CARTILHA

DE SEGURANÇA DIGITAL E ATUAÇÃO NO CAMPO

Pública

Pública

Agência de Jornalismo Investigativo

CARTILHA

DE SEGURANÇA DIGITAL E ATUAÇÃO NO CAMPO

Organização
Thiago Domenici

CARTILHA

DE SEGURANÇA DIGITAL E ATUAÇÃO NO CAMPO

Direção executiva
Marina Amaral
Natalia Viana

Organização e edição
Thiago Domenici

Conteúdo da cartilha
Thiago Domenici
Adriano Belisário
Lucas Teixeira

Colaborações
Ciro Barros
Julia Dolce
José Cícero da Silva

Revisão
Lilian do Amaral Vieira
Ricardo Jensen de Oliveira

Projeto gráfico, ilustrações e diagramação
Caco Bressane

Pública

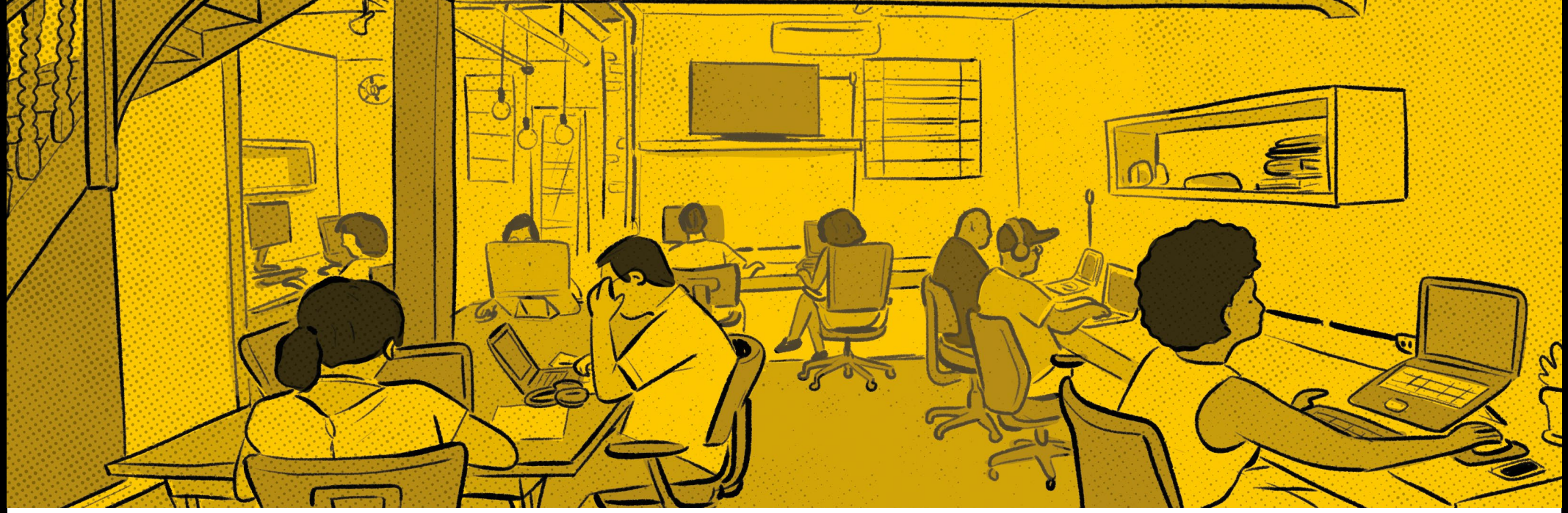
*Esta cartilha foi realizada dentro do projeto Amazônia sem Lei com apoio da **CLUA - Climate and Land Use Alliance** e opiniões aqui expressas não refletem a visão política da CLUA ou de suas afiliadas.*

ÍNDICE

APRESENTAÇÃO

Criada por repórteres mulheres em 2011, a Pública é a primeira agência de jornalismo investigativo sem fins lucrativos do Brasil. Nossas reportagens investigativas são pautadas pelo interesse público e feitas com base na rigorosa apuração dos fatos e na defesa intransigente dos direitos humanos. Em reconhecimento a esse trabalho, somos hoje o veículo mais premiado no Brasil de acordo com o ranking da Jornalistas & Cia de 2019.

Esta cartilha é fruto da nossa experiência ao longo dos últimos anos, sobretudo nas coberturas na região da Amazônia brasileira. Buscamos aqui, compartilhar o que aprendemos em termos de segurança da equipe em campo desde o primeiro projeto, Amazônia Pública, em 2012, até o atual projeto Amazônia sem Lei, que investiga a violência contra as comunidades.



Ao longo desses oito anos, investigamos a questão da propriedade da terra na Amazônia e a resistência dos povos indígenas, ribeirinhos e agricultores familiares contra a espoliação e a expulsão das comunidades de seu território. Mais de 200 reportagens foram publicadas sobre o tema — muitas vezes envolvendo violência, muitas vezes associada ao crime organizado — e, portanto, com situações de perigo para fontes e repórteres.

Dar voz e respeitar o protagonismo dos que vivem na terra, e a ela tem direito, é um compromisso jornalístico que caminha junto com a investigação do poder público e dos interesses privados que ameaçam os direitos humanos e o meio ambiente. Muitas dessas reportagens resultaram em ações efetivas dos poderes Executivo, Legislativo e Judiciário na apuração das denúncias, um resultado importante do jornalismo de impacto praticado pela nossa organização.

Cientes da importância de ter cada vez mais gente trabalhando com esses temas, dividimos aqui nossos protocolos de segurança para nossas equipes de reportagem e para que seu contato com as comunidades não agrave as graves situações de risco que a maioria delas enfrenta. E isso se refere tanto à segurança física no campo como à segurança digital, cada vez mais importante para preservar fontes e informações obtidas da apuração à publicação da reportagem.

A sistematização de fatores como a análise de riscos envolvidos numa viagem e a elaboração de um plano de emergência, bem como o levantamento prévio de informações sobre o trajeto, meios de transporte, locais de hospedagem, fontes locais, contatos de emergência, entre outros, será tratada na primeira parte da cartilha, que fala de segurança no campo.

No segundo bloco, o de segurança digital, disponibilizamos um diagnóstico elaborado pelos profissionais Adriano Belisário e Lucas Teixeira, da *Escola de Dados*, e posto em prática pela **Pública**. Além disso, para todos os casos fomos buscar informações em outras fontes fidedignas para complementar nossa pesquisa.

Por isso, é importante registrar: o material a seguir não tem a pretensão de ser definitivo — nem poderia. Em constante atualização e adaptação às diferentes realidades, este conteúdo é uma contribuição para melhor planejar e prevenir.

CUIDANDO DA SEGURANÇA NO CAMPO

O QUE FAZEMOS É PLANEJAR

Analise o contexto local, avalie as ameaças desse contexto, crie um plano de emergência.

Sem segurança não existe pauta. Ao longo de quase uma década fazendo a cobertura jornalística na Amazônia brasileira, podemos afirmar o que parece óbvio: a segurança começa na produção e pré-apuração das reportagens.

Ao fazerem a análise de ameaças, no campo e digital, a organização e o profissional precisam ter ciência de ferramentas que ajudam nesse processo. Perguntas básicas de planejamento são capazes de prever cenários incertos: "Quem pode me prejudicar?", "O que buscam?", "O que posso fazer se isso acontecer?".

Não é novidade que os conflitos configuram diferentes enredos na Amazônia, mas um problema tão antigo quanto o Brasil é a questão da terra — desde um território indígena demarcado que tem seu espaço invadido pela mineração e o garimpo até um agricultor familiar em disputa com grandes corporações do agronegócio.

Não se pode esquecer que a natureza violenta da ocupação das terras nesse bioma é uma das características da dinâmica do desmatamento que tanto causa indignação e preocupação a quem sabe da importância crucial de a floresta se manter em pé.

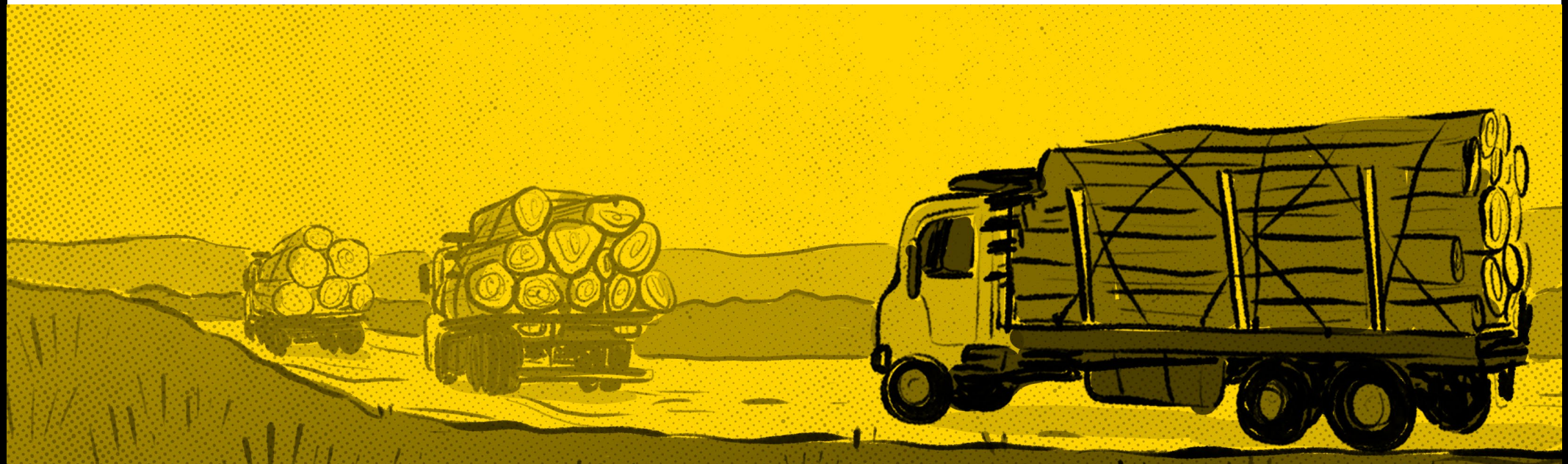
Como nossa cobertura foca em reportagens investigativas, que exigem profundidade e tempo de execução, nosso trabalho é aferir quais são os riscos em nome da melhor informação, da entrevista indispensável, por exemplo, e quais riscos são tão altos que não valem a pena diante dos eventuais benefícios.

Os repórteres precisam saber minimamente o contexto político, social, econômico e cultural de onde estão atuando. A segurança do profissional, assim como a das fontes, deve ser prioridade desde o início do trabalho. Sabemos que o papel do jornalista é evidenciar a história e jogar luz onde há escuridão — mas para isso não se pode tornar a fonte vulnerável, muitas já ameaçada de morte.

É importante conhecer o histórico dos conflitos (são armados ou não?), entendendo as causas (que tipo de pressão é feita?), os personagens (quem é quem no conflito?), a dinâmica e o tipo de disputa (envolve terra, água, alimentação etc.?).

Além disso, quando se está nos locais de apuração, vale a regra básica: ser discreto, não falar do tema em público (no saguão de um hotel, por exemplo), não usar um carro adesivado com o logo "imprensa" ou coisa do tipo, ou seja, ações que atraiam atenção desnecessária.

Para mapear o conflito, não pondere apenas aspectos geográficos, mas leve em conta mudanças de postura de fontes locais, como a mídia regional tratou a questão e se existe algum grau de envolvimento político e/ou policial na história a ser abordada. E sempre que possível estabeleça um canal de comunicação com alguma rede de direitos humanos local que saiba de sua presença.



ASPECTOS RELACIONADOS À SEGURANÇA DIGITAL

- **LIMPEZA**
Ao viajar, limpe informações sensíveis desnecessárias dos dispositivos que serão levados na viagem (celulares e notebook, por exemplo).

- **TECNOLOGIAS DE ATAQUE**
Desligue os dispositivos ao cruzar fronteiras, em especial em regiões que podem ter histórico de emprego de tecnologias sofisticadas de ataques digitais.

- **ANTIVÍRUS**
Instale programas antivírus, antispyware e firewall. Considere a possibilidade de usar software de código aberto (gratuito).

- **SENHAS**
Garanta o uso de senhas seguras nos dispositivos e não guarde arquivos sensíveis na nuvem.

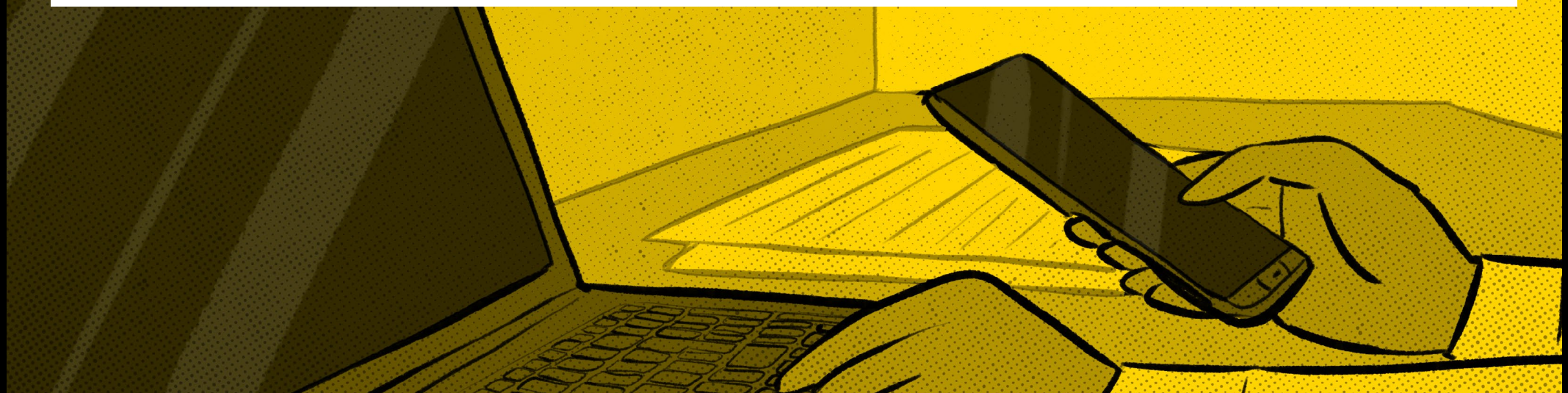
- **CRIPTOGRAFIA**
Garanta que os dispositivos tenham criptografia de disco ativada.

- **PRUDÊNCIA**
Não utilize o celular em situações ou conversas críticas. Deixe-o fora da sala, pois mesmo desligado pode estar espionando você. Carregue um gravador com cartão de memória.

- **PESSOAL X PROFISSIONAL**
O celular da cobertura não deve ser o pessoal, mas um específico da organização para o trabalho. O ideal é não misturar equipamentos pessoais ao viajar (na viagem, se for inviável deixar o celular pessoal de lado, guarde-o em local seguro e pouco acessível).

- **CÓPIA DE SEGURANÇA**
Tenha uma cópia de segurança dos arquivos que serão levados.

- **PROTEÇÃO**
Sempre bloqueie a tela do dispositivo ou computador, que durante a viagem de campo não deve ser o pessoal, com um ou mais método de proteção.



ASPECTOS RELACIONADOS À SEGURANÇA NO CAMPO

- **CONTEXTO**

Na análise de contexto local, leve em conta as questões sociopolíticas (o que há ao meu redor?), geográficas (onde estaremos mais vulneráveis?), atuação (o que vou fazer que pode me deixar vulnerável?).

- **AMEAÇAS**

Avalie ameaças potenciais, de que atores, sempre em conversas com seu contato local (fixer), editor etc.

- **COMUNICAÇÃO**

Crie um plano de comunicação, ou seja, estabeleça diálogo seguro e regular com um aliado confiável local e seu contato na base (na sua redação, por exemplo).

- **FONTES**

Com base em entrevistas e pesquisas de apuração antes da viagem, identifique a confiabilidade de fontes locais, mídia e universidades, polícia e sistema de justiça, governo. Antes de viajar, faça o máximo de contatos e entrevistas que ajudem no processo de identificação mais robusto do conflito.

- **SEGURANÇA**

Certifique-se de que as pessoas com quem você se comunica também adotam procedimentos de segurança e privacidade.

AÇÕES ESSENCIAIS

PROTOCOLO BÁSICO DE ATUAÇÃO NO CAMPO DA PÚBLICA

10 PONTOS DE SEGURANÇA E PLANEJAMENTO

1. EQUIPE

Viaje em dupla, em geral, repórter e fotógrafo/videomaker.

2. CONTATO LOCAL (FIXER)

Busque um guia local de confiança ou contato de movimento social, alguém que atue na região e ajude na articulação, no deslocamento e na logística.

3. PLANO DE VIAGEM

A adoção das medidas de segurança deve ser parte do plano de viagem dos profissionais que fazem trabalho de campo em ambientes de risco. Disponibilizamos nesta cartilha um *plano para ser adaptado à necessidade de cada profissional* ou organização, o que incluiu um plano de emergência com medidas básicas em caso de urgência.

4. VACINAS E DOCUMENTOS

A equipe deve ter a carteira de vacinação em dia para as viagens, assim como a documentação que a identifique para autoridades locais.

5. SEGUROS

A equipe deve ter seguro de saúde, seguro de vida e seguro de equipamentos (câmeras, gravadores, celulares, computadores etc.).

6. TRANSPORTE

"É preciso carro, barco, avião durante a reportagem?"; "Como chegar a determinado destino sem riscos?"; "Quanto tempo vou levar?". Esse planejamento inclui, por exemplo, o modelo de carro, já que ficar atolado em estradas pode ser muito inseguro.

7. DIREÇÃO E DESCANSO

Se a viagem for longa, será fundamental compartilhar a direção; também por isso, as duplas de repórteres são importantes numa viagem que envolve desgaste físico e mental. O descanso físico e mental também deve estar planejado no dia a dia da reportagem.

8. FONTES

Mapeie, com ajuda do guia local, as fontes indispensáveis de ouvir em campo para conseguir um material relevante. Faça perguntas simples: "Quem podemos ouvir pessoalmente em segurança?"; "Quem não podemos ouvir?"; "Que fontes procuramos primeiro, quais deixaremos para o final da apuração?"

9. CONTATO DE EMERGÊNCIA

Sempre deixe com o editor responsável o plano de viagem, além dos contatos de fontes que serão procuradas, guia local e locais de hospedagem. A comunicação entre editor e equipe inclui o envio periódico da localização via GPS (indicaremos ferramentas mais robustas de localização) e comunicação instantânea via Signal.

10. PRIMEIROS SOCORROS

É importante ter noções básicas de primeiros socorros e carregar um kit médico. É recomendável que a equipe tenha participado de cursos que capacitam os jornalistas a trabalhar em zonas de conflito (indicaremos algumas organizações que trabalham com a temática).

NÃO ESQUEÇA DE LEVAR:

- RG e/ou passaporte, original e cópia, com validade mínima de seis meses.
- Cartão com grupo sanguíneo e descrição de alergias para casos de urgência.
- Dinheiro em espécie — há lugares que não aceitam cartão de débito/crédito.
- Pendrives/cartões de memória para fazer cópias de segurança rápidas.
- Carregador de celular universal com adaptador para automóveis.
- Carteira de motorista.
- Guia de localização de ruas e estradas, on-line ou impresso.

EM CASO DE URGÊNCIA OU ATAQUE DIRETO

- Procure um lugar seguro.
- Revise os protocolos de segurança.
- Registre os detalhes do ataque.
- Informe organizações de direitos humanos/ liberdade de expressão sobre a ocorrência com o guia local).
- Faça backup se tiver registros em vídeo, áudio ou fotos do ataque.
- Contate sua organização imediatamente, caso precise de um advogado.
- Acione o seguro de saúde e procure apoio psicossocial e emocional.

CAPACITANDO JORNALISTAS NO CAMPO

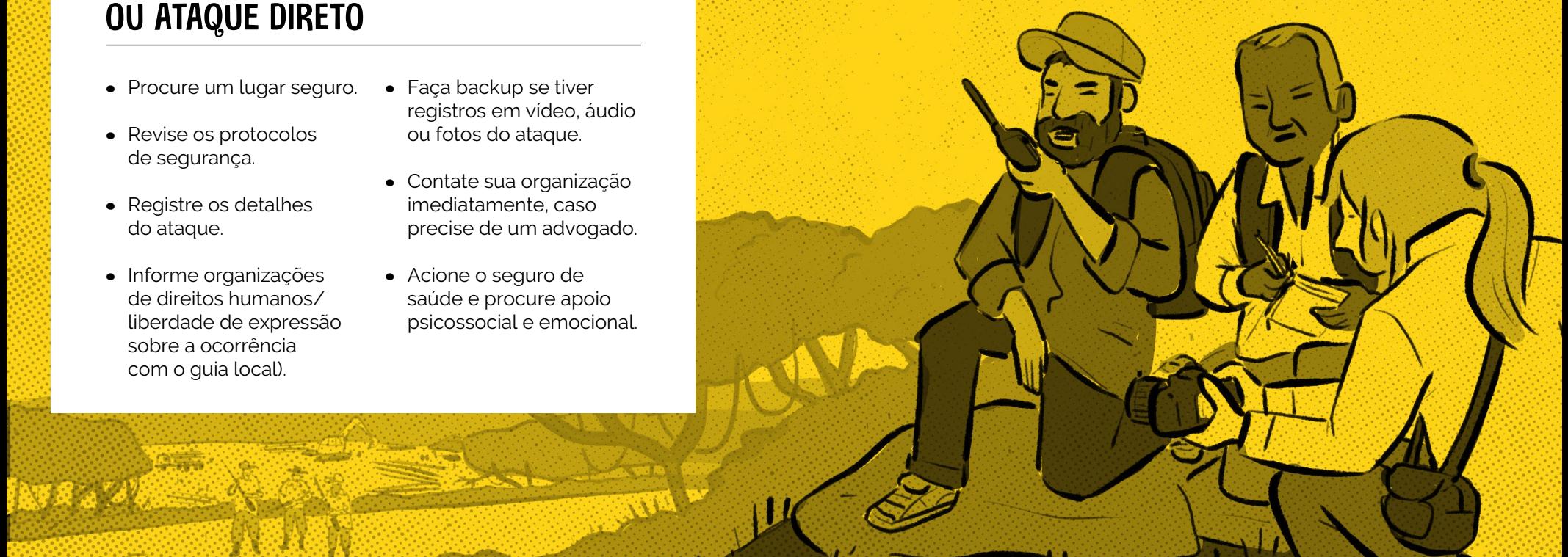
Algumas organizações internacionais oferecem cursos e guias voltados para formação de jornalistas para segurança em ambiente hostil e primeiros socorros.

- *Risc Training*

  Treinamento de jornalistas que trabalham em zonas de conflito e áreas remotas.
- *Repórteres sem fronteiras*

  Guia on-line com dicas práticas para repórteres em zonas de perigo.
- *Option Safety Group*

  Empresa inglesa dedicada à promoção de segurança.



TECNOLOGIA VIA SATÉLITE

Cada reportagem tem uma dinâmica diferente. Os dois sistemas abaixo são recomendados em caso de muitos dias em locais de difícil acesso, com pouco ou nenhum sinal de celular. São mecanismos que permitem o contato imediato, sem depender do sinal da telefonia tradicional:

- *https://www.globalstar.inf.br/*

Existem também equipamentos como o SPOT, que permite rastrear seus bens, enviar e receber mensagens, enviar sua posição GPS e status, marcar seus pontos de referência, acompanhar o progresso da sua rota em plataforma própria e notificar os serviços de busca e resgate em situações de emergência:

- *https://br.findmespot.com/pg/*

ISSO TAMBÉM IMPORTA

Outros materiais
Um bom planejamento leva em conta ainda material de apoio — avalie o que faz sentido em cada situação.


Lanterna


Chapéu ou boné

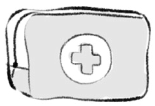

Ferramenta multiuso


Travas de alumínio


Canivete suíço


Manta isotérmica


Cinta para amarração com catraca


Kit de primeiros socorros


Mochila com múltiplos bolsos


Rede de dormir com tela


Tampão para olhos e ouvidos


Talheres portáteis


Soro fisiológico


Protetor solar


Repelente (avaliar com o guia local)

PLANO DE VIAGEM

O plano de viagem pode ser adaptado às necessidades do profissional ou da organização. Lembre-se de levar em consideração os aspectos de proteção das informações apontados ao longo desta cartilha.

DETALHES PESSOAIS

NOME COMPLETO:

NACIONALIDADE:

PASSAPORTE OU DOCUMENTO DE IDENTIDADE:

CELULAR:

TELEFONE:

ITINERÁRIO

LOCALIZADOR DO VOO;ÔNIBUS:

EMPRESA:

DATA:

ORIGEM:

HORA DE SAÍDA:

DESTINO:

HORA DE CHEGADA:

ACOMODAÇÃO

NOME COMPLETO:

TELEFONE:

E-MAIL:

ENDEREÇO:

PESSOA DE CONTATO:

OUTRAS INFORMAÇÕES:

LOCAL DA ATIVIDADE

NOME COMPLETO:

TELEFONE:

E-MAIL:

ENDEREÇO:

PESSOA DE CONTATO:

OUTRAS INFORMAÇÕES:

CONTATO

DETALHES DO CONTATO LOCAIS

ORGANIZAÇÃO OU PESSOA QUE SERÁ O PONTO DE CONTATO LOCAL:

ACOMPANHANTE

CONTATO DE EMERGÊNCIA LOCAL:

AUTORIDADE LOCAL CONFIÁVEL (EMBAIXADA, POLÍCIA, ETC):

INFORMAÇÃO MÉDICA

TIPO SANGUÍNEO:

ALERGIAS:

OUTRAS INFORMAÇÕES:

CONTATOS DE EMERGÊNCIA INDIVIDUAIS

NOME:

RELAÇÃO:

TELEFONE:

CELULAR:

NOME:

RELAÇÃO:

TELEFONE:

CELULAR:

PLANO DE CHECK-IN

QUEM SERÃO AS PESSOAS ENVOLVIDAS NA VIAGEM?

QUANDO ESSAS PESSOAS FARÃO O CHECK-IN?

EM QUAL CANAL DE COMUNICAÇÃO?

QUANTO TEMPO SEM CONTATO PARA INICIAR AS MEDIDAS DE EMERGÊNCIA?

ANÁLISE DE RISCOS

DETALHES DO TRABALHO DE CAMPO

QUAL O PROPÓSITO

QUAIS OS PARTICIPANTES ENVOLVIDOS?

QUAIS OS ATAQUES POSSÍVEIS?

É UM EVENTO PÚBLICO, PRIVADO OU SECRETO?

PLANO DE EMERGÊNCIA

CRIME COMUM

AMEAÇAS
IMPACTO
PROBABILIDADE
PREVENÇÃO (MEDIDAS PARA MITIGAR O RISCO)
MEDIDAS DE EMERGÊNCIA

ANÁLISE DE RISCOS

PLANO DE EMERGÊNCIA

ACIDENTES

AMEAÇAS
IMPACTO
PROBABILIDADE
PREVENÇÃO (MEDIDAS PARA MITIGAR O RISCO)
MEDIDAS DE EMERGÊNCIA

PLANO DE EMERGÊNCIA

CONFLITOS POR CAUSAS POLÍTICAS

AMEAÇAS
IMPACTO
PROBABILIDADE
PREVENÇÃO (MEDIDAS PARA MITIGAR O RISCO)
MEDIDAS DE EMERGÊNCIA

ANÁLISE DE RISCOS

PLANO DE EMERGÊNCIA

VIGILÂNCIA

AMEAÇAS
IMPACTO
PROBABILIDADE
PREVENÇÃO (MEDIDAS PARA MITIGAR O RISCO)
MEDIDAS DE EMERGÊNCIA

PLANO DE EMERGÊNCIA

BEM ESTAR

AMEAÇAS
IMPACTO
PROBABILIDADE
PREVENÇÃO (MEDIDAS PARA MITIGAR O RISCO)
MEDIDAS DE EMERGÊNCIA

CUIDANDO DA SEGURANÇA DIGITAL

APRESENTAÇÃO

Vulnerabilidades de segurança digital são tão comuns quanto desconhecidas pelos usuários menos atentos. De tão indispensáveis, os equipamentos eletrônicos (notebooks, smartphones etc.) se tornarão vulneráveis se a organização e o usuário não criarem o hábito de avaliar a segurança e a proteção de dados periodicamente.

Essas boas práticas no uso dos dispositivos digitais devem ser encaradas como parte fundamental da segurança do trabalho dos jornalistas e demais profissionais da equipe. Listamos a seguir algumas recomendações da Pública.

10 AÇÕES PRIORITÁRIAS

Resumimos 10 ações prioritárias a serem tomadas se sua equipe ou organização ainda não têm um diagnóstico profissional de segurança definido. Ou seja, são recomendações para quem está começando do zero.

1. Formar um posto ou equipe de segurança e resposta a incidentes, responsável por fazer um acompanhamento contínuo e garantir as melhores práticas em termos de softwares, hardwares e hábitos de uso. Pode-se definir de um a três membros com interesse no tema dentro da própria organização ou mesmo optar por um profissional externo.

2. Adotar a autenticação em duas etapas (two-factor authentication, sigla 2FA) de forma universal na organização e, mais urgente, ativar 2FA nos celulares da equipe que utilizam dispositivos de comunicação instantânea, como Signal.

3. Estabelecer um protocolo e uma rotina de criação de cópias de segurança de arquivos e bases de dados (backups), bem como outra de remoção periódica de dados sensíveis dos dispositivos de trabalho da equipe.

4. Recomenda-se que sejam mapeados os dispositivos (notebooks, smartphones) com informações críticas e aqueles mais sensíveis a acessos indevidos para, em seguida, proteger seus arquivos com criptografia de disco.

5. Elaborar um "plano de viagem" adaptado às necessidades da organização.

6. Partir sempre do pressuposto de que o celular é um dispositivo espião por definição: seu uso deve ser evitado caso o profissional queira esconder sua localização ou manter a privacidade das conversas no caso de telefonemas ou mensagens de texto.

7. Orientar os profissionais a respeito da criação de senhas fortes, revisar os acessos da organização e adotar novas práticas, especialmente com pessoas/dispositivos que concentrem informações ou credenciais mais críticas, fortalecendo o uso de chaveiros de senhas, de acordo com os níveis de acesso da equipe.

8. Adotar o uso constante do protocolo HTTPS e uma rede virtual privada (VPN), bem como a inclusão do Tor como opção de navegação, especialmente para investigações sensíveis. A organização deve disponibilizar à equipe computadores com sistemas operacionais orientados à privacidade dos usuários.

9. Adotar a tecnologia PGP (Pretty Good Privacy) para a troca de e-mails.

10. Estimular a prática individual de acompanhamento das informações pessoais expostas no ambiente on-line e buscar remover informações que foram expostas on-line, garantindo configurações de privacidade adequadas em redes sociais, bem como a adoção de configurações de visibilidade restritas nas redes utilizadas para se comunicar com familiares ou compartilhar informações pessoais. Além disso, evitar fornecer informações reais em cadastros on-line ou de endereços para entrega.

SENHAS FORTES PRA ONTEM

O kit básico de qualquer usuário de dispositivo eletrônico vai incluir uma senha que dificulte sua quebra. Por isso, é uma etapa fundamental para garantia da segurança digital.

Devido à grande diversidade e contas em diferentes plataformas é bastante comum a reutilização de mesmas senhas em múltiplos serviços, o que não é recomendado. E o motivo é simples: uma vez vazada a senha, ela pode ser utilizada para acessar outras contas.

Mesmo sistemas e protocolos que estabelecem padrões de senhas — "use minúsculas, maiúsculas, números e caracteres especiais" — não são tão eficazes em face das cada vez mais potentes técnicas de quebra de senhas.

Ainda que um chaveiro de senhas possa ser utilizado para facilitar o acesso a contas digitais, é importante que os usuários dominem a criação de senhas fortes — visto que as credenciais de acessos mais importantes, como a própria senha de acesso do chaveiro, a de inicialização do dispositivo, a do e-mail ou a de criptografia de disco, precisarão ser memorizadas.

Então lembre-se: usar combinações seguras e não repetir senhas é o básico para quem quer evitar grandes problemas.

COMO CRIAR SENHAS FORTES?

Em vez de pensar a senha como uma palavra (password), é recomendável pensá-la como uma frase secreta (passphrase), utilizando no mínimo seis palavras para os acessos mais críticos.

Quanto maior e mais aleatória for a sequência, mais dificuldade uma pessoa ou máquina terá de quebrar a senha. Ao tentarmos elaborar frases secretas, em geral recorremos a formulações já conhecidas, como versos ou letras de música, ou seja, sequências que são expressões ou construções gramaticais comuns, prejudicando assim a aleatoriedade da senha.

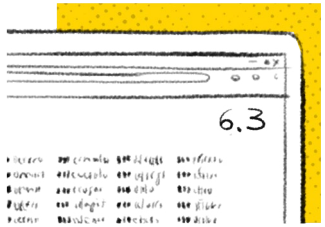
É importante lembrar desta palavra: "aleatoriedade". É nela que mora a força de uma boa senha. Nesse sentido, é recomendável utilizar técnicas que introduzem aleatoriedade no processo. Um exemplo de técnica é o Dadoware (Diceware), método que facilita a construção de senhas complexas.

DADOWARE

Para usar a técnica, basta seguir os seguintes passos.
Para começar, é preciso usar um simulador de um dado on-line, caso não tenha um físico — existem alguns *sites* que fazem o serviço gratuitamente —, para escolher os números que vão resultar em palavras aleatórias. Veja o exemplo:

- Entre no site, jogue o dado. Anote os números. Por exemplo, "6" e "3";

- Abra o *PDF do Dadoware* e, no canto superior direito, busque a página "6, 3". No exemplo, seria a página 33 do PDF;



- Escolha outros três números entre 1 e 6: por exemplo, "2","5" e "4";

- Na página identificada "6, 3", busque a palavra correspondente à sequência "2, 5 e 4". No exemplo, seria a palavra "taba";

- Repita os processos, mudando as páginas, para cada uma das 7 vezes restantes. No exemplo, a senha ficou da seguinte maneira: *"taba porém miudeza fera convite barrela álbum cacho"*

TABA PORÉM MIUDEZA FERA CONVITE BARRELA ÁLBUM CACHO

- Inicialmente, você pode anotar a senha em algum lugar seguro e recorrer a ela, mas deve tentar memorizar a sequência em vez de consultá-la em cada tentativa de acesso. Essas frases fortes podem ser utilizadas como mecanismo de acesso a contas críticas (como o e-mail principal) ou a senha mestra para um chaveiro, do que falaremos a seguir, onde os demais acessos ficam armazenados de forma criptografada.

USE UM CHAVEIRO DE SENHAS

Não é seguro manter senhas anotadas em blocos de nota no celular ou em alguma agenda, post-it ou coisa do tipo. Então, se a sua memória não é aliada, siga os passos abaixo:

Recomendamos o uso do *KeepassXC*, software livre e de código aberto com suporte a todas as plataformas desktop e mobile. É possível utilizar também o *KeepassWeb*, que permite acessar o chaveiro diretamente do navegador, armazenando o arquivo localmente ou por meio de plataformas como o Google Drive ou Dropbox.

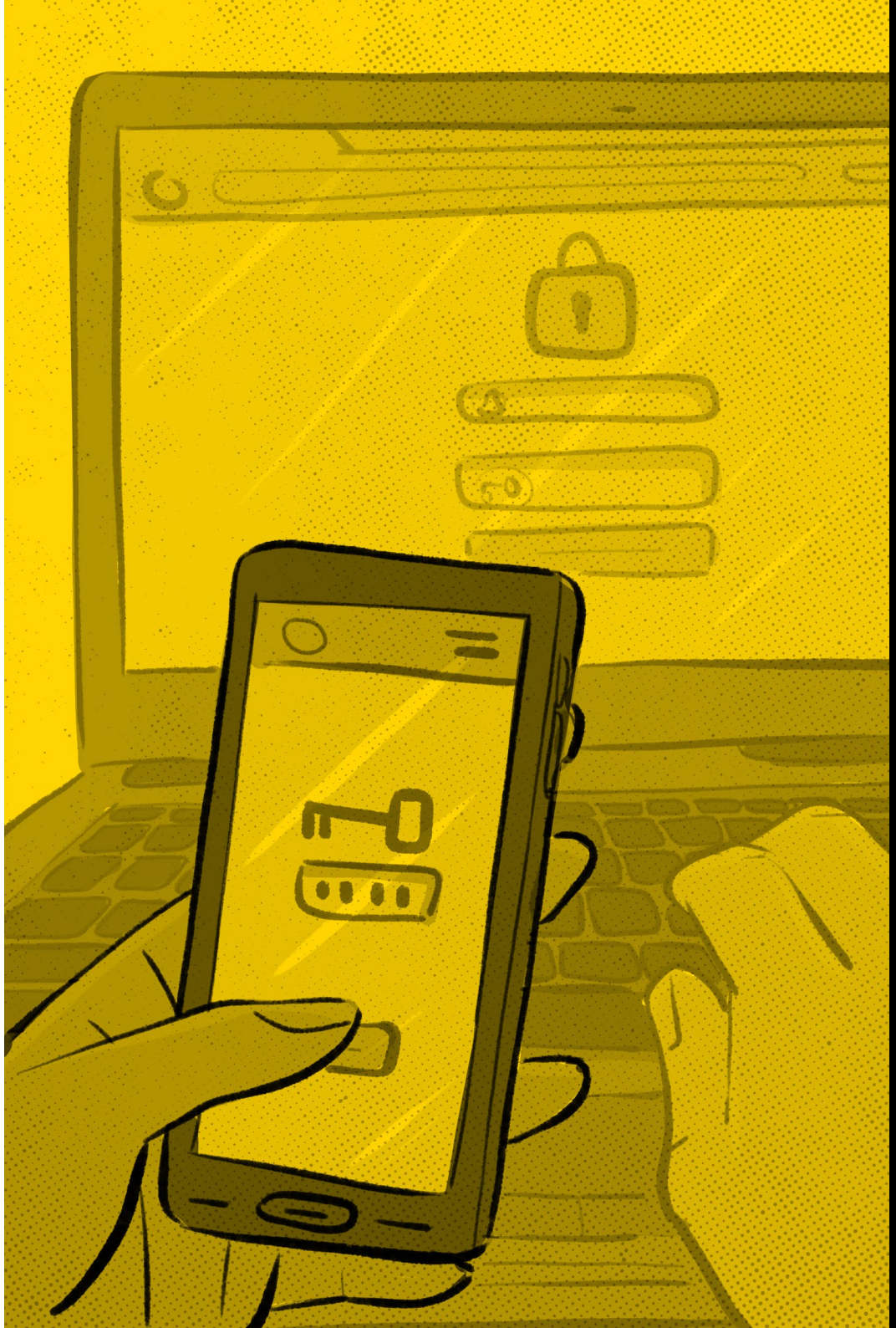
Para as contas institucionais, deve-se apoiar a manutenção de um chaveiro centralizado, compartilhado pelos profissionais e gerenciado de acordo com as necessidades de acesso de cada grupo ou função dentro da organização, por meio de arquivos separados.

Ao mesmo tempo, um chaveiro de senhas traz alguns pontos críticos a serem considerados, como o fato de criar um ponto de armazenamento centralizado, alvo importante para invasores. Por isso, é extremamente importante utilizar uma frase secreta forte como senha do chaveiro e, caso possível, manter o arquivo com as senhas de forma off-line.

DUPLA PROTEÇÃO JÁ

Dupla proteção, autenticação em duas etapas
O uso de senhas fortes têm mais eficácia se associado a essa etapa de segurança: a verificação em duas etapas — 2FA. Ela serve como uma dupla proteção contra invasões. Ou seja, mesmo que a sua senha tenha sido quebrada, o invasor terá mais essa barreira para ultrapassar.

A segunda etapa, geralmente, é um número aleatório enviado por meio de SMS, aplicativos especializados, notificações de push ou chaves de segurança (U2F), para o seu celular. E só a partir deste código único que se torna possível acessar a conta.



PRÓS E CONTRAS

No curto prazo, recomenda-se ativar 2FA para todos os dispositivos individuais ou da organização. No caso de envio de SMS, existe a possibilidade de interceptação — não consideramos o melhor método para 2FA. Em geral, mensagem de SMS é enviada de uma linha telefônica cadastrada no sistema, e a infraestrutura de telefonia no Brasil é particularmente vulnerável e pode ser explorada para interceptar mensagens SMS ou até mesmo sequestrar a linha inteira (o que é conhecido como "SIM Swap"), tanto por vias técnicas quanto por cooperação clandestina com operadoras ou "recuperação" da linha com documentos forjados.

Já o uso de aplicativos especializados — como o *Google Authenticator* ou o software livre *FreeOTP* — para geração dos códigos de autenticação é uma opção mais recomendável. Eles permitem substituir os tokens SMS por códigos temporários gerados no próprio celular, semelhantes aos já muito usados por bancos em pequenos dispositivos.

Essa opção evita as vulnerabilidades da rede de telefonia, permite a instalação em múltiplos dispositivos (útil tanto para uso coletivo quanto para backups) e não necessita de cobertura de celular ou sinal de Wi-Fi após cadastrado — ter um celular dedicado para esse fim e mantido em modo avião, por exemplo, se torna possível.

Para habilitar esse método de autenticação em algum serviço, o usuário utilizará um código QR que transmitirá a chave para o celular. Ela será renovada periodicamente pelo método *Time-Based One Time Password* (TOTP), sem que seja necessário acesso à rede de celular ou dados. Assim, mesmo que alguém tome controle da conta telefônica na operadora, não terá acesso aos códigos de autenticação no celular. É recomendável salvar ou ter uma cópia do código QR mostrado inicialmente, a fim de recuperar os códigos de acesso, caso se perca o celular ou dispositivo utilizado.

Há, ainda, softwares e sistemas operacionais que fazem essa autenticação por meio de notificação *push*, como o Gmail em aparelhos Android e o Apple's Trusted Devices. Ainda que possa ser mais conveniente, essa opção tem a desvantagem de depender de uma conexão com a internet no dispositivo que irá realizar 2FA.

Há um último método de 2FA conhecido como *Universal Second Factor (U2F)*, que consiste em um pequeno dispositivo que deve ser conectado a outro (via USB, NFC, Bluetooth ou outra tecnologia) na hora do acesso.

Essa tecnologia oferece uma vantagem importante em relação aos métodos anteriores: é imune a ataques de phishing, ou seja, quando é criada uma armadilha para que o usuário forneça seus dados para um serviço que parece oficial, mas é controlado pelo invasor. Por outro lado, por se tratar de uma tecnologia nova e em processo de padronização, há alguns pontos a serem ponderados, como o custo do dispositivo e o suporte dos navegadores.

Lembre-se: *é importante nunca compartilhar com ninguém — mesmo que as pessoas se identifiquem como representantes de empresas ou plataformas — códigos de autenticação enviados por telefone.*

A PRIVACIDADE MÁXIMA

CRIPTOGRAFIA SEM MEDO

A criptografia nada mais é do que enviar mensagens sensíveis a grupos ou pessoas que tenham o segredo do cofre.

Como se fosse um cofre com dois segredos, um que tranca e outro que abre os segredos.

A analogia do cofre serve para explicar o complexo sistema de algoritmos matemáticos que codificam dados do usuário para que só o destinatário da mensagem possa acessar o conteúdo.

Não há dúvida de que é um dos melhores métodos para proteger sua privacidade, mesmo em momentos em que você ache que ela não conta.

CRIPTOGRAFANDO SEUS DADOS

Quando se trata dos seus dados, o objetivo principal de criptografá-los — mesmo que você tenha criado um backup ou senhas seguras — é garantir sua privacidade ainda mais, protegendo e assegurando a sua propriedade intelectual.

A criptografia de endpoint, basicamente, adiciona uma camada extra de proteção para as informações confidenciais em seu computador e dispositivos, dados armazenados em mídia removível, como USB, CD, DVD, ou pastas e arquivos específicos.

No Brasil, o acesso indevido ao dispositivo físico que armazena informações (celulares ou computadores, por exemplo) ocorre quando há tentativas de invasão por meio de softwares ou mesmo por meio de roubos, furtos, apreensões judiciais — de modo que é fundamental tomar medidas preventivas para que a pessoa em posse do dispositivo não consiga ler as informações.

Hoje a criptografia de disco já é uma funcionalidade-padrão nos principais sistemas operacionais para celulares com lançamento recente. Para se ter ideia, em caso de perda de celulares Android, é possível tentar localizar e limpar todo o conteúdo do dispositivo remotamente utilizando o serviço "Encontre meu dispositivo". Para dispositivos da Apple, também é possível, porém os usuários devem habilitar essa opção anteriormente.

Opção de programa
O *VeraCrypt* é um programa para Windows, macOS e Linux que faz criptografia em arquivos e discos do computador. O aplicativo é seguro e gratuito para criar arquivos ocultos e protegidos dentro de qualquer volume do sistema operacional, seja do HD ou de dispositivos externos, como pendrives. Há várias opções de criptografia, e sua utilização pode ser obtida em *manuais na internet*. Para macOS, pode-se utilizar o *FileVault*, nativo, que criptografa o disco de inicialização no Mac, também muito seguro.

CRIPTOGRAFIA NAS COMUNICAÇÕES VIA E-MAIL

É recomendável a adoção de tecnologias PGP (Pretty Good Privacy) para a troca de e-mails, tanto internamente quanto com o público externo, quando possível.

O PGP funciona com duas chaves: uma pública, outra privada. Se alguém quiser enviar algo para você, terá de usar a pública e ter uma cópia dela para esse envio. A chave que abre a informação é privada, só você a tem.

Recomenda-se considerar a adoção de soluções de código aberto que permitem a troca de e-mails criptografados dentro do próprio Google Suite, como o *FlowCrypt*.

No longo prazo, visando reduzir ainda mais a vigilância corporativa, é possível a migração para serviços alternativos como o *Protonmail*, que já oferece um sistema nativo e acessível de ferramentas de e-mail criptografado.

Outra possibilidade é utilizar um cliente de e-mail instalado no próprio computador, o que apresenta a vantagem de fazer cópias de segurança locais das mensagens. Nesse caso, recomenda-se a adoção de clientes de e-mail como *ThunderBird*, que suporta a tecnologia PGP por meio do plugin Enigma.

Com o objetivo de facilitar a comunicação de forma segura entre os jornalistas e o público, é recomendável a disponibilização da chave pública e *fingerprint* de cada profissional em locais apropriados, como no perfil do Twitter ou na página com a biografia de cada um.

NAVEGAÇÃO ANÔNIMA

Sem rastros de navegação
A fim de evitar o acesso ao histórico e conteúdo da navegação dos usuários por terceiros, recomenda-se implementar práticas de navegação orientadas à privacidade: a chamada navegação anônima, ou seja, que não deixa rastros.

HTTPS, por exemplo, é uma camada adicional de segurança que permite que os dados sejam transmitidos por meio de uma conexão criptografada.

Por isso, pode-se utilizar a navegação associada a um plugin *HTTPS Everywhere* — elaborado pela *Electronic Frontier Foundation* — para garantir conexão HTTPS como padrão em todos os sites.

Outra boa opção nesse sentido é o *Brave*, um navegador de código aberto focado na privacidade do usuário que já habilita automaticamente o HTTPS e fornece outras proteções a fim de garantir o anonimato dos usuários, como a possibilidade de o usuário se conectar à *rede Tor*, uma rede voluntária global que busca embutir a proteção à privacidade e a segurança na internet a partir do próprio protocolo.

O *Tor Browser* é que permite navegar na web por meio da rede Tor. Ele é gratuito e oferece um excelente grau de proteção, mas tem a desvantagem de ser lento.

Ao contrário da "aba anônima" ou "incógnita" dos navegadores comuns, que somente apagam seus rastros locais, o Tor é focado em permitir acesso à internet sem deixar rastros identificáveis tanto na máquina quanto nos sites acessados, contendo diversas modificações úteis do Firefox, além de anonimizar o endereço IP.

O Tor também acessa sites na "*rede onion*" (popularmente associada à deep web), que mantém o anonimato do próprio site acessado, fortalece ainda mais a segurança da conexão e é usado, por exemplo, no sistema de recebimento de vazamentos *SecureDrop* e como espelhamento de plataformas web e agências de jornalismo para prover acesso a locais sob censura ou vigilância.

O Tor funciona também em celulares e dispositivos móveis, por meio do *Orbot* (Android) e o *Onion Browser* (iPhone). Baixe sempre os arquivos do site oficial (*Tor Project*).

COMUNICAÇÃO INSTANTÂNEA

Fortalecer práticas de segurança na comunicação interna e externa
Para chamadas de voz, é recomendado o uso de soluções de VoIP (voz sobre IP) com criptografia ponta a ponta, tal como o WhatsApp, Telegram ou Signal

O uso do *Signal* como plataforma de comunicação interna em tempo real é positivo, mas é importante ressaltar que essa medida precisa ser acompanhada de outras, a fim de garantir segurança à comunicação.

O uso do Signal por si só não impossibilita o acesso indevido às mensagens trocadas por meio do chat, visto que, se os usuários adotarem práticas de segurança fracas em relação aos seus dispositivos pessoais, o conteúdo poderá ser exposto.

Por isso, é preciso que cada profissional faça a ativação de *verificação em duas etapas do Signal*. Além disso, cada usuário deve seguir os protocolos de criptografia de disco e o uso de senhas e métodos de bloqueio de tela já recomendados. No caso da comunicação com fontes, é preciso uma avaliação de risco caso a caso.

Não se esqueça de estabelecer uma periodicidade para a remoção do histórico das mensagens através de chats efêmeros — o Signal possibilita a configuração dessas mensagens de 5 segundos a semanas — ou manualmente, deletando as conversas.

ISSO TAMBÉM IMPORTA

• RESTRINGIR ACESSOS A INFORMAÇÕES SENSÍVEIS VIA REDES SOCIAIS

A publicação espontânea em redes sociais é um dos principais vetores de disseminação de dados e informações sensíveis que podem ser utilizadas em ataques on-line, engenharia social e campanhas de difamação. Cabe aos usuários prestar atenção e garantir a configuração adequada de privacidade em redes sociais.

• RECONHECER E REDUZIR A DISPONIBILIZAÇÃO DE INFORMAÇÕES PESSOAIS

A utilização de informações pessoais da pessoa-alvo é fundamental para diferentes maneiras de ataques cibernéticos, como a exposição pública de informações sensíveis (*doxxing*), que é uma das mais recorrentes formas de ataque a jornalistas em ambientes digitais. Ou, ainda, o *phishing* e a engenharia social, um dos mais antigos e eficientes métodos de ataque digital.

Para prevenir esse tipo de ataque, pode-se adotar uma prática de redução de danos, controlando quais tipos de informação são expostas, e identificação de dados já públicos, seguida da solicitação de remoção ou adequação das práticas de segurança, caso a exclusão seja impossível.

Isso pode ser feito de forma automatizada por meio de serviços de alerta, que notificam o usuário caso algum termo apareça na web. O Google Alerta oferece uma boa solução gratuita para acompanhar a maior parte das páginas na web. Para um monitoramento mais completo, sugere-se também utilizar a função *'My Alerts' do Pastebin*, que é um famoso serviço de postagem anônima em que recorrentemente são publicados vazamentos de dados. O serviço permite o monitoramento de até três palavras-chave gratuitamente, porém exige registro.

É recomendável que cada pessoa faça uma busca por dados sensíveis, a fim de reconhecer e — quando possível — solicitar a remoção de páginas que contenham tais dados pessoais, tais como nome completo, CPF, telefone e endereço.

O Google tem uma política de remoção de conteúdo que permite a solicitação de retirada de informações do seu motor de busca que contenham os seguintes dados:

- números de identificação nacional, como CPF ou RG;
- números de contas bancárias;
- números de cartões de crédito;
- imagens de assinaturas;
- imagens de nudez ou de sexo explícito enviadas ou compartilhadas sem seu consentimento;
- registros médicos pessoais confidenciais.

Para solicitar a *remoção de dados no Google*, é preciso preencher um formulário. É possível solicitar também a exclusão de dados diretamente em alguns sites que hospedam automaticamente informações pessoais, a partir de dados públicos, como o registro de pessoas jurídicas.

É o caso, por exemplo do *Escavador* e do *CNPJReceita:* uma vez que seja localizada a página de perfil, há na página uma opção para solicitar sua remoção. Já o *CNPJ.biz* exige que a solicitação seja feita por meio de um formulário de contato.

CAPACITANDO JORNALISTAS EM SEGURANÇA DIGITAL

Algumas organizações oferecem cursos e guias voltados para formação de jornalistas para segurança digital.

- **ARTIGO 19**
  Guia de proteção e segurança para comunicadores e defensores de direitos humanos.

- **ABRAJI, OAB E OBSERVATÓRIO DE LIBERDADE DE IMPRENSA**

  Cartilha sobre medidas legais para a proteção de jornalistas contra ameaças e assédio.

- **REPÓRTERES SEM FRONTEIRAS**
  Guia de segurança digital.

- **ACCESSNOW**
  A *Linha de Ajuda* em Segurança Digital da Access Now trabalha com indivíduos e organizações em todo o mundo para mantê-los seguros on-line.

FONTES CONSULTADAS

1. Para mais detalhes sobre o funcionamento e instruções sobre a ativação, confira:
   - https://support.google.com/googleplay/answer/2812853?hl=pt-BR
   - General > Softwares updates > Automatic updates
   - Confira através do menu localizado em Preferências do Sistema > Segurança e Privacidade > FileVault
   - Confira através do menu localizado em Segurança > Configurações
2. https://www.google.com/android/find
3. E m 2016, o Lookout atuou em parceria com o Citizen Lab na análise técnica do Pegasus, aplicativo de espionagem altamente sofisticado e comercializado pelo NSO Group. Fonte: https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
4. https://support.microsoft.com/pt-br/help/4028544/windows-10-turn-windows-defender-firewall- on-or-off
5. https://support.apple.com/pt-br/HT205362
6. https://vallumfirewall.com/
7. https://www.murusfirewall.com/
8. https://www.av-test.org/en/antivirus/
9. https://ssd.eff.org/en/playlist/journalist-move#your-security-plan
10. https://www.kaspersky.com.br/home-security#all
11. https://www.lookout.com/products/mobile-endpoint-security
12. https://support.apple.com/pt-br/HT201642
13. https://play.google.com/store/apps/details?id=eu.faircode.netguard
14. https://play.google.com/store/apps/details?id=app.greyshirts.firewall&hl=en
15. https://objective-see.com/products/lulu.html
16. https://tinywall.pados.hu/

17. https://www.glasswire.com
18. https://www.sophos.com/en-us/products/free-tools/sophos-xg-firewall-home-edition.as px
19. https://www.sophos.com/en-us/products/next-gen-firewall/tech-specs.aspx
20. https://www.instructables.com/id/Raspberry-Pi-Firewall-and-Intrusion-Detection-Syst/
21. https://owncloud.com/
22. https://takeout.google.com/settings/takeout
23. https://helpdesk.rsf.org/digital-security-guide/clouds/
24. https://www.duplicati.com/
25. https://play.google.com/store/apps/details?id=com.koushikdutta.backup&hl=pt_BR
26. https://bvckup2.com/
27. https://www.cobiansoft.com/index.html
28. https://www.ascomp.de/index.php?php=prog&prog=backupmaker
29. https://support.apple.com/pt-br/HT201250
30. https://support.google.com/android/answer/2819582?hl=pt-BR
31. https://support.apple.com/pt-br/HT203977
32. https://meet.jit.si/
33. https://pastebin.com/alerts.php
34. https://f-droid.org/en/packages/dk.jens.backup/
35. https://www.wondershare.com/iphone-backup-and-restore.html
36. https://www.bleachbit.org/
37. https://www.ccleaner.com
38. https://play.google.com/store/apps/details?id=com.piriform.ccleaner&referrer=utm_source=piriform_android&utm_medium=playstore-link&utm_campaign=ccleaner-android
39. https://www.wondershare.com/pt-br/ios-data-eraser.html
40. https://www.panfone.com/ios-eraser/
41. https://ssd.eff.org/pt-br/playlist/jornalista-em-viagem#tutorial-como-deletar-dados-de-maneira-segura-no-macos
42. https://ssd.eff.org/pt-br/playlist/jornalista-em-viagem#tutorial-como-deletar-dados-de-maneira-segura-no-windows
43. https://debian.org
44. https://ubuntu.com/
45. https://tails.boum.org/index.pt.html
46. http://send.firefox.com
47. https://www.qubes-os.org/intro/
48. https://www.google.com/alerts
49. https://support.google.com/legal/troubleshooter/1114905#tss&ts=1115655%2C6034194%2C128 2865
50. https://www.escavador.com/
51. http://www.cnpjreceita.com
52. https://www.facebook.com/settings?tab=privacy
53. https://www.facebook.com/help/325807937506242
54. https://www.facebook.com/settings?tab=facerec
55. https://help.instagram.com/196883487377501
56. https://www.mailinator.com
57. https://www.guerrillamail.com/pt/
58. https://temp-mail.org/pt/
59. https://helpdesk.rsf.org/digital-security-guide/encryption/tools-and-services
60. https://pt.wikipedia.org/wiki/Pretty_Good_Privacy
61. https://chrome.google.com/webstore/detail/flowcrypt-encrypt-gmail-w/bnjglocicdkmhmoohhfkfk bbkejdhdgc
62. https://protonmail.com/pt_BR/
63. https://www.thunderbird.net/en-US/
64. https://enigmail.net/index.php/en/
65. https://securedrop.org/
66. https://www.globaleaks.org/pt-br/
67. https://onionshare.org/
68. https://share.riseup.net/
69. https://nextcloud.com/
70. Contra ataques DDoS, especificamente, porém, vale conferir este programa do Google que oferece proteção gratuita para veículos de imprensa: https://projectshield.withgoogle.com/landing
71. https://www.veracrypt.fr/en/Downloads.html
72. https://www.random.org/dice/
73. https://github.com/thoughtworks/dadoware/blob/master/livreto/dadoware-lista.pdf
74. https://web.archive.org/web/20170116234330/https://antivigilancia.org/pt/2015/11/um-chaveiro-para-sua-v ida-online/
75. https://www.eff.org/pt-br/https-everywhere
76. https://openvpn.net/
77. https://ssd.eff.org/pt-br/module/como-utilizar-o-keepassxc
78. https://authy.com/blog/understanding-2fa-the-authy-app-and-sms
79. https://www.yubico.com/authentication-standards/fido-u2f/
80. https://duo.com/product/multi-factor-authentication-mfa/authentication-methods/u2f-and-biometrics
81. http://brave.com
82. https://protonvpn.com/
83. https://www.torproject.org/download/
84. https://securedrop.org/
85. https://en.wikipedia.org/wiki/Facebookcorewwwi.onion
86. https://open.nytimes.com/https-open-nytimes-com-the-new-york-times-as-a-tor-onion-service-e0d0b67b7482?gi=c894ad179ae7
87. https://www.eff.org/privacybadger
88. https://github.com/gorhill/uBlock
89. https://adblockplus.org/pt_BR/android
90. https://helpdesk.rsf.org/digital-security-guide/
91. https://artigo19.org/
92. https://www.eff.org/deeplinks/2017/11/how-debug-your-content-blocker-privacy-protection
93. https://unesdoc.unesco.org/ark:/48223/pf0000232358
94. https://helpdesk.rsf.org/
95. https://ssd.eff.org/
96. https://gijn.org/digital-security/
97. https://securityinabox.org/en/
98. https://www.facebook.com/facebookmedia/blog/safety-tips-for-journalists
99. https://freedom.press/training/your-smartphone-and-you-handbook-modern-mobile-maintenan ce/
100. https://privacyforjournalists.org.au/
101. https://cpj.org/safety-notes/
102. https://newsrooms-ontheline.ipi.media/
103. https://the-field-guide-to-security-training-in-the-newsroom.readthedocs.io/en/latest/?mc_cid=62ce19ed91&mc_eid=03ff8f9b25#
104. https://rsf.org/pt

Pública

www.apublica.org/