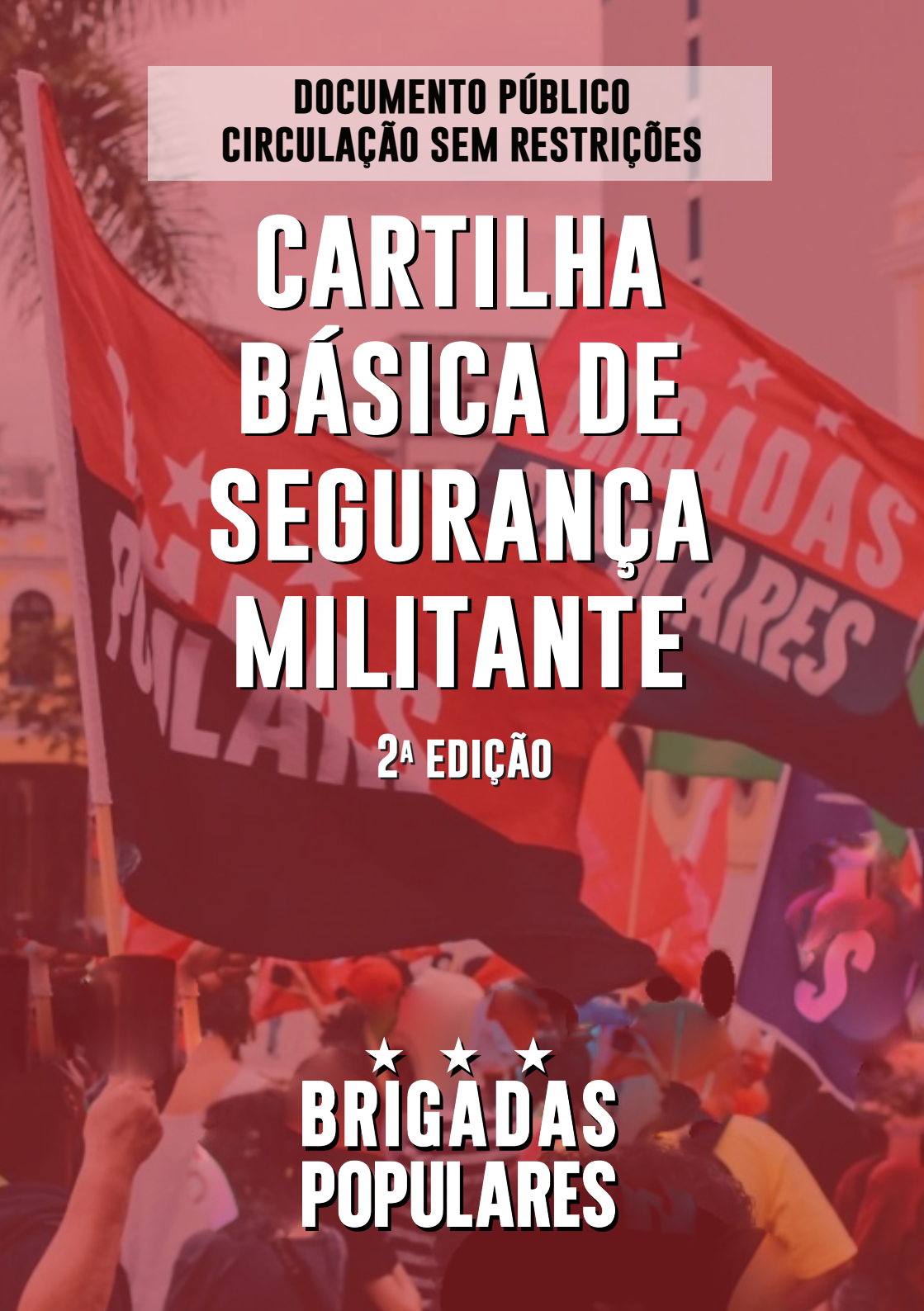
DOCUMENTO PÚBLICO
CIRCULAÇÃO SEM RESTRIÇÕES

CARTILHA BÁSICA DE SEGURANÇA MILITANTE

2ª EDIÇÃO



BRIGADAS POPULARES

SOBRE A CARTILHA E A CONJUNTURA

A primeira versão desta cartilha foi produzida em 2018. Embora lá – e desde sempre – o Brasil já fosse um **país violento e perigoso, em especial para negres, mulheres, pobres, LBGTQIA+s, indígenas, imigrantes, defensores de direitos humanos e militantes de esquerda**, dezenas de riscos se intensificaram e outros surgiram – ou ressurgiram – com afrouxamento dos controles sobre os órgãos de segurança, avanço do Partido Fardado e militarização da sociedade, tentativas de reabilitação do nazifascismo e organização de grupos da extrema-direita, empoderamento de agentes estatais e paraestatais da violência – como jagunços, capangas e milicianos – e proeminência dada aos discursos de ódio da direita.

Reflexos disto foram sentidos na segurança militante, no campo e nas cidades, com registos recordes de ameaças e ataques a defensores de direitos humanos, tanto com assassinatos de alto perfil – Marielle e Anderson, Bruno e Dom – quanto inúmeros de menor repercussão. Atentados terroristas da extrema-direita não tornaram-se apenas plausíveis como já foram registrados, em sua maioria por "lobos solitários" radicalizados, como no que vitimou Marcelo Arruda.

Nos últimos anos, houve um **aumento na preocupação com segurança dentro da esquerda**. Testemunhamos isso, nas Brigadas Populares, ao receber chamados para auxiliar em formações, análises e planejamentos de segurança em todo o país. Observamos que, apesar de mais militantes, organizações e entidades preocupando-se com a proteção, **o aumento nas medidas de segurança foi insuficiente para fazer frente aos riscos existentes em 2018 e muito abaixo do necessário para 2022.**

Elaboramos esta **segunda edição da Cartilha Básica de Proteção Militante** como uma contribuição para o debate e formação, e seguimos dispostos a auxiliar todas, todos e todes que lutam em defesa do povo e do Brasil o fazerem com maior segurança. Não achamos que temos todas as respostas corretas e soluções – o desafio é muito maior do que qualquer organização sozinha conseguiria enfrentar – e sugerimos que **não se confie cegamente nem nesta cartilha nem em nenhum material. É preciso buscar outros conteúdos, comparar, estudar e, acima de tudo, praticar, testar e implementar.**

Planos de segurança são específicos para cada situação, militante, organização e entidade. Não há respostas prontas ou um protocolo operacional padrão que dê conta de tudo. Para atuarmos em segurança, protegendo as/es/os nossas/es/os, é preciso trabalho sério e constante, responsabilizando-se individual e coletivamente, organizando as capacidades de autodefesa.

Os conteúdos cobertos neste material, de forma inicial, são **cultura de segurança, análise de ameaças, controle das informações e compartimentalização, segurança digital, física, em manifestações, em eventos e ameaças e acolhimento**. 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: **setembro de 2022**.

POR QUEM TOMBOU, NENHUM MINUTO DE SILÊNCIO
MAS TODA UMA VIDA DE LUTA

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. A atuação da esquerda, por si, contraria interesses daqueles no poder e no controle de aparatos de violência e o somente existir de algumas pessoas – como negras, mulheres, LBGTQIA+, indígenas – já as coloca em um grau de risco elevado por conta de racistas, machistas, LBGTQIA+fóbicos. **É importante é reconhecer este fato e trabalhar em cima dele.**

Sabendo que não estaremos num estado de total segurança, 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.

É possível atuar com riscos diminuídos, seguindo boas práticas de segurança, evitando o improviso, gerindo bem as informações e responsabilizando todas, todes e todos pela segurança coletiva: a corrente é tão forte quanto seu elo mais fraco. Pouco adianta que um grupo utilize um meio seguro e privado para se comunicar se alguém do grupo deixa as informações vazarem. Vulnerabilidades aumentam as chances de que um ataque seja conduzido; portanto, atuar para sanar ou diminuir estas brechas reduz as chances de que uma ameaça se concretize.

A segurança deve ser parte integrante da militância, tanto individual quanto coletivamente. Assim como para cada ação costuma se pensar nas implicações políticas, nas necessidades de estrutura e em ações de comunicação, 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. **Segurança não deve ser pensada como algo alheio, externo, restrito ao "grupo de paranoicos" ou planejada apenas nas ações mais perigosas: deve ser algo orgânico, parte da natureza da própria militância.**

ANÁLISE DE AMEAÇAS

As organizações e entidades são diferentes e atuam de maneira diferente, isto é óbvio. Assim, deve ser igualmente óbvio que **as ameaças são diferentes e, portanto, também as medidas de segurança necessárias.** Isto **também é verdade mesmo dentro de uma mesma organização ou grupo: as pessoas são diferentes, com diferentes condições materiais, e estão expostas à diferentes riscos.**

Uma liderança popular no campo enfrenta ameaças e tem condições de proteção distintas das de um sindicalista no meio urbano, bem como de uma mulher negra liderança comunitária em uma periferia ou de um jovem estudante universitário. Não se trata de fazer um ranking de ameaças (ou de opressões), mas **compreender as diferentes realidades e adaptar os planos de segurança conforme necessário**. Trata-se de uma **tarefa coletiva, responsabilizando-se o grupo para garantir que mesmo as pessoas com maior risco tenham condições de militar** – ninguém fica para trás, ninguém solta a mão de ninguém têm de ser mais do que apenas palavras de ordem.

Mas como avaliar cada situação, entender os riscos das diferentes atuações e conjunturas? É aí que entram as **análises de ameaças, ou de riscos – ou modelagens de ameaças/riscos**. Independentemente da terminologia, são uma ferramenta básica e fundamental para qualquer atuação segura. De modo simples, são análises de conjuntura voltadas para o próprio grupo e/ou pessoa e sua atuação, focando-se na segurança.

Assim como nas análises de conjuntura, há muitas metodologias, mais ou menos complexas. Descrevemos abaixo um método comum, de média complexidade e que leva um tempo razoável, mas de maneira alguma quer dizer que é o único ou o melhor. O importante é conseguir levantar dados como **quais são as forças, quais são aliadas e quais são adversárias, de que maneira elas podem atuar, quais os possíveis alvos de ataques e quais as vulnerabilidades.**

Neste exemplo de metodologia para análise de ameaças, elabora-se uma **lista com todas as frentes e tipos de atuação e trabalho**, bem como de tudo que se possui – os "**ativos**" como as redes sociais do grupo, os próprios militantes, sedes, computadores e celulares. Em seguida, é feita uma **segunda lista com os atores** com quem há relação e, se o tempo permitir, fazer a qualificação dos atores – qual a força de cada um, como é a relação deles com o grupo.

Tendo-se estas **duas listas, podemos cruzá-las, avaliando o que cada ator levantado pode fazer contra cada uma das atuações e ativos**. Por exemplo, se um ativo é uma sede e um dos atores foi um grupo de extrema-direita, entre os ataques que poderíamos levantar estão a invasão da sede, depredação e a emboscada de militantes chegando ou saindo de uma atividade; uma força de repressão poderia realizar ações como vigiar e monitorar a sede, reprimir ou prender militantes chegando ou saindo, invadir o espaço. As ações de atores diversos podem se repetir; se o tempo é curto, pode-se pular as repetições e, se há mais tempo, é possível analisar diferenças – afinal, um grupo de direita e uma força de repressão invadindo uma sede de esquerda teriam, provavelmente, causas e consequências diferentes.

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 extremamente sensível e devem ser protegidos adequadamente, pois seu vazamento facilitaria muito a vida de um adversário buscando fraquezas.

PRATICIDADE VERSUS SEGURANÇA

Uma organização que avalie que há monitoramento e ataques diretos de agências de inteligências dos EUA vai repensar toda comunicação digital, buscar soluções com criptografia sofisticada, preferir a troca presencial de informações e o uso de pessoas como mensageiros. Já outra, local, que atua numa universidade e tem como maior adversário uma reitoria de direita pode seguir na comunicação digital com alguns cuidados, sem precisar de mensageiros ou soluções sofisticadas – que, além de desnecessárias, impediriam seu funcionamento normal e **elevariam a curva de aprendizado para que militantes se adaptem à cultura de segurança**.

Outros exemplos simples incluem implantar soluções tecnológicas que podem

estar fora da realidade de maior parte da militância – **exigir troca de informações via e-mails com PGP em computadores com sistemas operacionais específicos inviabiliza a participação de quem acessa a internet exclusivamente via celulares, por exemplo**. HDs não criptografados (só com a senha do Windows, por exemplo), podem ser acessados por qualquer pessoa que tenha acesso físico a eles; criptografar os HDs dificulta que as informações sejam acessadas e é fácil de implementar; criptografar o HD e trancá-lo em uma masmorra dentro de um complexo de segurança com guarda 24 horas por dia dificulta o acesso físico de um adversário, mas, ao mesmo tempo, impede que o HD seja utilizado no cotidiano.

É **preciso medir o grau das ameaças e das vulnerabilidades e pesá-las contra as medidas de segurança possíveis, implantando-se aquelas que fazem sentido pro nível de risco existente**, que tem condições de arcar e que não vão impedir o funcionamento da organização, buscando um equilíbrio entre segurança e praticidade – uma análise que varia entre organizações e contextos.

CONTROLE DE INFORMAÇÕES

Com as redes sociais, é comum que cada vez mais as **pessoas compartilhem muitos detalhes de suas vidas**. Mas com quem essas informações estão sendo compartilhadas? Quem decide como serão utilizadas? **É importante administrar seus dados e seu compartilhamento, tanto no ambiente virtual quanto no real, e tomar o controle deles**, compartilhando publicamente apenas aquilo que se quer seja público, e**vitando 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. Além disso, se o seu perfil é público, qualquer pessoa pode coletar as informações – num processo com nomes como "**Rondas Virtuais**" e implementado por algumas polícias no Brasil, ou **OSINT** (*Open Source Intelligence*). Mesmo que exista restrição de privacidade, basta um contato antigo que discorda de sua militância ou um *fake* (perfil falso) que te adicionou e você deixou passar para lhe colocar em risco.

Com base em dados como curtidas, fotos, comentários, avaliações e *check-ins* é possível **traçar perfis precisos de pessoas, desde seus hábitos de consumo até sua rotina, trabalho, militância, amizades.** O quão detalhado é este perfil depende do quanto é compartilhado, claro, mas os métodos das gigantes de tecnologias são sofisticados e capazes de análises grandes com poucas informações – além de coletarem dados mesmo quando não percebemos ou queremos.

Para se proteger das coletas feitas por pessoas, **restrinja as configurações de privacidade das redes**, prefira **não usar seu nome** (ou, pelo menos, não seu nome completo), pesquise o que há sobre você no Google, Bing e DuckDuckGo, confira regularmente seus dados no **Registrato** (do Banco Central), **retire as informações** onde for possível e **feche contas, sites e afins que não tenham mais uso**. Para se proteger das coletas das empresas, **restrinja as permissões das redes e aplicativos**, busque criar **contas separadas** para fins diferentes (como pessoal, político, financeiro, estudo, compras) e **evite entregar seus dados** quando possível, mesmo que se perca um pouco de conveniência.

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 ou meio. Deve-se evitar perguntar sobre aquilo que não se precisa saber, bem como respeitar os protocolos de segurança de outras pessoas: n**ão compartilhar informações dela sem autorização e aceitar que "não" é uma resposta razoável** 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 E PRIVACIDADE

Conceitos **próximos mas distintos**. Para não entrar em discussões densas, exemplificamos: dados podem estar seguros em servidores de uma gigante de tecnologia (contando que ela usa parte de seus bilhões para protegê-los), mas não são privados se esta mesma gigante tiver acesso às informações. Por outro lado, os dados podem estar privados num servidor criado por voluntários de coletivos, organizações ou até pequenas empresas mas, com menos condições de infraestrutura do que as gigantes de tecnologia, sua segurança pode ser menos sofisticada. **O ideal é buscar sempre, claro, ter tanto segurança quanto privacidade.**

SEGURANÇA DIGITAL

No meio digital, é importante buscar utilizar programas, sistemas e plataformas de c**ódigo aberto; auditados por atores independentes e; livres**. Indo por partes, "**código aberto**" significa que a programação fica disponível para qualquer pessoa analisar e conferir que o programa faz apenas aquilo que se espera dele – não rouba dados escondido, por exemplo.

Como, claro, nem todo mundo tem condições de checar todos os programas que vai usar, linha de código por linha de código, é aí que entra o "**auditados por atores independentes**": pessoas em trabalham com esta checagem analisaram o programa, testaram em diversas situações e afirmam que se pode confiar nele. Evidentemente, é preciso que se possa confiar nas pessoas que estão fazendo esta checagem e, por isso, é importante conferir as credenciais de quem faz as auditorias, buscar estabelecer redes de confiança e ter atores de referência.

Sobre "**livre**", há um importante debate sobre o termo, FLOSS/FOSS, e a tradução de "free" (do inglês, podendo significar tanto livre quanto gratuito), mas pelo curto espaço, passaremos direto, focando no conceito básico de software livre, publicado com uma licença que permite que o usuário tenha liberdade para usar, modificar e redistribuir o código conforme quiser – uma perspectiva maior de coletividade e cooperação, diferente da competição e exploração das gigantes de tecnologia.

Partindo destes conceitos, podemos fazer algumas **recomendações básicas** e, nos materiais sugeridos (final da cartilha) existem sugestões e listas mais completas.

Antes de tudo, uma outra recomendação básica: **mantenha seus sistemas, aparelhos e programas atualizados** – boa parte das atualizações é para sanar problemas de segurança identificados e versões desatualizadas são alvos preferenciais de hackers.

Para **sistemas operacionais**, é recomendável evitar Windows (Microsoft), iOS (Apple) e os do Google (Chrome Books). Para a maioria dos usuários, a alternativa mais viável é **GNU/Linux**, que contem inúmeras diferentes opções. Algumas recomendações abaixo, com condições razoáveis de segurança e privacidade:

– **Debian**: Simples e leve, muitos usuários – o que significa uma comunidade grande, e maiores possibilidades de sanar dúvidas, correções de bugs e problemas técnicos – e um importante projeto de liberdade de software.
– **Fedora**: Também simples de usar e com grande número de usuários.
– **Qubes**: Mais complexo de instalar e usar, mas com foco maior na segurança. Exige um computador com configurações mais robustas.
– **Tails**: Muito leve e rodando a partir de um pendrive (ou CD), focado em privacidade, sem precisar ser instalado no computador e podendo ser retirado deixando poucos rastros. Boa alternativa para aparelhos compartilhados e quem não quer/pode trocar o sistema operacional.
– **Whonix**: rodando a partir de máquinas virtuais, focado em segurança e privacidade – mas não faz milagres: se o computador base estiver comprometido, ele não vai ser capaz de proteger sua atividade.

Criptografar é proteger dados para que só quem tem chave tenha acesso. As duas formas mais comuns de criptografia quando falamos de segurança digital militante são criptografia de **ponta-a-ponta e de disco**. A de ponta-a-ponta é para comunicação, em que só quem manda e recebe tem acesso ao conteúdo da mensagem – é o caso de mensagens no Signal e e-mails com PGP. De disco é a para proteger discos de armazenamento (ou parte deles), impedindo que sejam acessados mesmo que alguém tome seu computador – a senha de usuário do Windows, por exemplo, não impede isto, com os arquivos podendo ser facilmente acessados.

Criptografe seus discos (HDDs, SSDs) e mídias removíveis. Há opções nativas na maioria das opções GNU/Linux. Uma alternativa simples é o **VeraCrypt**, compatível com diferentes sistemas, capaz de criptografar o disco inteiro, partições, pendrives, pastas.

- Utilize o navegador **Mozilla Firefox,** com a extensão uBlock Origin, ativando opções como HTTPS em todas as páginas e/ou o Navegador **Tor**, também com uBlock Origin. Busque proteger sua conexão, seja usando a **rede Tor – a opção mais adequada para a maioria dos usos em militância**, geralmente capaz de esconder sua navegação do provedor, agentes da repressão e eventuais hackers – ou um VPN de confiança, que não te rastreie nem compartilhe dados com agências de inteligência.

- Utilize **provedores de confiança** para e-mail, documentos, nuvem e afins. Uma opção militante popular é o **Riseup**, que disponibiliza e-mail, nuvem limitada, VPN e ferramentas de edição de texto online. Há quem não recomende pelo coletivo se

originar nos EUA. Uma opção corporativa popular é o **Protonmail**, suíço, que oferece e-mail, agenda, nuvem e VPN; já **Tutanota** é uma empresa alemã que oferece e-mails com maior segurança. **CryptPad** é opção francesa de nuvem e edição online de documentos. Cabe ressaltar que já houve colaboração de empresas suíças, alemãs e francesas com a inteligência dos EUA, estando França e Alemanha dentro dos **"14 Olhos" – cooperação de agências de inteligência, diretamente conectadas com as revelações der Snowden.**

- Em **e-mails**, se for usar um cliente, use o **Thunderbird**, preferencialmente com criptografia **PGP**.

- Para documentos offline, prefira o **LibreOffice** às alternativas da Microsoft.

- Para buscas, **DuckDuckGo** é uma boa alternativa ao Google e Bing.

- Para **compartilhamento de arquivos, share.riseup.net** e **OnionShare** são opções. Busque **retirar os metadados dos arquivos** antes de compartilhar/fazer upload (por qualquer meio); opções para retirar metadados são **ExifCleaner** e **MAT2**.

- **Deletar de maneira segura os arquivos é difícil, especialmente em pendrives e SSDs**; por isso, **mantenha sempre os arquivos em meios criptografados.** Para deletar individualmente arquivos, **BleachBit** pode fazer de maneira melhor que só apagar da lixeira, ainda que não 100%. Para l**impar completamente o disco**, alguns fabricantes disponibilizam ferramentas como Secure Erase e há ferramentas como o DBAN que, para deixa os dados inutilizados para a imensa maioria dos adversários, especialmente no caso de HDs.

- O próximo passo é a **destruição física dos discos**. Neste caso também é mais simples em HDs que em SSD mas possível em ambos, desde que se garanta a destruição em **pedaços pequenos o suficiente (e os pedaços certos** – furar a caixa do HD mas manter o disco intacto não adianta de nada).

CELULAR

Os celulares fazem parte da vida de boa parte dos brasileiros – e a única forma de acesso à internet para muitas/es/os – e também estão integrados na militância. Infelizmente, **celulares são excelentes ferramentas para vigiar e monitorar pessoas**, passando dados para empresas, para o Estado e mesmo para adversários privados.

Por sua arquitetura e na maioria dos sistemas operacionais móveis, **celulares são extremamente vulneráveis, inclusive à clonagem** – de aparelhos e de chips. **Grampos nas linhas também são possibilidades reais e comuns**; **grampos ambientais** (o microfone do celular captando tudo que é dito) também são possíveis, embora muito menos comuns.

Evite ao máximo organizar e conversar sobre militância no celular, mantenha-o **longe de ambientes de reunião** e, se possível, deixe-o em casa quando for para alguma atividade sensível de militância. Mantenha o **sistema e os programas atualizados**. Prefira programas de software livre, código aberto e de lojas como **F-Droid**, não Google/Apple *Store*. Utilize **senhas fortes** (evite padrões de desenhar e pins de 4 dígitos) e o **criptografe o dispositivo**. Mantenha **localização, Wi-Fi e Bluetooth desligados** se não estão em uso, **limite as permissões dos aplicativos** e desinstale os que

não usa, **desative os downloads automáticos** de mensagens, **não baixe aplicativos ou arquivos desconhecidos** e tente **não concentrar muito conteúdo no celular, esvaziando e limpando** mensagens e arquivos sempre que possível.

Para conversar por texto, **prefira o Signal**, que possui criptografia de ponta a ponta (só quem manda e quem recebe a mensagem consegue ler) e é focado em segurança e privacidade. Outras opções são o **Briar, Element, Jami e Session**. Na medida do possível, evite o WhatsApp e o Telegram – ainda que ligações pelo WhatsApp tendam a ser mais seguras do que pela linha telefônica. **Em qualquer um dos aplicativos, procure ativar as mensagens temporárias** (autodestruição de mensagens e mídias após certo tempo), especialmente para mensagens sensíveis – de militância, pessoais, íntimas.

SENHAS

Não reutilize as mesmas senhas em diferentes serviços e avalie a necessidade de trocá-las com alguma frequência – fazendo-o pelo menos sempre que houver um vazamento ou comprometimento.

Senhas têm de ser fortes; muitas vezes, são criadas misturas de letras, números e símbolos (como $eNh4!, mas mais longas), mas um método melhor é usar **frases-senhas**: conjunto longo de palavras, sem sentido, garantindo senhas fortes e mais fáceis de lembrar (como VerdeNoiteCartãoQuedaSucoPrendedor). Uma dica para segurança e facilidade é o uso de um cofre (real ou virtual, criptografado, como o **KeepassXC**) para criar e armazenar senhas.

Utilize **verificação/autenticação em dois fatores em todos os serviços** que permitirem. As mais simples são com SMS mas existem outros métodos mais confiáveis, como por chaves USB ou por aplicativos autenticadores – o **Aegis** é uma boa opção. Proteja as opções de backup das verificações em duas etapas.

REUNIÕES E ATIVIDADES VIRTUAIS

Além dos procedimentos para segurança individual dos dispositivos, como proteção de redes e uso de GNU/Linux, alguns cuidados devem ser tomados em atividades virtuais. O primeiro é a escolha da plataforma; uma opção popular é o **Jitsi**, de código aberto e que suporta criptografia ponta a ponta em alguns navegadores, além de você poder hospedar sua própria sala (em vez de usar os servidores deles). Alternativas são o **Signal**, que suporta até 40 pessoas, o **Mumble** (apenas para voz e, para segurança, você deve hospedar o servidor), **Jami** e **Element**, com diferentes graus de facilidade de uso e capacidade de suportar salas com muitas pessoas.

Independente se para uma reunião ou atividade pública, é importante estabelecer **controle de acesso** – no nome da sala, senhas e permissões de entrada. Se a ideia é fazer uma transmissão de um debate, por exemplo, **a sala em que os debatedores estarão deve ser separada de onde as pessoas acompanham ou transmitida diretamente** num streaming, tomando cuidado de **proteger o link da sala de debate** e as contas usadas para criar ou transmitir a atividade. Além disso, é importante **designar alguém para acompanhar o público, moderar comentários e banir sabotadores.**

SEGURANÇA FÍSICA

Quando o assunto é a segurança, a **proteção física 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/e/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 tenha cuidado – não facilite o trabalho de potenciais adversários. Comunique-se constantemente com camaradas 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.

Principalmente para militantes que já passaram por situação de ameaça, deve-se pensar num **plano de segurança individual**, que mapeie os principais pontos de vulnerabilidade e que medidas podem ser tomadas para diminuir os riscos – como, por exemplo, garantir um **revezamento de militantes para acompanhar uma pessoa** que faz todo dia um deslocamento mais perigoso.

Condicionamento físico, formação em defesa pessoal e/ou artes marciais também podem ser importantes para lidar com ataques físicos, mas há vários poréns. Não se pode sobrestimar as capacidade individuais de defesa, deve-se cuidar para não se expor mais por uma falsa sensação de segurança e não deve haver uma recomendação geral de treinar lutas, uma vez que muitas pessoas tem impedimentos – por condições físicas ou qualquer outro – e não devem receber como tarefa "cuidar da própria segurança". **A responsabilidade é de todas/es/os e organização para autodefesa coletiva são o foco, sempre.**

Em **itens para se portar para defesa pessoal**, é importante prezar pela legalidade, efetividade, segurança de quem usa e do entorno e, caso se opte por portar algo, deve-se estudar táticas específicas e treinar exaustivamente com o que for escolhido.

> **Itens cortantes, como facas, são perigosos, potencialmente ilegais** e, mesmo com muito treino, **são riscos de vida** tanto para quem porta quanto para um possível agressor, mesmo que não haja intenção letal.

> **Itens contundentes, como cassetete e batons retráteis, exigem extensivo treino, são difíceis de portar** e podem ser tomados de quem está se defendendo por um adversário com mínimo de treino.

> **Itens de choque que lançam projéteis, como *tasers*, são de uso restrito** para forças de segurança e, portanto, fora de escopo de autodefesa civil. **Itens de cho-**

que por contato (como pequenos aparelhos ou "lanternas de choque") **são de legalidade dúbia e geralmente inúteis**, incapazes de parar um ataque.

> **Agentes químicos como sprays de pimenta também são de uso restrito** e, portanto, fora do escopo. **Há sprays legais baseados em outros agentes químicos**, como gengibre, mas é importante checar a legalidade de cada um sempre antes de adquirir. **Sua efetividade é bem menor que a dos restritos, mas, ainda assim, tem potencial de interromper ataques, além de serem fáceis de portar e usar**. Fabricações caseiras são desaconselháveis e potencialmente ilegais.

> **Armas de fogo obviamente exigem autorização legal para posse e eventual porte e um grupo se armando, ainda que legalmente, certamente receberá intensa atenção de autoridades**. Exigem um **alto grau de treino, preparo e segurança tanto no porte quanto na guarda**, além de atenção para regras de segurança – sendo as quatro básicas tratar toda arma como carregada e pronta para disparo; sempre apontar o cano para uma direção segura; dedo sempre fora do gatilho até o momento do disparo e; ter certeza do alvo e do que há atrás dele.

AMEAÇAS E ACOLHIMENTO

Por vezes, a pessoa pode ser ameaçada individualmente. Nestes casos, os **dois procedimentos mais comuns** são dar **visibilidade**, elevando o perfil da pessoa ameaçada e aumentando o custo de um eventual ataque. O segundo procedimento é a **retirada da pessoa do local** em que atua, deslocando-a temporariamente para um local mais seguro (muitas vezes contando com redes de acolhimento e parcerias solidárias). É **fundamental discutir qual é a melhor abordagem em cada caso e cada vida**, buscando sempre a alternativa mais segura, e sabendo que os dois caminhos **podem ser utilizados em paralelo em algumas das ameaças**.

Independente das táticas deliberadas, **deve-se buscar ao mesmo tempo medidas para reduzir as vulnerabilidades e mitigar riscos**, como garantindo pessoas para acompanhar quem foi ameaçado o tempo todo, acionamento de autoridades, busca por escolta e aprimoramentos na segurança da residência.

Precisa-se também elaborar uma **análise de ameaça da pessoa e iniciar um registro de incidentes de segurança**, sistematizando acontecimentos que fujam da normalidade – sejam ameaças diretas, ocorrências estranhas ou aparentes coincidências, buscando apontar se há algum tipo de padrão e/ou uma tendência do aumento do grau das ameaças e possibilidades de escalonamento ainda maior no futuro. Deve-se frisar que **embora a maioria dos ataques não parta do nada, em alguns casos há pouco ou nenhum indício prévio, e a ausência de ameaças diretas não é garantia de segurança.**

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. **Estas questões, inclusive, não devem se limitar a momentos de maior tensão: cuidado e auto-cuidado são parte fundamental da militância e da segurança militante.**

SEGURANÇA DE ESPAÇOS FÍSICOS E ATIVIDADES PRESENCIAIS

Tanto para a **proteção de atividades quanto de espaços físicos, é necessário mapear as redondezas** – levantando itens como de onde podem partir as ameaças, quais vizinhos são de confiança, quais as distâncias para unidades de polícia, quais as principais vias de acesso. No **próprio imóvel, também é preciso fazer levantamentos**, de elementos como quais os pontos de acessos, saídas de emergência, muros são mais fáceis de serem pulados, onde há arame farpado, concertina ou vidros quebrados, grades em portas e janelas, dispositivos de segurança eletrônica, a altura do imóvel e dos vizinhos, a visibilidade – tanto quanto da rua ou dos vizinhos pode ser visto de dentro quanto o inverso, a iluminação dentro e fora e diversas outras coisas, que variam de caso a caso.

A **preocupação inicial e o ponto básico de aprimoramentos de segurança é no perímetro,** seja com muros, cerca, barrancos ou sem nada, **e nos pontos de acesso**, como portas, janelas e portões. Pode-se melhorar os elementos existentes, adicionar novos, pensar em **diferentes camadas de segurança**. **As medidas de segurança física não devem ser encaradas como infalíveis: são para dissuadir, aumentando o tempo e os recursos necessários para uma invasão ou ataque**, tornando o imóvel menos atrativo que outros alvos – até certo ponto, porque muitos elementos de segurança visíveis numa rua em que as outras casas não possuem nada pode chamar mais atenção.

Medidas de segurança eletrônica e de monitoramento também entram nesta mesma lógica: não são barreiras intransponíveis, mas dificultam o trabalho de adversários. Especialmente no caso de sedes e locais de grande número de agendas, é preciso **fazer avaliações sobre o quão interessante ou não é ter um monitoramento** realizado por uma empresa ou **mesmo registros de câmeras** que poderiam ser tomados por um oponente interessado em saber quem são as pessoas presentes nas atividades.

Para atividades presenciais, é preciso tomar os mesmos cuidados com os levantamentos do imóvel e das redondezas, estabelecendo um **plano de segurança**, prevendo itens básicos como **por onde as pessoas vão entrar, se haverá controle de entrada** – como listas prévias ou pulseiras de acesso – e se haverá **revista** antes da entrada, quais as **saídas de emergência**, por **onde entram convidados** que necessitem de proteção, se há **necessidade de solicitar segurança para autoridades e/ou contratar segurança privada – ou formar uma equipe própria de segurança** –, se há **socorristas**, kits de primeiros socorros e pessoas capacitadas para utilizá-los e **planos de contingência** caso as coisas deem errado.

Fundamental **destacar pessoa (ou grupo de pessoas) como referência para segurança da atividade**, acompanhando todo o desenrolar do evento e fazendo ajustes conforme necessário. Principalmente se for algo realizado em público, nas ruas, como uma panfletagem, é importante que algumas **pessoas cheguem antes no local para avaliar as condições**, ver se há adversários ou algum indício de ameaça e comunicar o restante da organização – um trabalho básico de reconhecimento.

EM CASO DE ATAQUE ARMADO/TERRORISTA

Em caso de **ataques sérios** numa atividade – envolvendo, por exemplo, **tiros ou explosivos** – um dos protocolos possíveis é o **Corra, Esconda, Lute**, tradução direta do *Run/Hide/Fight* em uso nos EUA para o caso de atiradores ("*mass shooters*"). O protocolo se aplica a quem está no local mas não em função de segurança; quem está na segurança responsabilidades e outras linhas de ação, como interromper o atacante.

O protocolo é bastante simples: **se é possível fugir** – seja pela saída normal, saída de emergência, janela – **sem se expor e entrar diretamente na linha de perigo, fuja**. Deixe para trás pertences, não pare ou interrompa o fluxo e auxilie quem precisar.

Não sendo possível fugir – há um atacante na única via de escape, por exemplo – **busque se esconder.** Jogar-se no chão diminui a chance de ser atingido por estilhaços ou projéteis, mas o ideal é buscar cobertura e, preferencialmente, cobertura que tanto lhe esconda quanto proteja de disparos, como paredes maciças de concreto. Caso consiga se esconder numa sala, busque barricar a entrada e busque informar as autoridades de sua situação, mas mantendo o celular silenciado.

Por último, **se não houver alternativa e em último caso, busque lutar** com o agressor com toda e qualquer arma disponível, tentando coordenar com outras pessoas e focando em tomar o controle do armamento do atacante.

SEGURANÇA EM MANIFESTAÇÕES

É importante **planejar previamente as manifestações** e o que ocorrerá nelas, já montando **planos de segurança, pensando as rotas** (evitando ruas com poucas saídas e/ou que facilitem cercos policiais) **e designando pessoas para que cumpram tarefas específicas**, como cuidar de eventuais feridos, dialogar com órgãos de repressão e fazer a comunicação do ato – sabendo que algumas funções vão deixar as pessoas mais expostas e possivelmente transformá-las em alvos, como coordenar ou fazer fotografias/vídeos.

É fundamental também **comunicar pessoas que não vão de que você estará presente** (se possível, advogada/e/o) e n**ão ficar sozinha/e/o**, em especial na chegada e na saída – e, se possível, **só após chegar no local colocar camisetas, bones, adesivos e afins** que identifiquem a pessoa enquanto militante. **Busque uma dupla/trio para ficar com você durante toda a manifestação**. No caso de **organizações, entidades e coletivos, é interessante a formação de blocos, buscando manter unidade e coesão** durante toda a manifestação – em especial para se proteger caso aconteçam episódios de violência.

VESTIMENTAS

Proteja o máximo do corpo, deixando o **mínimo possível exposto, usando calça, manga comprida, um sapato fechado adequado para correr como 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 os agentes químicos) e **lentes de contato** (potencializam efeitos dos agentes químicos). **Evite passar muitos produtos na pele no dia**, pois podem ter interações com

alguns dos agentes químicos. Leve **outras mudas de roupa**, para troca para caso de contaminação e para dificultar identificação posterior.

OBJETOS

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

EQUIPAMENTOS DE PROTEÇÃO

Equipamentos de proteção devem ser usados com cuidado. **Estar protegido demais pode chamar atenção e lhe transformar num alvo** – paradoxalmente deixando você menos protegida/e/o. Se optar por levar equipamentos mas apenas utilizá-los em momentos de tensão, **saiba onde eles estão e como os colocar**, já que na correria ou pânico pode ser difícil vestir uma máscara ou colocar um óculos – treine antes, em casa. **Proteção para cabeça deve ser sempre uma prioridade**. As opções menos chamativas, como bonés e chapéus, são menos efetivas, e o inverso tende a ser verdade: capacetes de bicicleta, moto ou esportes radicais proporcionam melhor proteção contra golpes, disparos e batidas, mas chamam atenção. **Para os olhos**, é possível proteger contra impactos (como de balas de borracha) e agentes químicos (como lacrimogênio). Alguns **óculos de EPI de trabalho ou de esportes radicais** dão conta das duas coisas, se vedados e resistentes, mas dependem de muitos fatores para, por exemplo, parar um projétil (como distância, ângulo, munição e armamento utilizado). Confira as especificações antes de confiar. **Para a respiração**, **respiradores semifaciais ou faciais com filtros adequados** são a melhor opção, embora mesmo com filtros não específicos eles já auxiliem. Máscaras padrão N95 diminuem pouco o efeito, mas são melhores que nada, assim como bandanas e cachecóis. **Para as mãos**, luvas de EPI para quem trabalha com fogo ou altas temperaturas podem ser úteis.

O QUE É UTILIZADO PELAS FORÇAS DE REPRESSÃO

Os Procedimentos Operacionais Padrão variam de estado para estado, mas há diversas similaridades no uso de itens menos letais.

Objetos contundentes – cassetete, escudos, socos, espadas. Não há grande sofisticação nos instrumentos de força bruta, em uso pela humanidade há literais milênios. Por sua natureza, **só podem ser usados de perto e expõe quem os aplica**, sendo geralmente evitados como tática geral e reservados para **dispersão ou prisão de manifestantes** que ficaram para trás – ou utilizados por **guarnições que se sentem acuadas** (geralmente de batalhões da área e não de policialmente especializado, como Choque).

Munições de impacto controlado – As famosas balas de borracha, munições de elastômeros são geralmente disparadas de espingardas calibre 12. Há diversos tipos, inclusive com agentes químicos, mas as mais comuns são as mais simples, com **um a três projéteis de borracha**. Teoricamente devem ser disparados apenas a mais de 20 metros

e para baixo da linha da cintura, mas, na prática, a teoria é outra. Podem perfurar se disparados a curta distância e cegar se atingirem os olhos, além de causarem lesões em diversas regiões do corpo.

Agentes químicos – Pimenta e lacrimogênio, principalmente. Diferentes compostos químicos e diferentes métodos de aplicação. Podem ser **soltos por espargidores (sprays)**, de diferentes tamanhos e raios de aplicação; **lançados em granadas de mão**; **disparados via lançadores** (entre 37 e 46 mm). **O mais comum é pimenta em espargidores e gás lacrimogênio disparado de lançadores**. Há diversos tipos de granadas e projéteis, como a "bailarina", feito para se movimentar aleatoriamente e dificultar que seja chutada de volta, e munições de carga múltipla – se dividindo em diversos projéteis com lacrimogênio. **As granadas obviamente explodem e os projéteis são extremamente quentes ao serem disparados; eventual manipulação deve ser feita com cuidado e somente após identificar qual o tipo de artefato.**

Efeito moral – No conceito técnico, seriam apenas as granadas de efeito moral, que explodem com **grande barulho e soltando um pó inerte (e, no caso das de luz e som, emitindo grande luminosidade).** Na prática, o **"choque e pavor" é tática padrão para dispersar manifestações** – uma releitura da doutrina militar dos EUA, a ideia é **atordoar, causar confusão nas linhas inimigas e impedir uma reação**. O **uso intenso e repentino da violência, por diversos meios** – como lançamento simultâneo de lacrimogênio, granadas de efeito moral, disparos de balas de borracha e carga do Choque e Cavalaria – é a forma mais comum de atingir este objetivo, causando correria e buscando quebrar linhas de manifestantes, prendendo ou atacando os que ficam para trás se o restante corre.

Animais – Cachorros e cavalos são os animais mais utilizados pelas polícias nos Controles de Distúrbios Civis – o termo policial para manifestações que eles desejam reprimir. **Cachorros geralmente são usados para controles de áreas específicas** e para perseguições individuais, enquanto **cavalos costumam ser usados para controle de fluxo e direção do ato, bem como em cargas para forçar dispersão.**

PRIMEIROS SOCORROS

Caso afetado por **agentes químicos, não espalhe, não coce e não pressione para não espalhar mais**, utilizando **leite de magnésia para alívio paliativo ou água corrente** (não de garrafas) para **limpeza**, trocando de roupa o quanto antes. Ao chegar em casa, tome banho gelado, se possível, e tente lavar as roupas afetadas separadas das demais. **Retire da manifestação o quanto antes quem for ferida/e/o ou estiver bastante afetada/e/o, tomando cuidado para não se isolar. Casos 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. É importante ter pessoas **designadas para primeiros socorros básicos nos atos**, treinadas pelo menos em **Ressuscitação Cardiopulmonar (RCP**, focando em compressões torácicas) e medidas básicas de **controle de hemorragias** (como pressão direta e torniquetes). **Num kit, itens básicos são luvas, máscaras, álcool, soro fisiológico, gaze** e outras ferramentas que auxiliem no **controle de hemorragias** – como torniquetes, desde que com treino prévio.

REFERÊNCIAS E SUGESTÕES DE LEITURA

EM PORTUGUÊS

Comunicação – Riseup
https://riseup.net/pt/security
Coletivo AnarcoTecnológico Mariscotron:
https://www.mariscotron.libertar.org/
Front Line Defenders
https://www.frontlinedefenders.org/pt
Privacidade Digital
https://www.privacidade.digital/
Projeto Tor
https://www.torproject.org/pt-BR/
Projeto Tails
https://tails.boum.org/index.pt.html
PRISMBreak
https://prism-break.org/pt/
Proteção para Defensoras e Defensores de Direitos Humanos da Justiça Global
https://bit.ly/3KOgXJG
Proteção à Violência Política Para Defensoras e Defensores de Direitos Humanos
https://bit.ly/CBDDHGuiaViolenciaPolitica
Security in a Box
https://securityinabox.org/pt/
Surveillance Self-Defense - mais atualizada em inglês):
https://ssd.eff.org/pt-br

EM CASTELHANO

Manual de introducción – La seguridad en las organizaciones civiles y sociales – Comité Cerezo México
https://www.comitecerezo.org/IMG/pdf/ManualSeguridadWeb.pdf
Milpa Digital – comunicação e segurança digital para organizações comunitárias
https://milpadigital.org/
CodigoSur
https://codigosur.org/

EM INGLÊS

Coletivo tático de tecnologia
https://tacticaltech.org/
Fundo para Aprimoramento da Tecnologia código aberto
https://ostif.org/
Liga de defesa da internet
https://www.internetdefenseleague.org/
PrivacyGuides – Guia de Privacidade:
https://www.privacyguides.org/
PrivacyTools.io
https://www.privacytools.io/