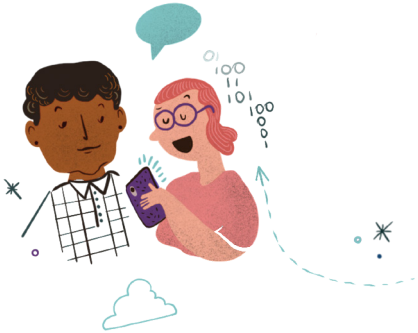

# manual de *autocuidados* digital feminista



akãhatã

equipo de trabajo en sexualidades y géneros

**O autocuidado digital coletivo**
**é como uma grande rede de EMPATIA:**
*ao cuidarmos de nós próprios*
*também se cuida  aes outres.*

# introdução

Este manual de autocuidado digital e feminista é uma proposta centrada em ações coletivas. Reconhecemos que a segurança digital depende da abertura de cada ume de nós para cuidar des outres. Portanto, os métodos para nos protegermos têm de ser pensados a partir da empatia coletiva. Pensar coletivamente dá força a cada ação que geramos a partir das nossas próprias individualidades e identidades.

Este manual é feminista porque assume que as desigualdades de gênero existem e reconhece a sua violência como estrutural; bem como o racismo, o capacitismo e outras opressões, que também são reproduzidas no campo digital.

Dada a impossibilidade da linguagem normativa de abranger todas as identidades que excedem o binarismo sexual, optamos por uma linguagem inclusiva para interferir com a norma. Utilizamos o "e" porque reconhecemos a multiplicidade de identidades apagadas pelo uso do masculino universal ou não incluídas no binário.

## » De que trata o manual?

Este manual é uma abordagem básica e introdutória a diferentes práticas de cuidados digitais, de uma perspectiva feminista e coletiva. Inclui reflexões sobre como realizar ações que nos permitam cuidar uns des outres e inclui ferramentas para acompanhar estas práticas.

## » Conceitos e definições fundamentáis

**_Risco**
Possibilidade de danos que me possam afetar a mim e/ou ao minha coletiva. Esta possibilidade depende do nível de vulnerabilidade em que eu estou. A fórmula básica do risco é:

$$\text{Risco} = \frac{\text{Ameaça} \times \text{Vulnerabilidade}}{\text{Capacidade de resposta}}$$

**_Ameaça**
Qualquer fenômeno, pessoa ou processo que constitua um risco.

**_Vulnerabilidade**
É a capacidade (alta ou baixa) que temos de lidar com riscos ou eventos que possam ocorrer.

**_Privacidade**
É a esfera da vida pessoal de um indivídue, que se desenrola num espaço reservado. A privacidade é um direito humano.

**_Dados pessoais**
É toda a informação relacionada com a nossa pessoa e que nos identifica ou nos torna identificáveis.



**_Direitos Digitáis**
São aqueles que permitem aos indivíduos aceder, utilizar, criar e publicar meios digitais; e aceder e utilizar computadores, outros dispositivos eletrônicos e redes de comunicações[1].

1 | Que são os Direitos Digitais?

**_Meta-dados**
Isto faz referencia aos dados e características que constituem os nossos dados. Por exemplo, o meta-dado de uma fotografia é o local onde esta foi tirada, o tipo de dispositivo utilizado para tirá-la, etc.

**_Hacking de informação**
Utilização de tecnologias para decifrar informação privada, a fim de prejudicar uma pessoa ou organização. Um possível hacking de informação poderia ser para as contas dos meios de comunicação social da sua coletiva: publicar ou apagar o seu histórico de publicações. Neste exemplo, o risco direto é perder a memória de todo o trabalho realizado.


**_Encriptação**
O processo de codificar alguns dados, documentos ou ficheiros de modo a que o conteúdo seja indecifrável e só possa ser acedido através de uma senha.

**_Chave PGP**
Pretty Good Privacy (Muito boa privacidade). É um protocolo para encriptar e-mails. Embora não seja de código aberto, é possível utilizar o standard OpenPGP.

# contexto, riscos e ameaças

Analisar a tecnologia como um processo é uma forma de compreender que cada tecnologia que aparece na nossa vida responde a interesses que se situam em contextos específicos. Por exemplo, grandes poderes que procuram desenvolver mecanismos para aumentar a vigilância da população; períodos específicos, tais como em pandemias, quando a localização de pessoas aumenta a utilização indiscriminada dos nossos dados pessoais.

Dentro dos nossos ativismos é importante ler estas tecnologias de forma crítica e ser criative na procura de formas de utilizá-las para nosso proveito. Aquilo que se apresenta como uma ameaça às nossas identidades e trabalho pode ser reutilizado de forma adaptativa, colaborativa e participativa. As reapropriações estratégicas de diferentes tecnologias podem potencialmente aumentar as nossas capacidades e o alcance das nossas vozes.

## » Análise de riscos e ameaças

**Quais são os riscos e ameaças que podemos encontrar nos nossos ativismos?**

Nenhum trabalho de ativistas está livre de riscos potenciais. No entanto, é importante reconhecê-los a fim de mitigá-los. Os riscos podem ser externos aos nossos coletivos, por exemplo, através da vigilância governamental, ou interna, por exemplo, através da infiltração de indivídues. Certos riscos podem ser considerados menores, tais como a invasão de uma conta ou perfil digital, e aumentam de perigo se as informações ou dados com que trabalhamos forem sensíveis ou contiverem dados pessoais.



**Estes riscos podem resultar em:**

_ Perda dos nossos dados pessoais e dos dados das nossas coletivas ou colegas.

_ Cessação das ações planejadas a serem levadas a cabo pelas nossas coletivas

_ Ameaças à integridade física de pessoas e dispositivos.

## » Possíveis fontes de ataque contra nós

Quem poderão ser os nossos potenciais adversários? Os nossos adversários pensarmos que são aquelas grandes entidades e seres acima das nossas cabeças: instituições públicas e governos, organizações religiosas, grupos fascistas e antidireitos. No entanto, é necessário pensar que os nossos adversários podem ser as pessoas mais próximas de nós. Os nosses parceires, membros da família e até os nosses amiges.

A vigilância, o assédio e a perseguição não ocorrem verticalmente de uma instituição para as nossas identidades digitais e as nossas corpas físicas; também podem ser encontrados dentro daquelas relações que consideraríamos horizontais e de pares. Um companheire ou parceire pode exercer violência e vigilância pedindo a sua senha ou pedindo provas da sua localização.

# por que autocuidados feministas?

## » Que são os autocuidados coletivos feministas?

O autocuidado digital é a forma como transferimos todos os cuidados físicos, emocionais e psicológicos para a dimensão digital. Isto implica repensar o que são estas práticas, como as realizamos e quem compõe as nossas redes de cuidados.

O autocuidado é feminista se for pensado de uma perspectiva coletiva, emancipatória e transformadora dos papéis e opressões tradicionais de gênero. Uma versão feminista do autocuidado também requer o reconhecimento de que a experiência de opressão e violência é agravada quando se intersecta com outros vetores como a capacidade, raça, sexualidade, etc. Pensar no autocuidado digital coletivo significa proteger-nos de uma forma empática, cuidarmos uns des outres e assim cuidarmos de nós.

As dimensões do autocuidado digital coletivo estão ligadas em paralelo com o nosso autocuidado físico. Assumir um maior controle dos dispositivos com que ligamos a nossa realidade ao mundo digital permite-nos não só proteger-nos a nós própries, mas também proteger aes outres. As ações que realizamos no mundo físico, tais como transportar os nossos dispositivos móveis ou tirar fotografias, podem ser ações que aumentam a vulnerabilidade da privacidade das nossas identidades digitais e as des outres.



**Por exemplo:**

_ Não deixar os nossos computadores ou dispositivos móveis desbloqueados em locais públicos

→ Permite que outras pessoas não acedam facilmente às nossas contas ou perfis.

_ Que os nossos computadores ou dispositivos móveis tenham uma senha segura

→ Permite que, em caso de roubo, as nossas contas e sessões sejam protegidas. .

## Mapa das organizações de apoio aos cuidados digitais na região

**_México**
. SocialTic
. La Clika
. La Sandía Digital
. Codeando México
. Luchadoras
. Rancho Electrónico
. Colectivo Disonancia
. Colectiva Mecha
. SeguDigital
. Vita Activa

**_Guatemala**
. CiberfeministasGT

**_El Salvador**
. Las Mélidas

**_Nicarágua**
. La quimera feminista
. Enredadas por el arte y la tecnología

**_Costa Rica**
. Sula Batsu
. Fundación Acceso

**_Panamá**
. Ipandetec

**_Brasil**
. Cl4ndestina
. Coding Rights
. Maria Lab

**_Colômbia**
. Fondo de Acción Urgente Latinoamericano
. Fundación Karisma

**_Equador**
. Taller comunicación mujer

**_Peru**
. Hiperderecho

**_Bolívia**
. Nodo Común
. Internet Bolivia

**_Paraguai**
. TEDIC

**_Chile**
. Proyecto Aurora de Amaranta

**_Argentina**
. Activismo feminista digital
. Las de Sistemas
. Chicas Poderosas

**_ Regional – Global**

. Derechos Digitales
. Dominemos las TIC
. Access Now
. Código Sur
. Surveillance Self-defense
. Digital Defenders
. Frontline Defenders
. Ciberseguras
. Tactical Tech
. Escuelafeminista.red
. Acoso en línea
. Asuntos del Sur - SISA
. Asociación para la Comunicación Progresiva

# conjunto de ferramentas

## » Ferramentas

### Senhas seguras

Cuidar as nossas senhas é um dos passos fundamentais para cuidar bem das nossas identidades digitais. Para consegui-lo, há passos muito simples a seguir:

_ Não utilizar a mesma senha para mais do que uma conta.

_ Saiba mais sobre gestores de senhas como o KeepassXC para gerir todas as senhas que criar.

» *O gestor de senhas* é um cofre onde pode guardar todas as suas senhas sob uma chave mestra. Se não for criative, também o ajuda a criar palavras-chaves fortes para usar com as suas contas.

» KeepassXC funciona com Linux, Windows y Mac.

» Para dispositivos celulares:

- Android: KeePassDX and KeePass2Android.
- Para iOS, Strongbox and KeePassium.

_ Utilizar senhas com caracteres especiais tais como pontos, vírgulas, pontos de exclamação, pontos de interrogação e até espaços.

_ Nunca deixem as suas senhas livres, que livre seja o amor!

**Auto-avaliação sobre senhas seguras:**

◊ Tenho uma senha alfanumérica nos meus dispositivos?

◊ Actualizo regularmente as minhas senhas?

◊ Tenho senhas diferentes para as minhas contas e para as contas da minha organização?



### Navegação segura

Há muitas maneiras de navegar no vasto mar da Internet em segurança e com um baixo nível de exposição a ataques ou riscos. Em primeiro lugar, é importante compreender a diferença entre uma navegação segura e uma não navegável.

A navegação segura envolve considerações prática tais como não aceder a páginas de origem duvidosa ou que pareçam suspeitas, *Para fazê-lo, pode verificar que na barra de endereço onde escreve o site web, depois do http, tenha uma "s". Isto significa que o website tem um certificado de segurança.* (Secure Sockets Layer). Pode verificar se o endereço onde navega, ou URL, é real. Por exemplo: https://www.nytimes.com/ e não um endereço duvidoso como http://www.newyorktimes.info. Verificar sempre a veracidade das ligações antes de introduzir qualquer um de seus dados pessoais.

Existem ferramentas tais como VPNs e navegadores como os TOR que **fornecem uma camada extra de segurança e anonimato durante a navegação.** Aquí está um exemplo de como eles funcionam:

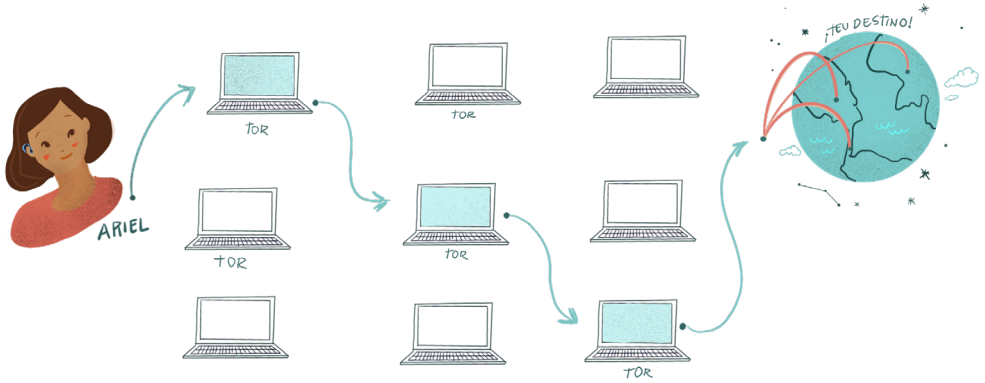
**_VPN:** uma VPN, o rede privada virtual, liga seu dispositivo a um servidor remoto no país da sua escolha, através de um túnel seguro. Esta encobre e protege o seu endereço IP, fazendo aparentar que está acedendo à Internet a partir de um servidor remoto e não da sua localização real.

· **Linux, Mac, Windows, iOS, Android / Bitmask:** https://bitmask.net/en

· **Linux, Mac, Windows, Android / RiseUp VPN:** https://riseup.net/en/vpn

· **iOS: / OpenVPN**

**_TOR:** The Onion Router (Tor) é um software gratuito que esconde a sua identidade encriptando o seu tráfego e encaminhando-o através de múltiplos servidores operados por usuaries conhecidos como nó de rede.




***O que é melhor? Os dois têm funções diferentes.***
Por exemplo: a maioria dos VPNs oferecem encriptação de ponta a ponta, privacidade e tornar os seus dados 100% invisível para hackers e espiões.

A menos que se utilize o sistema operativo Tor, este apenas protegerá os dados que são transmitidos através do seu navegador. VPNs, por outro lado, codificam todos os dados que viajam através da sua ligação.[2].

2 | Definitions of VPN and TOR by

Também pode converter em anônima a sua navegação utilizando *separadores incógnitos*. (Chrome) ou *separadores privados* (Firefox). Este tipo de navegação é recomendado quando você não esta utilizando os seus dispositivos ou estiver num computador acessível ao público. Ao navegar através deste tipo de separadores, os seus dados não serão guardados. Isto não significa que as páginas que visitar não reconhecerá que teve acesso a elas, mas que o dispositivo físico não guardará a sua informação.



***Conjunto de recomendações:*** utilizar Firefox já que é um navegador web gratuito e de código aberto. Também utiliza menos memória do que o Chrome, convertendo-o num navegador mais rápido. Utiliza DuckDuckGo[3] como motor de pesquisa, uma vez que não recolhe dados pessoais quando se pesquisa. Por conseguinte, não cria um perfil das suas preferências, mas mostra-lhe as informações relevantes para a sua pesquisa.

3 | DuckDuckGo

## Auto-avaliação sobre navegação segura:

- ◊ Eu saio das minhas contas quando as utilizo em dispositivos que não são meus?
- ◊ Utilizo sessões incógnitas ou secretas quando navego em dispositivos que não são meus?
- ◊ Utilizo navegadores seguros para não deixar vestígios das minhas preferências nos navegadores?

## Comunicação e envio de mensagens seguras

O envio seguro de mensagens tem dois componentes: um componente técnico e um componente comportamental de usuarie. Por exemplo, existem diferentes tácticas que podemos adotar para comunicar com mais segurança, mesmo que não tenhamos uma aplicação segura.

A aplicação mais recomendada é o Signal porque tem encriptação de ponta a ponta em todas as suas conversas, incluindo as suas conversas de grupo. Isto significa que ninguém será capaz de interceptar a sua comunicação, incluindo a empresa. O Signal também oferece acesso à aplicação protegido por senha.

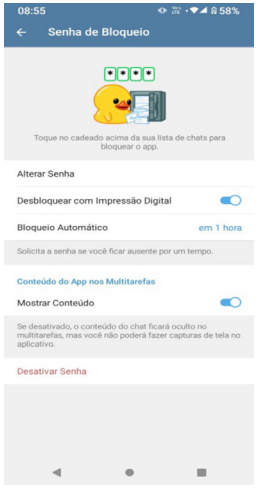
Se tiver pouco acesso à Internet, baixa capacidade de armazenamento no seu dispositivo e a sua única alternativa é o Whatsapp, ou outra plataforma de alto risco, é importante saber como utilizá-la com segurança. Para ello tenemos las siguientes recomendaciones:

_ **A sua fotografia de perfil não deve aparecer num ambiente íntimo**, com pessoas próximas de si, da sua família ou menores.

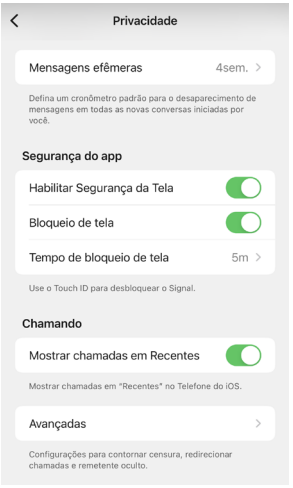
_ **Evite deixar um rasto onde possa ser reconhecide.** Certifique-se de que o seu nome na plataforma não é o seu verdadeiro nome. Usar pseudônimos criativos.

_ **Utilize uma senha para aceder à plataforma.** Por exemplo, nas configurações de Whatsapp pode definir uma senha para iniciar a sessão na aplicação.

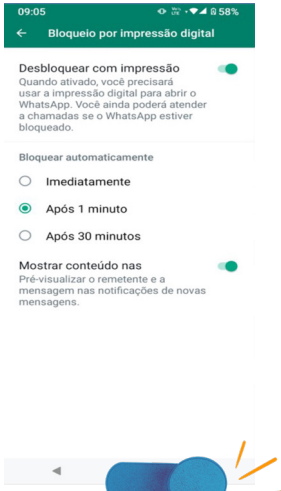
**Telegram**

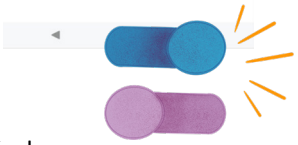



**Signal**




**Whatsapp**



Se precisar partilhar qualquer senha ou informação sensível, pode propor um esquema seguro para fazê-lo. Por exemplo, enviar primeiro os três últimos dígitos de uma senha, depois os três primeiros dígitos e finalmente os três dígitos do médio de uma senha.

**O quadro seguinte pode também ajudar a compreender melhor como funcionam as três aplicações mais populares de envio de mensagens.** 4

| | Whatsapp | Telegram | Signal |
|---|---|---|---|
| Verificação em duas etapas | ✓ | ✓ | ✓ |
| Bloquear o acesso ao aplicativo | ✓ * com impressão digital | ✓ * com código e, opcionalmente, impressão digital | ✓ * com impressão digital e código |
| Encriptação de ponta a ponta | ✓ | ✓ | ✓ |
| Acesso obrigatório aos contatos | ✓ | ✗ | ✗ |
| Bloco de imagens | ✗ | ✓ * conversas secretas | ✓ |
| Mensagens temporárias | ✓ | ✓ * conversas secretas | ✓ |
| Autodestruição de mensagens | ✓ * as mensagens temporárias podem ser reencaminhadas ou apoiadas | ✓ * só em chat segredos | ✓ |
| Bloqueio da aplicação no dispositivo | ✓ | ✓ | ✓ |
| Encaminhamento de conteúdos | ✓ * sem reencaminhamento do remetente | ✓ * opcional sem reencaminhamento do remetente | ✓ * em encaminhamento do remetente |
| Partilhar a minha informação com terceires | ✓ | ✓ | ✗ |
| Ferramentas para relatar e bloquear contactos ou grupos | ✓ | ✓ * incluindo stickers | ✓ |



**Para denunciar abusos nas plataformas de mensagens**[5]

**/ WhatsApp:** seguir estes passos para relatar um chat em grupo ou um contacto: https://faq.whatsapp.com/21197244/#Report

**/ Telegram:** pode reportar um contacto, grupo ou canal a partir das opções do celular.Para stickers o bots enviar um e-mail para abuse@telegram.org. Inclui o enlace e o @nombredeusuarie a reportar.

**/ Signal:** pode bloquear um número de telefone, contacto ou grupo.

4 | Signal vs Telegram vs WhatsApp

5 | Para reportar en chats

**Para videochamadas ou videoconferências seguras, pode utilizar Jitsi** (https://meet.jit.si/). Esta plataforma é software livre, não requer a criação de um usuarie, nem a instalação de uma aplicação no computador, apenas no dispositivo móvel. Pode adicionar uma senha, desfocar o fundo, partilhar telas, transmitir, etc.

Uma opção para a utilização de e-mails seguros é a encriptação de mensagens e a utilização de chaves de encriptação. No entanto, uma versão rápida e eficaz é o Mailvelope. (https://www.mailvelope.com/). Este software já é de código aberto e encripta o tráfego de correio eletrônico de ponta a ponta dentro de um navegador web. Além disso, pode ser integrado em aplicações de correio eletrônico existentes, tais como Outlook ou Gmail.

Também pode utilizar contas de e-mail seguras, como ProtonMail, o Riseup Email.

### Auto-avaliação sobre o envio seguro de mensagens:

- ◊ Utilizo aplicações seguras com encriptação de ponta a ponta?
- ◊ ¿ Não envio senhas ou conteúdos sensíveis através de aplicações de mensagens de alto risco?
- ◊ ¿ Utilizo nomes de código para os utilizadores das minhas aplicações de envio de mensagens?
- ◊ ¿ Verifico que nenhuma informação de outras pessoas, como fotos, aparece no fundo durante as minhas videochamadas?

## Partilha segura e colaborativa de conteúdos e documentos

Ao partilhar conteúdo, podem ocorrer fugas de informação: dados sobre as pessoas que enviam o conteúdo e também sobre aqueles que o recebem. Um dos primeiros passos antes de enviar documentação ou conteúdo é eliminar meta-dados. Assim, os documentos, se interceptados, não conterão informações que possam identificar locais, pessoas ou dispositivos. Para reduzir o risco ao partilhar fotografias, pode utilizar a aplicação **SendReduced** disponível para Android. Para *iPhone* como o fazer: abra a aplicação, seleccione as suas fotografias, toque no ícone de definições no canto inferior esquerdo e seleccione eliminar todos os meta-dados.

Para enviar documentos de forma segura e com maior privacidade (e também com autodestruição), pode utilizar os seguintes serviços de Rise Up:

- **pad.riseup.net** – editor de texto colaborativo em tempo real com autodestruição programada
- **share.riseup.net** – carregamento de arquivos (pastebin e imagebin)

***Sobre sexting:*** se deseja praticar sexting seguro ou troca de mensagens com conteúdo erótico, recomendamos que utilizasse stickers para cobrir o seu rosto ou qualquer marca no seu corpo com as quais possa ser identificade. Também recomendamos a utilização de plataformas de mensagens que permitam a autodestruição de mensagens. (como Telegram, o Signal) e onde as pessoas que recebem o seu conteúdo não podem realizar capturas de telas nem partilhas delas.

* ***Lembre-se:*** se a sua informação for partilhada sem o seu consentimento **¡Você não tem culpa!** Existem organizações que podem ajudar a remover conteúdos de plataformas onde os seus arquivos foram divulgados. Uma destas redes de apoio é a linha de apoio da organização de direitos digitais Access Now o Acoso.Online.



### Auto-avaliação sobre a partilha segura de conteúdos:

- ◊ Partilho conteúdos e documentos através de plataformas seguras?
- ◊ Descarrego documentos de fontes duvidosas ou de pessoas que não conheço?
- ◊ Descarrego aplicações apenas a partir de sítios seguros, tais como Apple Store o Google Play?
- ◊ ¿ Utilizo alguns rascunhos de meta-dados?

## Utilização segura das redes sociais

De Facebook a TikTok, passando por Instagram, Twitter o Pinterest as redes sociais são concebidas para nos fornecer espaços para "conhecer" as pessoas que nos interessam, atividades e coisas pelas quais somos mais apaixonades. No entanto, é necessário saber que **estas redes se alimentam dos nossos padrões de comportamento e aprendem com eles.** O que é que isto significa? Se curtirmos muitos vídeos de cachorrinhos, é muito provável que a única coisa que as redes nos mostrarão sejam cachorrinhos ou vídeos relacionados com cachorrinhos.¿ O que há de errado com isto? Não há nada de errado com os cachorrinhos. Contudo, à medida que avançamos para o domínio da política ou do nosso ativismo, as redes sociais podem se transformar numa caixa de ressonância para os nossos próprios interesses e assim distorcer as nossas experiências. Também não existe uma fórmula chave para combater a 100% estes algoritmos e as formas como eles aprendem com os nossos padrões de comportamento, mas existe a possibilidade de uma maior consciência da nossa experiência utilizando redes.

De uma perspectiva de *cuidados coletivos digitais*, é importante lembrar que as redes sociais são empresas privadas que procuram lucrar e zelar pelos seus próprios interesses. Assim, pode ver que estão constantemente atualizando os seus termos e condições de utilização. Uma regra geral é ler sempre cuidadosamente antes de dar um "ok" ou "aceitar". Em muitas ocasiões, *as plataformas atualizam as condições de privacidade que afetam a segurança dos nossos perfis*. Por conseguinte, a revisão regular destas condições é de importância vital para o autocuidado em rede.

**Algumas considerações para os usos dos sites de redes sociais mais populares**

| | FB | IG | TW | TK |
|---|---|---|---|---|
| Creación de pseudónimo como usuarie | ✗ | ✓ | ✓ | ✓ |
| Criação de um pseudónimo como usuarie | ✗ | ✓ | ✓ | ✓ |
| Adicionar o seu pronome pessoal ou gênero | ✓ | ✓ | ✓ | ✓ |
| Acrescentar autenticação em duas etapas para início de sessão da aplicação como na Web | ✓ | ✓ | ✓ | ✓ |
| Criar um perfil privado | ✓ | ✓ | ✓ | ✓ |
| Configurações de segurança das suas publicações (quem pode ver a sua publicação, quem pode responder) | ✓ | ✓ | ✓ | ✓ |
| Mensagens efêmeras (mensagens de apagamento automático após um tempo definido) | ✗ | ✓ | ✗ | ✗ |
| Configurações de segurança para a recepção de mensagens (só recebe mensagens de pessoas que segue, ou de pessoas que o seguem) | ✓ | ✓ | ✓ | ✓ |
| Definir a localização das suas publicações | ✓ | ✓ | ✓ | ✓ |
| Rever as mensagens em que está marcado antes de serem publicadas no seu perfil | ✓ | ✓ | ✗ | ✗ |

**FB:** Facebook **IG:** Instagram **TW:** Twitter **TK:** TikTok

### Auto-avaliação das utilizações seguras das redes sociais:

- ◊ Verifico as diferentes configurações de segurança das redes sociais onde tenho um usuarie ou a minha organização tem um perfil?
- ◊ Conheço os mecanismos de denuncia de ataques através das redes sociais?
- ◊ Tenho protocolos de segurança e definições de privacidade actualizadas para as minhas redes e para as redes da minha colectiva?
- ◊ Utilizo a mesma senha de acesso em mais do que uma das minhas redes?
- ◊ Carrego fotografias e conteúdos sem diretrizes de privacidade que poderiam expor outres colegas?

## Desintoxicação digital

"Desintoxicação digital" é o nome que damos às práticas pessoais ou coletivas que nos ajudam a nos desligar das nossas identidades e corpas digitais a fim de salvaguardar a nossa saúde mental, emocional ou física.

A desintoxicação digital pode ser tão simples como desligar o som das notificações nos nossos dispositivos móveis, não verificar os nossos e-mails aos fins-de-semana e até mesmo definir a cor das telas dos nossos telefones a preto e branco para reduzir os estímulos de utilização.

Muitas aplicações, desde a sua criação e desenho, utilizam padrões que nos tornam "viciades" [6] para que a tecnologia seja mais persuasiva na sua dinâmica de utilização. Por conseguinte, é importante reconhecer as utilizações que fazemos das nossas aplicações. As tecnologias não são neutras, elas são concebidas para captar a nossa atenção.

6 | Tecnología persuasiva



### Auto-avaliação:

- ◊ Reconhece os riscos digitais que podem me afetar a mim e à minha organização ou coletivo?
- ◊ Revisa as etapas e práticas do autocuidado digital coletivo quando penso em planejar as atividades da minha organização ou coletiva?
- ◊ Será que procura momentos durante o dia para me desligar do mundo digital e me aterrar no meu presente tangível?
- ◊ Será que adota as tecnologias de uma forma consciente dos riscos para a minha organização, para mim próprie e para os meus colegas?

**Mantra digital de autocuidado a repetir para nós próprias todos os dias**

## »O digital é real«.

## *O autocuidado feminista é colectivo, político, transformador e fortalecedor.*



# conclusões

Com este manual propusemo-nos repensar a noção de segurança digital e transformá-la numa ferramenta feminista para o autocuidado. Reconhecer que o digital é real é reconhecer que o assédio, abuso e violência que são reproduzidos no ciberespaço também são reais. A violência digital não está fora das lógicas (cis) sexista, racista, classista, capacitista e heterocêntrica que permeiam o mundo do tangível. Daí a nossa insistência em mobilizar as estratégias que construímos a partir dos feminismos para proteger as nossas corpas, as nossas coletividades e os nossos ativismos na web. O autocuidado feminista, como mecanismo de autodefesa digital, é uma forma de nos armarmos contra a violência sistemática que nos coloca em risco online.

**Mantermo-nos seguras é uma política feminista de cuidados coletivos**, e é no coletivo que nos situamos para gerar estratégias de autocuidado no ciberespaço. Se o autocuidado feminista envolve uma série histórica de reapropriações políticas, a nossa utilização de ferramentas digitais é também uma reapropriação subversiva. Podemos utilizar e transformar plataformas virtuais mesmo quando funcionam como espaços de reprodução de violência contra corporeidades historicamente violentadas. Ao mesmo tempo em que a tecnologia reproduz os lugares comuns da violência, nós reconfiguramos estes quadros normativos para expandir os nossos espaços de agenciamentos.

Cada vez existem mais ativistas e coletivas que utilizam várias tecnologias para organizar, divulgar informação, denunciar e exigir direitos. Cada vez son mais os movimientos sociales que utilizam o ciberespacio de formas disruptivas para movilizar estrategias de cambio. No entanto, a Internet não está livre de riscos e as vidas des ativistas não estão fora de perigo. É por isso que procuramos gerar redes para democratizar a utilização das tecnologias, reduzindo ao mesmo tempo a possibilidade de danos para aqueles de nós que assumiram o mundo digital em nome da transformação social. Este manual é em si mesmo uma prática de autocuidado digital feminista porque compreendemos que o autocuidado não é possível sem cuidar des outres.

À medida que os ataques hostis de grupos fascistas e antidireitos se deslocam para plataformas virtuais, surgem também novas formas de difundir o discurso do ódio, ameaças e outras formas de violência digital. Daí a importância de conceber instrumentos para ajudar a mitigar os efeitos da vulnerabilidade cibernética. Reduzir os riscos na utilização da Internet equivale a ampliar o âmbito das ações que es ativistas levam a cabo na Internet. Nesse sentido, o autocuidado digital feminista que propomos é também uma forma de ligar o mundo virtual com as transformações do mundo offline.



## Finalmente, enumeramos alguns pontos essenciais para reforçar o autocuidado digital feminista

**_ Reconhecer de onde vêm as tecnologias que utilizamo**s e que meios temos à nossa disposição para transformar as suas utilizações. É possível adaptar a utilização de ferramentas digitais em nosso benefício!

**_ As aplicações e plataformas que utilizamos estão em constante atualização.** Por conseguinte, é necessário rever periodicamente as alterações que podem afetar a minha segurança e privacidade e a do meu grupo. Realizar revisões periódicas das suas práticas. Pode utilizar: https://protege.la/checklists/

**_ Pensando com empatia sobre o outre** e como podem ser afetades pela nossa utilização de alguma forma de tecnologia ou meios digitais.

**_ Nenhuma prática única de cuidados digitais é infalível.** É necessário fazer um compêndio de práticas que, em conjunto, sirvam de escudo para cuidar de nós mesmes e des outres.

**_ Não tenham medo de experimentar novas ferramentas,** mas estejam conscientes das suas limitações e riscos. Faça contato com es colegas que conhecem estas tecnologias e obtenha sempre uma segunda opinião.

# agradecimentos

Este manual é um compêndio de aprendizagem a partir de experiências pessoais e coletivas, bem como uma compilação dos conhecimentos e experiências especializadas de muitas organizações latino-americanas de direitos digitais.
[Ver mapa para saber mais sobre eles].

**Obrigada a todas as pessoas envolvidas na construção deste material.**

» *Ilustrações:*
**Lu Sánchez** – Costa Rica

» *Layout:*
**Cristiana Castellón** – Nicaragua

» *Conteúdo:*
**Selene Yang** – Nicaragua

» *Supervisão do projeto:*
**Rosa Posa Guinea** – Paraguay

» *Edição:*
**Lucía Fernanda Bonilla** – Guatemala

» *Tradução:*
**Verónica Daniela Navarro** – Brasil/Argentina



**Com o apoio de**


# *manual de autocuidados digital feminista*