

# COMUNICAÇÃO SEGURA: UM GUIA BÁSICO PARA TEMPOS SOMBRIOS

## 1. SENHA NO TELEFONE É ESSENCIAL

Se você ainda não tem uma senha forte no seu telefone, coloque uma já. Criptografe seus dados. Caso seu aparelho caia na mão de terceiros, isto no mínimo vai dificultar que se acessem os seus dados.

Dispositivos Apple são criptografados de fábrica; em Androids é preciso escolher esta opção.

**iPhone:** vá em ajustes > código > ativar código. Na mesma tela, escolha a opção “exigir código imediatamente” e ligue a opção “eliminar dados”, que apaga todo o conteúdo do iPhone após 10 tentativas incorretas.

**Android:** vá em configurações > segurança > bloqueio de tela e selecionando a opção PIN. Na mesma tela, selecione a opção “criptografar dispositivo”.

**Todos os sistemas:** evite números repetidos ou sequências óbvias (seu dia ou ano de aniversário, por exemplo).

Mantenha a tela do seu telefone limpa, pois a polícia ou outras pessoas mal-intencionadas podem adivinhar a sua senha pelas marcas de gordura dos dedos.

## 2. DESATIVANDO O GPS

Dados de sobre a sua localização podem ser usados contra você pela polícia. Ao participar de protestos, desabilite o GPS. Desative a opção em:

**iPhone:** vá em ajustes > privacidade > serviços de localização.

**Android:** vá em configurações > pessoal > localização.

## 3. MAS E O WHATSAPP?

Embora WhatsApp e Messenger sejam as ferramentas de comunicação online mais usadas no Brasil, elas não são 100% seguras.

Use o Signal (<http://signal.org>) e comunique-se exclusivamente por ele.

Um policial ou agente governamental com acesso direto ao aparelho pode ler todas as suas conversas independentemente delas serem criptografadas. Por isso, configure o aplicativo para que as mensagens desapareçam após um tempo (de preferência o mais rapidamente possível).

Para fazer isso abra uma conversa, clique no nome do contato e selecione a opção “mensagens efêmeras”.

**IMPORTANTE:** Organize-se e somente comunique-se com aqueles que estejam dispostos a tomar as devidas precauções. Um elo fraco da corrente pode comprometer todas as partes envolvidas.

**NÃO COMPARTILHE INFORMAÇÕES SENSÍVEIS E PESSOAIS EM PLATAFORMAS NÃO-SEGURAS.**

## 4. SE PROTEGENDO DE PROVAS DIGITAIS PLANTADAS

Caso seu telefone seja retido pela polícia ou por um agente do governo, é possível que provas sejam plantadas. Por isso, é bom prevenir-se e poder provar que um telefone ou um SIM card não são seus. Remova o SIM card imediatamente ou restaure as configurações de fábrica. Caso não seja possível, faça-os ter trabalho mantendo seu telefone seguro e as informações criptografadas.

Telefones possuem um código único chamado IMEI, que na maioria dos casos pode ser acessado atrás da bateria, ou discando **\*#06#**

Anote o número que aparecer na tela: ele é exclusivo do seu telefone e não muda mesmo que outro SIM card seja colocado no lugar.

# COMUNICAÇÃO SEGURA: UM GUIA BÁSICO PARA TEMPOS SOMBRIOS

## 5. REDES SOCIAIS E MANIFESTAÇÕES

Evite manter suas redes sociais abertas a todos. Restrinja suas postagens a amigos (clicando ao lado da postagem no Facebook e removendo o ícone do globo). Tranque suas contas no Twitter e Instagram.

Evite marcar presença em manifestações divulgadas em redes sociais - compareça, porém não se marque no Facebook.

## 6. E POR E-MAIL?

De nada adianta se comunicar seguramente por Signal e não proteger suas comunicações por email. Se puder, use serviços como o **RiseUp.net**, um site que oferece email hospedado em servidores criptografados. Se não tiver acesso a este serviço, evite ao máximo se comunicar por email e de preferência ao Signal.

Utilize SEMPRE autenticação de dois fatores para TODAS as suas contas.

Com isto, cada vez que você se logar, precisará confirmar o login pelo telefone, tornando muito mais difícil que terceiros tenham acesso.

## 7. DOCUMENTANDO PROTESTOS

Embora seja importante documentar protestos, muito cuidado para não gerar material que possa ser usado futuramente contra os manifestantes caso caia na mão da polícia.

Evite tirar fotos ou fazer vídeos que mostrem claramente rostos ou outras características marcantes (tatuagens, por exemplo) de quem está protestando.

### FONTES E MAIS INFORMAÇÕES:

Security in a Box: Ferramentas de Segurança Digital para Todas as Pessoas  
<https://securityinabox.org/pt/>

Manual de Segurança: Medidas Práticas Para Defensores dos Direitos Humanos em Risco  
<https://www.frontlinedefenders.org/pt/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk>

Surveillance Self-Defense: Tips, Tools and How-Tos for Safer Online Communications (em inglês) - <https://ssd EFF.org/>