DOCUMENTO PÚBLICO DE CIRCULAÇÃO
IRRESTRITA E INCENTIVADA

CARTILHA BÁSICA DE SEGURANÇA MILITANTE

BRIGADAS POPULARES

SOBRE ESTA CARTILHA

O documento a seguir foi produzido pelas **Brigadas Populares** para incentivar e auxiliar na difusão de políticas mínimas de segurança entre a militância de esquerda, divulgando conteúdos básicos para ajudar na proteção das e dos que lutam em defesa do povo e do Brasil. **Os conteúdos cobertos, de forma inicial, são cultura de segurança, análise de ameaças, controle das informações e compartimentalização, segurança digital, física, em manifestações e ameaças e acolhimento.**

Existem diversos materiais semelhantes produzidos por uma grande quantidade de organizações e coletivos. Esta cartilha é mais um destes, chegando para somar e de maneira alguma se colocando como superior ou sequer suficiente para formação capaz de dar conta de todos os desafios da militância. Não confie cegamente em nenhum material – nem neste. Busque o maior número possível de referências e o que for mais adequado para sua realidade, sabendo que **não existe e nem há possibilidade de existir um material que garanta completamente a segurança** – o 100% de segurança é uma utopia, meta inatingível que devemos sempre buscar, tentando diminuir riscos e mitigar possíveis ameaças.

Este material está sob constante revisão e atualização. Comentários, críticas e sugestões, mais do que bem-vindos, são incentivados. Você pode entrar em contato por nacional@brigadaspopulares.org.br ou, se preferir, através do e-mail eomund@riseup.net (Impressão digital PGP: 41D5 60F8 EE8D A4C8 85BD 701E F828 B098 6A13 732C).

Data desta versão: outubro de 2018.

CONSIDERAÇÕES DA CONJUNTURA

A maioria das formações e políticas de segurança da esquerda estão centradas na defesa contra ataques da repressão estatal. No entanto, na atual conjuntura (Out/2018), é importante ressaltar que boa parte das ameaças parte de grupos organizados fora do Estado (ainda que alguns contem com agentes do Estado) ou mesmo de grupos e indivíduos não-organizados – mas cheios de ódio e procurando uma oportunidade para atacarem militantes. É importante considerar esse fator, esses atores e que eles podem vir a fazer parte do Estado ou serem auxiliados por ele.

CULTURA DE SEGURANÇA

Segurança é uma tarefa constante e fundamental para as organizações, coletivos e pessoas. Não há nenhum método, cultura ou norma que garanta 100% de segurança: sempre haverá riscos e ameaças para quem está atuando. O importante é reconhecer este fato e trabalhar em cima dele. **As medidas, normas, rotinas e procedimentos adotados devem ser para detectar, prevenir, reagir ou se recuperar de ataques, elevando os custos para eventuais adversários e diminuindo seus potenciais ganhos, de modo que a atuação se dê do modo mais seguro possível.**

Os riscos são reais e segurança completa não existe, mas **é possível atuar com riscos diminuídos, seguindo boas práticas de segurança, evitando o improviso, gerindo bem as informações e responsabilizando todas e todos pela segurança coletiva**: a corrente é tão forte quanto seu elo mais fraco. Pouco adianta que quase todo mundo use um meio seguro e criptografado para se comunicar se alguém do grupo deixa as informações vazarem.

A **segurança deve ser parte integrante da militância**. É preciso sempre pensar na segurança para planejar e executar ações, por mais corriqueiras que sejam. É preciso também buscar um equilíbrio: não deixar de fazer atividades por medo mas também não realizá-las sem garantir o básico – ou seja, não cair nem na paranoia paralisante nem num grande relaxamento.

ANÁLISE DE AMEAÇAS

Como cada atuação e conjuntura é diferente, cada procedimento de segurança deve ser pensado especificamente para aquela realidade. Uma ferramenta fundamental para isso é a análise de ameaças. Similar a uma análise de conjuntura, a ideia é levantar quais são os **ativos e atividades** que você/seu coletivo/organização possui/possuem, quem são os **potenciais adversários (bem como a relação com eles e o poder de cada um)** e, partindo disto, levantar **quais são os ataques que podem acontecer.** Tendo em mãos o que pode ser atacado, por quem e de que forma, fica mais fácil se **planejar para as ameaças, mitigando-as ou evitando-as** completamente. Quanto mais extensa e completa, melhor a análise. Os **resultados da análise são informação sensível e não devem ser compartilhados** ou vazados, pois poderiam facilitar muito a vida de um adversário buscando fraquezas.

CONTROLE DAS INFORMAÇÕES

Na era das redes sociais, é comum que as pessoas compartilhem *online* muitos detalhes de suas vidas. Mas com quem essas informações estão sendo compartilhadas? Quem tem controle sobre elas e como serão utilizadas? **É importante controlar suas informações e seu compartilhamento, tanto no ambiente virtual quanto no real**. É preciso tomar o controle das informações, compartilhando publicamente apenas aquilo que se quer seja público, **evitando exposição desnecessária e riscos para você e as pessoas com quem você milita**.

O que é postado nas redes sociais passa a ser compartilhado, no mínimo, com as **empresas donas destes serviços** – o *Facebook*, por exemplo, diz que tudo postado nele é de sua propriedade. Além disso, são compartilhadas publicamente, se suas **configurações de privacidade** não forem restritas. Mesmo que exista restrição, basta um contato antigo que discorda de sua militância ou um *fake* (criados aos milhares todos os dias) para colocar você em risco.

Com base em informações como *likes*, fotos, comentários, avaliações e *check-ins*, é possível traçar um perfil da pessoa, desde seus hábitos de consumo até sua rotina, trabalho, militância, amizades. O quão detalhado é este perfil, claro, depende do quanto é compartilhado, mas **métodos disponíveis de análise de informação permitem traçar com bastante precisão mesmo com, aparentemente, pouco detalhe**; só com os likes mais comuns ou e-mails trocados é possível traçar quais são os círculos de amizade e a relação entre as pessoas. Esses perfis podem ser usados desde para meios de propaganda (inclusive eleitoral) até monitoramento e perseguição (inclusive jurídica, havendo precedentes no Brasil).

COMPARTIMENTALIZAÇÃO

Compartimentalizar a informação quer dizer que cada um só deve saber do que é necessário para o cumprimento de suas tarefas. É importante **evitar a centralização de informações** em pessoas ou ferramentas, diminuindo perdas no caso de um ataque a uma pessoa/meio. Deve-se evitar perguntar sobre aquilo que não se precisa saber, bem como respeitar os protocolos de segurança de outras pessoas: não compartilhar informações dela sem autorização e **aceitar que "não" é uma resposta aceitável para perguntas sensíveis** na militância. **Não pergunte e não diga** o que não for preciso. Para que isto funcione, é fundamental confiança, camaradagem e transparência no que for possível: o sigilo é importante, mas não pode ser utilizado para compartilhar ou reter informações por interesses individuais.

SEGURANÇA DIGITAL

No meio digital, é importante utilizar programas de confiança. O que isso quer dizer? **Programas livres, de código aberto, auditados** por atores independentes. Isto significa fugir de sistemas operacionais como Microsoft Windows e os da Apple, partindo para **alternativas como sistemas Linux**. **Ubuntu** é a distribuição mais conhecida, mas você pode buscar a que mais se encaixa com suas necessidades. Outra boa opção é o Linux **Tails**, que pode rodar a partir de um pendrive, sem instalação, e é focado na privacidade.

Mantenha seus programas atualizados; **criptografe** seu HD e pendrives (uma opção simples é o VeraCrypt); migre para provedores de e-mail que não te vigiam e são seguros (como o **Riseup**) e tenha e-mails criptografados (**PGP**); utilize como navegador o **Mozilla Firefox** ou, preferencialmente, o **Tor Browser**; instale extensões de segurança no navegador, como **HTTPS-Everywhere, Privacy Badger, uBlock Origin e NoScript**; utilize o **DuckDuckGo** para buscas na internet; busque um **VPN** de confiança; restrinja privacidade das redes sociais e utilize-as só para divulgação, não para organização.

CELULAR

Seu celular te vigia, passa dados para empresas (e provavelmente para o Estado) e **é extremamente vulnerável**, inclusive à clonagem. Evite ao máximo organizar e conversar sobre militância no celular, **deixe-o longe de ambientes de reunião** e, se possível, deixe-o em casa quando for para alguma atividade de militância. Utilize **senhas fortes e criptografia**. Prefira o **Signal** para conversas ou, se não puder, o WhatsApp. Evite o Telegram.

DICAS BÁSICAS DE SENHAS

Não reutilize as mesmas senhas em diferentes serviços e as **troque regularmente**. Utilize **verificação/autenticação em dois fatores** em todos os serviços que permitirem. As mais simples são com SMS, mas existem outros métodos mais confiáveis. **Senhas têm de ser fortes**; muitas vezes, são criadas misturas de letras, números e símbolos (como $eNh4!, mas mais longas), mas outro método são as **frases-senhas**: conjunto longo de palavras, sem sentido, garantindo senhas fortes e mais fáceis de lembrar (como GalinhaCidadeNiobioArrozTremSalto). Utilize um cofre (real ou virtual, criptografado, como o **KeepassX**) para criar e armazenar senhas.

SEGURANÇA FÍSICA

Quando a preocupação é a segurança da militância, a **segurança física contra ataques deve ser sempre a prioridade**, pois é onde estão os mais graves riscos, como ferimentos, prisão e morte. Assim como para um ato, o ideal é que se planeje todo o cotidiano, **evitando ao máximo andar sozinha/o**, traçando **rotas pelos locais mais seguros e iluminados**, **variando a rotina** (inclusive datas/locais de reuniões), não trajando roupas ou adereços que indiquem militância (camisa, broche, boné de uma organização, por exemplo) em locais não seguros. **Não se exponha a riscos desnecessários, não seja previsível e seja cuidadosa/so – não facilite o trabalho de potenciais adversários**. **Comunique-se constantemente** com suas/seus parceiras/os e faça alertas ou peça ajuda em caso de problema. É melhor gerar alarmes falsos do que deixar uma ameaça real passar. No dia a dia, **verifique constantemente se há sinais de monitoramento** ou perseguição (como cruzar muitas vezes em locais aleatórios com a mesma pessoa ou o mesmo carro), inclusive em sedes e casas.

Buscar **formação em defesa pessoal** é também importante para evitar ataques físicos, mas **sem sobrestimar as capacidade individuais** de defesa e cuidando para não se expor mais por uma falsa sensação de segurança. Mesmo sem treino específico, o condicionamento físico em si também é importante para a militância. Um texto curto sobre o assunto é **Um Estudo de Educação Física**, de Mao Tsetung (https://tinyurl.com/MAOedfisica).

AMEAÇAS E ACOLHIMENTO

Por vezes, a/o militante pode estar **ameaçada/o individualmente**. Nestes casos, os **dois procedimentos** mais comuns são **dar visibilidade**, aumentando o custo de um eventual ataque ou **retirar a/o militante** do local em que atua, deslocando temporariamente a pessoa para um local mais seguro (muitas vezes contando com redes de acolhimento e parcerias solidárias). É importante discutir qual é a melhor abordagem em cada caso e cada vida, buscando sempre a alternativa mais segura.

Tanto num caso de ameaça individual quanto no caso de alguém, sem ameça direta, se sentir **acuado, com medo** – um sentimento totalmente legítimo – é importante **acolher a pessoa, mostrando-a que não está sozinha e que faz parte de uma coletividade**, dando apoio moral e afetivo. É importante não relevar a questão e, caso necessário, buscar **atendimento especializado** para saúde mental e/ou física.

SEGURANÇA EM ATOS

É importante **planejar previamente** as manifestações e o que ocorrerá nelas, já montando planos de segurança e designando pessoas para que cumpram tarefas específicas, como cuidar de eventuais feridos ou fazer a comunicação/cobertura do ato. É fundamental também **comunicar pessoas** que não vão de que você estará presente (se possível, um/a advogada/o) e **não ficar sozinha/o**, em especial na chegada e na saída. **Busque uma dupla/trio** para ficar com você durante toda a manifestação.

O QUE LEVAR

VESTIMENTAS Proteja o máximo do corpo, deixando o mínimo possível exposto, usando calça, manga comprida, tênis ou bota, capuz, boné, coberturas para o rosto. **Utilize** roupas pouco chamativas, que não sejam facilmente identificáveis de longe e que facilitem a corrida, sem adereços. **Evite** adornos ou coisas que fiquem presas/enganchadas, roupas de algodão (absorvem mais gás/pimenta) e lentes de contato (potencializam efeito de gás/pimenta). Leve outras mudas de roupa, para troca para caso de gás/pimenta e para dificultar identificação posterior.

OBJETOS Leve **documentos**, celular (preferencialmente não *smartphones* e limpe-o previamente, apagando mensagens e fotos), número de advogada/o, **água**, lanche energético (barra, etc), remédios (se utilizar algum). Não leve vinagre: **Leite de magnésia** é um antídoto muito mais eficiente. **Nunca porte nada ilegal nem com potencial ofensivo**, mesmo que seja um objeto cotidiano (como tesouras).

PRIMEIROS SOCORROS

Caso afetado por gás/pimenta, **não espalhe, não coce e não pressione** para não espalhar mais os químicos, utilizando **água corrente (nunca de garrafas) ou leite de magnésia para aliviar os sintomas** e trocando de roupa o quanto antes. Retire da manifestação, assim que possível, quem for ferida/o ou estiver bastante afetada/o, tomando cuidado para não se isolar. Feridas/os graves deverão ser encaminhados para socorro médico; se a situação permitir, saia da manifestação e consiga socorro sem ter de contar que estava participando da manifestação. Em caso de urgência, ignore e consiga o socorro o quanto antes, mesmo que isto signifique risco de prisão.

REFERÊNCIAS E SUGESTÕES DE LEITURA

EM PORTUGUÊS:

★ **Segurança da Comunicação – Riseup:**
https://riseup.net/pt/security

★ **Surveillance Self-Defense (SSSD) – Autodefesa contra vigilância:**
https://ssd.eff.org/pt-br

★ **Oficina Antivigilância:**
https://antivigilancia.org/pt/inicial-pt/

★ **Security in a Box – Ferramentas de Segurança Digital para todas/os:**
https://securityinabox.org/pt/

★ **Saúde da Internet – Mozilla:**
https://www.mozilla.org/pt-BR/internet-health/

★ **Coletivo AnarcoTecnológico Mariscotron:**
https://www.mariscotron.libertar.org/

EM INGLÊS:

TRADUÇÃO LIVRE DOS NOMES

Fundo para Aprimoramento da Tecnologia Código-Aberto: ★
https://ostif.org/

Coletivo tático de tecnologia: ★
https://tacticaltech.org/

Projeto Tor: ★
https://www.torproject.org/

Liga de defesa da internet: ★
https://www.internetdefenseleague.org/

Defensores na linha de frente: ★
https://www.frontlinedefenders.org/en/digital-security-resources

Ferramentas de privacidade: ★
https://www.privacytools.io/

★ ★ ★
BRIGADAS POPULARES

UNIDADE ABERTA POR UMA NOVA MAIORIA

Uma organização militante, popular e de massas. Na luta por uma nação livre, socialista, feminista, nacionalista e revolucionária! Venha construir conosco e fortalecer a nova maioria!

HTTPS://BRIGADASPOPULARES.ORG.BR/
/BRIGADAS.POPULARES
@BRIGADASPOPULARES