MINI MANUAL DE

# segurança digital para defensoras

instituto PACS
POLÍTICAS ALTERNATIVAS PARA O CONE SUL

# ficha técnica

**Instituto Políticas Alternativas**
**para o Cone Sul – PACS**

Avenida Henrique Valadares,
23, sala 504 – Centro,
Rio de Janeiro CEP

**www.pacs.org.br**

**Coordenação Geral:** Aline Alves de Lima

**Coordenação de Projeto:** Ana Luisa Queiroz

Este material é fruto da formação **"Segurança Digital para Defensoras"**, realizada pela **MariaLab** a convite do Instituto Pacs junto a mulheres defensoras de direitos humanos, da natureza e de seus corpos-territórios, em novembro de 2021. Seu conteúdo foi adaptado das relatorias da formação com o objetivo de ser um material de consulta e multiplicação dos saberes circulados ao longo dos três encontros.

**Organização e Edição:** Instituto Pacs

**Apoio na produção do conteúdo:** MariaLab

**Redação:** Ana Luisa Queiroz e Karoline Kina

**Projeto gráfico e ilustrações:** João Seno

**Revisão:** Jéssica Patrocínio

**Apoio:** Yasmin Bitencourt

**Brasil, 2022**

Distribuição Gratuita **2022**

**Dados Internacionais de Catalogação na Publicação (CIP)**
**(Câmara Brasileira do Livro, SP, Brasil)**

Cartilha de segurança digital / organização Instituto Pacs. -- 1. ed. -- Rio de Janeiro, RJ : Pacs, 2022.

ISBN 978-85-89366-52-6

1. Computadores - Medidas de segurança 2. Internet - Legislação - Brasil 3. Mídia digital 4. Proteção de dados - Direito - Brasil 5. Redes sociais 6. Tecnologia da informação I. Instituto Pacs.

22-124862 CDD-658.478

**Índices para catálogo sistemático:**

1. Segurança digital 658.478

Eliete Marques da Silva - Bibliotecária - CRB-8/9380

**Realização**

instituto PACS

**Apoio**

maria [lab]

FONDO DE MUJERES DEL SUR

MISEREOR IHR HILFSWERK

Brot für die Welt

**Campanha**

#MULHERES TERRITÓRIOS DE LUTA

# sumário

# Introdução

Entre fotos, estudos, trabalhos, séries, dancinhas e pix, a maioria de nós tem passado cada vez mais tempo conectada em nossos celulares, computadores, tablets, televisores e outros dispositivos de acesso à internet. Mesmo que o uso da rede aconteça por objetivos diferentes, com menor ou maior qualidade de acesso, a internet impacta o nosso convívio social e é, na maioria das vezes, uma ferramenta que pode facilitar a disseminação de informações, a comunicação e a conexão entre pessoas. E como não haveria de ser diferente, temos aproveitado esses espaços das redes sociais e outras ferramentas digitais para avançar também com nossas lutas e defender os nossos direitos e de nossos territórios.

Em diferentes casos, a denúncia de violações através das redes sociais garantiu que os crimes cometidos por empresas ou pelo próprio Estado fossem visibilizados. Para as mulheres, expor os casos de violência nas redes tem contribuído para o constrangimento dos seres agressores. Entretanto, atuar nas trincheiras digitais também traz riscos e condições de vulnerabilidade para mulheres ativistas e militantes, já que, assim como o mundo *real*, o mundo *virtual* também é marcado pelo patriarcado e suas violências de gênero. Reforçam e reproduzem as discriminações construídas por essa sociedade machista, patriarcal e racista, que fere, machuca e coloca em risco os nossos corpos e vidas.

De acordo com a pesquisa "*Indicadores Helpline: atendimentos sobre violações de direitos humanos na internet*", publicada pela SaferNet Brasil em 2017, as mulheres foram maioria **(67,4%)** nos atendimentos por *cyberbullying* e ofensas, além disso são as principais vítimas de exposição a conteúdos impróprios e violentos **(62,1%)**. Sabemos que no ambiente virtual a distribuição dos conteúdos acontece de forma muita rápida, em um efeito cascata e o alcance dessas violências é enorme.

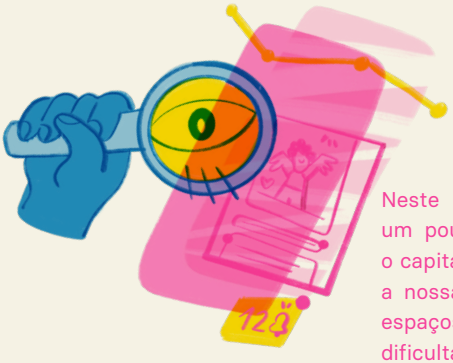
Pensando nisso, o Instituto Políticas Alternativas para o Cone Sul convidou a ***Maria Lab***, uma coletiva de mulheres que atua entre política, gênero e suas tecnologias, para organizar um curso sobre segurança digital voltado para mulheres defensoras de direitos humanos e ambientais. Esse material é um desdobramento da formação realizada em 2021 e traz conteúdos que nos ajudam a adotar práticas mais seguras de interação na internet, nos aplicativos e com nossos dispositivos, celulares e computadores. A proposta deste pequeno manual é trazer dicas e recomendações que nos auxiliem a diminuir os pontos vulneráveis da nossa vida social e de militância nos espaços digitais. Além disso, buscamos refletir a nossa segurança de maneira mais ampliada, ao pensar a nossa privacidade em casa, a proteção dos nossos dados e de nossas contas em aplicativos frente a possíveis invasores e também à violadores de direitos, mas que possamos fazer isso com tranquilidade e sabedoria, sem ansiedade.

as mulheres foram maioria **(67,4%)** nos atendimentos por cyberbullying e ofensas

"***Mas eu não tenho nada a esconder***" – mesmo quando escolhemos que nossa vida seja como um livro aberto, é muito importante que tenhamos assegurado o nosso direito à privacidade. Você pode guardar lembranças e memórias da sua vida em uma caixa de sapato e não ter nenhum segredo familiar ali dentro, mas isso não significa que todo mundo que mora com você tenha autorização de ficar mexendo nessa caixa. Isso vale tanto para seu celular e outro dispositivo individual que você tenha, como para as suas navegações pela *internet*. Somos agredidas também quando controlam, vigiam e grampeiam nossos aparelhos, seja em nossa vida pessoal ou no trabalho, na defesa dos direitos humanos e dos nossos territórios.

Há uma máxima que diz: *quando não está muito claro o que está sendo vendido, pode ser que o produto à venda seja você*. Essa expressão é muito boa para pensarmos sobre o valor dos nossos dados em uma sociedade capitalista. Aqui não estamos falando somente do seu número de CPF, sua identidade e documentos oficiais, mas sobre todos os dados que você produz quando acessa a internet. Os tipos de publicações você curte, o que você costuma passar mais tempo assistindo... Tudo aquilo que fazemos nas nossas redes gera um dado e essas informações podem ser uma mercadoria valiosa.

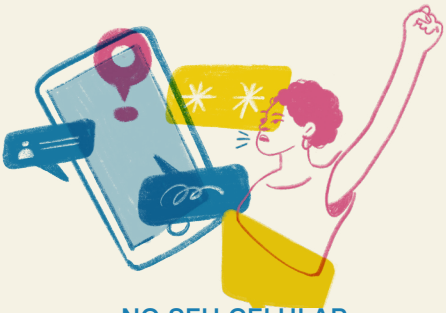
É muito importante que tenhamos assegurado o nosso DIREITO À PRIVACIDADE.



Neste material, vamos aprender um pouquinho mais sobre como o capitalismo também transforma a nossa vida em mercadoria em espaços virtuais e como podemos dificultar esse processo.

Discutir segurança digital é importante para entender o nível de vulnerabilidade das informações que temos em nossos aparelhos e para desenvolver um conjunto de ações a fim de proteger e controlar nossas comunicações e nossos dados. É importante que façamos esse debate e repensemos nossas práticas a partir das nossas possibilidades concretas, com os pés em nossos territórios. O objetivo principal dessa cartilha é apresentar algumas ferramentas para melhorar nossa capacidade individual e coletiva no cuidado e preservação das informações no mundo virtual, incentivar a adoção de hábitos mais seguros no uso de tecnologias, articular a segurança digital com ações que contribuam para a segurança física e psicológica das mulheres e ampliar nossas possibilidades de luta pelo bem viver.

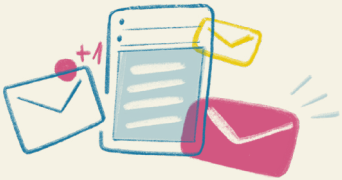
# Dicas de configurações para um ambiente digital seguro



## NO SEU CELULAR

- Ative a localização (GPS) do seu celular somente quando necessário, por exemplo, para encontrar um caminho no mapa ou pedir transporte por aplicativo;

- Configure uma senha de bloqueio do seu celular e dê preferência a senhas com letras e números. Evite usar a opção de ligar pontos, de biometria ou de reconhecimento facial.



## EM NOSSAS CONTAS DE E-MAIL, NO CELULAR OU COMPUTADOR

- Escolha a opção de autenticação de dois fatores: é uma opção para quem utiliza aplicativos de mensagem, já que é uma alternativa extra de segurança para a proteção das suas contas contra os ataques virtuais. A autenticação de dois fatores emite um aviso, em formato de mensagem ou e-mail, quando alguém tenta acessar seus aplicativos por outros aparelhos. A configuração pode ser habilitada na área de segurança do seu aplicativo.

- Configuração e opções de segurança e privacidade

## EM NOSSAS REDES SOCIAIS, NO CELULAR OU COMPUTADOR

- Autenticação de dois fatores

- Configuração e opções de segurança e privacidade

# Senhas

As senhas são as "portas de entrada" para nossas contas e também para nossos dispositivos, sejam eles computadores ou celulares. É provável que você já conheça algumas dicas básicas importantes, como evitar datas de aniversário ou nomes de pessoas próximas. Falando de senhas em geral, quando for possível, tente usar frases longas, misturar números e letras, maiúsculas e minúsculas, palavras em outras línguas ou até inventadas por você. Todas essas dicas dificultam possíveis invasões, sejam elas feitas por programas ou por pessoas que podem estar longe ou perto da gente. **Sabemos que fugir das datas e nomes conhecidos, criando senhas diferentes para diferentes dispositivos e redes pode ser um desafio para nossa memória, mas são estratégias importantes para sua segurança e que valem o esforço!**

No caso de celulares, os modelos mais atuais oferecem cinco opções: reconhecimento facial, digital, desenho de padrão, senha numérica e senha alfanumérica. O reconhecimento facial, além de ser uma tecnologia com recorrência de falha, ou seja, a câmera pode identificar outra pessoa como sendo você, é uma opção onde você entrega uma informação sensível, assim como o cadastramento da sua digital. Além disso, no caso da digital, alguém pode usar o seu dedo enquanto você está dormindo, sem que você perceba, esse é um ponto de atenção importante para quem sofre com violações de privacidade dentro de casa. No caso de senhas por desenho padrão, aquele de ligar os pontos, você pode estar vulnerável pelas marcas com o caminho da senha que deixam registro na tela do celular, feita pela sujeira e gorduras ali acumuladas. De todas as opções, a mais segura costuma ser a alfanumérica, já que pode ser uma senha que mistura letras, números e símbolos.

## regra de ouro

→ De qualquer maneira, lembre-se: **desconfiou de algo? Mude sua senha!** E ao mudar a senha em contas que podem estar conectadas em outros aparelhos, não esqueça de assinalar a opção de desconectar também.

As senhas são as "PORTAS DE ENTRADA" para nossas contas e também para nossos dispositivos, sejam eles computadores ou celulares

# Falando de celular

Os aparelhos celulares atuais possuem tantas funcionalidades que podem ser comparados a um pequeno computador. Vamos começar pela identificação do aparelho e do chip. Cada chip telefônico está associado a um CPF e possui um número de identificação chamado IMSI. Já o aparelho em si não precisa estar cadastrado em nenhum CPF para funcionar, mas mesmo assim possui também um número de registro, que nesse caso se chama IMEI. Esse número do aparelho, o IMEI, é a identificação dele na rede da telefonia. Quando temos um celular furtado, podemos, com esses números em mãos, solicitar o bloqueio deles junto à operadora. Em caso de grampos, trocar somente de chip pode não ser suficiente.

Mesmo quando desligamos o celular, ele segue se comunicando com a rede da operadora através de sinais de antena. Este é um funcionamento padrão da rede de telefonia celular e é o que permite que você tenha sinal no seu aparelho. Por isso, quando estamos em locais onde não há antenas muito próximas ou em uma área onde há muitos morros e serras ao redor, podemos ficar sem sinal no celular. Por outro lado, esse mesmo recurso é o que permite a localização do aparelho ainda que desligado.

## GRAMPO TELEFÔNICO

* O grampo telefônico costuma ser feito a partir da relação com o CPF da pessoa alvo de investigação ou perseguição e não é perceptível pelo usuário sem ferramentas específicas. O aparelho não esquenta e não dá ruídos na ligação grampeada. Se você suspeita estar sendo alvo de um grampo e não puder aguardar um encontro para trocar informações sensíveis pessoalmente, utilize outro aparelho ou prefira fazer chamadas por voz através de aplicativos de mensagens como o Signal, no qual a sua conversa estará criptografada.

## APLICATIVO ESPIÃO

* Os aplicativos espiões são programas que podem ser instalados em aparelhos celulares e computadores de diversas maneiras, possibilitando acesso a dados, localização, câmera, áudio e etc. Por isso, a senha inicial do seu aparelho, que mencionamos anteriormente, é muito importante para evitar o acesso físico aos seus dispositivos. Caso desconfie que algum aplicativo que você nunca baixou, "*surgiu*" no seu aparelho, cheque nas configurações do seu celular, na área "***dados do aplicativo***" o que há de diferente. Caso identifique um aplicativo espião, faça um ***backup*** (uma cópia de segurança dos seus dados) e formate o seu celular. Recomendamos também que não deixe de baixar um antivírus confiável no seu aparelho. Sugerimos o ***https://www.lookout.com/***

**atenção**

→ **Jamais empreste o seu celular desbloqueado!** A instalação de aplicativo espião é muito rápida e fácil de ser feita. E se quiser saber mais dicas de proteção do seu aparelho, acesse: **www.marialab.org**/como-evitar-que-agressores-tenham-acesso-ao-seu-celular

## O QUE É UM *MALWARE*?

✳ *Malware*, ou vírus como normalmente conhecemos, é um programa criado com a intenção de causar danos a um computador, celular, servidor ou a uma rede de computadores. Existe uma grande variedade de *malware* que pode ser utilizada para fraudes, roubo de informações ou causar um problema no funcionamento do seu dispositivo. Para proteger seus aparelhos, dados e contas, é importante ter um antivírus instalado e tomar outros cuidados, como evitar clicar em links desconhecidos ou baixar arquivos de sites que você não conhece.

# Lidando com o Google

A Google é uma empresa estadunidense que oferece uma variedade de serviços e aplicativos, desde o buscador até e-mails e mapas. Quando você tem uma conta do Google, mesmo que use só o Gmail, os demais serviços também estarão integrados.

Para o plano de negócios da Google é central a coleta de dados. A partir destas informações são criados perfis de consumidores que orientam os anúncios de empresas parceiras da Google.

Ninguém quer sentir-se o tempo todo vigiada e para evitar isso há algumas configurações de segurança e privacidade que você pode alterar na sua conta Google.

- Desative o histórico de atividades, de localização e de navegação no Youtube
- Desative os resultados personalizados de pesquisa
- Controle as suas informações de perfil e quem pode vê-las
- No compartilhamento de documentos, deixe restrito às pessoas que você convidar para ver e editar os arquivos.
- Sempre configure a conta com uma senha forte e troque-a com frequência.
- Habilite a autenticação em dois fatores
- Todas essas opções você encontra em “Gerenciar sua conta Google”

## PLATAFORMAS DE CÓDIGO ABERTO E CÓDIGO FECHADO

* Todo programa ou aplicativo precisa ser escrito em código para existir. É como uma receita de bolo: precisamos dos ingredientes que tem uma ordem certa para serem misturados e que juntos, depois de um certo trabalho, fica pronto pra ser comido. Os programas e aplicativos também tem uma receita, um código por trás que faz com que eles existam e funcionem. É esse código que vai determinar o que um programa pode ou não pode fazer. Se ele é capaz de enviar mensagens de texto, ou de texto e imagens, por exemplo.

* No caso de programas de código aberto a "receita" por trás deles é de domínio público. Claro que nem todas nós sabemos ler códigos de programação e você não precisa aprender isso para se proteger. Mas se um código está aberto, quer dizer que muitas pessoas, que conseguem, poderão ler e terão certeza de que aquele programa faz o que promete. Isso nos ajuda a ter segurança de que não há outras ações sendo feitas ao mesmo tempo no nosso celular, como uma coleta indevida de dados. Esses programas também podem ser chamados de *software livre.* Nesse caso, os programas podem receber indicações de melhorias em dinâmicas coletivas, já que a sua "receita" está aberta ao público. Já os aplicativos e programas de código fechado tem sua receita de funcionamento elaborada e mantida de maneira privada, inclusive, patenteadas, o que impossibilita um controle público sobre o seu funcionamento.

## O QUE É CRIPTOGRAFIA?

Criptografia é um método utilizado para a proteção de mensagens de modo que só você e a pessoa com quem você está conversando conseguem ter acesso ao conteúdo. A técnica consiste em criar códigos que embaralham a mensagem e impedem que ela seja lida ou compreendida por alguém que tente interceptar a sua comunicação. Lembram da língua do P, que muitas de nós já usamos quando criança? Pois então, quem não conhece a regra não consegue entender a conversa. Na criptografia é mais ou menos assim, mas a regra neste caso é uma chave de criptografia que é trocada entre você e seu interlocutor e sem ela não é possível entender a mensagem.

## APLICATIVOS DE MENSAGEM

Para a gente escolher um aplicativo seguro, vamos levar em consideração o que aprendemos sobre código aberto e criptografia, além de outros elementos. Na tabelinha abaixo vemos que os aplicativos mais comuns atualmente, não são os mais seguros. Aqui não estamos dizendo que você precisa abandonar os aplicativos mais comuns onde estão os grupos da família, de amigas, da igreja e até de debates políticos. Mas é importante você saber o nível de vulnerabilidade que as suas mensagens que circulam por eles estão expostas. Se você conseguir memória no celular para ter também instalada uma opção mais segura para servir como um canal de assuntos específicos, essa pode ser uma boa alternativa!

## COMO ESCOLHER

| |  whatsapp |  telegram |  signal |  messenger |
|---|---|---|---|---|
| Software livre | ✗ | +/- | ✓ | ✗ |
| Criptografia ponta-a ponta | ✓ | Só no chat secreto | ✓ | Só no chat secreto |
| Autenticação de chaves | ✓ | Só no chat secreto | ✓ | ✗ |
| Autodestruição de mensagens | ✓ | Só no chat secreto | ✓ | ✓ |
| Senha para entrar no app | ✗ | ✓ | ✓ | ✗ |
| Autenticação de dois fatores | ✓ | ✓ | ✓ | ✓ |
| Sigilo no número de telefone | ✗ | ✓ | ✗ | ✓ |

# referências


**www.marialab.org**/como-evitar-que-agressores-tenham-acesso-ao-seu-celular

**www.marialab.org**/wp-content/uploads/2020/12/Barricas-estrategias-coletividade.pdf

**www.marialab.org**/wp-content/uploads/2020/09/guia_pratica_estrategias_taticas_seguranca_digital_feminista.pdf





ISBN: 978-85-89366-52-6

9 788589 366526


instituto
PACS
POLITICAS ALTERNATIVAS
PARA O CONE SUL