a medida do quanto nós ou as pessoas à nossa volta estão abertas à ideia de mudar nossas práticas e vemos tais mudanças como lógicas, necessárias e valiosas. Atitudes são subjetivas e podem – como nossa percepção sobre ameaças - ser afetadas adversamente por experiências de estresse, medo e trauma. Na **Seção I | Prepare-se**, você encontra mais informações sobre como fomentar atitudes positivas em nós mesmas e em nossos grupos visando segurança.

Conhecimento

nesse caso refere-se ao nosso entendimento do mundo à nossa volta, e num sentido prático, nosso conhecimento do contexto político, econômico, social, tecnológico, legal e ambiental que impacta nossa segurança. Na **Seção II | Explore** você encontra uma série de passos que podem ser tomados para melhorar nosso conhecimento sobre nosso contexto desde uma perspectiva de segurança.

Habilidades

aqui se referem à nossa habilidade prática de nos engajarmos com e manipular esse ambiente, e pode incluir qualquer coisa desde atividade física e autocuidado, a habilidades de negociação política, habilidades técnicas como usar comunicação criptografada, e assim por diante.

Recursos

É importante lembrar que provavelmente temos uma capacidade finita para melhorar nossas atitudes, conhecimentos e habilidades. O

quanto conseguimos impactá-las é, entre outras coisas, um reflexo dos recursos a que temos acesso. Isso frequentemente é um desafio para defensores de direitos humanos, assim como para pessoas que são marginalizadas por sua identidade de gênero, religião, raça, etnia, tipo de corpo, status social, casta, etc, e é uma variável importante para o nosso planejamento de segurança.

No próximo exercício, você pode continuar a elaborar sobre suas capacidades existentes e as novas capacidades que você elencou criativamente no **Exercício 3.1c**. Você pode categorizá-las como sendo táticas de aceitação, proteção ou dissuasão e ter um senso de onde existe espaço para você desenvolver melhor suas capacidades. Em seguida, considere os recursos que você já tem ou que irá precisar para construir essas capacidades. Além disso, na **Seção IV | Ação *online***, você encontra dicas sobre capacidades concretas a serem construídas para cenários particulares.

3.2a Exercício

Táticas de aceitação, dissuasão e proteção

Propósito & Resultado	Neste exercício, você pode desenvolver melhor as novas capacidades que identificou como necessárias para aprimorar sua segurança. Pensar nelas em termos de estratégias de aceitação, dissusão e proteção irá lhe ajudar a ter um senso da sua estratégia geral de segurança e descobrir táticas adicionais para serem desenvolvidas.
Informações de entrada e Materiais	Se você quiser anotar os resultados do exercício, considere usar um formato como o do **Apêndice D**.
Formato & Passos	**Passo 1**: veja as novas capacidades a serem construídas que você identificou no **Exercício 3.1b**. Considere

se cada uma delas é:

- uma tática de aceitação
- uma tática de dissuasão
- uma tática de proteção
- uma combinação de algumas das táticas acima.

Passo 2: agora, para cada ameaça, considere as novas táticas que você pode empregar para:

- aumentar a tolerância e a aceitação do seu trabalho entre seus adversários ou na sociedade em geral
- dissuadir seus adversários de agir contra você através do aumento do custo de um ataque
- proteger-se de ameaças e responder mais eficientemente a elas.

Continue a elaborar sua lista de novas capacidades com as novas ideias que forem surgindo.

Passo 3: Para cada uma das novas capacidades que você identificou, considere os recursos (financeiros e materiais) que você irá precisar acessar para construir essas capacidades.

Recursos externos para construir capacidades

Uma vez que tenhamos identificado as novas capacidades a serem construídas, pode ficar evidente que iremos precisar de ajuda de parcerias externas para facilitar esse processo. Entre elas poderão estar incluídas consultorias, especialistas, treinadoras em questões relacionadas a bem-estar e segurança. Outras capacidades podem aparecer como recursos financeiros ou materiais acessados através de um financiador ou outra organização intermediária. Aqui, exploraremos algumas boas práticas e dicas úteis para nos engajarmos com esses recursos externos.

Treinamentos e consultorias externos

Em alguns casos, será necessário passar por um treinamento ou trazer uma especialista em segurança para explorar as melhores maneiras de lidar com certos tipos de ameaças ou emergências.

Treinamentos e consultorias externos geralmente são muito úteis para ajudar organizações a desenvolver planos e habilidades de segurança. Às vezes, é mais rápido e útil chamar uma especialista externa, especialmente se ninguém do seu grupo pode fazer um treinamento ou o contexto é muito específico. Por outro lado, é preferível que seus próprios colegas e equipe recebam treinamento, pois dessa forma conhecimentos e habilidades externos serão integrados no conhecimento institucional.

De qualquer forma, para se engajar com consultoras de um jeito construtivo e empoderador, pode ser útil pensar nos seguintes termos. Consultorias externas devem:

- fomentar seu empoderamento e independência com referência à sua própria situação de segurança
- ajudar-lhe a ter conversas efetivas sobre segurança
- entender segurança desde uma perspectiva pessoal e de gênero
- ajudar-lhe a conduzir análises efetivas da sua própria situação
- fazer perguntas críticas que talvez você não faça a si mesma
- ensinar-lhe as ferramentas e táticas que você acha relevantes para suas atividades
- sugerir possíveis soluções para problemas baseadas em experiências em outros contextos
- sugerir outras ativistas ou organizações com as quais você pode trocar experiências
- sugerir possíveis estruturas para documentos de política interna e planos.

Consultorias externas não devem:

- conduzir por você uma análise das práticas de segurança da sua organização (sem envolver membros do grupo)
- desenvolver planos de segurança para você
- fornecer soluções de segurança para você
- fornecer políticas ou planos de segurança para você
- fazer mudanças ou tomar decisões por você
- exigir o aumento das suas medidas de segurança imediatamente... seus próprios passos irão aumentar sua segurança!

Dicas sobre como escolher treinamentos ou treinadoras adequadas

- Entre em contato com especialistas que são de confiança de suas amizades ou outros defensores de direitos humanos.
- Seja bem clara sobre o que espera aprender mas respeite a opinião da treinadora em termos do que é alcançável num dado período de tempo.
- Deixe claro antecipadamente se você acha que a treinadora é apropriada para você. Considere quais tipos de experiências ou conhecimentos (por exemplo, do seu contexto local) ela deve ter? Qual linguagem combina com vocês? Qual período de tempo? Qual lugar? Quanto tempo você terá depois para praticar ou trabalhar com as novas habilidades, conhecimentos ou recursos?

Recursos materiais para segurança

Como o exercício acima pode ter mostrado, construir novas capacidades de segurança pode frequentemente ter implicações financeiras. Exemplos podem incluir:

- substituição de *hardwares* ultrapassados (tais como computadores) que podem estar vulneráveis a ataques

- contratação de uma psicóloga em meio período para dar apoio a colegas em risco de trauma
- trabalhar menos horas e dedicar mais tempo à análise da nossa situação de segurança, o que pode ter efeitos colaterais como, por exemplo, nas datas limites da captação de recursos
- instalação de câmeras de vigilância em casa ou no escritório como proteção contra arrombamentos.

Embora você possa ter recursos em mãos que podem ser investidos em tais melhorias, não custa nada dar uma olhada nas várias organizações que buscam fazer melhorias de segurança com preços mais em conta para defensores de direitos humanos. Para ter uma lista delas, veja o *website* Segurança Holística.

3
Criando Planos e Acordos de Segurança

A conclusão lógica do processo que viemos seguindo até aqui - diagnosticar nossa situação de segurança, nossas capacidades e vulnerabilidades e identificar novas capacidades a serem construídas – é criar ou atualizar nossos planos e acordos relacionados à segurança com respeito ao nosso trabalho de direitos humanos. Esses planos podem ser formais, escritos em documentos, ou acordos informais compartilhados, dependendo da cultura do seu grupo ou organização. O que é mais importante lembrar é que eles são **acordos ou documentos vivos** e devem estar sujeitos a atualizações regulares através da repetição dos passos que nos fizeram chegar neste ponto.

Podemos organizar esses planos e acordos segundo uma lógica que faça sentido para nós, como:

- por atividade (por exemplo, plano para protestos, ou um plano para monitorar e documentar missões)
- por região (por exemplo, um plano para operar em zonas de conflito, um plano para trabalhar em áreas rurais)
- por indivíduos (por exemplo, um plano para advogadas, um plano para o departamento financeiro)
- por dia da semana de acordo com um padrão de trabalho
- por qualquer outra métrica que corresponda ao nosso trabalho.

Criar planos e acordos de segurança pode não necessariamente ser uma atividade nova para nós. Na verdade, na vida cotidiana, fazemos e implementamos planos de segurança o tempo todo. Por exemplo, cada vez que você sai de casa por um longo período de tempo, você pode decidir razoavelmente trancar as portas e garantir que todas as janelas estejam fechadas, e talvez até pedir a uma amizade ou vizinha para ficar de olho na casa. Embora possa parecer um simples senso comum, isso se qualifica como um plano de segurança.

O que diferencia defensores de direitos humanos de outras pessoas é que o nosso trabalho requer que tenhamos uma abordagem mais organizada sobre planejamento de segurança. Pode ser que necessitemos de mais planos de segurança do que o usual e soframos de maiores níveis de estresse que as outras pessoas. Portanto, é uma boa ideia que sejamos organizadas e explícitas – dentro de nossa organização, nosso grupo ou apenas com nós mesmas – sobre como nos comportamos em certas circunstâncias.

Elementos que compõem planos e acordos de segurança

Existem diversas maneiras para organizarmos nossos planos e acordos de segurança, segundo o jeito que trabalhamos ou o que quer

que seja mais prático. Entretanto, a maioria dos bons planos de segurança servirá a um dos seguintes propósitos ou a ambos:

Prevenção de ameaças

A maioria dos planos de segurança incluirá táticas que visam evitar que ameaças identificadas se concretizem (ou seja, reduzindo sua probabilidade de acontecer). Exemplos de táticas de prevenção podem incluir criptografia de uma base de dados de contratos para reduzir a chance de que ela possa ser acessada por adversários, ou empregar um guarda de segurança no escritório para reduzir a probabilidade de que ele seja invadido.

Resposta de emergência

Também chamados de planos de contingência, essas são as ações que serão tomadas em resposta a uma ameaça que se realiza. Eles geralmente têm o objetivo de diminuir o impacto do evento e reduzir a probabilidade de danos adicionais ao final das contas. Exemplos de táticas de resposta de emergência podem incluir levar um kit de primeiros socorros consigo enquanto estiver viajando, para o caso de pequenos acidentes, ou máscara e óculos num protesto para o caso de gás lacrimogêneo ser usado.

Ambos propósitos estão explicados em mais detalhes abaixo.

Prevenção de ameaças

Como foi mencionado, medidas preventivas envolvem o emprego de táticas que nos ajudam a **evitar** uma ameaça ou reduzir sua probabilidade.

Muitas dessas táticas refletirão estratégias de **aceitação, dissuasão e proteção ou autodefesa**, como exploradas no capítulo anterior. Assim, elas podem incluir campanhas legais ou outras formas de engajamento com o público ou com autoridades civis e militares

para conscientizar e aumentar a aceitação da legitimidade do nosso trabalho; fortalecer os laços com nossos aliados para aumentar o custo potencial de agressões contra nós, e qualquer número de táticas que constroem nossas próprias capacidades e agilidades frente às ameaças que identificamos ao nosso trabalho.

Embora, num primeiro momento, esses tipos de medidas requererão tempo e espaço para serem implementadas, em breve se tornarão aspectos "normais" de nosso trabalho e de nossas vidas pessoais.

Planos de emergência

Infelizmente, é um fato da vida que mesmo os mais bem desenhados planos podem falhar, especialmente no caso de incidentes de segurança. Esses são os momentos onde, talvez devido a uma mudança rápida das circunstâncias, experimentamos uma agressão ou acidente que pensamos que podíamos prevenir.

Nesses casos, é imperativo que tenhamos planos de antemão para reduzir o impacto em nós e em nossas amizades, família ou organização.

Como já foi discutido, existem algumas ocorrências comuns para as quais todas as pessoas devem se planejar e que podem ter nada que ver com nossas atividades pelos direitos humanos. Por exemplo, podemos ter um kit de primeiros socorros em casa, para o caso de acontecer um acidente durante o dia – mesmo para quando estivermos cozinhando ou limpando a casa! Embora possa parecer senso comum, isso é um plano de contingência realista e (tomara que) efetivo: no caso de um pequeno acidente em casa, um bom kit de primeiros socorros lhe ajudará a se recuperar mais rápido.

Como defensores de direitos humanos, também temos que nos preparar para incidentes comuns que podem surgir de nosso contexto geográfico, social, econômico ou tecnológico, tais como:

- desastres e acidentes naturais
- roubo ou crime violento, não relacionado com nosso trabalho
- perda de dados digitais
- eventos de significância emocional, como problemas em nossa família ou relações pessoais, que também podem afetar nossa segurança.

Adicionalmente, como descobrimos através dos exercícios até aqui, também existem ameaças que são diretamente relacionadas ao nosso trabalho e às atividades que realizamos nele. Exemplos comuns durante uma atividade como um protesto podem incluir:

- prisão
- violência física ou
- ser atingida por gás lacrimogêneo.

Nossas táticas de prevenção e planos de emergência em geral lidam com as mesmas ameaças; primeiro buscando reduzir sua probabilidade, e depois tentando diminuir seu impacto depois que ocorrem. Assim, essas táticas são as "duas faces da mesma moeda" e os melhores planos de segurança incluirão ambas. Enquanto pensamos num plano de prevenção, definimos nossas ações para reduzir a probabilidade de dano; num de emergência, nosso objetivo é reduzir o dano que possa acontecer, evitando que outras pessoas sejam afetadas, e dissuadindo o agressor (onde exista um) de causar mais estrago.

Bem-estar e dispositivos eletrônicos

Alguns aspectos importantes comumente esquecidos num planejamento de segurança são as táticas para o nosso bem-estar e táticas para lidar com nossos dispositivos eletrônicos e informação digital. Bem-estar nesse caso se refere às ações que tomamos para manter

nossa energia física e a uma abordagem focada em nosso trabalho e nossa segurança – elas podem incluir considerações como onde e quando iremos comer, dormir, relaxar e desfrutar de nossa vida enquanto fazemos nosso trabalho. Dispositivos e informações se referem a quais aparelhos dependemos para fazer nosso trabalho, e as táticas que empregaremos para garantir que nossa informação e comunicação não podem estar acessíveis para outras pessoas.

Quando falamos de defensores de direitos humanos individualmente, um plano simples de segurança pode parecer mais ou menos com o seguinte:

Objetivo

Missão para coletar testemunhos de vítimas de abusos de direitos humanos em uma área rural.

Ameaças

- Assédio ou aprisionamento pela polícia.
- Apreensão de computador e telefone móvel.
- Perda de dados como consequência.
- Comprometimento do anonimato das vítimas como consequência.

Prevenção - ações e recursos

- Alertar colegas e embaixadas e organizações internacionais amigáveis sobre essa missão, sua duração e local.
- Compartilhar detalhes de contato das autoridades locais e/ou agressores com embaixadas e organizações internacionais.
- Verificação de rotina com colegas a cada 12 horas.
- Os testemunhos serão salvos em um disco criptografado imediatamente após terem sido escritos.
- Os testemunhos serão enviados criptografados com GPG para colegas sempre ao fim do dia.

- A caixa de entrada e a pasta de emails enviados serão limpos no dispositivo após o uso.
- Indicadores de segurança e verificações de rotina serão compartilhados por mensagem criptografada.

Resposta - ações e recursos

- Preparar uma mensagem de alerta (em código) para ser enviada em caso de vigilância ou de estar sendo seguida.
- Preparar uma mensagem de alerta (em código) para ser enviada em caso de prisão.
- Ter o número de uma advogada na discagem rápida.

Plano de emergência

- Em caso de prisão, enviar mensagem de alerta e chamar advogada.
- Ao receber a mensagem de alerta, colegas alertarão embaixadas e organizações internacionais amigas.
- Pedir para que apelos urgentes sejam enviados por organizações internacionais às autoridades.
- Ceder a senha do disco criptografado caso esteja sob ameaça de abuso.

Considerações sobre bem-estar

- Comer num bom restaurante local, pelo menos duas vezes por dia.
- Desligar o telefone celular e todos os outros dispositivos durante as refeições.
- Ligar para a família através de um canal seguro para conversar ao fim do dia.

Dispositivos e informações

- Telefone móvel com mensageiro e aplicativo de chamada criptografados.
- Computador com disco criptografado e criptografia GPG para emails.

O exemplo acima, entretanto, ainda implica a cooperação de aliados para construir estratégias de aceitação e dissuasão. Quando falamos de grupos ou organizações, o processo de planejamento pode envolver alguns passos extras para garantir que todas as vozes sejam ouvidas durante o processo. Iremos explorar esse aspecto na próxima seção.

Além disso, como foi mencionado na **Seção I | Prepare-se**, ter planos sólidos e atualizados de segurança são um ótimo acompanhamento para nossa **resiliência e agilidade** – mas não pode ser um substituto. Enquanto é de grande ajuda passar por um processo de análise e planejamento que sejam o mais racional e objetivo possível, como sabemos, precisamos também estar preparadas para o "inesperado". A esse respeito, precisamos também desenvolver um senso de centramento e calma que será bem usado quando surgirem situações para as quais não fizemos – ou não poderíamos ter feito – um plano. Assim, planos e acordos de segurança são ferramentas úteis e importantes, da mesma forma que a habilidade de ser ágil e deixá-los de lado caso a situação exija.

4
Segurança em Grupos e Organizações

Existe uma série de outras questões que aparecem quando abordamos o planejamento de segurança dentro de um grupo ou organização estruturados. Organizações desenvolvem suas próprias hierarquias, culturas, estratégias e meios para planejar nos quais o processo de construção de estratégias e planos de segurança devem "se conformar".

O processo de planejamento de segurança num grupo pode ser estressante por diversas razões. Isso nos força a aceitar a possibilidade genuína de coisas desagradáveis acontecerem conosco no curso de nosso trabalho e que podem fazer com que nós ou nossas amizades e colegas nos fragilizemos ou fiquemos assustadas. Tam-

bém pode ser difícil de considerar todas as possíveis variáveis e chegar a acordos práticos sobre elas.

Além disso, para chegar a uma mudança organizacional bem-sucedida, temos que identificar um processo que possa tanto ser suficientemente inclusivo quanto respeitoso das hierarquias onde necessário. Precisamos também reconhecer a natureza pessoal da segurança e a necessidade de que a mudança seja gerenciada de modo a encorajar abertura e a reconhecer as distintas necessidades de diferentes membros do grupo de acordo com não apenas as ameaças que enfrentamos, mas também com aspectos como identidade de gênero.

Nesse capítulo, iremos explorar algumas das questões chave sobre construção e melhoria de estratégias e planos de segurança dentro de organizações.

Criando e mantendo planos de segurança

É importante ter o seguinte os seguintes pontos em mente quando formos criar planos de segurança seguindo uma análise de risco como mostrada nos segmentos anteriores, como parte de um grupo ou organização.

Conquistando adesão

Quando estivermos introduzindo novas pessoas a planos existentes, é importante passar por alguns pontos chave dos passos anteriores para que elas entendam como você chegou à conclusão que essas ameaças são plausíveis o suficiente para terem planos. Lembre-se, como foi explorado na **Seção I | Prepare-se**, segurança pode ser um assunto bastante difícil de lidar pois está misturada não apenas com nosso instinto psicológico, mas também com nossas experiências individuais de estresse, cansaço e trauma. Temos que lembrar de ser pacientes e compassivas e trabalhar com as percepções de nossas amizades e colegas ao invés de considerar (talvez falsamente) tudo como sendo “objetivo”. É importante não assustar as pessoas, mas

tentar criar um espaço relaxado e seguro no qual elas possam expressar suas questões e preocupações e se comprometer a agir de determinado jeito durante emergências.

Construção participativa

Algumas pessoas não irão reagir particularmente bem à construção de um plano ou acordo de segurança sem terem sido consultadas. Atividades de alto risco e emergências podem ser situações muito estressantes e é importante que cada pessoa esteja confortável com o papel e as responsabilidades designadas a elas e que haja um espaço para expressar suas preocupações sobre isso. A esse respeito, é importante que o processo de planejamento e segurança seja tão aberto e participativo quanto possível ao mesmo tempo que ainda mantém um comprometimento mínimo de todas as pessoas envolvidas.

Representado papeis

Em alguns casos, pode ser útil bolar uma cena para que os membros da organização possam praticar como responder a uma certa emergência. É claro, isso deve ser feito cuidadosamente: evite representar papeis em cenas que possam fazer com que qualquer membro do grupo se sinta perturbado, especialmente aqueles que foram vítimas de violações no passado. Tenha certeza de estar atenta a como os membros da organização se sentem sobre qualquer ideia de cena antecipadamente e dê a eles a oportunidade de sair caso achem necessário.

Planejando novamente e outras considerações

Lembre-se que todos os planos de segurança devem ser documentos e processos vivos. Uma vez que tenham sido “escritos” ou acordados, eles não devem ser colocados num quadro ou disco rígido compartilhado para nunca mais serem lidos! Pelo contrário, eles devem ser reavaliados e discutidos com regularidades, especialmente

quando novos membros se juntam ao grupo para facilitar sua aceitação e permitir que novos membros se familiarizem com eles. Faça com que isso seja parte do seu planejamento de segurança. Inclua datas fixas para rever suas práticas e planos de segurança. Também é útil incluir questões de segurança no seu processo de planejamento estratégico para garantir que segurança não fique para depois. Fazendo isso, você estará ajudando a garantir que considerações de segurança sejam parte de como você vê sua estratégia, desenvolve atividades, faz a alocação necessária de recursos financeiros e aponta de forma pró-ativa as brechas existentes em termos de capacidades.

Planejando emergências em grupos e organizações

Da mesma forma que defensores de direitos humanos individuais, grupos e organizações também devem fazer planos de emergência ou contingência para o caso de nossas tentativas de reduzir a probabilidade de uma agressão ou um acidente falhem. Quando estivermos criando tais planos em grupo ou organização, aqui estão alguns elementos chave para se ter em mente.

Definição de emergência

O primeiro passo para a criação de um plano de emergência é decidir em que medida definimos uma situação como uma emergência – ou seja, o ponto onde devemos começar a implementar as ações e medidas de contingência que planejamos. Às vezes, isso será autoevidente: por exemplo, um plano de emergência para prisão de uma amizade ou colega provavelmente definirá o momento da prisão como o ponto onde uma emergência deve ser declarada. Em outros casos, entretanto, pode ser menos óbvio: se uma colega que está realizando uma missão de campo para de responder seu telefone e não consegue ser encontrada por outros canais, quanto tempo deveremos esperar antes de definir a situação como uma emergência? Esses são acordos que, no caso de cada ameaça, terá que ser decidido por você, suas amizades e colegas.

Papeis e responsabilidades

Dependendo do número de pessoas envolvidas (em seu grupo de afinidade, coletivo, organização, etc.), pode ser útil que cada pessoa tenha papeis claros que elas estejam cientes e estejam previamente de acordo. Isso deve ajudar a reduzir a desorganização e o pânico no caso de um incidente. Para cada ameaça, considere os papeis que você talvez assuma e as coisas práticas envolvidas no ato de responder a uma emergência.

Em muitos casos, uma importante estratégia para emergências é a **ativação de uma rede de apoio**. Uma rede de apoio consiste de uma ampla rede de nossos aliados, que podem incluir nossas amizades e família, comunidade, aliadas locais (por exemplo, outras organizações de direitos humanos), elementos amigáveis do Estado e aliados nacionais ou internacionais como ONGs e jornalistas aliadas. Ativar uma rede de apoio, ou alguns elementos dela, durante uma emergência pode aumentar bastante o custo da agressão para seus responsáveis e fazer com que eles cessem novos ataques.

Volte ao seu mapa de atores (estabelecido no **Exercício 2.3 a/b**) e pense, para cada cenário de uma ameaça, as formas pelas quais seus aliados podem ser capazes de te apoiar. Pode ser útil estabelecer contato com eles e verificar se eles estarão afim de lhe ajudar e saber o que você espera que eles façam em situações de emergência. No caso de oficiais do Estado, é bom considerá-los em termos dos seus posicionamentos e talvez fazer referência a quaisquer leis locais ou internacionais que possam ser úteis para justificar essas posições.

Canais de comunicação

Coordenar uma reposta a uma emergência sempre envolve coordenação de ações e com frequência uma boa dose de improvisação. A esse respeito, a comunicação digital é cada vez mais importante. É importante estabelecer quais são os meios mais efetivos de comunicação com cada ator em diferentes cenários – e também identificar

meios secundários por precaução. Para emergências, esteja atenta que pode ser útil ter diretrizes claras sobre:

- o que comunicar
- quais canais usar (pense na sensibilidade da informação e a segurança do canal: está criptografado?)
- para quem?

Sistema de alerta e resposta rápida

Um Sistema de Alerta e Resposta Rápida é uma ferramenta útil para coordenar nossa resposta a uma emergência – que pode começar no caso de um acidente ou um ataque, ou quando existem indicadores muito fortes de que algum deles seja iminente. O Sistema de Alerta e Resposta Rápida é essencialmente um documento (eletrônico ou de outro tipo) centralizado que é aberto em resposta a uma emergência e inclui:

- todos os detalhes sobre os indicadores de segurança e incidentes que podem acontecer, com uma linha temporal clara
- indicadores claros a serem alcançados que significarão que o risco diminuiu novamente
- ações de cuidado posterior que podem ser tomadas para proteger as pessoas envolvidas de futuros danos e ajudá-las a se recuperar física e emocionalmente. Em alguns casos, será importante consultar profissionais para estabelecer a melhor conduta – por exemplo, em caso de eventos traumáticos, de violência física ou sexual, ou acidentes envolvendo materiais perigosos
- uma descrição clara das ações que foram tomadas e serão tomadas para alcançar esses indicadores, com uma linha temporal.

O Sistema de Alerta e Resposta Rápida fornece uma documentação útil para análise subsequente do que aconteceu e sobre como melhorar nossas táticas de prevenção e respostas à ameaças no futuro.

Para além da criação de uma estratégia ou uma série de planos individuais de segurança, as organizações devem levar em conta um gerenciamento de segurança e sua implementação por administradores, uma equipe e voluntárias como um processo de reavaliação constante. Organizações que implementam perfeitamente medidas corretas de segurança o tempo todo são raras e provavelmente sempre haverá espaço para melhorias. Mantenha isso em mente: é uma boa ideia avaliar regularmente a medida na qual nossa estratégia e planos de segurança são não apenas consistentes com o contexto no qual estamos operando (veja a **Seção II | Explore**), mas também que eles são aceitos e implementados pelos membros da organização.

Avaliação

Embora estejamos frequentemente atentas que existe espaço para melhorar a forma como implementamos nossas práticas de segurança, às vezes pode ser desanimador identificar por onde começar, o que priorizar e quem deve estar envolvida. É útil realizar uma avaliação da situação atual, pois ela irá nos ajudar a identificar em mais detalhes os aspectos particulares que precisamos melhorar do gerenciamento organizacional de segurança.

Essa avaliação e o processo subsequente de melhoramento necessitarão ser administrados, coordenados e realizados por pessoas tanto de dentro quanto de fora da organização. A equipe interna que pode estar envolvida pode incluir:

- o quadro de diretores e diretores executivos
- equipe de administração
- equipe regular e voluntárias.

Entidades externas que podem estar envolvidas no processo podem incluir:

- doadores
- consultorias e treinadoras externas.

Envolver cada um desses atores no processo tem suas próprias vantagens e desvantagens.[18] Entretanto, tendo em mente a natureza pessoal da segurança, é importante que desde o início, o processo seja realizado de forma inclusiva, participativa, transparente e sem julgamentos. Hierarquias formais dentro de organizações podem frequentemente ser um "ponto de engessamento" quando chega o momento de lidar com um processo sensível e pessoal como esse; é importante que o gerenciamento continue sensível e ciente das necessidades programadas e da equipe de "campo" ou voluntárias, que em geral são aquelas que se colocam em alto risco e/ou são menos remuneradas pelo seu ativismo. A equipe e as voluntárias devem também respeitar o fato de que a administração enfrenta uma tarefa difícil de padronizar uma abordagem de segurança e está fazendo isso – é o que se espera – para que todo mundo seja contemplado.

Critérios de avaliação

Como mencionado, um primeiro passo lógico para melhorar as atitudes, os conhecimentos e as habilidades da organização com respeito à segurança é realizar uma auditoria da situação atual para identificar as prioridades de melhoramento.

18 Para mais detalhes, veja o Capítulo 1.3 "Gerenciando mudanças organizacionais em direção a uma melhoria da política de segurança" no *Novo Manual de Proteção para Defensores de Direitos Humanos* (2009), Protection International.

Ao avaliar como os protocolos de segurança da organização são seguidos e implementados pela administração, pela equipe e pelas voluntárias, é importante observar algumas questões e indicadores concretos para evitar se sobrecarregar. Pode ser útil considerar os seguintes pontos:[19]

Experiência adquirida em segurança

Quanta experiência na implementação de práticas de segurança existe entre os membros da organização? Essa experiência está distribuída igualmente entre a equipe ou está concentrada entre alguns indivíduos?

Atitudes e atenção

As pessoas estão atentas à importância da segurança e proteção? Suas atitudes para isso são, em geral, positivas? Elas estão dispostas a continuar melhorando? Quais são as barreiras que elas percebem para fazer isso? Considere se isso flutua entre atitudes e atenção voltadas à segurança digital, segurança física e bem-estar psicológico.

Habilidades, conhecimentos e treinamento

Como mencionado anteriormente, para construir novos conhecimentos e habilidades, recursos, tempo e espaço precisam ser colocados à disposição para o treinamento (seja formal ou informal). Esse treinamento está disponível para os membros da organização? Isso inclui treinamentos em bem-estar psicossocial e segurança digital?

19 Baseado no Capítulo 2.1 "Avaliando a performance organizacional de segurança: a roda de segurança" do Novo Manual de Proteção para Defensores de Direitos Humanos (2009), Protection International.

Planejamento de segurança

Em que medida o planejamento de segurança está integrado no nosso trabalho? O quão frequente as análises de contexto (veja **Seção I | Prepare-se**) são realizadas e os planos de segurança são criados? Os planos são atualizados regularmente, e incluem gerenciamento de dispositivos digitais e gerenciamento de estresse?

Atribuição de responsabilidades

Existe uma divisão clara das responsabilidades para a implementação de nossas práticas de segurança? Em que medida essas responsabilidades são respeitadas, e quais são os potencias bloqueios para isso?

Liderança e Comprometimento

Em que medida os membros da organização estão envolvidos no planejamento de segurança da organização, e em que medida eles respeitam os planos existentes? Quais são os problemas que emergem aqui e como eles podem ser superados? Como o processo pode se tornar mais participativo?

Resposta aos indicadores

Com que frequência os indicadores de segurança são compartilhados e quão frequentemente eles são analisados e atitudes são tomadas em seguida se necessário?

Avaliação regular

Quão frequente é a atualização das estratégias e planos de segurança? Existe de fato um processo concreto para isso, ou ele acontece quando surge a necessidade? Como ele pode se tornar mais regular, quais outros problemas existem e como eles podem ser superados? No exercício abaixo, você poderá explorar algumas questões con-

cretas para lhe ajudar a estabelecer a medida na qual os planos de segurança são seguidos dentro da organização.

3.4 Exercício

Avaliação do desempenho de segurança da organização

Propósito & Resultado	Este é um exercício básico que verifica as percepções dos membros da organização com respeito à implementação de medidas de segurança na organização.
Informações de entrada & Materiais	Materiais para desenho ou uma cópia do exercício da roda de segurança (**Apêndice E**)
Formato & Passos	Pode ser que você queira focar no desempenho de segurança geral da organização, ou em um aspecto mais específico das práticas de segurança, como segurança digital, bem-estar psicossocial, segurança de viagens, segurança em zonas de conflito, etc. **Passo 1**: Utilize a "roda de segurança" organizacional (**Apêndice E**) ou desenhe um círculo e divida-o em oito seções, cada uma com um título (como no diagrama) ou crie sua própria roda de segurança. **Passo 2**: Para cada segmento da roda, preencha com uma cor que, na sua opinião, reflita a medida com que sua organização implementa boas práticas. **Passo 3**: para cada segmento, cada pessoa deve identificar as barreiras que atualmente estão bloqueando-a ou a organização em geral de melhor atender às boas práticas. **Passo 4**: considere também quais são as potenciais soluções para cada barreira ou problema.

Passo 5: Compare os resultados entre os membros da organização. Onde houve consenso e onde existem diferenças? Por que será que isso acontece?

Passo 6: Juntas, tentem identificar as áreas que devem ser priorizadas para melhoramento.

Priorizando áreas para melhoramento

Uma vez que a avaliação da situação atual foi realizada, devemos ter uma ideia sobre quais áreas devem ser priorizadas para melhoramento. Um plano para o melhoramento deve ser pensado a partir daí e disseminado entre a equipe e a administração. O plano deve:

- ter um objetivo claro em termos de novas boas práticas a serem implementadas
- uma linha temporal incluindo quem precisa estar envolvida no processo e o que esperar dessas pessoas
- estipular claramente os recursos necessários para a melhoria a ser realizada.

A administração deve garantir que a equipe e as voluntárias terão o tempo para realizar qualquer treinamento necessário ou alguma outra construção de capacidade necessária para que essa melhoria aconteça.

Superando a resistência ao planejamento de segurança[20]

Frequentemente acontece que, dentro de organizações, existe resistência entre algumas pessoas da administração, da equipe ou das voluntárias aos protocolos de segurança que se espera que elas sigam. Pode haver um grande número de razões para isso.

---

20 Baseado no material do Capítulo 2.3 do *Novo Manual de Proteção para Defensores de Direitos Humanos* (2009), Protection International, p. 153.

Quando estiver tentando lidar com resistência ao planejamento de segurança dentro da organização, é importante ter em mente que, como exploramos anteriormente, segurança é um conceito profundamente pessoal. Como tal, as pessoas podem ter razões pessoais particulares para resistir a certos protocolos que impliquem em mudanças em suas vidas pessoais, em seu tempo livre, ou em suas relações; eles também podem acarretar ter que aprender novas habilidades que são desafiadoras e que consomem suas energias que já estão sob estresse.

A melhor abordagem para lidar com resistência a mudanças nas práticas de segurança, portanto, é criar um espaço seguro no qual indivíduos possam falar confortavelmente das suas preocupações sobre isso. Como observado na **Seção I | Prepare-se**, é uma boa ideia praticar escuta ativa e comunicação não-violenta para facilitar um debate aberto e construtivo.

Abaixo, temos alguns estereótipos comuns de resistência, a razão por trás dessa resistência e as possíveis respostas para ajudar a superá-la dentro de grupos, organizações ou comunidades. É crucial buscar criar um espaço para discutir segurança dentro de um grupo para que as opiniões e experiências de todo mundo sejam respeitadas e ouvidas. Estar atenta às personalidades, dinâmicas de poder e hierarquias é muito importante quando estivermos decidindo como responder para superar essas resistências.

Estereótipos comuns de resistência

"Não estamos sendo ameaçadas" ou *"Nosso trabalho não é tão exposto ou polêmico quanto o de outras organizações"*.

Pensamento por trás do estereótipo

O risco continua o mesmo, ele não muda ou depende do fato de que o contexto do trabalho pode se deteriorar ou que o cenário pode mudar.

Respostas para superar a resistência

- O risco depende do contexto político. Como o contexto político é dinâmico, da mesma forma é o risco.

"O risco é inerente ao nosso trabalho como defensores de direitos humanos" e *"Já estamos atentas àquilo que estamos sendo expostas"*.

Pensamento por trás do estereótipo

As pessoas aceitam o risco e isso não as afeta em seu trabalho. Ou, o risco não pode ser reduzido, o risco está lá e não tem o que fazer.

Respostas para superar a resistência

- Deparar-se com um risco inerente não significa aceitar o risco.
- O risco tem pelo menos um impacto psicológico em nosso trabalho: no caso menos pior, ele induz um estresse que afeta o trabalho e possivelmente também afeta o bem-estar pessoal da pessoa e do grupo.
- Os riscos enfrentados por defensores de direitos humanos são feitos de vários elementos – ameaças de forças externas tentando impedir ou parar seu trabalho e a relação das vulnerabilidades e capacidades das defensoras com essas ameaças. Ao identificar e analisar ameaças e seus riscos, defensores de direitos humanos são capazes de perceber vulnerabilidades e capacidades/forças existentes e realizar esforços direcionados para reduzir suas vulnerabilidades e aumentar suas capacidades. Isso irá reduzir o risco mesmo que ele não seja totalmente eliminado. Criar espaço na organização para analisar riscos e acordar conjuntamente sobre estratégias para reduzi-los pode ter um efeito empoderador sobre

os indivíduos e o grupo, aumentando o senso individual e coletivo de segurança para melhor continuar seu trabalho.

"Nós já sabemos como lidar com o risco", ou *""Sabemos como nos cuidar"* e *"Temos muita experiência"*.

Pensamento por trás do estereótipo

O atual gerenciamento de segurança não pode ser melhorado e por isso não vale à pena fazê-lo. O fato de que não sofremos dano no passado garante que não seremos afetadas no futuro.

Respostas para superar a resistência

- O gerenciamento de segurança está baseado no entendimento de que os riscos enfrentados por defensores de direitos humanos resultam do ambiente político e do impacto que o seu trabalho tem nos interesses dos diferentes atores. Devido a esse contexto ser dinâmico, o risco também o é, requerendo constante análise e adaptação de estratégias. Além disso, os atores mudam de posição e de estratégias, fazendo com que defensores de direitos humanos também precisem se adaptar para gerenciar os riscos.
- A experiência de fazer avançar os direitos humanos e defender os direitos de outras pessoas requer que constantemente avaliemos nossa estratégia, criemos espaço para nosso trabalho e identifiquemos apoio. Da mesma forma, é assim que acontece com o gerenciamento de segurança. Se você quer fazer a diferença no seu trabalho e proteger as pessoas com quem e para quem trabalha, você precisa estar bem e segura. E ao mesmo tempo existe uma certa obrigação moral de que você não coloque as pessoas com quem trabalha em mais riscos.

"Sim, a questão é interessante, mas existem outras prioridades".

Pensamento por trás do estereótipo

Existem outros assuntos mais importantes que a segurança das ativistas.

Respostas para superar a resistência

- Primeiro e mais importante, ativistas são pessoas. Elas têm família, amizades, comunidades que precisam delas e das quais elas

precisam. Autocuidado é um ato político. Os adversários das ativistas visam causar-lhes dano, medo, ansiedade e/ou estresse para impedir ou parar seu trabalho. Estar viva e bem é um pré-requisito para continuar a lutar contra injustiças.

"E como iremos pagar por isso?"

Pensamento por trás do estereótipo

Segurança é cara e não pode ser incluída nas propostas de levantamento de fundos.

Respostas para superar a resistência

- Pensar que ao invés da segurança ser uma fraqueza, ela é um poder que, no fim, irá beneficiar as pessoas com quem e para quem você trabalha.
- Segurança é um conceito bastante individual. Em muitos casos, ela está intimamente ligada às atitudes e aos comportamentos da ativista. Melhorar a segurança de alguém frequentemente requer uma mudança de atitude e uma subsequente mudança no comportamento e nas práticas que geralmente não custam absolutamente nada – pelo menos não em termos monetários.
- Doadores e parcerias estão interessadas na continuação do trabalho das ativistas. Eles preferirão trabalhar com uma organização que reconhece as questões de segurança ao invés de correr o risco de acabar com seu trabalho e de ter uma perda potencial dos seus investimentos.

"Se prestarmos tanta atenção à segurança não seremos capazes de fazer o que é realmente importante, que é trabalhar com as pessoas e devemos isso a elas."

Pensamento por trás do estereótipo

Nossa própria segurança e bem-estar não têm impacto sobre nossa habilidade de ajudar as outras pessoas. Nossa segurança e bem-estar são irrelevantes para aquelas com quem e para quem trabalhamos.

Respostas para superar a resistência

- Segurança é um conceito bastante individual e requer que cada indivíduo tome decisões sobre os riscos que são aceitáveis para

si. Ser sensíveis à nossa segurança é parte de nossa resistência contra aqueles que querem nos causar danos pelo trabalho legítimo que fazemos. Somos muito menos capazes de cuidar das outras pessoas se não cuidamos de nós mesmas.

- Se cuidamdos de nós mesmas e de nossa segurança, estaremos melhor preparadas para cuidar das outras ao nosso redor.
- Pessoas correm riscos ao confiar em nós para lidar com suas situações e se não trabalhamos sobre nossa segurança, isso também irá afetá-las; elas poderão escolher confiar em outra organização que planejou adequadamente sua segurança e assim também está garantindo mais segurança para outras pessoas.

"Não temos tempo pois já estamos sobrecarregadas".

Pensamento por trás do estereótipo

É impossível arranjar tempo em nossa agenda de trabalho.

Respostas para superar a resistência

- Existe uma falsa distinção entre pensar sobre segurança e bem-estar e o nosso trabalho. Segurança e bem-estar tornarão nosso trabalho mais sustentável. É estrategicamente mais eficiente no longo prazo criar esse espaço.
- Gerenciar segurança não precisa tomar muito tempo. Frequentemente basta fazer pequenas mudanças em nosso trabalho cotidiano.
- No longo prazo, perderemos menos tempo respondendo a emergências se estivermos previamente preparadas, e mais que isso, teremos que lidar menos frequentemente com as consequências físicas, emocionais e econômicas de emergências que nos afetam como seres humanos e organizações.

"A comunidade está com a gente: quem se atreveria a nos machucar?"

Pensamento por trás do estereótipo

Somos parte da comunidade. A comunidade não é fragmentada, não muda, nem seus membros e suas opiniões. A comunidade não pode ser influenciada.

Respostas para superar a resistência

- A comunidade não é homogênea e também é feita de pessoas que podem afetar negativamente nosso trabalho.
- Sob pressão, às vezes, até aquelas que querem nos apoiar podem ficar contra nós.

"Na nossa vila, as autoridades se mostraram compreensivas e têm colaborado."

Pensamento por trás do estereótipo

As autoridades locais não são afetadas pelo nosso trabalho de direitos humanos e não mudarão sua forma de agir. Não existe hierarquia entre autoridades nacionais e locais.

Respostas para superar a resistência

- A memória histórica da organização terá exemplos de autoridades locais se opondo ao trabalho por direitos humanos quando seu limite de tolerância foi excedido.
- As autoridades locais têm que seguir ordens de cima. Elas são feitas de pessoas que podem ter interesse em proteger agressores.
- O contexto político muda.
-

5
Melhorando o Impacto Positivo de suas Medidas de Segurança e Reduzindo os Possíveis Impactos Negativos: A Abordagem "Não Cause Danos"

Mudar nossas práticas relacionadas à segurança pode tanto ter impactos positivos quanto negativos. À medida que construímos novas práticas de segurança, vale à pena pensar como podemos aumentar o impacto positivo sobre a nossa segurança e a de outras pessoas, ao mesmo tempo que monitoramos e tentamos reduzir quaisquer impactos negativos que essas práticas possam causar.

Precisamos começar da perspectiva de que, como defensores de direitos humanos em risco, frequentemente estamos operando num contexto caracterizado por conflitos. Esses conflitos podem ser armados ou não armados e a violência a qual estamos sujeitas pode ser física, direta e/ou armada, ou pode ser econômica, de gênero, institucional, estrutural, psicológica, etc. Às vezes, comunidades ativistas são afetadas por conflitos dentro de organizações, comunidades ou movimentos. No mínimo, raramente estamos livres de dinâmicas de privilégio (relacionadas a identidade de gênero, orientação sexual, raça, religião, etnia, linguagem, status socioeconômico, etc.) e outras formas de violência estrutural.

Quando começamos a adotar novos comportamentos relacionados com segurança, podem haver algumas consequências negativas não intencionais que podem acabar afetando esses conflitos. Isso não significa que mudar nossas práticas é uma ideia ruim – pelo contrário, é uma boa ideia estar atenta às potenciais consequências negativas para que possamos tomar decisões realmente embasadas.

Para alcançar isso, é útil se engajar com a **Abordagem Não Cause Danos (NCD)**.[21] Ela presume que todas as nossas ações e comportamentos têm consequências, tanto positivas quanto negativas.

Ações + Comportamentos = Consequências.

No contexto de conflitos tanto internos quanto externos ao grupo, nossas ações e comportamentos podem criar **divisão** adicional entre as pessoas (piorando, portanto, o conflito) ou **conexão** adicional entre as pessoas (aliviando o conflito). Abaixo, iremos considerar algumas formas pelas quais nossas ações e comportamentos podem ter efeitos positivos ou negativos sobre esses conflitos quando implementamos mudanças em nossas práticas de segurança.

Ações e recursos

Entendemos ações como qualquer coisa que fazemos e que trazemos para uma situação existente, incluindo os recursos obtidos, usados e transferidos durante o curso de nosso trabalho e enquanto implementamos nossas práticas de segurança. Recursos para segurança e bem-estar são frequentemente considerados como valiosos e o acesso a eles pode ser limitado. À medida que você expande suas ações e recursos para se engajar com segurança dentro de seu grupo ou organização, qual pode ser o impacto dessas transferências de recursos em si, em seus aliados e em seus oponentes?

Existem algumas consequências potencialmente negativas que deve-se estar atenta aqui e elas podem facilmente se tornar sérias questões de segurança. Quatro formas pelas quais isso pode acontecer são:

21 Para mais informações veja CDA Collaborative, Do No Harm http://www.cdacollaborative.orgprograms/do-no-harm/

1 Competição vs inclusividade

Fornecer recursos (como treinamento, *hardware* para computador ou recursos de bem-estar) apenas para pessoas selecionadas dentro de um grupo pode aumentar as tensões já existentes ou criar novas. Por outro lado, ser inclusivo sobre usar e compartilhar seus recursos pode ajudar a conectar as pessoas e fortalecer sentimentos de inclusividade. Se os recursos não podem ser compartilhados entre todos os membros do grupo, é importante ter uma comunicação clara sobre por que esse é o caso (talvez devido aos altos níveis de risco dos indivíduos em questão) e obter o apoio do grupo para essa decisão.

2 Substituição vs apreciação

Adotar novas práticas ou implementar novos recursos pode significar que velhas práticas, tradições ou mesmos papeis de pessoas sejam substituídos ou colocados de lado. É importante que as estratégias e recursos existentes sejam reconhecidos e substituídos somente quando justificados e de uma forma que respeite os esforços dispendidos neles.

3 Seletividade e relações de poder

Os membros do grupo que recebem qualquer treinamento atenção, responsabilidades, etc. a mais podem, através do seu acesso a novos conhecimentos e recursos, também ganhar mais "poder" informal ou formal ou influência dentro do grupo. Isso pode agravar tensões existentes ou levar a tensões novas. Por outro lado, onde for possível, incluir todo o grupo ou a organização pode melhorar a aceitação de medidas de segurança e reforçar o senso de unidade do grupo.

4 Padrão de vida e de trabalho

Isso é particularmente relevante no caso de membros da equipe e voluntárias. Quem recebe qual treinamento? Quem recebe dinheiro por quais atividades? Quem se beneficia mais das práticas de segu-

rança ou sofre mais com o peso da vida e trabalho cotidianos? Quem possui qual acesso à comunicação devido a viver em ambientes rurais ou urbanos? Como pode-se fazer uma ponte entre essas diferenças que dividem?

Comportamentos e mensagens éticas implícitas

Quando estivermos construindo nossas capacidades e adotando novas práticas, também temos que estar atentas ao nosso comportamento, a como ele muda e como isso pode impactar nas outras pessoas. Nossos comportamentos mandam mensagens não verbais e implícitas a nossas companheiras de ativismo, colegas, ao nosso grupo, organização, alianças e adversários. A interpretação dessas mensagens pode, como com nossas ações, levar a mais conexão ou divisão dentro do grupo. É bom considerar cada uma de nossas novas práticas e as potenciais mensagens que elas enviam para as pessoas ao nosso redor e, onde for possível, buscar verificá-las. Abaixo, exploraremos quatro formas comuns pelas quais nossos comportamentos podem levar a um aumento da conexão ou da divisão dentro do grupo.

1 Características culturais

Uma “lente” pela qual as outras pessoas interpretam nossos comportamentos é, sem dúvida, a cultura. Em ambientes multiculturais, é uma boa ideia considerar como novas práticas de segurança podem ser interpretadas através desse filtro. Por exemplo, noções como privacidade, ou o valor de certos recursos ou tradições culturais, ou as formas de tomada de decisão frequentemente variam bastante entre diferentes culturas. Esteja atenta aos seus arredores culturais e verifique se as novas medidas de segurança que você está tomando estão sendo interpretadas de maneiras que não ofendam ou causem divisão.

2 Diferentes valores para diferentes vidas

Isso pode ser especialmente relevante em grupos e organizações que são constituídas de diferentes nacionalidades ou culturas e onde estão presentes diferentes níveis de "especialidades" – que ocasionalmente refletem estruturas sociais de classe. Se certos grupos ou membros não estão incluídos nos planos de emergência de sua organização, eles podem interpretar isso como um sinal de que a organização não se importa tanto com sua segurança. Algumas organizações internacionais, por exemplo, não refletem e criam um plano de evacuação de emergência para sua equipe local e focam apenas no pessoal internacional. Isso pode ser interpretado como "o bem-estar de algumas pessoas da equipe é mais valioso que o de outras". Além disso, a importância de estar atenta com a segurança da equipe administrativa, do pessoal da limpeza e de outras pessoas que também trabalham na organização é frequentemente deixada de lado: pense em quem irá atender o telefone para receber uma chamada de emergência ou quem provavelmente irá reconhecer os potenciais indicadores de segurança no prédio? Uma abordagem inclusiva não apenas permite mais coesão e apropriação das medidas de segurança nos grupos, mas também melhora a segurança de todas as pessoas.

3 Medo, tensão e desconfiança

Adotar novas medidas de segurança também pode ser interpretado como um aviso de existe uma falta de confiança sobre e entre as colegas, outras ativistas e envolvidas externas. Por exemplo, criptografar suas chamadas de telefone pode ser entendido como uma declaração de que você não confia na sua companhia de telefone; de maneira similar, se você diz estar menos prontamente disponível para certas atividades perigosas, isso pode levar a um aumento da desconfiança entre suas companheiras ativistas. Assim, é importante simplesmente tornar claro as razões para as suas novas medidas de segurança e a lógica por trás delas de uma maneira franca, aberta e honesta. Ouça os comentários e veja como as pessoas ao seu redor

reagem para ver se existe qualquer consequência que possa ser evitada ou trabalhada, e faça o que puder para manter a confiança em ambas direções. No caso de adotar novas medidas radicais de segurança e com isso chamar potencialmente a atenção negativa de seus adversários e atores neutros – como através da criptografia da comunicação ser notada pela companhia de telefone ou pelo provedor de internet –, considere usar, em paralelo aos novos, métodos antigos ou corriqueiros para diminuir as suspeitas.

4 Uso de recursos

Quaisquer novos recursos - como *hardware* ou *software* de computador, treinamentos, veículos, acesso a apoio psicossocial, etc. – que se tornaram disponíveis para aumentar a segurança – devem ser usados com responsabilidade pelas pessoas que têm acesso a eles. Os membros do grupo ou da equipe que não têm acesso priorizado a tais recursos podem ficar com a impressão que eles são usados por suas colegas para o seu próprio benefício se o propósito desse uso não for compartilhado no grupo ou organização. A exclusividade pode dar a entender que aquela pessoa que controla os recursos pode usá-los para os seus propósitos sem ser responsabilizável.

Para analisar seu comportamento e o que suas práticas de segurança dizem às outras pessoas, pode ser útil desenhar uma tabela como a do exemplo no **Apêndice F** e pensar nos exemplos dados antes de preenchê-la para você.

Você deve considerar nossas práticas sob a luz desses conceitos e falar sobre elas em um espaço seguro com suas amizades, família e colegas para tentar fortalecer os efeitos positivos em suas relações, e diminuir os seus efeitos negativos. Refletir sobre nossa estrutura de segurança nos termos dessas questões pode evitar que produzamos novos tipos de cenários de ameaças (segundo nossa configuração de segurança) devido a essas implementações. Na verdade, buscamos criar mais atividades e comportamentos que conectem as pessoas, e isso beneficiará a segurança de todo mundo.

Conclusão

Através das seções **Prepare-se**, **Explore** e **Monte Estratégias**, abrimos um caminho que parte da definição da segurança para nós e da criação de um espaço para segurança dentro de nossas organizações, passa pela realização de uma análise e um diagnóstico da nossa situação de segurança, até o planejamento da manutenção e melhoria de nossa segurança durante nosso trabalho como defensores de direitos humanos.

Como você irá implementar essa série idealizada de passos dependerá muito da natureza do seu trabalho e de quem trabalha com você. É importante manter em mente que eles representam um processo cíclico em evolução, e a constante reavaliação de nossa situação e a atualização das estratégias e planos é o ideal.

Embora as três seções neste manual foquem no gerenciamento de um processo de criação de capacidades de segurança em grupo, o próximo passo seria conhecer ferramentas e táticas específicas que você pode colocar em prática para aumentar a segurança em diferentes aspectos do seu trabalho.

Na **Seção IV | Ação**, você encontrará ferramentas e táticas extraídas da comunidade de defensores de direitos humanos, treinadoras e especialistas em segurança e bem-estar que podem ser implementadas em atividades particulares de alto risco para o trabalho de direitos humanos.

Leituras para Aprofundamento

- **CAPACITAR Emergency Response Tool Kit**

  Como uma resposta ao trauma do furacão Katrina, o kit inclui práticas básicas e simples ensinadas pelo Capacitar

para empoderar as pessoas para lidarem com o estresse de situações desafiantes.

http://www.capacitar.org/emergency_kits.html

- **CDA Collaborative, Do No Harm**

  Uma estrutura para analisar os impactos da ajuda em conflitos e para agir na busca da redução dos impactos negativos e maximizar os impactos positivos.

  http://cdacollaborative.org/cdaproject/the-do-no-harm-project/

- **Insiste, Persiste, Resiste, Existe: Women Human Rights Defenders' Security Strategies**

  Esse relatório junta vozes de mulheres defensoras de direitos humanos de todas as partes do mundo no combate à violência e à discriminação em contextos complexos – em situações de conflito aberto ou velado, de violência armada organizada, assim como nos fundamentalismos.

  http://kvinnatillkvinna.se/en/publication/2013/04/18/insiste-persiste-resiste-existe-2009/

- **Integrated Security: The Manual**

  Esse manual cobre todos os aspectos do trabalho e da vida de ativistas, desde saúde e redes pessoais a espaços seguros de trabalho. Esse manual mostra como você, defensora de direitos humanos, facilitadora, organização de direitos humanos, doador/apoiadora ou organização que trabalha em contextos de emergência e desenvolvimento podem montar Oficinas Integradas de Segurança.

  http://integratedsecuritymanual.org

- **New Protection Manual for Human Rights Defenders**

  O propósito desse manual é fornecer conhecimento adicional e algumas ferramentas a defensores de direitos humanos que podem ser úteis no aprimoramento da sua compreensão sobre segurança e proteção.

  http://protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/

- **Security in-a-Box: Tools and Tactics for your Digital Security**

  Um kit digital de segurança para ativistas e defensores de direitos humanos de todo o mundo.

  https://securityinabox.org

- **Security to Go: A Risk Management Toolkit for Humanitarian Aid**

  Um guia simples e fácil de usar para não-especialistas em segurança para montar sistemas básicos de segurança e gerenciamento de risco em novos contextos ou situações de resposta emergencial.

  https://www.eisf.eu/library/security-to-go-a-risk-management-toolkit-for-humanitarian-aid-agencies/

- **Workbook on Security: Practical Steps for Human Rights Defenders**

  Um guia passo a passo para produzir um plano de segurança para você e/ou sua organização, seguindo uma abordagem sistemática para avaliar sua situação de segurança e desenvolver estratégias e táticas de redução de riscos e de vulnerabilidades.

  https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk

Apêndices

Prepare-se
Explore
Monte estratégias

Bibliografia

- Barry, J. (2011) Integrated Security: The Manual. Um projeto da Kvinna till Kvinna Foundation. Disponível em:

  www.integratedsecuritymanual.org

- Barry, J. and Nainar, V. (2008), Insiste, Persiste, Resiste, Existe: Women Human Rights Defenders' Security Strategies. Um projeto conjunto da Urgent Action Fund for Women's Human Rights, Front Line Defenders e The Kvinna till Kvinna Foundation. Disponível em:

  http://kvinnatillkvinna.se/en/publication/2013/04/18/insiste-persiste-resiste-existe-2009/

- Bell, J. and Spalding, D., Security Culture for Activists. Um projeto da The Ruckus Society. Disponível em:

  www.ruckus.org/downloads/RuckusSecurityCultureForActivists.pdf

- Bertrand, M., Monterrosas, E., and Oliveira, I. (2014) Programa de Asesorías en Seguridad y Protección para Personas Defensoras de Derechos Humanos. Um projeto do Peace Brigades International Mexico Project. Disponível em:

  http://www.pbi-mexico.org/fileadmin/user_files/projects/mexico/images/News/Reducido_GuiaFacilitacion.pdf

- Camfield, J. and Tuohy, S. (2015) SAFETAG Manual. Um projeto de Internews. Disponível em:

  https://safetag.org

- Cane, P. M., CAPACITAR Emergency Response Tool Kit. Um projeto de Capacitar International. Disponível em:

http://www.capacitar.org/emergency_kits.html

- CDA Collaborative, Do No Harm

  http://cdacollaborative.org/cdaproject/the-do-no-harm-project/

- Chenowith, E. & Stephan M. J. (2013) Why Civil Resistance Works, Columbia University Press.

- Davis, J. (2015) Security to Go: A Risk Management Toolkit for Humanitarian Aid. Um projeto do European Interagency Security Forum (EISF). Disponível em:

  https://www.eisf.eu/library/security-to-go-a-risk-management-toolkit-for-humanitarian-aid-agencies/

- Eguren, E. and Caraj, M. (2009) Protection Manual for Human Rights Defenders, Protection International, 2nd Ed. Um projeto de Protection International. Disponível em:

  http://protectioninternational.org/publication-page/manuals/

- Lakey, G., Spectrum of Allies. Um projeto de Training For Change. Disponível em:

  http://www.trainingforchange.org/tools/spectrum-allies-0

- Martin, B. (2012) Backfire Manual: Tactics Against Injustice, Irene Publishing. Também disponível em:

  http://www.bmartin.cc/pubs/12bfm/index.html

- Rimmer, A. (2011), Workbook on Security for Human Rights Defenders. Um projeto de Front Line Defenders. Disponível em:

  https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk

- Shields, K. (1993) In the Tiger's Mouth: An Empowerment Guide for Social Action, New Society Publishers. Exercício do Barômetro Social disponível em:

https://organizingforpower.files.wordpress.com/2009/05/allies-chart-new1.jpg

- United Nations Office of the High Commision for Human Rights (OHCHR), Declaration on Human Rights Defenders. Disponível em:

  http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Declaration.aspx

- Voisin, J., MAT: Metadata Anonymisation Toolkit. Disponível em:

  https://mat.boum.org

Apêndice A

Como Uso Meu Tempo?[22]

Separe um tempo para pensar nas formas como você gasta o seu tempo. Reflita e escreva suas respostas às seguintes questões sobre o seu trabalho, seus recursos, mecanismos de adaptação e saúde. Você não precisa compartilhar as respostas com ninguém. Se estiver realizando esse exercício num grupo, pode ser interessante refletir sobre como você se sente quando olha para o uso do seu tempo dessa forma.

1. **Seu trabalho**	horas / dia	dias / semana	horas / semana
a. No total, quantas horas por dia você gasta trabalhando como ativista (pagas ou não pagas)? Quantos dias numa semana você faz esse trabalho? "Trabalho" nesse sentido significa reuniões (dentro ou fora do escritório), eventos, oficinas, conferências, conversas do trabalho, responder emails, trabalhar d escritório ou de casa, eventos "sociais" do trabalho, colaborações, etc.			
Em média, quantas horas por dia você gasta com trabalho não pago (ativismo)? Quantos dias por semana?			

22 Baseado no material de Barry, J. et al. (2011) *The Integrated Security Manual*, Kvinna Till Kvinna. http://www.integratedsecuritymanual.org/sites/default/files/wriex_howdoiusemytime.pdf

Em média, quantas horas por dia você gasta com trabalho pago (ativismo)? Quantos dias por semana?			
b. Em média, quantas horas por dia você gasta em trabalho que não tem relação com seu ativismo (geralmente, sua principal fonte de renda)? Quantos dias por semana?			
c. Em média, quantas horas por dia você gasta com trabalho doméstico (limpeza, administração, compras, cuidado com outras pessoas, etc.)? Quantos dias por semana?			

2. **Seus recursos**	horas / dia	dias / semana	horas / semana
a. Treinamento: em média, quantas horas por dia você gasta nos seus treinamentos (isso pode incluir, escola, aulas, biblioteca, cursos, leituras, oficinas, cursos diplomados, estudando para provas, tese)? Quantos dias por semana?			

b. Alimentação: em média, quantas horas por dia você gasta comendo?

Quantas vezes em média você come por dia? _____

Geralmente você pula alguma refeição no dia? _____

Se sim, qual delas? _____

Você substitui alguma refeição por “comida rápida”? _____

Se sim, qual delas? _____

_____

_____

c. Exercícios físicos: em média, quantas horas do dia você gasta fazendo alguma forma de exercício físico por dia? Quantos dias por semana?			
d. Cuidado pessoal: em média, quantas horas por dia você gasta com cuidado pessoal? Quantos dias por semana?			
d. Cuidado pessoal: em média, quantas horas por dia você gasta com cuidado pessoal? Quantos dias por semana?			
e. Descanso: em média, quantas horas por dia você gasta com descanso de qualidade (dormir ou cochilar)? A que horas geralmente você vai para a cama? A que horas geralmente você acorda?			
f. Práticas contemplativas ou de desenvolvimento pessoal: em média, quantas horas por dia você gasta com desenvolvimento pessoal (estar consigo mesma, refletir, meditar, outras práticas contemplativas ou espirituais, ir em seções para a saúde e/ou terapia)?			
g. Quantas horas por dia você gasta com as suas **relações interpessoais**:			

família, amizades, companheiras/os, outras? Quantos dias por semana?			
h. Quantas horas por dia você gasta com **atividades prazerosas/ relaxantes/ acolhedoras)**? Quantos dias por semana?			

Faça uma lista dessas atividades aqui: _____

_____

_____

2. **Saúde**	horas / dia	dias / semana	horas / semana
a. Quando foi a última vez que você visitou uma profissional de saúde ou curadora/curandeira?			
b. Quantas vezes por ano você faz uma checagem geral de saúde?			
c. Você sente dor no seu corpo neste momento? Se sim, onde?			
d. Se você tem dor no corpo, quais passos você toma para aliviá-la?			
e. Se você tem problemas médicos, quais são eles?			
f. Se você tem problemas sérios de saúde, você já falou sobre eles com uma profissional de saúde/curadora com a qual se sente confortável?			
g. Algum outro comentário sobre saúde?			

Apêndice B

Escaneando Dispositivos Digitais em Busca de Indicadores de Segurança

O que vem a seguir é uma lista de verificação, que não pretende ser exaustiva, sobre formas através das quais você pode verificar seus dispositivos digitais regularmente para estabelecer uma linha-base (um estado "normal" do aparelho) e perceber indicadores de segurança com mais facilidade.

Escaneado dispositivos em busca de *malwares* ou *spywares*

Para usuárias de computadores que rodam Windows ou MacOS, é importante escanear regularmente seus dispositivos em busca de *malwares* e *spywares*. Para mais informações sobre isso, veja o guia de ferramentas para Avast! e Spybot em *Security in-a-Box*. [23],[24]

Verificando sua *firewall*

É uma boa ideia ganhar familiaridade com as configurações da *firewall* do seu computador – e instalar uma caso ela já não esteja instalada. A *firewall* ajuda a determinar quais programas e serviços podem estabelecer conexões entre o seu dispositivo e a internet.

Se você abrir suas configurações de *firewall*, você deverá ser capaz de encontrar uma lista de quais programas e aplicações podem enviar e receber informações para e da internet. Você poderá ver muitas aplicações que você não reconhece: é uma boa ideia pesquisar seus nomes em uma ferramenta de busca para determinar se elas são nocivas ou não.

23 https://securityinabox.org/en/guide/avast/windows
24 https://securityinabox.org/en/guide/spybot/windows

Verificando o gerenciados de tarefas

Em computadores com Windows, você pode abrir o gerenciador de tarefas pressionado CTRL + ALT + DEL; Isso fará abrir uma lista de todos os programas e serviços que estão rodando em seu computador. Se você ver qualquer coisa suspeita, você pode procurar na *web* para descobrir mais sobre ela. Você pode pará-la selecionando-a e clicando e "finalizar tarefa".

Autenticação em duas etapas para contas *online*

Muitos serviços *online* como Gmail, Riseup mail, Twitter e Facebook permitem que usuárias configurem uma "autenticação em duas etapas", o que significa que fora a sua senha, você precisará entrar com um código enviado para o seu telefone celular para poder entrar na sua conta. Se usar esse método, você será avisada caso alguém tente acessar suas contas.

Entretanto, tenha em mentre que isso não evita que certos agentes, tais como oficiais de justiça e outros agentes do Estado, exijam seus dados dos provedores de internet e companhias telefônicas. Muitos desses provedores cederão esses dados caso sejam requisitados. No seu mada de atores, você poderá levar em conta a relação entre aqueles responsáveis por guardar dados sensíveis seus, tais como provedores de emails e internet, e o governo (caso eles sejam contrários ao seu trabalho).

Também pode ser bem difícil para você ter acesso às suas contas caso o seu telefone não consiga se conectar a uma rede ou se estiver viajando sem "*roaming*".

Marcando seus dispositivos e verificando-os contra adulteração

Se você está preocupada que alguém pode adulterar ou acessar seus dispositivos eletrônicos, como o seu computador ou telefone, é possível deixar marcas que sejam bastante difíceis de replicar em certas

partes como o seu cartão SIM do telefone e a capa protetora do disco rígido do seu computador. Por exemplo, você pode fazer isso escrevendo nas peças com uma caneta UV que só pode ser detectada com uma luz ultravioleta (UV), ou com um esmalte de unha específico, o que deixará na peça um padrão quase impossível de replicar. Verifique as marcas com regularidade, especialmente depois de alguma pessoa teve, ou talvez tenha tido, acesso aos seus dispositivos para garantir que nada foi adulterado.

Conversando com uma especialista de confiança atualizada em TI

Se você está trabalhando individualmente, é bom manter uma relação com uma especialista em Tecnologia da Informação (TI) de confiança que está por dentro das mais recentes questões e ferramentas de segurança e poder verificar os seus dispositivos e garantir que eles estão "saudáveis". Ela não precisa necessariamente ser uma *expert*, mas idealmente deve ser alguém bem informada e atualizada. Se você não tem acesso a uma especialista de TI, procure um hackerespaço, um *hub* de TI, *maker spaces*, *"Crypto Parties"* ou comunidades *online* para conseguir ajuda. Entretanto, tente reduzir a medida em que você tem que confiar cegamente nessas pessoas: ler materiais tais como *Security in-a-Box* e *Me and My Shadow* lhe dará um bom embasamento sobre o assunto e lhe ajudará a dar a direção da conversa.

Entenda melhor como seus dispositivos funcionam e as tecnologias de informação que você usa. Foque nos dispositivos que são centrais para o seu trabalho e segurança.

Em uma organização, ter uma especialista interna em TI é muito útil. Entretanto, é importante que ela seja alguém de confiança e que entenda os tipos de riscos e ameaças que você enfrenta. Se você tem uma pessoa assim à sua disposição, ela pode realizar regularmente as verificações dos dispositivos da organização e garantir que eles estejam "saudáveis", evitando falhas e respondendo quaisquer questões que você venha a ter.

Apêndice C

Analisando Ameaças Declaradas

Do livro do Front Line Defenders sobre Segurança para Defensores de Direitos Humanos:

1. Quais são exatamente os fatos em volta da ameaça declarada?

- Quem disse o quê, quando e como?
- Se foi por telefone, quais eram os barulhos de fundo?
- Qual foi a linguagem e o tom usados?
- Isso foi depois de alguma (nova?) atividade sua?

2. Existe um padrão de ameaças declaradas ao longo do tempo?

Padrões podem incluir o seguinte:

- Você recebe uma série de chamadas ou mensagens com ameaças
- Você foi seguida por dois dias e o seu filho foi seguido ontem
- Outra defensora de direitos humanos foi chamada para interrogatório pelas autoridades e depois ela foi presa. Agora você foi chamada para interrogatório.

Pode haver padrões envolvendo:

- O tipo de ameaças feitas
- Os meios pelos quais a ameaça foi feita (pessoalmente, por telefone, etc.)
- O momento das ameaças (dia da semana e hora)
- Os agentes das ameaças (caso sejam conhecidos)
- O lugar onde as ameaças foram feitas

- Os eventos que precederam a ameaça, tais como uma declaração da sua organização na imprensa.

3. Qual parece ser o objetivo da ameaça declarada?

- Está claro na ameaça o que o perpetrador quer de você? Caso não esteja claro, às vezes o objetivo pode ser deduzido do momento em que a ameaça foi feita. Quais ações você está planejando ou realizou recentemente?

4. Você sabe quem está fazendo a ameaça declarada?

- Frequentemente, você não conhece. Não tire conclusões precipitadas.
- Seja o mais específica possível. Se, por exemplo, é um policial, qual a sua delegacia? Qual o seu posto?
- Considere se uma ameaça assinada vem realmente da pessoa/organização cujo nome está na assinatura.
- Se você sabe quem está fazendo a ameaça, considere se o perpetrador possui ou não os recursos para levá-la a cabo.
- Caso possua, isso aumenta a probabilidade de que o perpetrador realmente ataque após ter ameaçado.

5. Por fim, após analisar as questões acima, você acha que a ameaça declarada irá se realizar?

- Essa é uma avaliação difícil e não tem como ter 100% de certeza.
- Sua resposta levará em conta o seu contexto, incluindo a história de ataques a defensores de direitos humanos no seu país, as capacidades do perpetrador, e o grau de impunidade para com eles.
- Quando estiver em dúvida, escolha a opção que lhe pareça a mais segura.

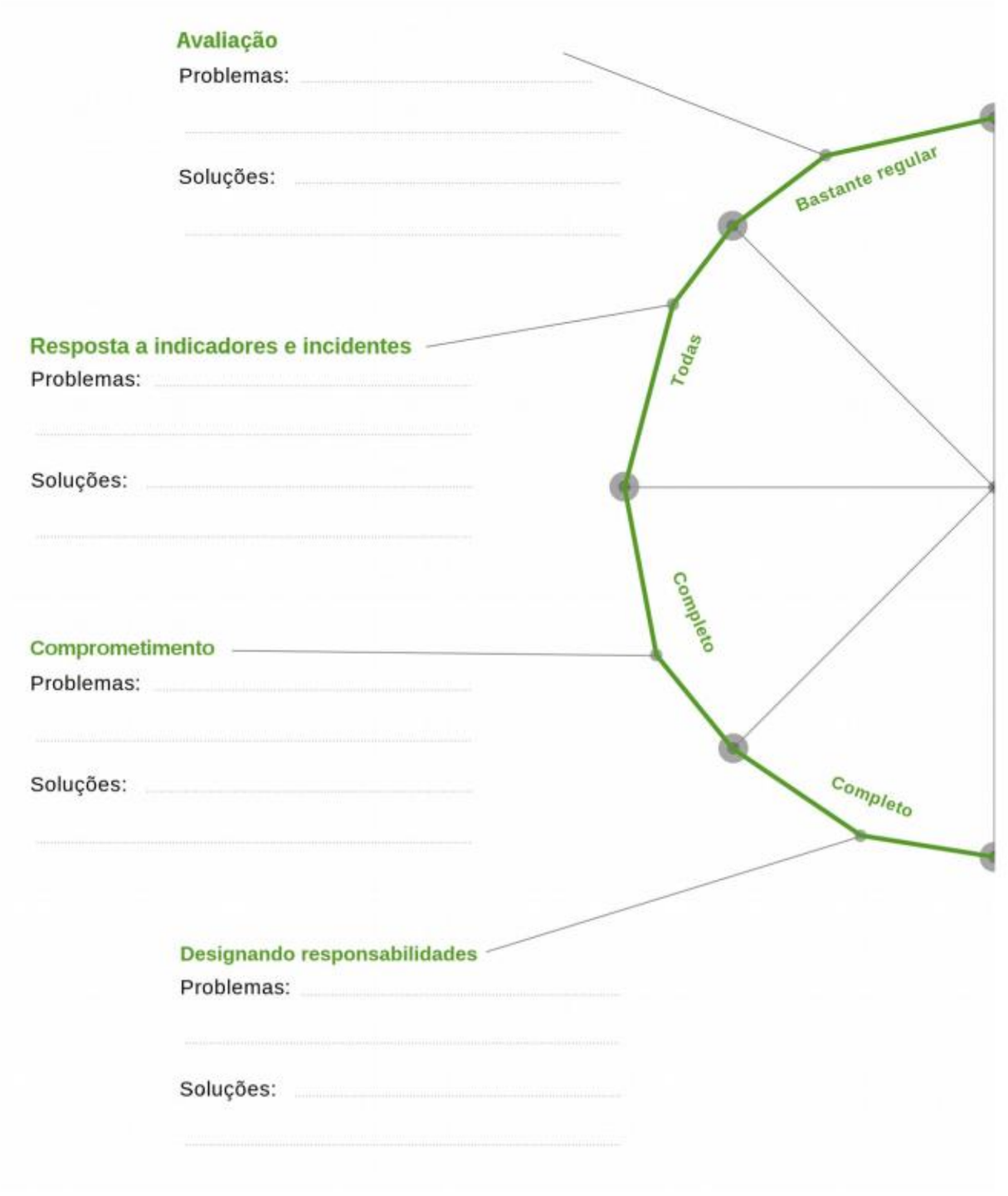
Identifique Novas Capacidades

Ameaças identificadas Considere a quem, por quem, como e onde.	**Capacidades e práticas existentes**	**Vulnerabilidades e brechas nas práticas existentes**

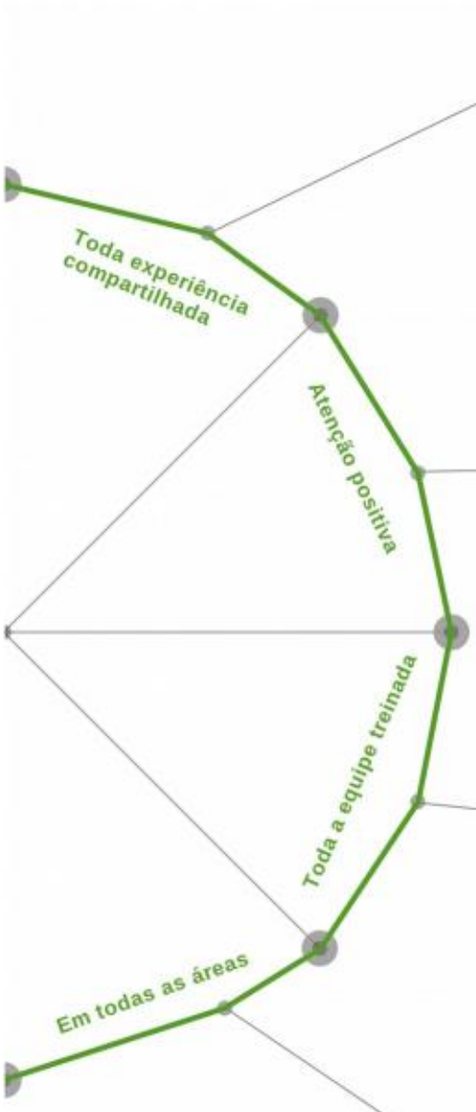
Novas capacidades necessárias	Estratégia		
	Aceitação	Dissuasão	Proteção

Apêndice E

Roda de Segurança[25] para Avaliar o Gerenciamento de Segurança da Organização



25 Baseado no Capítulo 2.1 "Avaliando a performance organizacional de segurança: a roda de segurança" do *Novo Manual de Proteção para Defensores de Direitos Humanos* (2009), Protection International.



Experiência adquirida em segurança

Problemas: .....

.....

Soluções: .....

.....

Atitudes e atenção

Problemas: .....

.....

Soluções: .....

.....

Habilidades, conhecimentos e treinamento

Problemas: .....

.....

Soluções: .....

.....

Planejamento de segurança

Problemas: .....

.....

Soluções: .....

.....

Apêndice F

Não Cause Dano: Verificando nossas Ações e Transferências de Recursos

Ações/recursos	Impactos
	Competição vs inclusividade Perguntas a serem feitas: • Quem está em vantagem / desvantagem? • Pode haver competição por esse recurso? • Como podemos pensar nossas atividades para sermos mais inclusivas?
Exemplo Treinamento externo em segurança para membros da equipe	• aquelas que não participam se sentem deixadas para trás • competição por quem pode viajar • Treinamento = construção de capacidade = melhores oportunidades de trabalhos mais bem pagos competição entre departamentos/ grupos/membros por dinheiro para treinamento • concorrência entre outras atividades e treinamento •

Impactos

Efeitos da substituição vs apreciação e pertencimento Perguntas a serem feitas: • Quais práticas existentes devem ser reconhecidas e preservadas/integradas? Ou, por que elas devem ser modificadas, abolidas, etc.? • As novas medidas afetam positivamente ou negativamente as responsabilidades de quem?	**Seletividade e relações de poder** Perguntas a serem feitas: • O recurso está ligado a poder? • O recurso adicionará poder a alguém? • Como isso pode ser equilibrado ou usado construtivamente?
• membros da equipe que eram responsáveis pelo treinamento em segurança de outras pessoas foram diminuídas como "participante" normal • tempo, que anteriormente era usado para outros treinamentos ou excursões, agora é usado para treinamentos de segurança.	• pessoas treinadas, se sentirão ou serão vistas como mais importante • mais conhecimento = mais poder na hierarquia

Apêndice G

Não Cause Dano: Verificando nosso Comportamento e As Mensagens Éticas Implícitas

	Mensagens e
Comportamento/Ação	**Você mesma**
Mudar toda a comunicação por email por emails criptografados	**Mensagem:** • Tenho algo importante a esconder • Me preocupo comigo mesma e com minha comunidade **Impacto:** • Comunicação mais segura • Peso da responsabilidade • Aumento de paranoia ou de medos infundados
Decidir você mesma que não irá trabalhar nos finais de semana	**Mensagem:** • Me preocupo comigo mesma • A família é importante **Impacto:** • Está cuidando da família • Energias recarregadas • Evitou estafa

possíveis impactos em/por

Colegas/Grupo	Oponentes/Adversários
Mensagem: • Se não criptografarmos, não temos nada importante • Se eu não (conseguir) criptografar, não me importo comigo mesma ou com minha comunidade **Impacto:** • Sentimento de vergonha • Resistência a todas as medidas de segurança devido à frustração com criptografia ou gasto de tempo...	**Mensagem:** • Estão criptografando, logo têm algo a esconder • Passaram a criptografar de um dado momento em diante: algo importante irá acontecer em breve • Com quem estão trocando emails criptografados? Esses são os contatos mais importantes **Impacto:** • Perigo de forte vigilância digital ou física para você e sua comunidade
Mensagem: • Tal pessoa se considera mais importante que seu trabalho • Tal pessoa não é mais capaz de trabalhar sob pressão • Considera o ativismo meramente um trabalho **Impacto:** • Perda de confiança • Respeito por autocuidado • Ciúme • Quebra do espírito de equipe	**Impacto:** • Menos atividades nos finais de semana • A família é importante, logo a família pode ser um bom ponto de pressão

Comportamento/Ação	Mensagens e Você mesma
Regra da organização: os monitores de direitos humanos sempre vão em pares para manifestações políticas	**Mensagem:** • Nosso trabalho está em risco (ou se tornou mais arriscado) • Somos importantes para nossa organização **Impacto:** • Questão: Será que é muito arriscado para mim? • Questão: Será que é muito arriscado para mim? • Questão: A organização está paranoica? • Sentimento de reconhecimento

possíveis impactos em/por	
Colegas/Grupo	**Oponentes/Adversários**
O mesmo que individual	**Impacto:** • O aumento da presença de monitores significa que virão mais reclamações • É necessário mais esforço para lidar com monitores

Esse manual foi desenvolvido pelo Coletivo Tactical Technology, uma fundação holandesa registrada. Para questões relacionadas ao manual, ou com respeito à tradução, distribuição ou reuso desse conteúdo, por favor entre em contato conosco em ttc@tacticaltech.org.