

# Gerenciador de senhas: 5 opções para você nunca esquecer os seus códigos

Você já pensou em usar um gerenciador de senhas? Se não, suas contas podem estar vulneráveis a algum tipo de uso indevido.

A verdade é que sempre existe a chance de as plataformas serem *hackeadas*. Isso significa que se alguém quiser acessar suas informações, pode não ser muito difícil executar a tarefa.

Por isso, desde 1999 (ano do gerenciador de senhas mais antigo), existem *softwares* que oferecem um leque de funções capazes de otimizar a segurança das suas contas virtuais.

Se você nunca teve contato com esse tipo de serviço, pode parecer desnecessário. Mas vamos convencê-lo do contrário.

## Por que usar gerenciadores de senhas?

Você deve ser um desses três tipos de pessoa: tem a mesma senha para todos os sites; tem um sistema próprio de variação de senhas; ou mantém tudo escrito em *post-its*.

A primeira opção é muito perigosa. Se alguém descobre a senha de uma plataforma menos segura, a primeira coisa a fazer é tentar a mesma senha em outros lugares. E aí você tem um grande problema.

Já a segunda opção pode até ser uma boa, mas dá um pouco de trabalho. Você pode acabar se enrolando em algum momento. Outro problema.

E, por último, manter tudo escrito é um tanto arcaico e impede que você acesse suas informações quando estiver fora de casa,

por exemplo, viajando.

## 0 brasileiro na mira dos criminosos



Você precisa estar sempre atento à segurança das suas informações. Assim, cuidar das suas senhas a todo instante é fundamental. Ou seja, elas devem ser mantidas a “sete chaves”. E as estatísticas comprovam isso.

Por exemplo, um estudo divulgado em 2017, envolvendo a Google e a Universidade da Califórnia, não foi nada positivo pra nós, brasileiros. Os cientistas mostraram que nós somos as maiores vítimas dos ladrões de senha – 18% dos casos identificados na pesquisa.

Os cientistas monitoraram sites que os criminosos utilizam para distribuir dados roubados. E o eles encontraram, principalmente, foi:

- 1,9 bilhão de senhas vazadas de outros serviços;

- 788 mil senhas roubadas por ladrões especializados;
- 12,4 mil senhas roubadas por meio do clone de páginas (sites de [phishing](#)).

Outro dado relevante da pesquisa está relacionado à proteção das informações. Ou seja, os cientistas afirmam que a maioria das vítimas de roubo de senhas não utilizavam recursos para dificultar o acesso dos criminosos. Apenas cerca de 3% tomavam esse cuidado.

Ter os seus dados pessoais invadidos pode lhe trazer muitos inconvenientes e prejuízos financeiros também. E, nesses casos, o gerenciador de senhas é seu aliado, uma vez que ele investe pesado no quesito segurança.

## Como guardar senhas de forma segura

O gerenciador de senhas nasceu para resolver essa questão. A principal função é oferecer uma senha mestra, que se aplica a todas as suas contas.

Logo de cara, você deve se perguntar: os funcionários da empresa terão acesso à minha senha? Onde ela ficará armazenada?

A primeira coisa que você precisa saber é que a senha ou chave mestra é protegida por encriptação em todos os apps da lista. Por isso, nem mesmo quem trabalha nas empresas pode acessá-la.

A segunda coisa a saber é que as informações, dependendo do *software*, podem ficar armazenadas de formas diferentes: [em uma nuvem](#), em um só HD (como do seu computador), *off-line* (no próprio programa) ou em um pendrive (que você pode conectar a qualquer computador). Alguns oferecem mais de uma opção.

## O que os gerenciadores de senhas

# podem fazer por você



Os gerenciadores, além de manter seus dados encriptados, oferecem funções que ajudam a melhorar ainda mais a segurança nas plataformas nas quais você se inscreve.

Os *softwares* oferecem opções de:

- Alterar as senhas de todos os seus logins com um clique.
- Logar nos sites para você.
- Sincronizar o programa em todos os seus aparelhos (ou manter em apenas um, se for de sua preferência).
- Analisar suas senhas para saber se já são fortes e como podem ser melhoradas.
- Gerar senhas fortes.
- Completar formulários automaticamente.
- Compartilhar suas senhas com contatos de emergência, quando você precisar.
- Acessar as senhas offline.
- Carteira virtual (guardando suas informações de cartão

de crédito para facilitar [compras online](#)).

- Autenticação em duas etapas (veja a explicação abaixo).
- Usar uma chave física (como pendrive) para acessar os logins.

Nem todos os aplicativos da lista cumprem tudo isso com destreza, mas procure escolher aquele que oferece o que mais se adequa às suas necessidades.

Você vai precisar, também, considerar os preços: de opções gratuitas até 40 dólares por ano. Mesmo assim, quase todos disponibilizam versão *free* com a maioria das funcionalidades disponíveis.

## Lastpass

O Lastpass foi um dos primeiros gerenciadores que tornou realmente fácil a tarefa de guardar e proteger as senhas. Com ele, você pode fazer uma análise do nível de segurança das suas senhas e, caso elas sejam consideradas fracas, você cria novas opções que afastem o perigo.

Uma funcionalidade interessante do gerenciador de senhas Lastpass é o aviso automático sobre plataformas que tenham sofrido algum tipo de ataque. Ele envia uma notificação e você pode mudar a sua senha na hora, para não se transformar em mais uma vítima.

Alguns gerenciadores de senhas, entre eles o Lastpass, utilizam formas adicionais de proteção da sua senha mestra (a chamada autenticação em duas etapas). Uma delas depende de outros programas, sendo o principal o [Google Authenticator](#).

Além do gerenciador de senhas, você instala o Authenticator e escolhe entre duas opções: ou acessa os dois apps toda vez que for se conectar às suas contas ou faz uma vez e deixa gravado. A primeira é mais segura.

A autenticação em duas etapas por meio de um pendrive é outra alternativa oferecida pelo Lastpass. Nesse caso, toda vez que você for se conectar, precisa estar com o dispositivo USB, previamente configurado, conectado à máquina. No caso do Lastpass, essa integração é feita com o Sesame.

O Lastpass é suportado em iOS, Windows e Android, além de quase todos os *browsers*. Com armazenamento ilimitado, o Lastpass também tem a opção de salvar notas encriptadas – onde você pode guardar a senha da sua conexão WiFi, por exemplo.

Se precisar mandar suas senhas para alguém, ao invés de usar o Whatsapp, você pode enviar pelo aplicativo de forma segura.

As compras pela internet também ficam mais fáceis e protegidas com os gerenciadores de senhas. Isso porque o preenchimento das informações de pagamento e endereço é automático.

O *download* do gerenciador de senhas Lastpass é gratuito, mas algumas configurações e os aplicativos para smartphone só estão disponíveis na versão paga (12 dólares anuais).

## **Dashlane**

Lançado em 2012, o Dashlane tem uma das interfaces mais fáceis de se usar, entre todos os gerenciadores de senhas disponíveis.

Ocorre que alguns usuários encontram dificuldades em fazer a gestão de suas senhas nas plataformas. No entanto, no [Dashlane](#), esse problema é minimizado e, assim, fica mais fácil não ter preguiça.

Dentro da própria interface, é possível alterar suas senhas de vários sites com um clique, para que você não permaneça muito tempo com a mesma senha. Suas informações também podem ser compartilhadas com os contatos de emergência que você selecionar (no máximo 5, para o plano *free*).

O Dashlane também notifica quando algum site no qual você está inscrito sofre ataques. Suas senhas não ficam armazenadas em um servidor e, segundo o site da plataforma, *hackers* são contratados todos os meses para testar a segurança.

Se você esquecer a sua senha mestra, terá que refazer todos os acessos. Isso é bom, porque é um reforço a mais na segurança. A autenticação em duas etapas é feita pelo Google Authenticator.

As funções de carteira virtual e autopreenchimento também estão disponíveis no Dashlane. O fato de ser bem completo faz dele um dos principais concorrentes do Lastpass.

O Dashlane é um gerenciador de senhas com versões para Mac, Android e iOS, Safari, Chrome, Firefox e Internet Explorer. Entretanto, a sincronização em todos os dispositivos está disponível apenas para o Premium, que é um dos mais caros: 40 dólares anuais.

## **Keepass**

O Keepass é o gerenciador de senhas gratuito e *open source* da lista. A interface é um pouco difícil de usar, mas o banco de dados é encriptado e mantido sob o seu total controle.

Ele é construído de forma portátil – você pode instalá-lo no pendrive e levar para qualquer lugar. Também é o *software* que funciona em mais plataformas: todos os *browsers* e sistemas.

O Keepass tem gerador de senhas, possibilidade de sincronização com outros apps (já que é *open source*, consegue boa abrangência nesse sentido). Também é permitido o acesso *offline* e sua encriptação é uma das mais seguras.

A desvantagem do gerenciador de senhas Keepass é que sua interface não é tão fácil e talvez seja preciso um conhecimento um pouco mais aprofundado de informática para compreender a utilização das funcionalidades.

## 1password

O 1password também é admirado pela interface agradável. Possui funções parecidas com os demais gerenciadores de senhas: carteira virtual, armazenamento de notas, preenchimento automático, gerador de senhas.

Essa última tem um diferencial: não só gera nova senha, mas ajuda a customizar de forma que não seja uma mistura de caracteres que você jamais lembraria.

O 1password funciona em quase todos os *browsers* e a interface é boa em qualquer um deles. Também tem a opção de ser usado em um só local ou sincronizar pelas nuvens (Dropbox, iCloud e até na sua rede WiFi).

Sua função de monitoramento da web é uma das melhores e reporta qualquer informação de ataque aos serviços da internet em que você estiver inscrito.

O *software* é pago e custa 3 dólares por mês. Existem condições especiais para os planos familiares e empresariais.

## Roboform

O Roboform é o gerenciador de senhas mais antigo – desde 1999. Há alguns anos, passou por atualizações que permitiram que ele permanecesse na corrida com os novos concorrentes e, por isso, tem fãs que não o deixam.

O programa tem a opção de portabilidade (levar no pendrive a qualquer lugar), sincronização nos dispositivos, gerenciamento offline e boa interface.

É possível utilizá-lo em muitos *browsers* e uma função interessante é a possibilidade de identificar, como favoritas, as plataformas que você mais usa, para acesso rápido. Também, tem preenchimento automático e um bom gerador de senhas.



Por ter muita experiência na área, esse gerador de senha oferece segurança em um nível mais elevado. Não é tão famoso quanto os outros, mas, ainda assim, mantém-se como uma boa opção.

O Roboform é gratuito só para os primeiros 10 *logins*. A partir daí, ele cobra 20 dólares por ano.

## As desvantagens dos gerenciadores de senhas

Como nem tudo é perfeito, até mesmo os gerenciadores de senhas oferecem algumas fraquezas. Por exemplo, eles podem ser feitos com um código fraco, deixando a sua senha um pouco vulnerável.

Você acaba correndo o risco de ter suas senhas descobertas, caso alguém consiga decifrar sua chave mestra. Se quiser evitar que isso aconteça, prefira os aplicativos com autenticação em duas etapas.

Antes de começar a usar, pesquise sobre sites que bloqueiam o uso de gerenciadores de senhas. Alguns desenvolvedores alegam que esse uso facilita ataques automáticos, que enfraquece a proteção contra *phishing* e até negam a compatibilidade com os serviços.

Ainda assim, Maria Varmazis, especialista em segurança e privacidade do site Naked Security, [resolveu testar os gerenciadores de senhas depois de ler vários artigos](#).

Antes, Varmazis mantinha senhas simples para sites que não eram tão importantes, algumas mais difíceis para aqueles que não deveriam ser invadidos e as mais complicadas para serviços financeiros.

Entre os motivos para se usar um gerenciador de senhas, Varmazis destaca que é quase impossível você se lembrar de todas as senhas. No caso dela, ficou sem acesso à conta de e-

mail durante uma viagem, o que pode ser muito irritante. Além disso, existem as facilidades já citadas acima, como a criação de senhas fortes.

Sempre há um jeito de melhorar alguma coisa na sua vida. Uma das formas de você descobrir como avançar, é por meio da leitura. Encontre novos *life hacks* nos livros do [12min](#).

E, falando em gerenciadores, que tal aprender a [gerenciar melhor as suas tarefas](#)?

Se você está buscando mais produtividade, vai gostar deste microbook:

[Produtividade Para Quem Quer Tempo](#)