



**SEGURANÇA DIGITAL:**  
CONCEITOS E FERRAMENTAS  
BÁSICAS



**Edição:** Maio de 2020.

**Autora:** Oriana Hernández

**Projeto Gráfico e Diagramação:** Aliz Segovia

**Colaboradores:** Carlos Guerra, Mario Felaco

**Tradução:** coletivo Mar1sc0tron

**Suporte para tradução em português**



Este guia foi desenvolvido como parte da iniciativa “Dados Criptografados” (“**Datos Bajo Llave**”) da organização Conexo.

**Para consultar mais recursos, lhe convidamos a visitar:**

<https://conexo.org/datos-bajo-llave/>

**Para a versão deste guia em html, acesse:**

<https://conexo.org/conceptos-y-herramientas-basicas>



# ÍNDICE

<b>PARA QUEM É ESTE GUIA</b>	<b>04</b>
<b>O QUE É SUSCETÍVEL DE SER MUDADO. O QUE DEVEMOS PROTEGER</b>	<b>05</b>
<b>ANTES DE COMEÇAR</b>	<b>07</b>
<b>1 SENHAS</b>	<b>09</b>
a. Como criar senhas seguras	
b. Evite estes hábitos	10
Recomendações	13
Use frases como senhas	
Use gerenciadores de senhas	
Mude as senhas de serviço mais importantes	
para manter sua privacidade	14
<b>2 AUTENTICAÇÃO DE DOIS FATORES (2FA OU DE DUAS ETAPAS)</b>	<b>15</b>
a. O que é a autenticação de dois fatores	
b. Como ativar a autenticação de dois fatores	16
c. Serviços de uso frequente onde se pode ativar a autenticação	
de dois fatores	17
Recomendações	18
<b>3 TELEFONE CELULAR</b>	<b>20</b>
a. Chamadas:	
Recomendações	
b. Mensageria:	21
SMS	22
Mensageria instantânea ou chats	
Whatsapp	23
Signal	24
Recomendações	25
c. Rastreamento	26
Recomendações	
d. Proteção física das informações em telefones celulares	
Recomendações	
e. Outros hábitos	27
<b>4 PHISHING</b>	<b>28</b>
O que é o phishing	
Recomendações	

<b>5</b>	<b>MALWARE</b>	<b>31</b>
	O que é o malware	
	O que podemos fazer para detectar e eliminar um malware de nossos equipamentos	
	Recomendações	32
<b>6</b>	<b>NAVEGAÇÃO SEGURA, EVASÃO DE CENSURA E ANONIMATO</b>	<b>33</b>
	Rede sem fio	
	Recomendações	
	HTTPS	34
	VPN	36
	O que é uma VPN	
	Vantagens e desvantagens de usar uma VPN	37
	Vantagens	
	Desvantagens	
	Recomendações	38
	TOR	39
	Recomendações	40
<b>7</b>	<b>EMAILS SEGUROS</b>	<b>41</b>
	Recomendações	
<b>8</b>	<b>PROTEÇÃO FÍSICA DA INFORMAÇÃO</b>	<b>45</b>
	Recomendações	
<b>9</b>	<b>SEGURANÇA EM REDES SOCIAIS</b>	<b>48</b>
	Recomendações	
	<b>REFERÊNCIAS</b>	<b>50</b>
	<b>LISTA DE CHECAGEM DE SEGURANÇA DIGITAL</b>	<b>51</b>





## PARA QUEM É ESTE GUIA

Este guia foi escrito pensando em jornalistas, defensores e defensoras de direitos humanos, ativistas e pessoas que, independentemente da sua área de atuação profissional, desejam iniciar-se no caminho da segurança digital e da privacidade. A adoção total ou parcial das recomendações oferecidas aqui dependerá dos riscos que está enfrentando a pessoa ou organização interessada em implementá-las. É por isso que antes de começar, recomendamos que se realize uma avaliação de riscos.

O guia de [SAFETAG](#) define o risco como “**a avaliação atual da probabilidade de que aconteçam eventos danosos. O risco pode ser avaliado comparando as ameaças que um agente enfrenta com suas vulnerabilidades e suas capacidades para responder ou mitigar as ameaças emergentes**”. Assim:

$$\text{Risco} = \frac{\text{Ameaça x Vulnerabilidades}}{\text{(Capacidade)}}$$



**Ameaça:** é um possível ataque que tem o potencial de causar dano à vida, à informação, às operações, ao meio ambiente e/ou à propriedade.



**Vulnerabilidade:** é um atributo ou característica que faz com que uma entidade, um ativo, um sistema ou uma rede seja suscetível a uma dada ameaça.



**Capacidade:** é a combinação das fortalezas, atributos e recursos disponíveis de uma pessoa ou organização que podem ser usados para reduzir o impacto ou a probabilidade de ameaças.

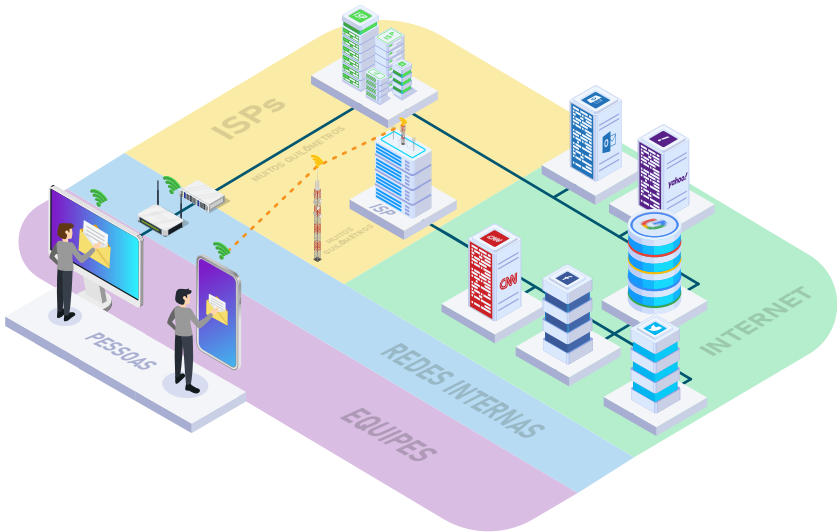


Para mais informações sobre como realizar uma análise completa de risco, recomendamos consultar o manual “[Seguros e Documentados para o Ativismo](#)” (SDA).



## O QUE É SUSCETÍVEL DE SER MUDADO E O QUE DEVEMOS PROTEGER

Quando falamos de segurança digital, normalmente nos referimos ao conjunto de ações que podemos realizar para proteger e ter controle sobre nossas comunicações, informações e, em geral, sobre nossos dados. Com isso, procuramos garantir sua disponibilidade, integridade e confidencialidade. Mas, **o que exatamente devemos proteger? Como fazer para que isso aconteça? Por onde começar?** Uma maneira de explicar o que é segurança digital pode ser através da seguinte imagem:



Na imagem, mostramos como é o percurso normal da informação quando navegamos na Internet. Vemos como uma pessoa, utilizando seu computador, se conecta a uma rede Wi-Fi para enviar, por exemplo, uma email. Para isso, a informação passa, num primeiro momento, pela infraestrutura do seu provedor de serviços de Internet ou ISP e depois entra na Internet, neste caso, no servidor da Google.

Em seguida, para que a informação possa ser consultada pelo destinatário, este deve ter um equipamento (no exemplo, um telefone celular) que acesse a Internet através do seu próprio ISP.

É possível identificar na imagem vários componentes que tornam a comunicação possível: os usuários e usuárias, os equipamentos, as redes internas, os ISPs e, finalmente, o que denominamos de “Internet”.

Para melhorar nossa segurança digital será necessário tomar medidas em cada um desses componentes porque cada um possui vulnerabilidades que podem ser aproveitadas por atacantes. A ordem em que implementamos as medidas de proteção ou o componente onde desejamos começar não é o mais importante, mas conseguir cobrir cada um deles para fechar todas as possíveis “portas de entrada” a nossos dados.

É por isso que se diz que a segurança é um processo no qual vamos adicionando camadas a cada um dos componentes que intervêm na administração da informação. **Não existe uma ferramenta mágica** que vai te proteger contra qualquer ataque.



Nosso desejo com este guia é lançar o convite para você iniciar esse processo colocando em prática as recomendações que lhe oferecemos em cada um dos temas.



## ANTES DE COMEÇAR

O que vem a seguir são algumas premissas relacionadas ao mundo da segurança. É útil conhecê-las antes de começar a colocar em prática o conteúdo deste guia:



É comum dizer, em segurança digital, que **“a corrente arrebenta no elo mais fraco”**. Se você faz parte de uma organização, é muito conveniente que todas as pessoas membros possam colocar em prática as recomendações acordadas, pois assim conseguirão estar mais seguras. Como indivíduo, é recomendável ver sua segurança como um todo e não pensar que com apenas uma medida você já estará segura: é útil pensar que talvez exista outra maneira de ter acesso a seus dados que seja diferente daquela que você acabou de garantir a segurança.



A maior parte das melhorias que podem ser realizadas na sua segurança depende de uma mudança em seus hábitos. Outra parte depende de que você comece a utilizar novas ferramentas ou aplicativos. E outra ainda, de que as ferramentas que você já utiliza sejam configuradas corretamente.





Mesmo que você coloque em prática todas as recomendações deste guia, **sua informação nunca estará 100% segura**. Apenas estará diminuindo a probabilidade de ocorrência ou o impacto dos seus riscos. Por isso, é conveniente realizar com regularidade uma avaliação dos mesmos e projetar planos para sua mitigação.



Falamos de **segurança holística** quando, de forma coordenada, são utilizadas ferramentas e táticas para o bem-estar e a segurança **psicossocial, física e digital**. Convidamos você a consultar materiais que abordam técnicas para melhorar sua segurança física e psicossocial, assim como buscar recursos adicionais, além deste guia, para a parte de segurança digital.



As ferramentas que apresentamos a seguir se caracterizam por levar em conta a **segurança e a privacidade das pessoas** que as utilizam; se submeterem a auditorias independentes; estarem bem valorizadas pela comunidade de segurança digital; serem geralmente transparentes sobre a forma como funcionam (incluindo suas falhas) e não possuírem custo monetário (ou, ao menos, possuem uma versão gratuita).



# 1 | SENHAS

Uma senha é um texto cujo uso permite que as pessoas acessem um determinado tipo de informação, contas de determinados serviços, entre outros.

Hoje em dia, apesar de que existam múltiplas formas de autenticação (PINs de 4 ou 6 dígitos, padrões, reconhecimento de voz e facial, etc.), as senhas continuam sendo a **principal porta de acesso a nossas contas de usuários e dispositivos**. É por essa razão que ter senhas de acesso seguras, que dificilmente possam se hackeadas, é fundamental.

Neste capítulo, mostraremos como criá-las, quais hábitos é conveniente mudar e quais alternativas para o gerenciamento de senhas existem no mercado.

## A

## COMO CRIAR SENHAS SEGURAS

As **senhas seguras** são aquelas que incorporam na sua criação os seguintes elementos:



**Tamanho:** quanto mais comprida, mais segura será a senha. Quando criamos senhas, é recomendável que elas sejam tão compridas quanto possível ou o serviço permita. Mesmo que não haja um consenso sobre qual deveria ser o tamanho mínimo, 15 caracteres é um número recomendável. E o máximo? Pode ser de 100 caracteres ou mais.

**Uso de diferentes tipos de caracteres:** maiúsculas, minúsculas, números e símbolos.



**Que não seja previsível:** uma das técnicas empregadas para conseguir senhas é o uso da “engenharia social”. Embora, a princípio, ela consista em usar a psicologia para obter informações sobre a vítima, as características desse tipo de informação fazem com que elas possam ser obtidas através das publicações que a própria pessoa realiza em redes sociais e outras páginas da Internet. Neste sentido, a recomendação é não utilizar informações pessoais (nomes de animais de estimação, datas importantes, nomes de familiares, dados pessoais) na criação das senhas.



Outra técnica utilizada pelos atacantes para conseguir uma senha são os chamados “**ataques de força bruta**”, que consistem em testar no sistema todas as combinações possíveis de senhas de forma sistemática e sequencial.

Também existem os “**ataques de dicionário**” onde são testadas todas as palavras registradas numa grande lista (um “dicionário”) e suas combinações, de forma que aquelas senhas que consistem, por exemplo, de palavras comuns sejam facilmente conseguidas pelo atacante.

Neste sentido, se você consegue incorporar todas as características que descrevemos anteriormente nas suas senhas, isso forçará uma pessoa mal-intencionada a empregar maiores recursos (tempo e hardware, principalmente) e **difícilmente** ela descobrirá sua senha.

**B**

## EVITE ESTES HÁBITOS



**Repetir senhas:** se alguém hackea uma de suas contas, pode hackear todas. Lembre daquele caso, em junho de 2016, quando Mark Zuckerberg, CEO do Facebook, utilizou a mesma senha do LinkedIn no Twitter. Os atacantes haviam roubado em 2012 uma base de dados de senhas do LinkedIn e graças a isso conseguiram acessar à conta do Twitter de Zuckerberg.



### **Respostas ruins para as perguntas de segurança:**

muitos serviços oferecem como alternativa de recuperação de conta perguntas que ao serem respondidas corretamente permitem acessar novamente o serviço. A recomendação é **responder a essas perguntas de segurança com outras senhas**, evitando assim que terceiros acessem nossos dados por essa via.

**Emails de recuperação não seguros:** da mesma forma que o ponto anterior, outra via de acesso a nossas contas pode ser através de emails alternativos ou de recuperação. A recomendação neste caso é mudar a senha e as respostas às perguntas de segurança do email de recuperação por senhas seguras. Assim, estaremos fechando outra porta de acesso aos nossos dados. A eliminação do email de recuperação também é uma alternativa que recomendamos realizar quando for possível.



### **Deixar cópias físicas ou digitais acessíveis:**

as notas no celular, os documentos de texto no computador, as notas adesivas nos monitores e as anotações de senhas em quadros e blocos de notas são considerados como **péssimos hábitos** se nosso objetivo é ter a maior segurança possível em nossas contas.

### **Acessar serviços através de equipamentos que não são confiáveis:**

não é recomendável acessar nossas contas de usuário a partir de computadores e equipamentos que **não são confiáveis**. Alguns equipamentos podem estar infectados com **programas espíões capazes de capturar suas senhas**.





**Compartilhar senhas:** as senhas contêm informações privadas que não deveriam ser compartilhadas com nenhuma outra pessoa. Se se trata de uma conta cuja várias pessoas têm acesso, como pode ser o caso das redes sociais de uma organização, é importante compartilhar a senha por **vias seguras** e armazená-las também em lugares seguros.



**Guardar senhas no navegador:** devido às vulnerabilidades que foram registradas em diversos momentos, os navegadores não são considerados lugares seguros para o armazenamento de nossas senhas. Além disso, é comum que os navegadores nos perguntem se desejamos armazenar neles uma senha que acabamos de digitar. O melhor para evitar de clicar em “aceitar” é ir na configuração do navegador e **desabilitar a opção de guardar senhas**.



**Excesso de confiança:** existem cada vez mais técnicas enganosas através das quais os usuários podem estar facilitando o acesso à informação não autorizada a desconhecidos. Navegue sempre em **páginas seguras** (com **HTTPS**), verifique se o endereço da página na barra superior do navegador está correto e **desconfie** de qualquer anúncio, email, chamada, entre outras formas de comunicação, que solicitem informações pessoais.



**Cuidado com a mudança frequente de senhas:** estudos demonstraram que a mudança frequente de senhas **poderia não ser tão seguro** devido a que o usuário precisa realizar pequenas mudanças na senha anterior formando padrões cada vez **mais fáceis** de adivinhar e estes padrões também são conhecidos pelos atacantes. Se você criou uma senha com todos os elementos que descrevemos anteriormente como seguros, então **não será necessário** mudar com frequência essa senha a menos que se suspeite que ela tenha sido roubada por um terceiro não autorizado.





## RECOMENDAÇÕES

1

### USAR FRASES COMO SENHAS

O uso de uma frase é uma alternativa para senha segura que consiste em utilizar uma sequência de palavras para acessar nossas contas. **O importante é que seja comprida** e que não corresponda a uma informação pessoal. Por exemplo:



#### USO FRASES COMO SENHAS

Esta bem poderia ser uma chave segura e teria a vantagem de ser fácil de memorizar. **Adicionaremos mais segurança** se alterarmos a frase incorporando números, símbolos ou mudando algumas letras, por exemplo: “**UsoFr@sesC0m0senh@\$**”, ou agregando mais palavras.

2

### USAR GERENCIADORES DE SENHAS

Uma alternativa mais definitiva para a criação, o armazenamento e a gestão de senhas é o uso de um “**gerenciador de senhas**”. Atualmente, existem vários serviços com versões desktop, aplicativos ou armazenamento na nuvem. Alguns deles são: [LastPass](#), [1password](#), [Passpack](#), KeePass nas suas diversas versões (de preferência, o [KeePassXC](#)), [Dashlane](#), entre outros.

LastPass...

1Password

PASSPACK

KeePassXC

DASHLANE

Embora haja variações entre os programas e a decisão de qual usar dependa de nossas necessidades específicas, a característica mais importante é que todos os gerenciadores permitem armazenar de forma segura nossas senhas. Assim, uma vez que tenhamos carregado no serviço todas as informações, apenas teremos que lembrar da chave de acesso de nosso gerenciador de senhas, da mesma forma que um cofre.

**3**

## **MUDAR, PELO MENOS, AS SENHAS DOS PRINCIPAIS SERVIÇOS E EQUIPAMENTOS**

Se, até este ponto do guia, você considera que suas senhas, ou seus hábitos em relação a elas, não são os melhores, lhe convidamos a realizar algumas mudanças, começando pelos seguintes serviços e equipamentos:



**ACESSO AO  
COMPUTADOR E  
TELEFONE CELULAR**



**EMAILS**



**BANCOS**



**SERVIÇOS  
NA NUVEM**



**REDES  
SOCIAIS**



2

## AUTENTICAÇÃO DE DOIS FATORES (2FA OU DE DUAS ETAPAS)

A

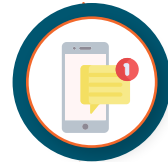
### O QUE É A AUTENTICAÇÃO DE DOIS FATORES

A **autenticação de dois fatores**, também chamada de **duas etapas**, consiste em ativar um segundo elemento (além da senha) para conseguir acesso a nossas contas. Desta forma, estaremos **mais seguras** porque serão necessárias ambas vias de autenticação para poder realizar o acesso. Este segundo elemento pode ser:



**Algo que você sabe:** consiste em **agregar** uma segunda senha para conseguir acessar sua conta.

**Algo que você tem:** consiste em introduzir um código que somente você poderá obter através de uma mensagem de texto, de um aplicativo ou de um dispositivo específico ou token.



**Algo que você é:** consiste em utilizar a **autenticação biométrica**, ou seja, as características do corpo de uma pessoa, para verificar sua identidade. Por exemplo, através de impressões digitais, rosto ou íris. Devido ao risco de extração não autorizada de dados e das vulnerabilidades desses métodos, a **autenticação** através de informação biométrica não é um método que recomendamos quando esta informação fica armazenada em servidores externos.

# B

## COMO ATIVAR A AUTENTICAÇÃO DE DOIS FATORES

Recomendamos **ativar o duplo fator** em todos os serviços que possuem essa opção. Dependendo do serviço, a autenticação de dois fatores pode consistir especificamente em:



**Envio de SMS:** o código chegará a seu **telefone celular** através de uma mensagem de texto.

**Aplicativos de autenticação:** você encontrará o código de acesso num aplicativo que **não precisa de sinal telefônico** ou **Internet** para funcionar.



**Segunda senha:** introduzir uma **segunda chave** ou código de **6 dígitos** (como no caso do *Whatsapp*).

**Token:** envio de um **token** de autenticação.



**Ativação de uma chave de segurança:** são **hardwares** que se conectam através das portas USB ou por conexão sem fio para realizar a autenticação.

Outras opções podem incluir **notificações** em algum dispositivo, envio de um código através de email ou de dispositivos físicos que **geram códigos**.

**C****SERVIÇOS DE USO FREQUENTE ONDE SE PODE ATIVAR A AUTENTICAÇÃO DE DOIS FATORES**

Estes são alguns dos principais serviços onde você **pode ativar** a autenticação de dois fatores:

**WhatsApp****Signal****Gmail****Outlook****facebook****Instagram****Linked in****slack****TeamViewer**

A página <https://twofactorauth.org> possui uma lista completa para consulta.



## RECOMENDAÇÕES

Dado que as **mensagens de texto (SMS) são inseguras** e é possível que você não consiga obter o código de acesso no caso de estar fora do seu país de residência, recomendamos que ative o **duplo fator** através do uso de um aplicativo móvel de autenticação.

Este aplicativo é **seguro** e sempre será possível obter seus códigos de acesso não importando o lugar onde você está. Os aplicativos que recomendamos são:



AUTHY

Disponível para [iOS](#) e [Android](#)



Google Authenticator

Disponível para [iOS](#) e [Android](#)

Para ativar qualquer um dos dois é preciso:

**1** Baixar o aplicativo escolhido da **PlayStore** (para usuários Android) ou **AppStore** (para usuários iOS).

**2** Ir às **configurações de segurança** do serviço que você deseja ativar o duplo fator.

**3** Escanear o **código de barras** com seu celular e seguir as instruções.

Deste momento em diante, cada vez que você deseja **acessar** a uma conta onde tenha ativado o duplo fator, o serviço pedirá sua senha e também o **fator de autenticação**.



Recomendamos que você tenha um ou dois “**dispositivos de confiança**”. Dessa forma, sempre será possível acessar aos serviços em caso de roubo ou perda do telefone celular já que nos dispositivos que você marcou como de “**confiança**” o serviço só pedirá a senha e não o código de autenticação para realizar o acesso.

Recomendamos também procurar a **opção de emergência** ou de segurança nos serviços que tenham essa opção para que você possa ter acesso a suas contas em caso de não poder usar os outros métodos de autenticação. Esses códigos devem ser guardados da **maneira mais segura possível**, por exemplo, em um gerenciador de senhas.

Alguns aplicativos oferecem o serviço de backup dos códigos únicos em servidores na nuvem: **não recomendamos utilizar essa opção a menos que seja para migrar as senhas para outro dispositivo e logo em seguida desativá-la.**





## 3 | TELEFONE CELULAR

Este capítulo oferece recomendações com relação a chamadas, chats, rastreamento e proteção física da informação contida em dispositivos móveis.

### A

## CHAMADAS

Quando você realiza uma chamada tradicional a partir de um telefone fixo ou de um celular, a chamada não é criptografada de ponta a ponta. Se estiver usando um telefone celular, a chamada pode ser fracamente criptografada entre o telefone, as torres de telefonia celular e o resto da rede telefônica.

À medida que a conversa viaja através da rede, **ela é vulnerável a interceptação** por parte da companhia telefônica e, por extensão, de qualquer governo ou qualquer outra organização que tenha poder sobre ela. Também existem técnicas que outras pessoas podem usar para escutar este tipo de chamada se estão perto do seu telefone.



## RECOMENDAÇÕES



É muito recomendável que você abandone o hábito de realizar chamadas usando um telefone fixo com **linha cabeada** ou um **celular com linha móvel** e comece a chamar unicamente a partir de **aplicativos que criptografem** as chamadas de ponta a ponta, como *Whatsapp* ou *Signal*.



Em caso de que seja **indispensável** fazer uma chamada através de linhas telefônicas tradicionais, **evite** falar de **temas sensíveis** que coloquem em risco sua segurança.



## O QUE VOCÊ PRECISA SABER SOBRE CRIPTOGRAFIA

Geralmente, **criptografia** se refere ao processo matemático de tornar uma mensagem ilegível, exceto para a pessoa que possui a chave para descriptografá-la.

Existem duas formas principais de criptografia: quando a informação está em **repouso** e quando está em **trânsito**.



A **criptografia em repouso** se refere à codificação da informação armazenada em um dispositivo.



A **criptografia em trânsito** se refere a uma codificação da informação que está se movendo através de uma rede de um lugar para outro.

Na Internet, existem duas maneiras mais — **frequentes** — de criptografar os dados em trânsito:

**A**

**Criptografia da camada de transporte (HTTPS através de TLS):** a criptografia da camada de transporte protege as mensagens à medida que viajam de um dispositivo aos servidores de um serviço, aplicativo ou página web e dos servidores até o dispositivo de potenciais destinatários. No meio do caminho, o provedor de serviços de mensageria (ou a página web em que você está navegando, ou o aplicativo que está utilizando) pode ver cópias não criptografadas das suas mensagens.

**B**

**Criptografia de ponta a ponta (E2E):** a criptografia de ponta a ponta protege as mensagens em trânsito do remetente até o receptor final. Ela garante que a informação se converta numa mensagem secreta desde o remetente original (a primeira **ponta**) e que somente seja descriptografada pelo destinatário final (a segunda **ponta**). Ninguém, incluindo os administradores do aplicativo que você está usando, pode **“escutar”** e ter acesso ao conteúdo.

Retirado de “[O que é preciso saber sobre criptografia?](#)” do programa Surveillance Self-Defense da Electronic Frontier Foundation.



## SMS

**Não é recomendável** se comunicar através de **mensagens de texto (SMS)** já que o provedor de serviço, ou até as pessoas próximas ao seu telefone, podem facilmente ter acesso a elas.

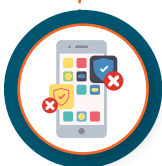


## MENSAGERIA INSTANTÂNEA OU CHATS

Quando dizemos que um aplicativo de chat é **seguro** estamos nos referindo a que ele **atende a várias características**, entre elas destacamos: criptografia em trânsito, criptografia de ponta a ponta, documentação dos processos, auditorias independentes, transparência da operação (incluindo a comunicação das falhas do programa aos usuários), entre outras.



Nem todos os aplicativos que encontramos no mercado possuem essas características de segurança. **Recomendamos que**, de agora em diante, quando você quiser usar um novo aplicativo de mensageria, **verifique** quais dessas características ele possui e, assim, avalie se vale a pena usá-lo.



A seguir, mostraremos as características do *Whatsapp*, por se tratar do aplicativo de mensageria mais utilizado, e do *Signal*, que é a alternativa que consideramos mais segura e que melhor respeita a sua privacidade.



## WhatsApp

Entre as características positivas mais evidentes que o WhatsApp possui para nossa segurança temos:



**Criptografia em trânsito**



**Criptografia de ponta a ponta**



Possibilidade de ativação de um **código de duplo fator** de autenticação.

No entanto, o aplicativo possui outras características que podem representar uma ameaça para nossa segurança, como por exemplo:



**Compartilha** informações com *Facebook*.



Armazena uma quantidade importante de **metadatos**.



Incentiva a **criação de backups** das conversas na nuvem, que podem ser comprometidos através de técnicas conhecidas.



Em alguns dispositivos Android, ele armazena automaticamente imagens, vídeos e mensagens de áudio em diversas áreas do telefone, fazendo com que essa informação **permaneça acessível mesmo depois de que a conversa tenha sido apagada**.











Seu código fonte é fechado, o que faz com que não seja possível conhecer com exatidão como seus algoritmos funcionam nem suas possíveis vulnerabilidades.



## Signal

O Signal conta com um conjunto de características positivas para nossa segurança. Elas são:

-  **Criptografia em trânsito**
-  **Criptografia de ponta a ponta**
-  Possibilidade de ativação de um **código de duplo fator** de autenticação.
-  Possibilidade de **ativação de mensagens efêmeras** para todos os membros de uma conversa.
-  **Armazena somente os metadados necessários** para o seu funcionamento.
-  **Não compartilha** informações com outras companhias.
-  Apesar de ter a opção de fazer backups na nuvem, **não incentiva** seu uso.
-  **Seu código fonte se encontra disponível**, o que torna possível sempre ser auditado por terceiros.



### O QUE SÃO METADADOS?

*“Geralmente, os metadados são descritos como tudo exceto o conteúdo das suas comunicações. Podemos pensar nos metadados como o equivalente digital do envelope de uma carta”.*

Retirado de “Por que os metadados são importantes” do programa Surveillance Self-Defense da Electronic Frontier Foundation.

**Os tipos mais comuns de metadados** são o número de telefone, endereços de email, nomes de usuário, dados de geolocalização, data e hora das chamadas telefônicas, informação sobre o dispositivo que você está usando, o assunto dos emails, entre outros.



## RECOMENDAÇÕES



Baixe o *Signal* e comece a usá-lo para suas conversas mais sensíveis, incluindo em grupos, de forma segura.

Além disso, **recomendamos ativar a opção de mensagens efêmeras** para cada conversa: essa funcionalidade apaga automaticamente os chats para todas as pessoas envolvidas após uma determinada quantidade de tempo (de 5 segundos até uma semana, dependendo do que você escolher).



### NA CONFIGURAÇÃO DO SIGNAL:

- 1 **Ative o bloqueio de registro:** é o equivalente à verificação de duas etapas do *Whatsapp*. Consiste em um PIN que o app solicitará no momento de registrar seu número de telefone em um novo celular.
- 2 **Desative os backups** (habilitados somente no Android).
- 3 Confira se os “**dispositivos vinculados**” são unicamente aqueles que você autorizou.



### NA CONFIGURAÇÃO DO WHATSAPP:

- 1 **Ative a verificação** em duas etapas.
- 2 **Ative** a funcionalidade “**Mostrar notificações de segurança**”.
- 3 **Desative os backups** e apague aqueles que você já tiver realizado anteriormente.
- 4 **Confira** em “**Whatsapp Web/Desktop**” se os dispositivos vinculados são unicamente aqueles que você autorizou.

## C

## RASTREAMENTO

Tanto seu aparelho celular quanto o chip são rastreáveis e estão continuamente transmitindo informações para as antenas de telefonia móvel, fazendo com que seja possível determinar sua localização. **Desligar o telefone após ter chegado a um lugar não é uma boa prática se você deseja esconder onde se encontra.**



### RECOMENDAÇÕES



Se deseja ter uma reunião com uma pessoa e você não quer que sua localização seja conhecida, o recomendável é combinar a data e hora do encontro por um meio seguro (como o Signal), deixar o telefone ligado onde normalmente você estaria e ir à reunião sem o celular ou outro dispositivo passível de rastreamento.

## D

## PROTEÇÃO FÍSICA DAS INFORMAÇÕES EM TELEFONES CELULARES

Para a proteção física do seu celular e da informação contida nele, recomendamos as seguintes práticas:



### RECOMENDAÇÕES



**Senha de acesso:** adicione uma senha de acesso ao seu telefone que seja alfanumérica (que faça uso de todo o teclado). Não se recomenda o uso de padrões, PINs de 4 ou 6 dígitos ou reconhecimento de voz ou facial como forma de acesso ao celular.



**Criptografe o dispositivo:** ter uma senha de acesso não é suficiente para proteger a informação contida no seu dispositivo móvel. A **única forma que evitará** que alguém possa ter acesso à sua informação em caso de roubo ou perda é a ativação da criptografia de disco. **Os smartphones** mais recentes ativam automaticamente a criptografia ao colocar uma senha de acesso. Porém, em dispositivos mais antigos é conveniente verificar se essa funcionalidade está ativada nas configurações de segurança.



**Ative a opção Find My Device (Android) ou Find My iPhone (iOS):** recomendamos ativar antecipadamente a funcionalidade **Find My Device**, se você usa *Android*, ou **Find My iPhone** se você usa *iOS*. Com ela, você poderá rastrear, recuperar, bloquear ou inclusive restabelecer a configuração de fábrica do seu telefone perdido ou roubado acessando sua conta Google ou Apple, dependendo do caso. Quando você marca seu dispositivo como perdido, **nenhuma pessoa, a não ser você, poderá desbloqueá-lo.**

## E

## OUTROS HÁBITOS

Na maioria dos casos, nos telefones celulares um malware tem a forma de um aplicativo. Para evitá-lo, recomendamos:

- ✓ **Baixar** aplicativos somente das **lojas oficiais** (*AppStore* ou *PlayStore*).
- ✓ Baixar somente **os aplicativos necessários**.
- ✓ **Revisar frequentemente** quais permissões (como acesso à câmera ou ao microfone) cada aplicativo possui.
- ✓ **Evitar** carregar o telefone usando cabos ou portas USB em dispositivos desconhecidos.
- ✓ **Atualizar o sistema operacional**, assim como os aplicativos, assim que exista uma nova versão disponível.
- ✓ **Fazer backup frequentemente** das informações mais importantes na nuvem ou em outros dispositivos.





## 4 | PHISHING

### O QUE É PHISHING



O *phishing* é uma **técnica de ataque** que busca enganar a vítima para que ela entregue informações sensíveis, baixe um **arquivo** infectado ou digite sua senha em uma página falsa.



É provável que você receba mensagens de email, *Whatsapp* ou SMS com links, arquivos ou softwares maliciosos que aparentemente provêm de fontes conhecidas como *Facebook*, *Twitter*, *Google*, algum banco, entre outros, dizendo que sua conta foi comprometida e que você deve acessá-la **urgentemente** para poder recuperá-la. Se isso acontecer, é muito provável que esteja enfrentando um ataque de phishing.

A seguir, oferecemos algumas recomendações que poderão lhe ajudar a **reconhecer esses ataques** assim como qual a melhor forma de evitá-los.



### RECOMENDAÇÕES



**Desconfie de mensagens que pressionam por ações rápidas ou urgentes:** muitas vezes essas mensagens se aproveitam de situações de risco ou emergência para convencer a vítima de tomar decisões apressadas.



**Antes de fazer qualquer coisa, verifique as páginas oficiais:** se você suspeita que a informação que recebeu pode estar correta, a recomendação é que a verifique diretamente nas páginas oficiais dos bancos, empresas de correio, entre outras, dependendo do caso. Se, pelo contrário, a mensagem de alarme que você recebeu não se refere a contas comprometidas, mas a pessoas ou familiares em risco, a sugestão é que, antes de fazer qualquer coisa, tente contactar diretamente a pessoa aparentemente afetada. **Em nenhum desses casos é recomendável clicar nos links sugeridos pela mensagem suspeita.**



**Verifique quem lhe mandou a mensagem:** se a mensagem se diz pertencer a uma rede social ou empresa de email, verifique se as contas de email usadas são as oficiais. Se a mensagem parece vir de **uma pessoa conhecida, fale com ela através de outro meio** (preferencialmente ao vivo) e pergunte se, de fato, ela enviou essas mensagens e para quem.



**Não baixe nenhum arquivo, instale software ou abra link da web antes de verificar sua procedência e veracidade:** para verificar para onde aponta um link encurtado, recomendamos utilizar o serviço [unshorten.me](https://unshorten.me) ou [unshorten.it](https://unshorten.it)



**Mantenha seus softwares atualizados:** os ataques de phishing que utilizam **malware** frequentemente se baseiam em vulnerabilidades do software para instalar o malware e comprometer seus dispositivos.



**Utilize um gerenciador de senhas com preenchimento automático:** outra vantagem do uso de gerenciadores de senha que possuem a funcionalidade de **preenchimento automático** de campos de usuário e senha é que essas informações estão associadas à URL onde ela será usada. Se o atacante consegue levar você até uma página maliciosa, seu gerenciador de senhas **não reconhecerá** o lugar que está tentando roubar suas informações.



**Utilize o Google Drive para visualizar documentos.** Em vez de baixar os documentos recebidos, recomendamos que carregue-os no *Google Drive*. Isso converterá o documento numa versão web, o que, quase certamente, impedirá a instalação de um software malicioso. Antes de clicar na tela, tenha certeza de que efetivamente você está com uma pré-visualização do *Google Drive*. Algumas mensagens malintencionadas têm se aproveitado desse nível de confiança e tentam simular o desenho gráfico da interface do Google para obter cliques.



**Ative a autenticação de duas etapas.** Como explicamos anteriormente, a ativação de **2FA** impedirá que o atacante acesse suas contas de usuário, mesmo tendo conseguido a senha de acesso, pois será preciso um segundo fator de autenticação que somente você possui.



Para melhorar suas habilidades de detecção de phishing, convidamos você a realizar um teste de phishing projetado por *Jigsaw* em conjunto com Google: <https://phishingquiz.withgoogle.com/>.

### O QUE É UM MALWARE



Um *malware* é qualquer programa, aplicativo ou código que executa funções indesejadas em nossos dispositivos. Eles **podem chegar até nós** através de emails maliciosos, arquivos baixados da Internet, pendrives USB, documentos infectados ou qualquer outro canal por onde recebemos informações.



Um *malware* pode realizar qualquer ação que um programa legítimo faria, mas com **más intenções**. Assim, ele poderia, entre outras coisas, mostrar o que aparece na sua câmera, ver seus arquivos, o texto que escreve no teclado (que geralmente inclui suas senhas), apagar informações e inclusive pode inutilizar seu equipamento. Um malware **pode afetar qualquer equipamento capaz de executar um código**. Ou seja, nossos computadores, telefones celulares e também equipamentos de rede e dispositivos da “**Internet das Coisas**”, como televisores inteligentes ou equipamentos domésticos conectados à Internet, podem ser afetados por malwares.

### O QUE PODEMOS FAZER PARA DETECTAR UM MALWARE E ELIMINÁ-LO DE NOSSOS EQUIPAMENTOS



Apesar de que não se pode garantir que não temos um malware operando em nossos equipamentos, especialmente devido a técnicas cada vez mais criativas usadas para escondê-lo e disfarçá-lo de aplicativos benignos, a grande maioria dos softwares maliciosos é conhecida e **pode ser detectada e eliminada**. No entanto, a melhor estratégia que podemos adotar não é detectar e eliminar malwares em nossos equipamentos, mas evitar que eles sejam infectados. Em primeiro lugar, isso pode ser alcançado através de **hábitos rigorosos** no uso de nossos dispositivos.



## RECOMENDAÇÕES



Manter o sistema operacional e demais softwares **atualizados e na sua versão original**. Leve em consideração que as atualizações também se aplicam para os aplicativos de telefone celular e complementos de navegadores.



Instalar somente **aplicativos de confiança** e obtidos através de canais oficiais.



Instalar e manter atualizado um **programa de antivírus**. Atualmente as opções comerciais gratuitas possuem níveis de proteção similares ou equivalentes às versões pagas. **Evite ter mais de um antivírus instalado** já que eles não conseguem operar bem em conjunto e podem tornar seu computador mais lento e não detectar corretamente ameaças reais. Um antivírus que recomendamos e que oferece uma versão sem custo é o [Avira](#).



Instalar um programa **antimalware** que complemente o antivírus e que busque mais tipos de ameaças através de outros tipos de técnicas. Todos os vírus são um tipo de malware, porém, o malware inclui muito mais que apenas vírus. Os antivírus e antimalwares **podem operar bem ao mesmo tempo**. Para um antimalware, recomendamos [Malwarebytes](#).



**Revisar as recomendações contra phishing** oferecidas neste guia, pois foi demonstrado que esta é a via **mais utilizada** para infectar usuários com malware.



Evitar ou limitar as **atividades arriscadas** como a busca e o uso de software não legítimos ou “pirata”, frequentar páginas da web que oferecem streaming de séries e filmes ou baixar aplicativos de **páginas não oficiais**.



6

## NAVEGAÇÃO SEGURA, EVASÃO DE CENSURA E ANONIMATO

Quando usamos a Internet, existem informações privadas ou sensíveis que **não queremos revelar para terceiros não autorizados** (como dados pessoais, comunicações com denúncias anônimas, fontes jornalísticas, entre outros). A seguir, oferecemos algumas recomendações para que você navegue na Internet de forma **mais segura**.

### REDE SEM FIO



A **proteção** de redes sem fio, especialmente através de uma configuração correta e o uso de roteador é essencial para evitar o monitoramento de nossas atividades e ataques a nossa rede. Sugerimos que você siga as seguintes recomendações para a proteção de sua **rede domiciliar**:



### RECOMENDAÇÕES

- ✓ **Configurar** uma senha de acesso à rede.
- ✓ **Desabilitar** as funções WPS e UPnP.
- ✓ **Selecionar** o protocolo WPA2 (ou WPA3 se estiver disponível) em vez de WEP ou WAP que já não são considerados seguros.
- ✓ Habilitar uma **rede de convidados**, se for possível.
- ✓ Atualizar o roteador.
- ✓ **Baixar um aplicativo de mapeamento de rede** para verificar se todos os equipamentos conectados são conhecidos. Algumas sugestões são [Ping Tools](#) (Android) e [Fing Network Scanner](#) (iOS) ou utilizar as ferramentas oferecidas pelo seu roteador.
- ✓ Ter um **software antivírus** e antimalware instalado, atualizado e ativado.

Além disso, lembre-se que as **redes sem fio públicas** são especialmente perigosas. Evite acessar esse tipo de redes e, caso seja necessário acessá-las, **utilize uma VPN**.



Para mais informações sobre a proteção de redes sem fio, consulte o guia da organização Derechos Digitales “Recomendações de segurança em redes domésticas para trabalho remoto” (março de 2020).

## HTTPS

HTTPS é um **protocolo de transmissão de dados** que adiciona criptografia na camada de transporte, protegendo a informação que você envia ao navegar pela Internet, partindo do dispositivo utilizado até os servidores da página que quer consultar.

**Quando você navega em páginas web com HTTPS, isso evita que terceiros, incluindo seu provedor de serviços de Internet (ISP), possam capturar a informação que é intercambiada com a página que você está consultando.** Isso não acontece nas páginas onde não está ativado o protocolo HTTPS, ou seja, nas que utilizam HTTP.

Na imagem a seguir, vemos o que acontece com a **informação que viaja usando HTTP e a que viaja usando HTTPS**. No lado esquerdo está representado o que se vê na tela e no lado direito o que se transmite na rede:

Usuário:	mariasilva
Senha:	****
Saldo:	c



Usuário:	mariasilva
Senha:	maria1984
Saldo:	R\$215,75

Usuário:	mariasilva
Senha:	****
Saldo:	R\$215,75

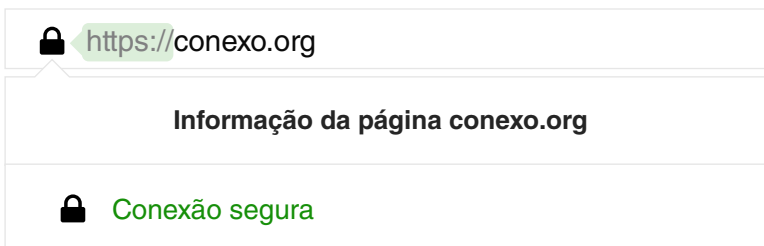


7xisHopXC4o5SIBQXDf
Uy0366XFnuuVCiX/3Ve
dA6XN33AVhAHVHgC
WlaNr/LNh20

Podemos observar que com **HTTP** a informação de usuário e senha pode ser **capturada de maneira legível** dado que o canal por onde ela passa não está criptografado. Por outro lado, com o protocolo **HTTPS**, essa captura de dados **não é possível** porque a informação viaja através de um canal criptografado.



Ao usar **HTTPS**, seu provedor de serviços de Internet, mesmo que possa ver que você está consultando um determinado endereço (URL), **não pode ver em qual parte específica da página você está** nem qual a informação que está trocando com ela (como nome de usuário e senha).



**A implementação do protocolo HTTPS** em uma página web determinada depende inteiramente dos responsáveis pela administração de tal página. Isso é feito através da instalação de **certificados TLS/SSL**. Como usuário, o que você pode escolher é navegar unicamente em páginas com HTTPS para estar segura ou, pelo menos, evitar trocar informações com páginas que ainda utilizem o protocolo HTTP.

O uso de HTTPS não garante que a comunicação esteja de fato acontecendo com o serviço desejado: **recomendamos** que se esteja muito atenta com o endereço da página que você visita.



Se você é parte da administração de uma página web e deseja ativar um certificado TLS/SSL para implementar HTTPS, uma alternativa é usar Lets Encrypt. Ela é uma autoridade certificadora gratuita, automatizada e de código aberto que outorga os certificados digitais que são necessários para habilitar HTTPS de uma forma amigável.

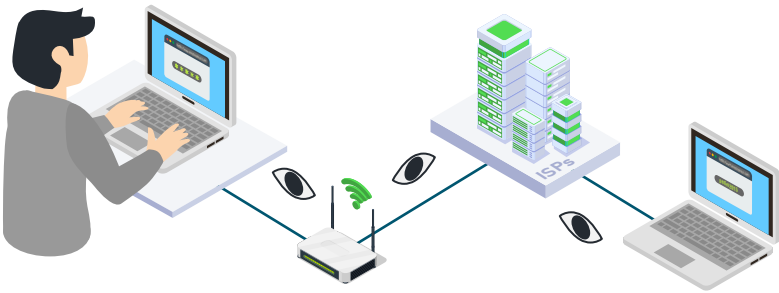


# VPN



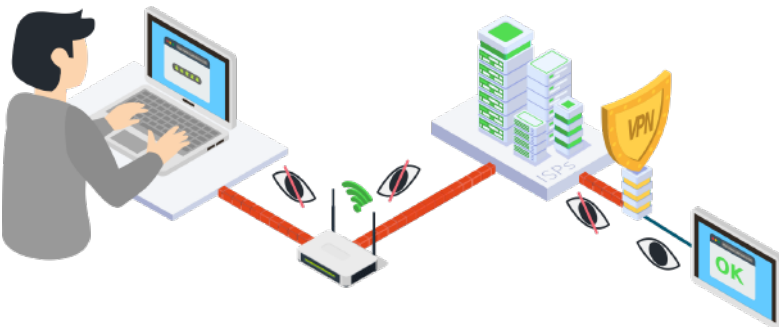
**O que é uma VPN:** uma VPN (Rede Privada Virtual) é uma tecnologia que estabelece um **túnel seguro** de comunicação entre **dois ou mais dispositivos**, o que permite navegar pela web de forma mais segura e privada, mesmo se você estiver usando uma rede Wi-Fi pública.

A imagem a seguir mostra como funciona uma **conexão sem VPN**:



Podemos ver como o usuário **acessa a Internet** através de uma rede Wi-Fi e, a seguir, a partir do roteador, ele envia a informação ao provedor de serviço de Internet (ISP) para posteriormente alcançar o servidor da página web que deseja consultar. Neste tipo de conexão sem VPN, o ISP é capaz de ver quais são as páginas por onde o usuário navega assim como a informação que é transmitida se a página consultada não possui HTTPS.

A imagem a seguir mostra como é uma **conexão com VPN**:



## VANTAGENS E DESVANTAGENS DE USAR UMA VPN

### VANTAGENS



**Criptografar a informação que é enviada no caminho que vai desde a origem (seu dispositivo) até o servidor VPN.** Isso é uma vantagem quando, por exemplo, você precisa navegar numa página onde não está configurada uma conexão HTTPS ou você suspeita que suas comunicações estão sendo vigiadas.



**Esconder do provedor de serviços de Internet (ISP) as páginas por onde está navegando.**



**Ocultar sua identidade do serviço que você quer consultar como destino final (por exemplo, google.com).** Isso acontece porque o destino final presume que quem realiza a consulta é o servidor VPN.



**Ter acesso às páginas que foram bloqueadas pelo seu provedor de serviços de Internet.**

### DESVANTAGENS



**É possível que ao ativar uma VPN sua conexão se torne mais lenta.** Neste caso, recomendamos ativá-la somente quando for navegar em páginas sem HTTPS ou sensíveis, quando quiser entrar em páginas bloqueadas ou quando estiver realizando trabalhos de investigação. Você também pode tentar mudar de servidor VPN, procurando por um que esteja mais perto da sua localização.



Um serviço de VPN, assim como outros serviços que ajudam a navegar anonimamente (por exemplo, TOR), **também podem ser bloqueados.** Se você percebe algum bloqueio, denuncie-o através dos meios que tem à disposição para que a comunidade que apoia a Internet livre ajude a restabelecer o serviço ou ofereça alternativas de conexão.



### Sobre a navegação privada ou em modo incógnito

A navegação privada, ou também chamada em modo incógnito ou em janela privada, é uma função de privacidade de alguns navegadores web que **evita que sejam armazenados permanentemente** (nos dispositivos) o histórico de navegação, cookies e o cache da web, para evitar que possam ser recuperados por terceiros no futuro. É importante não confundir essa opção com a navegação com HTTPS ou com VPN.



## RECOMENDAÇÕES

Baixe uma VPN para cada um dos seus dispositivos móveis e computadores que você pode manter ligado de forma permanente para obter as vantagens de segurança que descrevemos anteriormente. Se você não pode manter a VPN sempre ligada por falta de largura de banda, entre outras, recomendamos utilizá-la, pelo menos, para a navegação durante trabalhos de investigação ou outros similares, cujo conhecimento por parte de terceiros possa lhe colocar em risco.

Sugerimos os seguintes serviços de VPN:



PÁGINA WEB	<a href="#">TunnelBear</a>	<a href="#">Psiphon</a>	<a href="#">ExpressVPN</a>	<a href="#">Mullvad</a>
PLANOS E CUSTOS	Sem custo até 500MB mensais. Existem planos pagos disponíveis.	Sem custo.	\$12,95 dólares por mês. Até 5 dispositivos conectados simultaneamente por conta. Existem outros planos disponíveis.	\$5,5 dólares por mês. Até 5 dispositivos conectados simultaneamente por conta.
DISPONÍVEL EM	iOS, Android, MacOS, Windows e como extensão nos navegadores Chrome, Firefox e Opera.	iOS, Android e Windows.	iOS, Android, MacOS, Windows e como extensão nos navegadores Chrome e Firefox.	iOS, Android, MacOS, Windows e Linux.
KILL SWITCH	✓	✗	✓	✓



### A opção “Kill Switch”

A opção denominada “*kill switch*”, que nem todos os serviços de VPN possuem, consiste em bloquear todo o tráfego de Internet se, por alguma razão, a conexão cai e o aplicativo de VPN se desconecta. Dessa forma se impede, entre outras coisas, que sejam reveladas ao ISP as páginas que você estava consultando antes da conexão ser interrompida. Ou seja, isso garante que o tráfego (e os dados) não passem acidentalmente por fora do túnel seguro.

### Você utiliza serviços de streaming?

Se você é usuário frequente de serviços de streaming (retransmissão contínua de áudio e vídeo, em geral), **EdgeWise Connect** é uma VPN capaz de mudar a transmissão de dados de Wi-Fi para dados móveis do celular, evitando que pontos de acesso (roteadores) lentos ou disfuncionais interrompam suas atividades na rede. Quando o usuário se encontra dentro do alcance de uma rede Wi-Fi que funciona bem, EdgeWise retornará automaticamente o tráfego para Wi-Fi para deixar de consumir dados móveis. Na sua versão gratuita, este software oferece 3 horas de conexão diária.



## TOR

A rede Tor é uma rede de servidores distribuídos em diferentes partes do mundo que possui o objetivo principal de **facilitar o anonimato** dos usuários fazendo com que seus dados passem por múltiplos servidores antes de chegar ao destino. A melhor analogia seria com um servidor VPN, com a diferença de que a rede Tor utiliza uma cadeia de servidores que é diferente para cada seção de usuário.

Esta plataforma mantém protocolos de comunicação próprios que dificulta a análise dos dados interceptados. Porém, não está projetada para competir com a criptografia empregada nas infraestruturas de VPN.





## RECOMENDAÇÕES



Baixar o [Navegador Tor](#) de forma anônima, acessar páginas bloqueadas pelo seu ISP ou visitar páginas próprias da rede Tor (através dos chamados “**serviços onion**”). Tenha em mente que, assim como acontece com o uso de uma VPN, com Tor também pode ser que a conexão com a Internet fique mais lenta.



Se você deseja **anonimato** e, ao mesmo tempo, ter as vantagens de criptografia em trânsito das VPN, navegue usando o *Tor Browser* com a VPN ligada. Seria como adicionar uma camada de segurança sobre a outra.



Para **proteger sua privacidade** em relação ao comércio de dados, recomendamos instalar no navegador as extensões [UBlock Origin](#) e [Privacy Badger](#) que bloqueiam os rastreadores para coleta de dados. Você também pode considerar migrar para o Firefox pois ele é a alternativa entre os navegadores web que oferece mais opções para proteger a **privacidade dos usuários** através da eliminação do histórico de navegação e cookies quando termina uma seção, entre outros.

## 7 | EMAILS SEGUROS

Os **emails** são um dos meios mais utilizados para comunicação e, da mesma forma que com o resto das ferramentas que abordamos neste guia, é importante que aprendamos quais são as características de segurança que devemos buscar nos serviços que utilizamos e qual é a configuração mais adequada para obter uma **maior segurança e privacidade**.

A primeira coisa que você precisa saber é que nem todos os serviços de email incluem as mesmas características de segurança. Por exemplo, **nem todos permitem** a autenticação de dois fatores, assim como nem todos oferecem criptografia de ponta a ponta. A seguir mencionaremos as características de segurança que são importantes buscar nos serviços de email que você utiliza, assim como uma tabela comparativa com as características de segurança de alguns serviços de email.



### RECOMENDAÇÕES

É importante que os serviços de email que você utiliza contem com:



**HTTPS:** para a transmissão de dados em trânsito de forma segura.



**Autenticação** de dois fatores (2FA).



**Atualizações contínuas** das versões dos softwares para desktop, aplicativos e versões para web.

A próxima **recomendação** é que você possa escolher, pelo menos para os assuntos mais sensíveis, opções de email que ofereçam criptografia de ponta a ponta ou possibilidade de que você mesma criptografe suas mensagens através do uso de PGP/GPG. Como explicamos anteriormente, este tipo de criptografia permitirá que **somente você e o destinatário** (e não a empresa provedora) possa ver o conteúdo do email.



### O que é PGP/GPG?

O PGP (Pretty Good Privacy) é um protocolo que utiliza uma combinação de métodos de criptografia, como o de chaves pública/privada, para manter os dados seguros. Este processo pode ser utilizado para criptografar arquivos de texto, emails, arquivos de dados, entre outros.

O **OpenPGP** é o padrão PGP para uso público.

O **Gnu Privacy Guard**, também chamado **GnuPG** ou **GPG**, é uma implementação completa, gratuita e de código aberto do padrão OpenPGP.

Ao utilizar esse tipo de criptografia, **será necessário** uma chave – virtual – privada capaz de abrir o conteúdo das suas comunicações e arquivos. É importante que somente você tenha acesso a ela e por isso deve ser armazenada em um lugar seguro.

Além disso, **descubra** onde está registrada a empresa que provê o seu serviço de email e onde estão seus servidores. Isso é importante porque as empresas devem se ajustar à legislação do lugar onde operam, o que significa que, se estiver contido na lei, uma empresa pode ser obrigada a fornecer informações sobre seus usuários ao governo.

Por exemplo, as empresas que oferecem serviços de email que estão sediadas na Europa devem ajustar-se ao **Regulamento Geral de Proteção de Dados da União Europeia**. Hoje em dia, este regulamento é considerado como a normativa geral que mais respeita a privacidade e a segurança dos usuários. É a partir dela que os países membros da União Europeia devem implementar suas leis de proteção de dados.



## VOCÊ USA GMAIL? VERIFIQUE TAMBÉM O SEGUINTE:

- ✓ Nas [configurações de Segurança](#) da sua conta Gmail ative a verificação em duas etapas, **verifique** se você conhece os dispositivos conectados à conta, se as senhas dos aplicativos correspondem aos serviços que foram ativados e que a “atividade recente relacionada com segurança” não mostre nada suspeito.

- ✓ Na opção **Configuração > Filtros e endereços bloqueados**, verifique se não existe algum email ao qual se envia a informação que você recebe.
- ✓ Na opção **Configuração > Reenvio e correio POP/IMAP**, a não ser que você utilize um cliente de email como Outlook, é recomendável que desabilite ambas opções (POP e IMAP).
- ✓ Veja os [relatórios de transparência da Google](#). São relatórios relacionados com a privacidade e a segurança da empresa, solicitações de conteúdo e informas adicionais. Particularmente, você pode consultar as [solicitações de informação sobre usuários em todo o mundo](#).



## OUTRAS RECOMENDAÇÕES:



Revise a **configuração** de segurança e privacidade, incluindo dispositivos e conexões recentes.



Avalie se **não seria interessante utilizar diferentes contas de email** para suas atividades. Assim, você pode manter separadas as comunicações pessoais das profissionais.



Avalie se **não seria interessante utilizar emails descartáveis** para serviços ou ferramentas que você deseja testar e que necessitem um registro através de email. Uma recomendação é o [10minutemail.com](#).



Dedique um tempo para **revisar as políticas de privacidade**, particularmente a parte sobre os dados coletados pelo serviço, o uso que fazem deles e como a empresa se comporta frente a uma solicitação por parte de terceiros.



Abaixo, mostraremos uma tabela comparativa com as principais características de alguns serviços de email:



	<a href="#">Gmail</a>	<a href="#">Tutanota</a>	<a href="#">Protonmail</a>
<b>HTTPS</b>	✓	✓	✓
<b>AUTENTICAÇÃO DE DOIS FATORES</b>	✓	✓	✓
<b>LOCALIZAÇÃO</b>	EUA	Alemanha	Suíça
<b>CRIPTOGRAFIA DE PONTA A PONTA</b>	✗	✓	✓
<b>PGP/GPG E ONDE ESTÁ A CHAVE PRIVADA</b>	<p>É possível configurar PGP/GPG através da configuração de Mailvelope no email (consulte se o seu provedor permite) ou do Enigmail + Thunderbird. Em ambos casos, somente o usuário terá acesso à chave privada.</p>	<p>A criptografia com PGP/GPG acontece de forma transparente para facilitar seu uso. Porém, para isso, o servidor da empresa conserva a chave privada e não é possível que o usuário obtenha uma cópia.</p>	<p>A criptografia PGP/GPG ocorre de forma transparente para facilitar seu uso. Porém, para isso, o servidor da empresa conserva a chave privada. Adicionalmente, é possível que o usuário baixe uma cópia da chave.</p>
<b>PLANOS E CUSTOS</b>	<p>Sem custo até 15GB (com anúncios). Suite por \$5,40 dólares/usuário/mês (com 30GB no GDrive). Outros planos estão disponíveis.</p>	<p>Sem custo até 1GB de armazenamento para o domínio Tutanota. Para domínios personalizados é \$ 1,20 euro mensal até 1GB de armazenamento. Outros planos estão disponíveis.</p>	<p>Sem custo até 500MB de armazenamento. Para obter até 5GB de armazenamento são \$5 euros mensais. Outros planos estão disponíveis.</p>
<b>DISPONÍVEL EM</b>	Browser, iOS e Android.	Browser, iOS, Android, Windows, MacOS e Linux.	Browser, iOS e Android.



8

## PROTEÇÃO FÍSICA DA INFORMAÇÃO

Nossos arquivos podem ser **vulneráveis a ataques** durante as comunicações (no momento de enviá-los e recebê-los) pois elas podem estar comprometidas ou sendo monitoradas.

Entretanto, também são **vulneráveis os equipamentos que estão parados**, dado que eles podem cair em mão equivocadas e tornarem-se inacessíveis. A seguir, apresentamos recomendações para a proteção de seus arquivos frente a esses possíveis ataques.



## RECOMENDAÇÕES

### CRIOGRAFIA DE ARQUIVOS

É recomendável que você criptografe seus arquivos em cada um dos seus dispositivos para evitar que terceiros possam acessá-los em caso de roubo, perda, entre outros. Isso pode ser feito das seguintes maneiras:



**Criptografia completa do disco rígido:** através da ativação de **FileVault** (usuários MacOS), **Bitlocker** (usuários Windows), **LUKS** (usuários Linux) ou **Veracrypt** (para qualquer sistema operacional).

Para **ativar a criptografia de todo o disco** é necessário configurar o equipamento com uma senha de acesso que impeça que terceiros possam obter sua informação.



FileVault



BitLocker



LUKS



VeraCrypt



Para criptografar telefones celulares, consulte a seção “**Telefone Celular**” deste guia.



**BitLocker** não se encontra disponível no Windows 10 Home. Para ativá-lo, precisamos obter a versão profissional do sistema operacional da Microsoft (Windows 10 Pro).



**Criptografia de outros volumes de armazenamento:** uma alternativa à criptografia completa do disco rígido é criptografar volumes de armazenamento portáteis, tais como pendrives USB ou volumes específicos no disco rígido. As ferramentas que permitem realizar isso são **VeraCrypt** (usuários Linux, MacOS e Windows) e **BitLocker** (usuários Windows).

## APAGANDO ARQUIVOS



Quando você apaga um arquivo do seu computador, incluindo quando você esvazia a “**lixeira**”, na verdade a informação não é apagada, apenas se disponibiliza o espaço ocupado pelo arquivo para ser usado a qualquer momento por uma nova informação. Nesse sentido, é possível recuperar os dados “**apagados**” com algum software específico ou métodos forenses.



Se você deseja **apagar de forma segura** a informação contida em unidades de disco tradicionais – não em discos de estado sólido (SSD) – ou em unidades USB, o recomendável é utilizar programas especializados como o [CCleaner](#) ou [Eraser](#) que sobrescrevem o espaço que ocupava a informação “apagada” de forma a dificultar muito sua recuperação.



**Apagar de forma segura** a informação contida em unidades SSD, unidades flash USB e cartões SD é muito difícil devido ao seu projeto (eles utilizam uma técnica chamada “**nivelção do desgaste**”). Para proteger os arquivos contidos nessas unidades, **recomenda-se a criptografia completa de disco** em conjunto com estratégias de backup e outras medidas adicionais tais como evitar levar consigo os equipamentos com informação sensível durante viagens, entre outras.

## BACKUP DE ARQUIVOS

Para garantir a disponibilidade da informação é importante que você faça backups ou cópias de segurança dos seus arquivos. Recomenda-se que os backups sejam realizados através de **serviços ou ferramentas seguras** e que seja levado em consideração os seguintes critérios:

- ✓ Criptografia.
- ✓ Fácil restituição.
- ✓ Localização física distante dos locais que podem ser atacados.
- ✓ Na Internet.
- ✓ Que sejam Frequentes.
- ✓ Cópias incrementais.

Existe uma estratégia de backup bastante conhecida chamada de “**Backup 3-2-1**” que consiste em:

- ✓ Ter pelo menos três (3) cópias dos seus arquivos.
- ✓ Armazená-las em dois (2) meios diferentes (físico e virtual).
- ✓ Conservar uma (1) cópia num lugar fora dos locais que poderiam ser vulneráveis.



Nesta seção, oferecemos alternativas para a proteção dos seus arquivos contidos nos seus equipamentos, porém, não esqueça de **tomar medidas de proteção do espaço físico** onde estão esses equipamentos, como sua casa ou escritório.



## 9 | SEGURANÇA EM REDES SOCIAIS

Nos últimos anos, as **redes sociais** se converteram em uma das principais vias usadas para nos comunicarmos, informarmos e trocarmos ideias. Entretanto, assim como em outros meios, elas também podem ser usadas por atacantes que podem comprometer nossos dados e nossa segurança. Por outro lado, as redes sociais constituem uma das principais fontes de **comércio de dados** e funcionam de maneiras que afetam fortemente a privacidade de seus usuários.

Para **evitar estas ameaças** oferecemos as seguintes recomendações relacionadas não apenas à segurança, mas também à privacidade da sua informação:



### RECOMENDAÇÕES



Defina se a sua participação na **rede social** será através do seu nome ou de um pseudônimo (em inglês, alias).



Defina o endereço de email que estará **associado à sua conta**. Se é pessoal, de trabalho ou um anônimo criado para este fim.



Quando você selecionar sua **foto de perfil**, avalie se usará a mesma em todas as redes, se mostrará seu rosto e se ela pode mostrar mais informações sobre você do que deseja revelar.



Configure uma **senha segura** de acesso e leve em consideração o resto das recomendações que oferecemos na seção **Senhas** deste guia. Por exemplo, veja como configurar as respostas às perguntas de segurança.



**Ative** a autenticação de dois fatores.



**Evite ter conversas sensíveis** através dos chats ou de mensagens diretas nas redes sociais.



**Olhe com atenção as opções de privacidade e segurança.**

Por exemplo, escolha se você deseja que encontrem o seu perfil através do seu número de telefone ou escolha quem pode ver suas publicações, entre outros. No Twitter, recomendamos que você **desative as opções de localização nos tweets** da mesma forma que as opções de tag de fotos de terceiros.



Configure as **notificações** de forma que possam lhe avisar quando exista uma **atividade suspeita** na sua conta, por exemplo, uma tentativa de início de sessão em um novo equipamento.



Dedique um tempo para **revisar as políticas de privacidade**, particularmente a parte sobre os dados coletados pelo serviço, o uso que fazem deles e como a empresa se comporta frente a uma solicitação por parte de terceiros.



**Lembre-se** que, mesmo que você realize as configurações adequadas, tudo o que você subir nas redes tem a possibilidade de se tornar público. Antes de publicar, **avalie a conveniência** de compartilhar uma determinada informação.



## REFERÊNCIAS

- Citizen Lab. (Última atualização: 22 de fevereiro de 2020). Improve your online safety with advice from experts. Extraído de: <https://securityplanner.org/#/>
- Derechos Digitales. (Junho de 2018). Confiável e seguro? Um panorama sobre as potenciais vulnerabilidades do Whatsapp. Santiago de Chile. Extraído de: <https://www.derechosdigitales.org/wp-content/uploads/Confiable-y-seguro.pdf>
- Guerra, Carlos. (2018). SDA Seguros y Documentados para el Activismo. Santiago de Chile. Extraído de: [https://sdamanual.org/assets/pdf/sda\\_es.pdf](https://sdamanual.org/assets/pdf/sda_es.pdf)
- Electronic Frontier Foundation. Surveillance Self-Defense. Tips, Tools and How-Tos for Safer Online Communications. Extraído de: <https://ssd.eff.org/>
- Tactical Tech. Manual de Segurança Holística. Berlim, Alemanha. Extraído de: <https://holistic-security.tacticaltech.org/> (disponível em português)
- Derechos Digitales.(2018). Torificate. Extraído de: <https://tor.derechosdigitales.org/torificate>
- Internews. SAFETAG. A Security Auditing Framework and Evaluation Template for Advocacy Groups. Extraído de: <https://safetag.org/guide/>
- Guerra, Carlos. (Marzo 2020). Recomendaciones de seguridad en redes caseras de cara al teletrabajo. Santiago de Chile. Extraído de: <https://www.derechosdigitales.org/wp-content/uploads/Recomendaciones-de-seguridad-en-Redes-caseras-de-cara-al-teletrabajo.pdf>
- Fundação Karisma. (Novembro de 2016). Seguridad, Protección y Privacidad de Twitter. Extraído de: <https://web.karisma.org.co/pagina-principal/que-hacemos/campanas/seguridad-proteccion-y-privacidad-de-twitter/>
- Protege.la y SocialTIC. (Junho de 2018). Checklist de Seguridad Digital para tu Computadora, Celular y Cuentas en Línea. Extraído de: <https://protege.la/checklist-de-seguridad-digital-%E2%9C%85/>

# LISTA DE CHECAGEM PARA MELHORAR A SEGURANÇA DIGITAL

BASEADA NO GUIA  
"SEGURANÇA DIGITAL: CONCEITOS E FERRAMENTAS BÁSICAS"  
DE CONEXO

Maio de 2020

**A**

## SENHAS

- Suas senhas são compridas ou utilizam diferentes tipos de caracteres e não são previsíveis.
- Evita repetir senhas de acesso entre os diferentes serviços/dispositivos que você utiliza.
- Responde às perguntas de segurança para a recuperação de contas com informação não previsível ou senhas.
- Você configurou de forma segura os emails alternativos de recuperação de contas.
- Evita deixar cópias acessíveis com informação de acesso às suas contas de usuário e dispositivos.
- Evita acessar suas contas de usuário a partir de dispositivos que não sejam de confiança.
- Se for necessário, compartilhe unicamente suas senhas por canais seguros e você muda elas quando não é mais necessário compartilhá-las.
- Evita guardar senhas nos navegadores web.
- Quando muda suas senhas, você cria novas senhas evitando o uso de padrões.
- Utiliza gerenciadores de senhas para a criação e o armazenamento das mesmas.

**B**

## AUTENTICAÇÃO DE DOIS FATORES

- Se você é usuário do Whatsapp, ativou a verificação em duas etapas.
- Se você é usuário do Signal, ativou o bloqueio de registro.
- Para os serviços em que se aplica, você ativou a autenticação de dois fatores através de aplicativos de autenticação, token ou chaves de segurança em vez de mensagens de texto (SMS).
- Ativou a autenticação de dois fatores em todas as contas de usuário que você utiliza que permitem essa opção. (Por exemplo, emails, redes sociais, entre outros).
- Você guardou de maneira segura os códigos de recuperação de emergência que o serviço oferece (se for o caso) ao habilitar a autenticação de dois fatores.

**C**

## TELEFONE CELULAR

### Chamadas e mensageria instantânea ou chats

- Pelo menos para conversas sensíveis, você realiza chamadas usando aplicativos com criptografia de ponta a ponta, evitando telefones fixos ou móveis.

- Pelo menos para conversas sensíveis, você envia mensagens usando aplicativos de mensageria instantânea com criptografia de ponta a ponta, evitando SMS.
- Se você é usuário do Whatsapp, ativou a verificação em duas etapas.
- Se você é usuário do Whatsapp, ativou as notificações de segurança.
- Se você é usuário de Whatsapp, verifica os códigos de segurança (chaves de segurança) das pessoas com quem você conversa através de outros canais seguros.
- Se você é usuário do Whatsapp, desativou as cópias de segurança e apagou os backups que possam ter sido feitos anteriormente.
- Se você é usuário do Whatsapp, verificou se na opção "Whatsapp web/desktop" só estão vinculados os dispositivos que você autorizou.
- Se você é usuário do Signal, ativou o bloqueio de registro.
- Se você é usuário do Signal, ativou as mensagens temporárias, pelo menos para as conversas mais sensíveis.
- Se você é usuário do Signal, verifique através de outros canais seguros o número de segurança das pessoas com quem conversa.
- Se você é usuário do Signal (no Android), desativou os backups.
- Se você é usuário do Signal, revisou na seção "dispositivos vinculados" se apenas estão listados os dispositivos que você autorizou.

### Rastreamento

- Quando você vai a reuniões sensíveis, toma medidas para evitar o rastreamento através do seu celular e o chip.

### Proteção física das informações em telefones celulares

- Você configurou uma senha de acesso ao seu telefone celular, de preferência, alfanumérica.
- Ativou ou verificou se o seu celular e o cartão SD estão criptografados.
- Ativou o aplicativo Find My Device (para usuários Android) ou Find My iPhone (para usuários iOS).
- Você baixa os aplicativos para o seu celular apenas das lojas oficiais (AppStore ou PlayStore).
- Você tem o hábito de baixar somente os aplicativos necessários.
- Revisa quais as permissões (como acesso à câmera ou ao microfone) estão cedidas aos aplicativos que usa e desativa aquelas que são desnecessárias para o funcionamento do aplicativo.



- Evita carregar a bateria do telefone usando cabos ou portas USB de dispositivos desconhecidos.
- Mantém atualizado o sistema operacional, assim como os aplicativos.
- Você cria frequentemente cópias das informações mais importantes na nuvem ou em volumes criptografados.
- Mantém a opção de Bluetooth desligada quando não está em uso.

## D

## PHISHING

- Desconfia de mensagens que pressionam a tomar ações rápidas ou de urgência, verificando sua legitimidade por vias alternativas.

### Quando você recebe mensagens suspeitas:

- Consulta os canais oficiais da entidade a que a mensagem faz referência como forma alternativa de verificação segura da informação.
- Consulta por vias alternativas as pessoas as quais a mensagem faz referência como forma alternativa de verificação segura da informação.
- Evita clicar nos links contidos na mensagem recebida.
- Verifica quem mandou a mensagem.
- Evita baixar arquivos ou instalar software que estejam no anexo da mensagem.
- Verifica a veracidade dos links encurtados contidos na mensagem através de ferramentas como unshorten.me, unshorten.it ou getlinkinfo.com.
- Mantém atualizado os softwares dos seus dispositivos.
- Você utiliza um gerenciador de senhas com preenchimento automático dos campos de usuário e senha para suas contas de usuários.
- Ativou a autenticação de dois fatores para todas as suas contas de usuários onde isso é possível.

## E

## MALWARE

- Você mantém o sistema operacional e os demais programas (navegadores, aplicativos, editores de texto, entre outros) atualizados e em sua versão original.
- Instala e mantém atualizado um programa antivírus no seu computador.
- Instala e mantém atualizado um programa antimalware no seu computador.
- Você analisa as unidades USB, de forma automática ou manual, através de um antivírus ou antimalware antes de executar um programa ou arquivo contido nelas.
- Segue as recomendações contra phishing oferecidas no guia de segurança da Conexó para evitar a instalação de malware através dessa via.
- Evita ou limita atividades arriscadas como a busca e o uso de softwares não legítimos ou "pirata", visitas a páginas web de streaming de séries e filmes, ou de baixar aplicativos a partir de páginas que não sejam as oficiais.

## F

## NAVEGAÇÃO SEGURA, EVASÃO DE CENSURA E ANONIMATO

### Rede sem fio

- Você configurou uma senha de acesso à rede.
- Desabilitou as funções WPS e UpnP.
- Configurou o uso do protocolo WPA2 ou WPA3 (se estiver disponível) em vez de WEP ou WAP.
- Habilitou uma rede de convidados, se for possível.
- Mantém o roteador atualizado.
- Utiliza aplicativos de mapeamento de rede para verificar se todos os equipamentos são conhecidos.

### Navegação

- Você verifica se as páginas por onde navega utilizam HTTPS.
- Evita a navegação, ou pelo menos a troca de informações, em páginas que ainda utilizam o protocolo HTTP.
- Mantém seu navegador atualizado.
- Pelo menos para consulta de temas que possam lhe colocar em risco, você navega através de uma VPN ou usando o Tor nos seus dispositivos móveis e computadores.
- Quando acessa a Internet usando redes públicas ou não confiáveis, você navega através de uma VPN.
- Quando escolhe um serviço de VPN, você leva em conta que ela tenha a opção "kill switch".

## G

## EMAILS SEGUROS

### Os serviços de email que você utiliza contam com:

- HTTPS para a transmissão de dados em trânsito de forma segura.
- Autenticação de dois fatores (2FA).
- Atualizações contínuas das versões dos softwares para desktop, aplicativos e versões para web.

### Você usa o Gmail?

- Configurou uma senha segura de acordo com as recomendações oferecidas no guia da Conexó.
- Ativou a verificação em duas etapas.
- Configurou de forma segura o email de recuperação.
- Realizou a "Verificação de Segurança" oferecida pela Google para a sua conta de email.
- Na opção Configuração > Filtros e emails bloqueados, você verificou que não há nenhum email ao qual esteja sendo reenviada a informação que recebe e que não tenha sido configurado por você.
- A não ser que você utilize um cliente de email como Outlook, na opção Configuração > Reenvio e correio POP/IMPA, desabilitou as opções POP e IMAP.

#### Outros:

- Pelo menos para temas sensíveis ou que possam lhe colocar em risco, você utiliza serviços de email que oferecem criptografia de ponta a ponta ou você mesma criptografa seus email através do uso de PGP/GPG.
  - Revisou e ajustou as configurações de segurança e privacidade nos serviços de email que você utiliza.
  - Utiliza contas diferentes de email para suas diferentes atividades profissionais e pessoais.
  - Conhece a política de privacidade dos serviços de email que você utiliza, pelo menos o que esteja relacionado com os dados que coletam, o uso que fazem deles e como se comportam frente a uma solicitação de informação por parte de terceiros.
- Você evita ter conversas sensíveis através dos chats ou mensagens diretas nas redes sociais.
  - Conhece, revisa e configura segundo suas necessidades as opções de privacidade e segurança nas redes sociais.
  - Configura, quando estão disponíveis, as notificações de forma que possam lhe avisar quando exista uma atividade suspeita na sua conta, por exemplo, uma tentativa de início de sessão a partir de um novo dispositivo.
  - Você conhece as políticas de privacidade das redes sociais que utiliza, pelo menos aquilo que está relacionado com os dados que coletam, o uso que fazem deles e como se comportam frente a uma solicitação de informação por parte de terceiros.
  - Levando em conta que tudo que você sobe nas redes tem a possibilidade de se tornar público, você avalia, antes de publicar, a conveniência de compartilhar uma determinada informação.

## H PROTEÇÃO FÍSICA DA INFORMAÇÃO

- Ativou ou verificou se o seu celular e o cartão SD estão criptografados.
- Para os arquivos contidos no seu computador, você criptografou seu disco rígido através da ativação do FileVault (usuários MacOS), BitLocker (usuários Windows), LUKS (usuários Linux) ou Veracrypt (para qualquer sistema operacional)
- Para os arquivos contidos em outros volumes (por exemplo, discos externos), você ativou a criptografia através das ferramentas correspondentes.
- Para a informação contida em unidades de disco tradicionais – não nos discos de estado sólido (SSD) – ou em unidades USB, você apaga a informação através de programas especializados como CCleaner ou Eraser.
- Realiza backups dos seus arquivos seguindo as recomendações do guia de segurança da Conexó (cópias criptografadas, de fácil restituição, localizadas fisicamente longe dos lugares que possam ser atacados, na internet, frequentes e incrementais).
- Você pensou e desenvolveu políticas de segurança em caso de viagens profissionais e pessoais.

## I SEGURANÇA EM REDES SOCIAIS

- Você escolheu conscientemente se a sua participação nas redes sociais é através do seu nome ou de um pseudônimo (alias).
- Escolheu conscientemente o email associado à sua conta (anônimo, pessoal ou profissional).
- Escolheu conscientemente a foto de perfil das suas contas em redes sociais de forma a evitar mostrar mais informação sobre você do que deseja revelar.
- Configurou uma senha segura de acesso.
- Configurou de forma segura o email de recuperação.
- Configurou de forma segura as respostas às perguntas de segurança.
- Ativou a autenticação de dois fatores.