CARTILHA

SEGURANÇA DA INFORMAÇÃO

Fundo Brasil

SUMÁRIO

ÍNDICE DE BOXES

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

APRESENTAÇÃO

A segurança de defensoras e defensores de direitos humanos sempre foi uma preocupação do Fundo Brasil de Direitos Humanos, desde sua fundação.

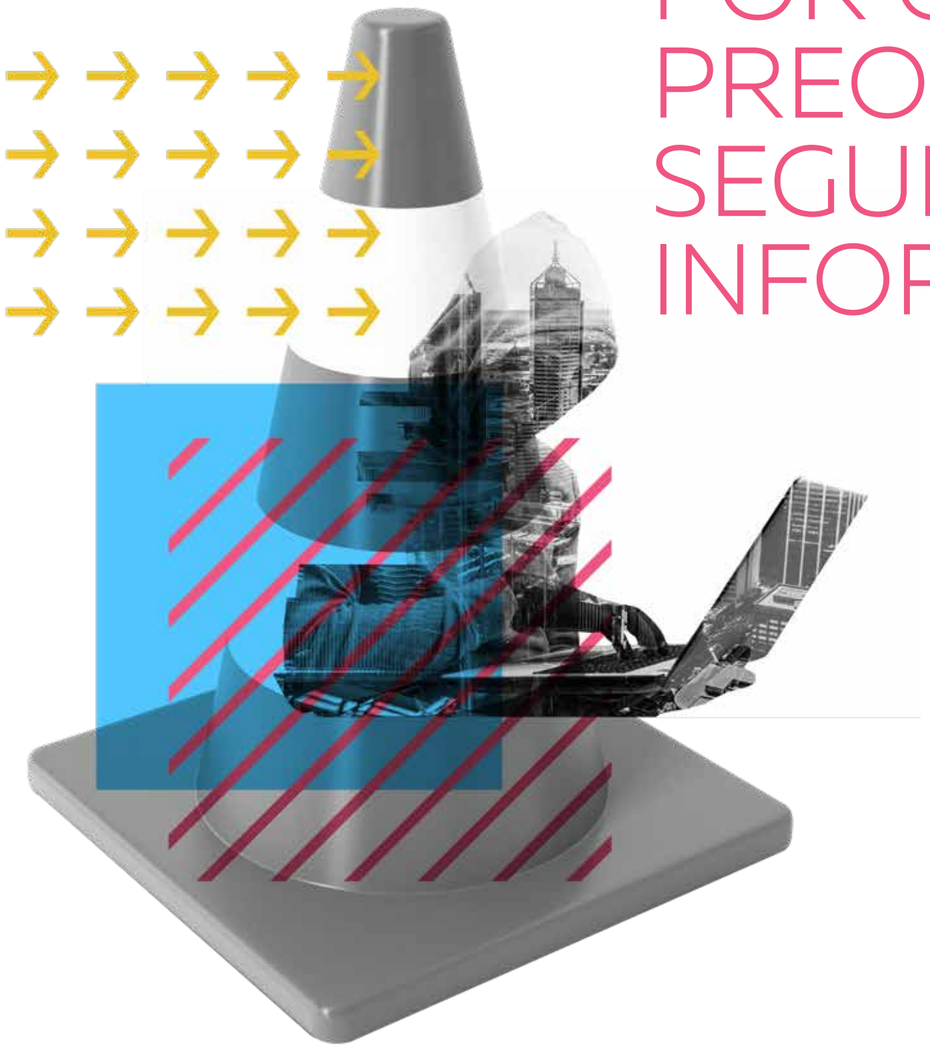
Desde 2018, contudo, o Fundo Brasil desenvolve um programa cujo objetivo é incentivar que a segurança integral seja uma prioridade das organizações de defesa de direitos, a partir do fortalecimento das capacidades de tais organizações. Em 2022, as iniciativas voltadas a defensoras e defensores de direitos humanos já apoiaram mais de 40 projetos de organizações de sociedade civil, além de centenas de pedidos de apoio emergencial - apoios dados à situações envolvendo ameaças críticas a segurança de ativistas e organizações.

O Fundo Brasil lança agora cartilhas cujo objetivo é facilitar o acesso a informações essenciais para organizações da sociedade civil, sobretudo aquelas com menos acesso a recursos, sobre segurança e proteção de sua atuação em tempos de retrocessos em direitos e aumento da violência política.

Essas cartilhas foram desenvolvidas a partir das experiências de apoio e diálogos recentes do Fundo Brasil. Contudo, o debate sobre segurança integral tem longa trajetória. Há um considerável acúmulo de conhecimento sobre o tema disponível, desenvolvido por diversas organizações da sociedade civil. Essas cartilhas querem sobretudo, ser uma ponte entre vocês, interessadas/os em segurança, e quem já vem estudando e atuando nessa área há muitos anos. Elas se pretendem como primeiro passo.

Priorizar e garantir a segurança de defensoras e defensores é uma caminhada constante, tão constante quanto emergência de ameaças contrárias a uma sociedade mais democrática e mais justa.

Esperamos que os materiais aqui disponíveis possam ajudar nesse caminhada.



POR QUE SE PREOCUPAR COM SEGURANÇA DA INFORMAÇÃO?

O Brasil e a América Latina apresentam um dos mais altos números de assassinatos de defensoras e defensores de direitos humanos do mundo. Esse quadro tem se agravado nos últimos anos, seja nas lutas do campo ou da cidade.

Nesse contexto, o debate sobre segurança da informação ganha centralidade. Com a pandemia de coronavírus que atingiu o mundo em 2020, a troca de informações por meios eletrônicos se intensificou e, com isso, mais oportunidades para vigiar, criminalizar ou perseguir ativistas tornaram-se disponíveis. Mencionamos diversos exemplos ao longo deste material.

Esta cartilha quer oferecer, para organizações e movimentos sociais que estão preocupados com a questão da segurança de suas informações, dicas de primeiros passos para aprimorar suas práticas de segurança.

Aqui você vai encontrar sugestões simples que possam criar *camadas de proteção* para sua organização e ajudar vocês a se aproximarem do debate sobre segurança da informação.

Aprimorar suas práticas de segurança é algo que leva tempo e exige esforços coletivos. Aproxime-se, entenda um pouco mais, mude alguns hábitos e, sobretudo, converse com seus parceiros de trabalho ou organizações parceiras sobre ameaças e segurança. Não se preocupe em mudar suas práticas abruptamente, tampouco se apresse para adotar as sugestões aqui contidas. O importante agora é começar essa caminhada.

6 PASSOS PARA AUMENTAR A SEGURANÇA DA INFORMAÇÃO EM SUA ORGANIZAÇÃO

Vamos começar a conversar sobre como você pode adotar algumas medidas que vão te ajudar a incrementar a segurança da informação na sua organização.

SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um desdobramento do tema "segurança" que se dedica a pensar sobre como manter algo ou alguém confortável, sem perigo a sua integridade. No âmbito da informação ela pode ser definida como "a preservação da confidencialidade, integridade e disponibilidade da informação" (HINTZBERGEN, 2018). Em outras palavras, trata-se do ramo da segurança que busca defender as informações pessoais e institucionais de forma que apenas seus proprietários tenham acesso a elas ou quem tenha recebido autorização dessa pessoa. Evitando que outros tenham acesso ou usem essas informações!

Para pensar na segurança das nossas informações é preciso pensar em que informações nós produzimos, guardamos, compartilhamos e quem deve ter acesso a essas informações. Podemos chamar essas informações (relatórios, endereços, documentos pessoais e institucionais, fotos, vídeos, mensagens, e-mails, dentre outras) de dados.

Para mantermos esses dados seguros em um mundo de circulação rápida de informações, a principal ferramenta é a *criptografia*. Criptografia nada mais é do que uma forma de embaralhar as informações de um jeito que só quem está envolvido na comunicação possa ler. Só quem possui as chaves para descriptografar (ou desembaralhar) são as pessoas que deveriam ter acesso aos dados.

Veja o esquema abaixo para visualizar o processo da criptografia:

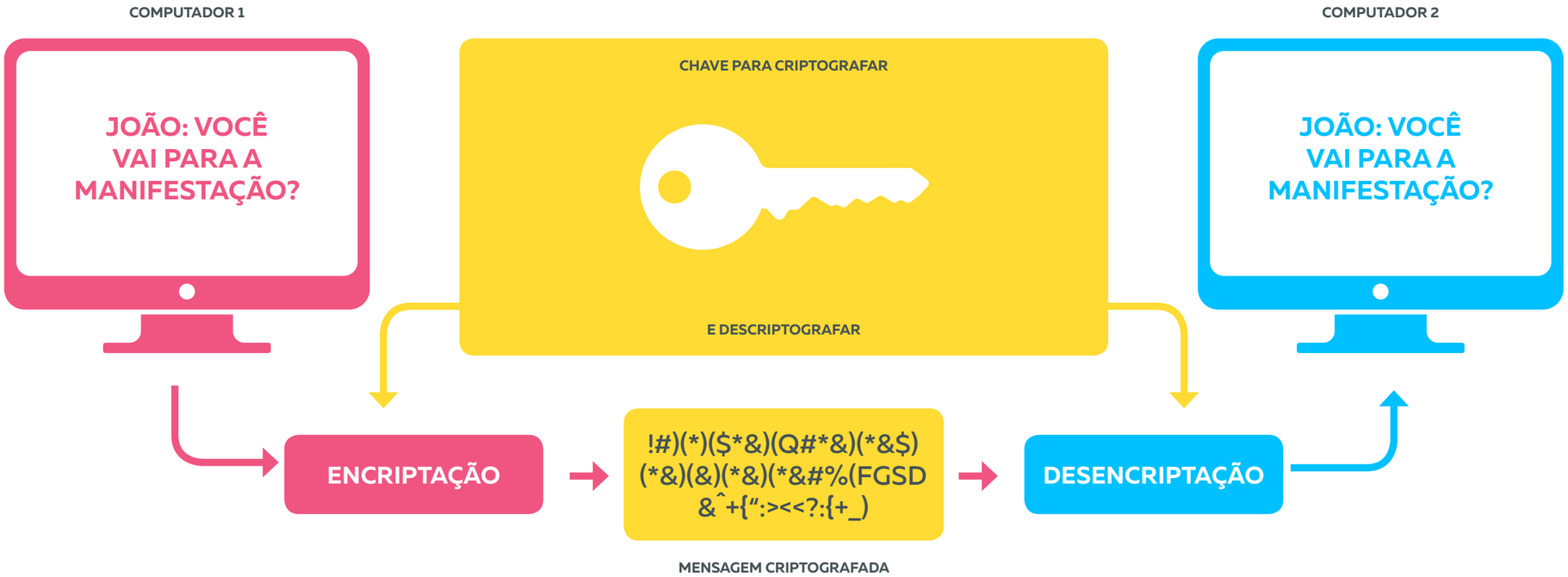


Figura 1 - Criptografia com uma chave (simétrica)

Depois de falar de criptografia, precisamos falar de *metadados*. Os metadados são outro tipo de informação que produzimos e muitas vezes não sabemos ou não damos a devida importância. São informações sobre as informações, por assim dizer.

Parece difícil, mas na verdade não é! Quando você tira uma foto, faz um relatório ou manda um e-mail, o equipamento grava no arquivo informações como lugar, hora e outras informações para que o sistema entenda e saiba o que fazer com ele. Em um e-mail, por exemplo, o servidor grava na mensagem o remetente, destinatário, assunto e outras informações. É importante saber disso porque os metadados não podem ser criptografados, o que exige ainda mais cuidado. Vamos falar mais sobre isso nas nossas sugestões!

Vamos começar?

1 TENHA CÓPIA DE TUDO QUE É IMPORTANTE (BACKUP)

Vamos começar essa pequena lista de medidas básicas com algo que muitos só percebem a importância no momento do aperto: a garantia de acesso às nossas informações.

Um defeito repentino nos equipamentos não é a única possibilidade de perda de informações com a qual você deve se preocupar. Você já ouviu falar em sequestro de dados ou **ransomware**? Acontece quando alguém, através de um vírus, infecta outros computadores e impede que uma pessoa ou uma organização tenha acesso aos arquivos. Para a devolução do acesso, o invasor exige altas somas de dinheiro. Sequestro de dados tem sido cada vez mais frequente. Os atacantes têm escolhido pequenas empresas e organizações na tentativa de extorquir dinheiro ou simplesmente impedir o trabalho desenvolvido.

Em 2019, uma organização de luta pelo direito à terra, localizada na região norte do Brasil, sofreu um ataque desse tipo. Todos os computadores da organização foram paralisados afetando não só os trabalhos, como a saúde mental da equipe. Foram necessários meses de trabalho com o auxílio de parceiros para reestabelecer o funcionamento da organização.

1

Esse tipo de ataque ou defeito inesperado de equipamentos são rapidamente contornados quando a organização possui cópias de segurança de todos os arquivos essenciais ao funcionamento da organização. É o conhecido backup.

Para isso, individualmente é possível usar programas do sistema operacional, programas específicos ou soluções simples como ter um HD externo. Já experimentou fazer uma pesquisa na internet sobre o sistema operacional que você usa (Windows, Mac OS X e Linux são os mais comuns no mercado)? Ele pode ter soluções integradas!

Os backups podem ser realizados em mídias (discos rígidos de computadores, CDs ou DVDs) ou serviços na internet – a chamada "nuvem" - como Google Drive, Dropbox, OneDrive ou um serviço construído pela própria organização.

CUIDADO COM O BACKUP EM NUVEM!!!

Organizações da sociedade civil que trabalham com segurança da informação não recomendam backups em serviços comerciais de nuvem como Dropbox e Google Drive. Empresas como o Google foram protagonistas de um mercado onde ferramentas são oferecidas em troca da coleta massiva de informações de suas usuárias e usuários. Informações que são mercantilizadas e que não se tem certeza o quanto delas estão sendo repassadas para terceiros ou a governos. Além disso, já se sabe que esses serviços "leem" o conteúdo de todos os arquivos salvos em seus servidores. Caso opte pela nuvem, o ideal é que sua organização mantenha sua própria nuvem e seus dados estejam criptografados (ESCOLA DE ATIVISMO, 2018).

Box 2 - Cuidado com o backup em nuvem

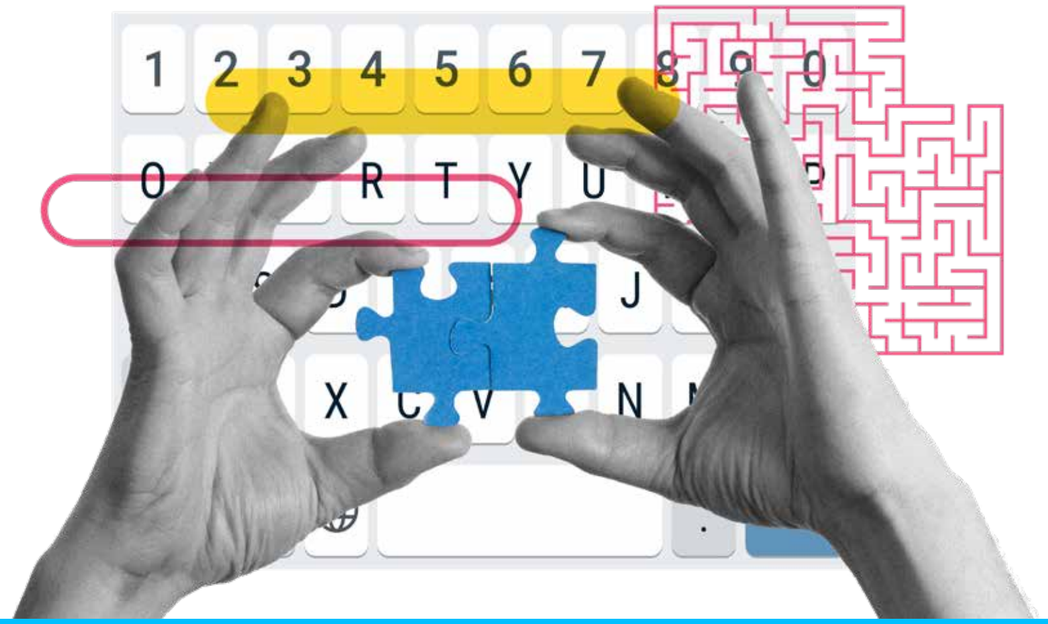
Para as organizações que mantém uma rede interna de computadores, é essencial que não só os computadores como o servidor realizem backups periódicos. Dialogue com o profissional que cuida desses equipamentos para providenciar essas cópias em uma máquina ou em um disco externo da organização.

Já imaginou se aquela organização tivesse um backup de seus arquivos?

2 SENHAS SEGURAS

Todo mundo já ouviu em algum momento que é importante criar senhas mais fortes e todo mundo conhece alguém que usa a mesma senha para todos os serviços que utiliza. Infelizmente cuidados com senhas não são exagero!

Senhas são o mecanismo de autenticação mais utilizado na internet e o fato de você ainda não ter tido problemas não quer dizer que um dia não terá. Pois, junto com o uso dessas plataformas pela sociedade civil, cresceram também os ataques às contas das organizações.



INVASÃO DE CONTAS VISAVA GRUPO DE MULHERES NO FACEBOOK

Em 2018, um grupo no Facebook ganhou notoriedade por mobilizar quase 2 milhões de mulheres contra o candidato da extrema direita à presidência da república do Brasil. O grupo sofreu ataques de hackers que mudaram o nome do grupo e depois o tiraram do ar. Uma das administradoras foi o principal alvo dos ataques e teve suas contas no Facebook e no WhatsApp invadidas. Outras administradoras foram ameaçadas de terem seus dados pessoais vazados (BECKER, 2018).

Box 3 – Invasão de contas visava Grupo de Mulheres no Facebook

Sua organização também usa contas do Facebook, Instagram ou Google para ações institucionais? Você sabia que senhas frágeis podem ser facilmente roubadas e todo seu material publicado em suas contas deletado ou adulterado, prejudicando as ações da organização?

2

FORMAS MAIS COMUNS DE ROUBO DE SENHA (CERT.BR, 2020B)

- **Uso das senhas em computadores infectados, invadidos ou em sites falsos (phishing);**
- **Computador invadido que contenha arquivo com senhas anotadas;**
- **Engenharia social: utilização de informações públicas ou internas da organização (datas ou acontecimentos significativos) para deduzir as senhas.**

Box 4 – Formas mais comuns de roubo de senha

Por isso, criar o hábito de construir senhas fortes é essencial e a primeira coisa é compreender que uma senha forte é aquela que é formada por 12 ou mais caracteres. Dentre eles devem estar letras maiúsculas e minúsculas, números e símbolos aleatórios. Essas senhas podem ser construídas por você (**confira essa sugestão de como criar senhas fortes**), mas também podem ser criadas por aplicativos gratuitos e seguros nos quais você pode guardar todas as suas senhas: um gerenciador de senhas. Esses aplicativos não só guardam suas senhas em um arquivo criptografado, como oferecem a possibilidade de criar senhas fortes para você. Os mais recomendados são as versões do KeePass ou parceiros desse projeto para **Windows**, **Mac** ou **Android**, pois são gratuitos e de código aberto. Outros gerenciadores recomendados são o **Password Safe** e o **1password**.

Outra questão essencial é quem tem acesso as senhas institucionais. Pois, o descontrole sobre essa informação tem aumentado o número de ataques a indivíduos e organizações. Uma senha segura na mão de um profissional que não trabalha mais na instituição reduz drasticamente a segurança dessa senha.

É importante que somente as pessoas que precisam acessar as informações tenham as senhas de acesso institucionais e que estas sejam alteradas periodicamente (semestralmente ou anualmente). Quem realmente precisa ter acesso às contas da sua organização?

Antes de seguirmos para o próximo passo, você precisa saber que no mundo da informação suas senhas valem dinheiro. Isso mesmo, grupos de hackers constantemente invadem servidores e vendem pacotes de senhas e dados pessoais de usuários. Um dos maiores vazamentos de dados da história aconteceu em junho de 2021 e 8,4 bilhões de senhas estavam sendo comercializadas em fóruns de hackers (MENDES, 2021).

DESAFIO: SUAS SENHAS SÃO MESMO SEGURAS?

Entendeu o porquê que você precisa ter atenção com suas senhas? Não? Pois vamos te fazer um desafio, você topa? A Kaspersky Lab, uma empresa internacional de segurança virtual, disponibiliza na internet uma ferramenta que avalia sua senha e informa se ela já apareceu em algum banco de dados de senhas que vazaram. Que tal acessar o verificador de senhas e avaliar suas senhas?

Box 5 – DESAFIO: Suas senhas são mesmo seguras?

3 ESCOLHA UM SERVIDOR QUE NÃO LEIA SEUS E-MAILS E ARQUIVOS (E-MAIL E DRIVE SEGUROS)

Apesar das redes sociais terem deixado o e-mail aparentemente ultrapassado, esse ainda é um dos principais meios de trocas de informações associado com os serviços de armazenamento de arquivos online. É por essas ferramentas, por exemplo, que seguem os relatórios de projetos, por onde se trocam documentos e contratos. Já parou para pensar que podem estar lendo tudo o que você envia ou armazena? Vamos explicar.

A maioria absoluta das empresas comerciais que oferece serviços gratuitos tem sua principal fonte de renda na comercialização dos dados de seus usuários. Todas as informações que você insere em plataformas como Google, Yahoo, Hotmail ou UOL, podem ser vendidas a empresas que buscam vender produtos e serviços. O pagamento pelos serviços dessas plataformas são seus dados.

Além do comércio de dados, há um problema de segurança das mensagens enviadas e arquivos armazenados nessas plataformas. Serviços como o Gmail guardam cópias não protegidas dos e-mails enviados em seus servidores, sujeitas a acesso por invasão, assim como por funcionários e a própria empresa.

Através do *docs* e do Drive, o Google foi um dos principais responsáveis pela popularização das ferramentas de compartilhamento e armazenamento de documentos. Porém, apesar da sensação de segurança que muitos usuários têm com o serviço, já se sabe que o **Google lê todo o conteúdo dos arquivos colocados em seu Drive**, assim como faz no Gmail (MACEDO, 2015). Prática também realizada por seu principal concorrente, o Dropbox. Além disso, não adianta deletar, pois os servidores mantêm cópias dos documentos mesmo após sua exclusão pelo usuário.

3

QUE INFORMAÇÕES SUAS O GOOGLE COLETA? TUDO!

Além ter acesso às suas mensagens e arquivos na nuvem, o Google coleta dados de tudo o que você faz nos demais serviços da empresa. Confira algumas (COUTINHO, 2021):

- Aplicativos abertos no celular Android;
- Anúncios vistos nos aplicativos parceiros da empresa;
- Informações pessoais (senhas ou cartões de pagamento, por exemplo);
- Sua localização e os percursos que faz durante o dia com o celular;
- Permissões concedidas a sites frequentados;
- Informações sobre todos os downloads que você fez;
- Pacotes de dados de sites visitados;
- Pesquisas realizadas no navegador;
- O que for digitado na busca (mesmo antes de apertar 'enter');
- Idioma, preferências, cliques em botões, estatísticas de desempenho e uso da memória (Google afirma que pode compartilhá-las com terceiros)

Box 6 – Que informações suas o Google coleta? TUDO!

O acesso da empresa ao conteúdo dos arquivos dos usuários é muito problemático, em especial para organizações sociais em países que estão passando por crises políticas agudas e avanço da extrema direita. Não é possível ter certeza do quanto de informação é fornecido pela empresa aos governos. Você acha isso improvável? Leia mais sobre o Caso PRISM no box da próxima página e depois pesquise sobre o assunto.

3

CASO PRISM (EUA)

O programa PRISM (CARTA CAPITAL, 2013) foi um acordo sigiloso entre o governo estadunidense e empresas (Microsoft, Google, Facebook, Yahoo!, Apple, YouTube, AOL, Paltalk e Skype) para que estas fornecessem secretamente dados sobre suas usuárias e usuários. Edward Snowden, ex-administrador de sistemas da CIA e ex-contratado da NSA[10], tornou públicos detalhes do programa.

Box 7 – Caso PRISM

METADADOS DO SEU E-MAIL

Os metadados de e-mail (assunto, remetente, destinatário, data e hora de envio) são cruciais para sua funcionalidade mais básica. A criptografia de ponta-a-ponta não inclui essas informações, pois elas precisam ser descriptografadas para que o roteamento adequado ocorra. Isso é uma limitação do sistema de E-mail (PRIVACIDADE DIGITAL, 2021).

Box 8 – Metadados do seu e-mail

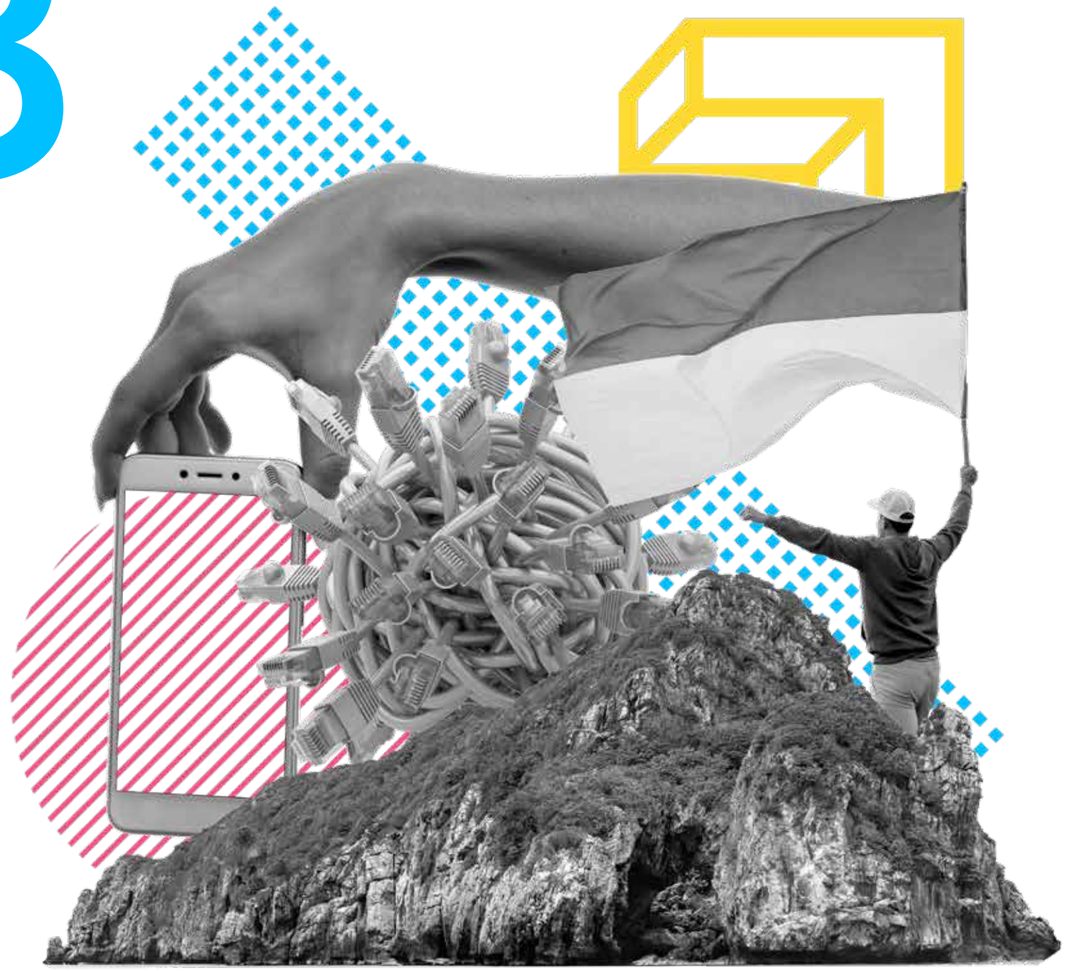
Com relação aos e-mails também é preciso ter atenção ao fato de que as informações básicas de metadados (lembra?) circulam pela Internet, por seu provedor e servidor de e-mail. Você sabia que, com esses dados que todo e-mail possui, é possível saber quem mandou a mensagem, quando, onde, o assunto e para quem mandou?

Como você sabe, toda mensagem de e-mail vem com remetente, destinatário, data, assunto e outras informações. Esse conjunto de informações chama-se "cabeçalho" e, quando a mensagem é enviada, alguns servidores acrescentam a identificação do provedor que enviou e o que recebeu a mensagem (IP de usuários). Informações que podem fornecer até uma localização aproximada dos usuários, que não podem ser protegidas por meio de criptografia e são coletadas de forma ampla.

Algumas pessoas podem achar que estamos falando de uma "teoria da conspiração", mas nos últimos anos mensagens em redes sociais já são utilizadas para criminalizar ativistas. A coleta de metadados de usuários pode ser usada para incriminar ativistas por associação criminosa, assim como foi já foi feito com informações de redes sociais (veja o box sobre a *Operação Firewall2*).

10 A National Security Agency (NSA), maior órgão de dados de criptologia do mundo, é a responsável pela segurança do Estados Unidos da América.

3



OPERAÇÃO FIREWALL 2

Na véspera da partida final da Copa do Mundo de 2014, a Delegacia de Repressão aos Crimes de Informática (DRCI) realizou a operação "Firewall 2" (BARÓN, 2014), decorrente de investigação de possíveis manifestações que poderiam ser realizadas no encerramento do torneio internacional.

A 27ª Vara Criminal do Rio de Janeiro emitiu 26 mandados de prisão contra participantes de protestos tendo como base investigações que traziam como provas mensagens em redes sociais, especialmente o Facebook. Dentre as pessoas detidas estava Elisa Quadros Sanzi, conhecida como Sininho, acusada de ser integrante dos *Black Blocs*.

Box 9 – Operação Firewall 2

Por esses motivos, sugerimos que a organização estimule seus profissionais a utilizarem serviços já existentes de e-mails seguros para tratar de assuntos institucionais ou escolha um servidor seguro de e-mail para criação dos e-mails a serem usados por sua equipe.

As melhores opções são de serviços mantidos por ativistas ou grupos comprometidos com liberdade de expressão e a privacidade dos usuários. Confira o quadro abaixo com algumas sugestões desses servidores e avalie a possibilidade de mudar:

3

Tabela 1 – Servidores com serviço de e-mail seguro

PROVEDOR	ENVIO DE MENSAGENS	ARMAZENAMENTO	OUTRAS INFORMAÇÕES
ProtonMail	Criptografia ponta-a-ponta	Política de zero acesso (e-mails, contatos do catálogo de endereços, e calendário[13] e drive)	Contas com 500 MB de armazenamento para plano gratuito. E-mail de código aberto.
Tutanota	Criptografia ponta-a-ponta	Política de zero acesso (e-mails, contatos do catálogo de endereços e calendários)	1 GB de armazenamento com seu plano gratuito. E-mail de código aberto. O Tutanota oferece uma versão para organizações sem fins lucrativos gratuitamente ou com grandes descontos.
Riseup.net	Necessita de um programa[14] para implementar criptografia ponta-a-ponta	Política de zero acesso (e-mails e contatos de catálogo de endereços)	Endereço de IP não é incluído na mensagem Necessário ter um convite de alguém que já é usuário

13 O Protonmail atualmente possui um aplicativo para calendário (Proton Calendar) em versão para teste. A versão Beta está disponível para Android no Google Play.

14 Sistema de E-mails do Riseup.net não é criptografado de ponta a ponta, para isso é necessário a instalação do plug-in Mailvelope no navegador ou outra solução baseada em OpenPGP.

3

SOFTWARE DE CÓDIGO ABERTO

Qualquer serviço pode afirmar que eles estão criptografando seus dados com segurança ou protegendo suas informações de login. Os especialistas em segurança só podem verificar se essas afirmações são verdadeiras e se não há um jeito de burlar a segurança (backdoor) da criptografia se tudo sobre as informações de segurança (o código do cliente) for publicado como código aberto, se for público (TUTANOTA, 2019). Isto é o que torna um serviço de e-mail e outras ferramentas de código aberto muito mais seguras do que um serviço de código fechado (software proprietário).

Box 10 – Software de código Aberto

UM DRIVE SEGURO E ACESSÍVEL?

Até pouco tempo atrás não existiam serviços gratuitos de armazenamento de arquivos. Recentemente foi lançada uma opção básica gratuita e outras com preços acessíveis e compromisso com privacidade. Em novembro de 2020, o **Protonmail** lançou um serviço de drive que, segundo seus desenvolvedores, "você criptografa seus dados em seu próprio dispositivo antes de enviá-los para nossos servidores seguros, o que significa que não temos a capacidade de acessar seus arquivos" (CRAWFORD, 2020). Em julho de 2021, o **Proton Drive foi liberado para todos os usuários de planos pagos** e no primeiro semestre de 2022 uma versão básica foi liberada para todos os usuários Protonmail.

Box 11 – Um drive seguro e acessível?

Com relação ao armazenamento de informações em nuvem, a melhor alternativa aos serviços gratuitos é a contratação de nuvem privada ou construir uma "nuvem" no servidor da organização com aplicativos como o Nextcloud ou Owncloud. Os aplicativos são gratuitos, mas não existem serviços gratuitos que ofereçam manutenção e os equipamentos para hospedar os arquivos, havendo assim um custo.

Se sua organização não tem condições financeiras e precisa de serviços como o Google, recomendamos realizar uma avaliação cuidadosa dos arquivos que serão armazenados nessas plataformas. Não permita que sejam armazenados nesse serviço documentos que possam causar dano institucional ou a terceiros, assim como comprometer ações estratégicas ainda em construção.

4 PUBLICAÇÕES SEGURAS NAS REDES SOCIAIS

As redes sociais já fazem parte da vida da maioria das pessoas e das organizações e são centrais em suas estratégias de comunicação.

O primeiro risco a ser enfrentado nesse campo é o fornecimento de suas informações a terceiros por essas empresas ou ao Estado (lembra do caso PRISM?).

No caso de uma organização de defesa de direitos, sugerimos ainda que os cuidados se concentrem em não fragilizar defensoras e defensores de direitos, assim como a própria instituição. Isso significa que além de evitar invasões de perfil (ver passo 02), é preciso estar atentas às fragilidades que podem não estão visíveis, mas estão inseridas nas publicações que realizamos nessas redes. Um exemplo é a participação em atos e manifestações públicas. Feita a escolha de publicar informações sobre a participação nesses atos, é comum que se divulguem fotografias tiradas por profissionais da organização que estiveram no local. Entretanto, você sabia que é possível extrair metadados desse tipo de fotos que dizem o modelo do aparelho que tirou a foto, data, hora e localização?

Além dos metadados das fotos poderem expor ativistas, é importante considerar que as próprias fotos podem identificar os participantes do ato. Essas informações, em um contexto de criminalização da luta por direitos, tornam-se potenciais ameaças, pois podem ser utilizadas como provas em processo penal.

COMO PUBLICAR FOTOS SEGURAS NAS REDES?

Você pode extrair metadados com programas próprios. Mas, se você vai tirar fotos do seu celular, é bem mais fácil desligar o wireless, a localização (GPS) e a conexão de dados (3g ou 4g) antes de tirar a foto. Com essas medidas simples, você evita o registro da localização na imagem. Além disso, sempre evite registrar os rostos dos ativistas presentes, seja em primeiro plano ou em segundo plano. Assim as chances de suas fotos serem usadas para incriminar a você ou outra ativista é bem menor.

Box 12 – Como publicar fotos seguras nas redes

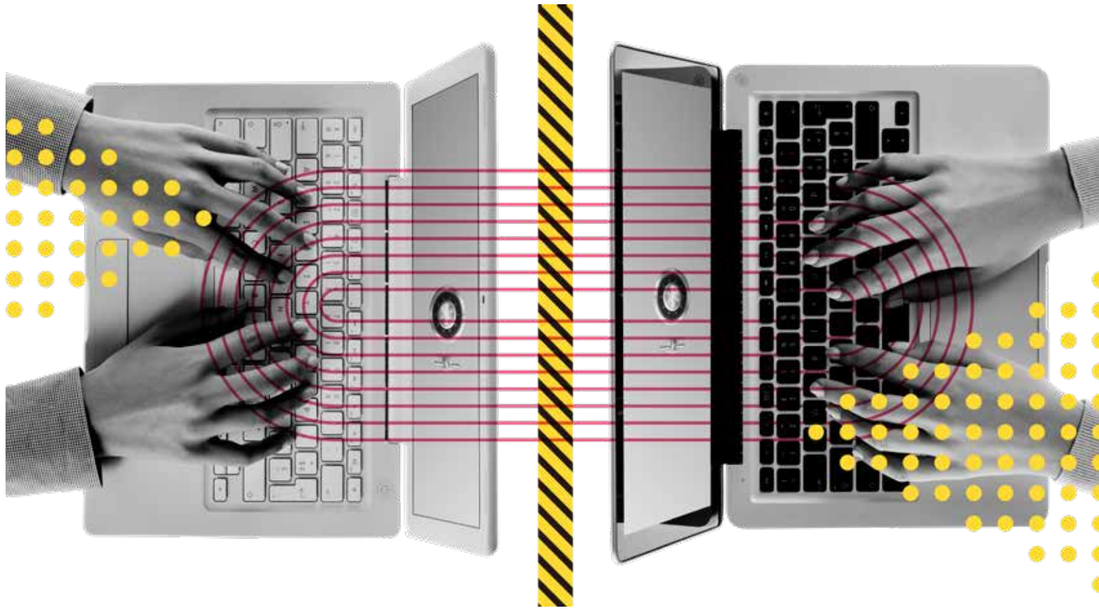
Você acha isso um exagero? Lembre-se que em 2014 publicações de Facebook foram os elementos de prova contra ativistas durante a copa mundial de futebol de 2014 (veja o box *Operação Firewall 2*). Além disso, em diversos estados, participantes das manifestações de 2013 e 2014, foram processados sob a largamente criticada "teoria do domínio do fato".

Segundo essa perspectiva, manifestantes e lideranças eram processadas por qualquer crime cometidos na manifestação, normalmente crime de dano ao patrimônio, sob a alegação de que teriam organizado ou ajudado a organizar o ato.

5 TRABALHO REMOTO NÃO PRECISA SER TRABALHO INSEGURO

Uma das grandes facilidades que surgiram nos últimos anos e foram impulsionadas pela pandemia de Covid-19 são as ferramentas de trabalho remoto e cooperativo. Os mais usados certamente são os aplicativos de armazenamento de documentos, de edição de texto, planilhas, formulários e de realização de reuniões. As ferramentas mais usadas e frágeis são os de servidores e editores de documentos online, sobretudo do Google. Para evitar a exposição de dados dessa plataforma, há a possibilidade de usar os chamados "pads" e "calcs". Esses serviços, como os oferecidos pelo **Riseup.net**, o **hackmd.io** e **Vedetas**, são editores colaborativos em tempo real com formato mais simples, em código aberto e que não exigem cadastro.

Destacamos que essas são alternativas de desenvolvimento coletivo de conteúdo com opções de formatação limitadas. Além disso, o conteúdo é temporário, não sendo armazenado indefinidamente nos servidores desses serviços. O que se torna uma medida de segurança. Proteger as informações em seus relatórios e documentos é tão importante quanto proteger suas trocas de mensagens.



Reuniões virtuais também exigem cuidado. *Zoom* e o *Google Meet* são as ferramentas mais utilizadas no mercado, mas possuem diversos "furos" de segurança. Ambos são softwares de empresas, os dados não são criptografados, há uma coleta massiva de metadados e não sabemos o que essas empresas fazem com os dados coletados de quem participa das reuniões.

No caso do *Zoom*, inclusive, já aconteceram vazamentos de dados de usuários (DEMARTINI, 2020) e em março de 2020 foi revelado que o **aplicativo do Zoom para telefones da Apple estava enviando dados para o Facebook**, mesmo se o usuário não tivesse conta nesta rede social (COX, 2020).

5

SOFTWARE PROPRIETÁRIO

Ao contrário do software livre ou de código aberto, software proprietário é aquele cuja cópia, redistribuição ou modificação são proibidas pelo seu criador ou distribuidor. Normalmente, para utilizar, copiar ou redistribuir, deve-se solicitar autorização ao proprietário, ou pagar para poder fazê-lo (KUSZKA, 2013). No que diz respeito a segurança não é possível para a comunidade internacional auditá-lo e verificar se realmente não há problemas ou caminhos escondidos para vazar informação, pois seus códigos são mantidos em segredo. Exemplos são *Zoom*, *Google Meet*, *WhatsApp*, *Telegram* e outros.

Box 13 – Software Proprietário

Para manter a segurança de suas reuniões a principal alternativa disponível é o **Jitsi Meet**, um serviço focado em privacidade, que dispõe da opção de criptografia ponta-a-ponta; todos os dados dela desaparecem ao fechar a janela da reunião e seu código ainda é aberto. A outra opção, ainda pouco utilizada pela sociedade civil no Brasil, é o **Big Blue Button**, que tem sido utilizado para reuniões com muitos participantes e por ambientes acadêmicos.

Fechando as sugestões sobre trabalho remoto, mais que ferramentas seguras, é essencial adotar boas práticas! Deve-se sempre optar por reuniões com senha e sala de espera para que o organizador da reunião autorize a entrada. Assim como não divulgar os links publicamente e enviá-lo somente para quem for participar da reunião. Essas medidas impedem situações de invasão de reuniões ou o que está sendo chamado de *Zoombombing* (RUPP, 2020).

ZOOMBOMBING

"A principal questão que vem assombrando o uso de serviços de videoconferência, especialmente o Zoom, é o crescimento assustador dos casos de zoombombing: a invasão de salas e a sabotagem de atividades através do compartilhamento de imagens e mensagens nazistas, racistas e LGBTfóbicas. Os principais alvos dos ataques são grupos que trabalham ou que se propõem a debater questões raciais e de gênero, o que indica que as invasões são ações coordenadas que visam ameaçar, intimidar e calar a voz das pessoas que lutam por justiça social. Nas últimas semanas os ataques tem se intensificado, atingindo também o espaço acadêmico, com a invasão de defesas de teses, ou mesmo de aulas." (Para saber como evitar essa prática acesse a íntegra do artigo da Escola de Ativismo sobre Zoombombing)

Box 14 – Zoombombing

6 MANDE MENSAGENS E FAÇA LIGAÇÕES SEGURAS (WHATSAPP, TELEGRAM, SIGNAL E TELEFONIA TRADICIONAL)

Segundo pesquisa sobre o uso de Tecnologia da Informação e Comunicação no Brasil de 2019 (**TIC Domicílios 2019**), 92% das atividades realizadas na internet correspondem o envio de mensagens instantâneas, "seguido pelo uso de redes sociais (76%) e chamadas por voz ou vídeo (73%)." Ou seja, passamos um bom tempo de nosso dia utilizando aplicativos de mensagens.

No Brasil, a pandemia de Covid-19 aumentou o volume já considerável do trabalho da sociedade civil que passa por esses aplicativos, em especial pelo *WhatsApp*. A primeira coisa que precisamos falar sobre a segurança de suas mensagens é algo que você provavelmente já sabe: o WhatsApp e o Telegram não são seguros!

Mas qual é o problema com essas plataformas?

São vários e ao primeiro deles já nos referimos antes: ambos são aplicativos de software proprietário (veja o box *Software Proprietário* no Passo 05), sendo impossível verificar se são realmente seguros. Com relação ao WhatsApp, ainda soma-se o fato de seu **termo de uso prever que o aplicativo pode fornecer informações dos usuários ao Facebook** e outros aplicativos do grupo, como Instagram e Messenger (RODAS, 2021). Isso sem falar que o Facebook já se envolveu em um caso de fornecimento de dados de seus usuários ao governo estadunidense (veja o box sobre o caso *PRISM* no Passo 03).

Algumas organizações tem adotado recentemente o **Telegram** como uma alternativa a eventuais bloqueios judiciais sofridos pelo WhatsApp e porque o aplicativo seria mais seguro. Mas, apesar dessa reputação, ele possui diversos problemas:

PROBLEMAS DE SEGURANÇA DO TELEGRAM

- **Usa um protocolo de criptografia considerado falho por especialistas;**
- **Não oferece criptografia ponta-a-ponta por padrão, apenas no chat secreto (conversas normais e grupos não são seguros);**
- **O chat secreto já foi apontado como falho e possibilitaria que invasores recuperassem mensagens apagadas;**
- **Segundo sua política de privacidade a empresa coleta metadados (endereço IP, os dispositivos e aplicativos do Telegram usados, histórico de alteração de nome de usuário, etc.).**

Tabela 2 – Problemas de segurança do Telegram

6

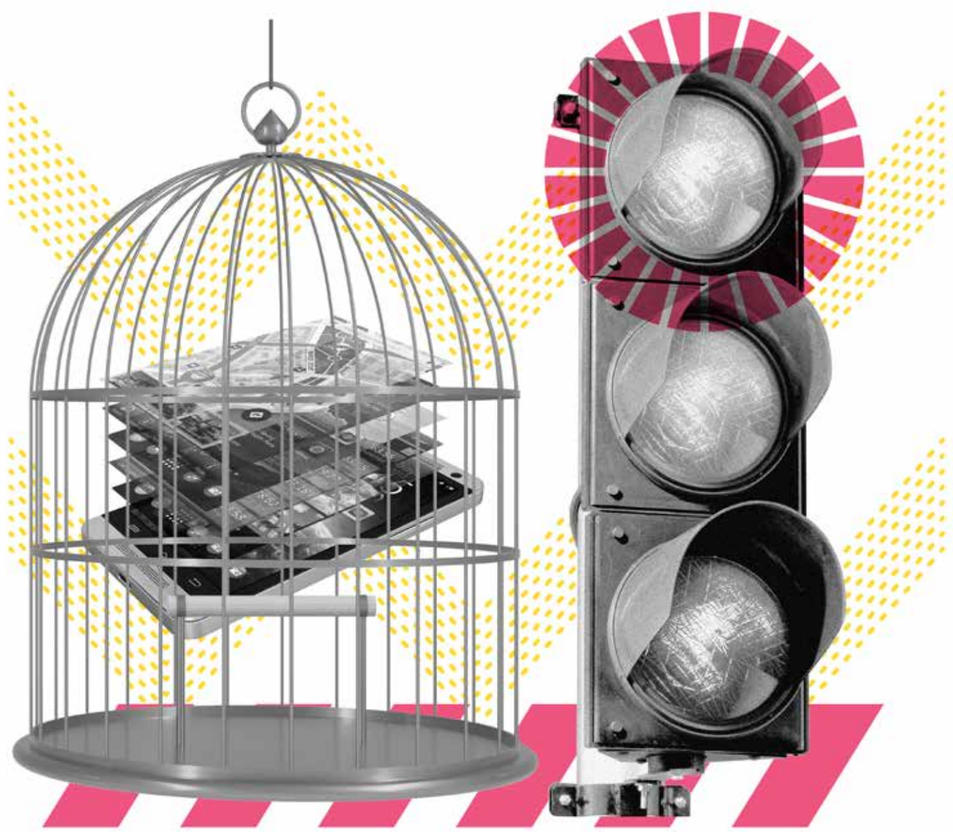
Você ainda acha que dá para usar esses aplicativos para tudo?

Pois bem, você também já deve ter ouvido que a única alternativa segura que dispomos é o **Signal**. Desenvolvido por uma organização sem fins lucrativos, seu diferencial é o cuidado na segurança da informação: criptografia ponta-a-ponta em todas as comunicações. Sendo assim, é o meio ideal para compartilhamento de informações sigilosas, assim como para construção de estratégias pensadas a longo prazo.

CHAMADAS (APLICATIVOS X TELEFONIA)

A CPI dos grampos identificou quase 400 mil grampos legais, sem contar as interceptações ilegais. Trata-se de uma prática difundida no Brasil. Por isso, é importante que as organizações e movimentos sociais considerem que todos os seus integrantes estão grampeados, pois esta é a forma de atuação do Estado brasileiro. Atualmente a forma mais segura de realizar conversas de áudio é fazê-las através do aplicativo Signal, ou, na impossibilidade, pelo Telegram ou WhatsApp. Dessa forma, as informações não serão transmitidas pela rede de telefonia e sim pela internet. No caso do Signal seguirão certamente criptografadas.

Box 15 – Chamadas (aplicativos x telefonia)



Agora que você sabe dos problemas e nós sabemos que há uma dificuldade de migrar repentinamente todas as comunicações institucionais, o que fazer? Que tal experimentar uma forma mais segura sem ter que mudar tudo de repente?

Com a preocupação de ajudar a construir camadas de segurança sem ter que mudar tudo, propomos uma forma de utilização conjunta desses aplicativos onde cada um cumpre um papel diferente[24]. Dê uma olhada:

24 A proposta apresentada aqui foi construída pela cientista da computação, **Nina da Hora**, na formação "segurança digital", ministrada para organizações parceiras do Fundo Brasil de Direitos Humanos. Nina também é pesquisadora da área de tecnologia e se identifica como HackerAntirracista.

PROPOSTA DE USO ESTRATÉGICO DE APPs DE MENSAGENS			
PLATAFORMA	**VULNERABILIDADES**	**COMO USAR**	**EVITE**
WhatsApp	• Código secreto; • Propriedade do Facebook; • Coleta metadados; • Compartilha informações com "parceiros"; • Não confiável.	• Grupos para divulgação de informações superficiais ou públicas; • Informações que não impactem a organização nem os indivíduos.	• Compartilhamento de informações confidenciais e estratégicas; • Senhas, datas, links de reuniões, estratégias, campanhas.
Telegram	• Servidor pertence uma empresa; • Criptografia caseira (não segue padrões internacionais); • Conversas comuns e grupos não criptografados; • Coleta metadados.	• Sempre usar o mecanismo de Chat Secreto – autodestruição de mensagens; • Construção de ações pontuais; • Compartilhamento de datas, links de reuniões, estratégias de curto prazo e campanhas.	• Debate de estratégias a longo prazo; • Chat comum e grupos – não criptografados.
Signal	• Não possui	• Compartilhamento de informações extremamente sigilosas (ex: diálogos entre integrantes da direção, ações estratégicas); • Debates de estratégias a longo prazo • Ligações de áudio e vídeo para dialogar sobre informações sensíveis (localização, ações estratégicas)	

Tabela 3 – Proposta de uso estratégico de apps de mensagens

6

Compartilhamos a opinião de vários profissionais da área de tecnologia de que em breve será essencial para as organizações e movimentos não mais utilizarem o WhatsApp e o Telegram. Entretanto, entendemos que essa transição deve ser um processo gradual no qual as organizações têm um papel pedagógico a cumprir junto à população.

Por fim, com relação a telefonia tradicional, lembramos que a prática da interceptação telefônica (grampo) é uma prática consolidada das forças de segurança e que não existe nenhum controle efetivo sobre ela (veja o box sobre chamadas).

BARRIGA DE ALUGUEL

'Barriga de aluguel' consiste na inserção de linhas telefônicas de pessoas que não são alvos de investigações policiais formais, de forma disfarçada, em pedido de quebra de sigilo telefônico feito à Justiça. Assim, formalmente passa a existir uma autorização judicial para executar a interceptação que, na verdade, é parte de um monitoramento ilegal.

Box 16 – Barriga de aluguel

Assim, considerando a difusão da prática, a facilidade de instalação do grampo e a dificuldade de identificar, sugerimos uma avaliação constante das informações a serem tratadas por meio de ligações telefônicas. Além disso, sempre que possível, utilizar aplicativo Signal para chamadas de áudio onde serão tratadas informações sensíveis.

Quadro resumo

PASSO	MEDIDAS	EVITE
1. Faça Backup	· Realizar cópias periódicas de segurança de arquivos essenciais ao funcionamento da organização; · Utilizar computador, HD-externo ou nuvem da organização;	Backups em serviços comerciais de nuvem
2. Mude sua relação com suas senhas	· Crie senhas fortes: 12 ou mais caracteres (letras maiúsculas, minúsculas, números e símbolos aleatórios); · Adote um gerenciador de senhas; · Defina e restrinja quem precisa ter as senhas de acesso às contas institucionais;	Senhas curtas, relacionadas a eventos conhecidos da instituição e que constam em bancos de senhas vazadas
3. Escolha um servidor que não lê seus e-mails e arquivos	· Adote servidores de e-mails que se comprometem a proteger e não ter acesso a suas mensagens (Política de zero acesso); · Caso seja indispensável, analise a possibilidade de adotar um drive seguro (Proton Drive);	Drives e e-mails de serviços "gratuitos". Inserir informações estratégicas em drives comerciais
4. Faça publicações seguras nas Redes Sociais	· Faça publicações seguras que não expõem informações sobre defensoras/es; · Publique fotos sem metadados de localização e que não identifiquem as defensoras/es que estavam no local;	Inserir informações sensíveis nessas plataformas
5. Trabalho remoto não precisa ser trabalho inseguro	· Utilize "pads" e "calcs", como os oferecidos pelo Riseup.net, o hackmd.io e Vedetas; · Utilize plataformas e práticas seguras para videoconferências (senha, sala de espera, não divulgar publicamente links);	Utilizar serviços "gratuitos" de edição compartilhada de arquivos
6. Mande mensagens e faça ligações seguras	· Use o WhatsApp apenas para grupos de divulgação de informações superficiais ou públicas; · Use o chat secreto do Telegram para construção de ações pontuais e estratégias de curto prazo (indisponível para grupos); · O Signal pode ser utilizado para qualquer troca de informações, sendo ideal para troca de informações sensíveis por texto, áudio ou ligação;	WhatsApp e Telegram para envio de informações sensíveis Ligações pela telefonia tradicional

CONTINUE AVANÇANDO: SUGESTÕES DE MATERIAIS E ORGANIZAÇÕES QUE TRABALHAM NO TEMA

Nessa seção você encontrará alguns links de materiais que vão te ajudar a entender mais sobre o assunto, além de ter acesso a aplicativos ou serviços gratuitos que não estão listados no corpo da cartilha.

A guia de facilitação e aprendizagem em segurança da informação	· Guia elaborado pela **Escola de Ativismo**, em 2018	**pdf**
Cartilha de segurança na internet	· Conjunto de fascículos produzidos pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (**CERT.br**)	**link**
Evelyn.vedetas	· Planilhas editadas colaborativamente on-line, tipo "calc", disponibilizado pela servidora feminista **Vedetas**.	**link**
Guia de proteção e segurança para comunicadores e defensores de direitos humanos	· Guia elaborado pela organização **Artigo 19**	**pdf**
Guia de proteção para defensoras e defensores de direitos humanos	· Guia elaborado pela **Justiça Global**	**pdf**

Guia Prática de Estratégias e Táticas para a Segurança Digital Feminista	· Guia elaborado pelo **CFEMEA** com o objetivo de proporcionar às mulheres maior autonomia e segurança na internet	**pdf**
MariaLab	· Organização "que atua na intersecção entre política, gênero e suas tecnologias".	**link**
Pequeno Guia em PDF para uso do BBB	· Guia em PDF para uso do Big Blue Button, disponibilizado pela organização **MariaLab**	**link**
Safer Nudes	· "Guia Sensual de Segurança Digital" elaborado pela organização **Coding Rights**	**link**
TIC domicílios 2019	· "Realizada anualmente desde 2005, a pesquisa TIC Domicílios tem o objetivo de mapear o acesso às Tecnologias da Informação e Comunicação nos domicílios urbanos e rurais do país e as suas formas de uso por indivíduos de 10 anos de idade ou mais."	**pdf**
Comitê Brasileiro de Defensoras e Defensores de Direitos Humanos (CBDDH)	· "articulação composta por diversas organizações e movimentos da sociedade civil que desde 2004 acompanha atua na proteção a defensoras e defensores de direitos humanos em situações de risco, ameaça, ataque e/ou criminalização em decorrência de sua militância."	**link**

REFERÊNCIAS

BARÓN, Francho. A ordem de prisão de 23 ativistas no Rio desata uma polêmica. EL PAIS Brasil, Rio de Janeiro, 19 jul 2014. Disponível em: <https://brasil.elpais.com/brasil/2014/07/20/politica/1405810378_758119.html> Acesso em: 15 out 2021.

BECKER, Fernanda. Grupo "Mulheres contra Bolsonaro" no Facebook sofre ataque cibernético. EL PAÍS Brasil, 16 set 2018. Seção Brasil. Disponível em: <https://brasil.elpais.com/brasil/2018/09/14/politica/1536941007_569454.html> Acesso em: 8 set 2021.

CARTA CAPITAL. O fim das liberdades civis e a credibilidade de Obama. Carta Capital, 17 jun 2013. Seção Mundo. Disponível em: <https://www.cartacapital.com.br/mundo/fim-das-liberdades-civis-e-perda-de-credibilidade-da-administracao-obama-3352/>. Acesso em: 15 out 2021.

CASTELO BRANCO, Dácio. O que é ransomware? Aprenda tudo sobre a ameaça e como removê-la. Canaltech, 16 set 2021. Disponível em <https://canaltech.com.br/seguranca/o-que-e-ransomware-como-remover/>. Acesso em: 26 out 2021.

CERT.br et al. Cartilha de segurança na internet: Fascículo Backup. CERT.br, 2020a. Disponível em <https://cartilha.cert.br/fasciculos/backup/fasciculo-backup.pdf>. Acesso em: 10 out 2021.

Cartilha de segurança na internet: Fascículo Senhas. CERT.br, 2020b. Disponível em <https://cartilha.cert.br/fasciculos/senhas/fasciculo-senhas.pdf>. Acesso em: 10 out 2021.

COUTINHO, Dimítria. O Google está de olho: saiba quais dados o Chrome coleta sobre você. IG, 20 mar 2021. Tecnologia. Disponível em: <https://tecnologia.ig.com.br/2021-03-20/o-google-esta-de-olho--saiba-quais-dados-o-chrome-coleta-sobre-voce.html>. Acesso 17 out 2021.

COX, Joseph. Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account. Motherboard, 26 Mar 2020. Disponível em: <https://www.vice.com/en/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account>. Acesso em: 03 nov 2021.

CRAWFORD, Douglas. Early access to Proton Drive is here! You can now secure your files with end-to-end encryption. Protonmail, 16 nov 2020. Disponível em: <https://protonmail.com/blog/proton-drive-early-access/>. Acesso em: 03 nov 2021.

DEMARTINI, Felipe. Vazamento de dados do Zoom compromete mais de 500 mil usuários. Canaltech, 14 Abr 2020. Segurança. Disponível em: <https://canaltech.com.br/seguranca/vazamento-de-dados-do-zoom-compromete-mais-de-500-mil-usuarios-163316/>. Acesso em: 15 mai 2021.

ESCOLA DE ATIVISMO. A guia de facilitação e aprendizagem em segurança da informação. Escola de Ativismo, 2018. Disponível em <https://escoladeativismo.org.br/wp-content/uploads/2018/08/AGUIA-DIGITAL-_-V7.pdf>. Acesso em: 15 set 2021.

HINTZBERGEN, Jule et al. Fundamentos de Segurança da Informação: com Base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018, edição Kindle, Cap. 3.1.

JITSI MEET. Disponível em: **<https://meet.jit.si/>**. Acesso em: 15 mai 2021.

KEEPASS PASSWORD SAFE. Disponível em: **<https://keepass.info/>**. Acesso em: 15 mai 2021.

KUSZKA, Boris. O software livre é gratuito? Canaltech. Software. 11 out 2013 **<https://canaltech.com.br/software/O-software-livre-e-gratuito/>**. Acesso em: 03 nov 2021.

MACEDO, Joyce. Privacidade: como deixar de fornecer suas informações pessoais para o Google. Canaltech. Mercado. 23 mai 2015. Disponível em: **<https://canaltech.com.br/mercado/privacidade-como-deixar-de-fornecer-suas-informacoes-pessoais-para-o-google/>**. Acesso em: 03 nov 2021.

TUTANOTA. Medidas de segurança a serem observadas em um serviço de e-mail seguro. Tutanota, 21 nov 2019. Disponível em: <https://tutanota.com/pt_br/blog/posts/secure-email-security-measures/> Acesso em: 01 nov 2021.

MENDES, Felipe. RockYou2021: o que se sabe sobre vazamento de arquivo com bilhões de senhas. Portal UOL, 23 jun 2021. tilt UOL. Disponível em: **<https://www.uol.com.br/tilt/noticias/redacao/2021/06/23/o-que-ja-sabemos-sobre-o-vazamento-de-arquivo-com-84-bilhoes-de-senhas.htm>**. Acesso em: 11 out 2021.

O que é Phishing? Canaltech. Disponível em: **<https://canaltech.com.br/seguranca/O-que-e-Phishing/>** Acesso em: 28 out 2021.

PASSWORD SAFE AND MANAGER. Disponível em: **<https://passwordsafe.app/>**. Acesso em: 15 mai 2021.

PRIVACIDADE DIGITAL. Metadados de Email. Privacidade.digital. 20 Jul 2021. Email Seguro. Disponível em: **<https://www.privacidade.digital/provedores/email/#metadados>**. Acesso em: 01 nov 2021.

RODAS, Sérgio. Nova regra do WhatsApp sobre dados pessoais contraria LGPD, dizem advogados. Conjur, 11 Jan 2021. Disponível em: **<https://www.conjur.com.br/2021-jan-11/regra-whatsapp-compartilhamento-dados-desrespeita-lgpd>**. Acesso em: 03 nov 2021.

RUPP, Isadora. 'Zoombombing'- Sequestro machista de videoconferências tenta calar as mulheres na política brasileira. EL PAÍS Brasil, 19 Ago 2020. Brasil. Disponível em: **<https://brasil.elpais.com/brasil/2020-08-19/sequestro-machista-de-videoconferencias-tenta-calar-as-mulheres-na-politica-brasileira.html>**. Acesso em: 3 nov 2021.

Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2019 [livro eletrônico] [editor] Núcleo de Informação e Coordenação do Ponto BR. -- 1. ed. -- São Paulo: Comitê Gestor da Internet no Brasil, 2020. Disponível em: **<https://www.cetic.br/media/docs/publicacoes/2/20201123121817/tic_dom_2019_livro_eletronico.pdf>**. Acesso em: 15 mai 2021.

Zoombombing - Como evitar e se proteger de um ataque no Zoom. Escola de Ativismo. Disponível em: **<https://escoladeativismo.org.br/como-se-defender-de-um-ataque-no-zoom/>**. Acesso em: 3 nov 2021.

Expediente

Editorial

Edição: Equipe Fundo Brasil

Pesquisa e redação: Alexandre Pachêco

Projeto Gráfico: Brazz Design

Fundo Brasil