HISTÓRIA / DEMOCRACIA / DIREITOS

Suas contas protegidas

8 **temas para entender**
e participar com consciência

Senhas diferentes, verificação em duas etapas e preparação para recuperar o acesso

ORGANIZAÇÃO
Régys Borges da Silveira

1ª EDIÇÃO · 2026

Antes de começar

Perder uma conta pode afetar outras: o e-mail costuma receber mensagens de recuperação e o celular pode confirmar acessos. Esta cartilha organiza os cuidados para entrar, guardar credenciais e preparar uma alternativa antes de precisar dela. Faça ajustes pelo serviço oficial e não compartilhe senhas nem códigos para pedir ajuda.

O que você vai encontrar

01 Descubra quais contas abrem outras portas

02 Uma senha vazada não precisa abrir todas as contas

03 Organize senhas sem deixá-las à vista

04 Ative uma segunda etapa e cuide dos códigos

05 Entenda a chave de acesso antes de criar uma

06 Estar conectado também é uma autorização

07 Prepare a recuperação antes de perder o celular

08 Se houver suspeita, procure o caminho oficial

Os exemplos sem indicação de um caso real são situações didáticas. As explicações resumem regras e práticas; não substituem a consulta à fonte ou orientação para um caso pessoal.

01 Descubra quais contas abrem outras portas

O e-mail de recuperação merece atenção especial.

E-mail	Pode receber recuperação de outras contas
Conta do sistema	Pode guardar acessos e configurações
Alternativa	Precisa continuar disponível

Faça uma lista dos serviços importantes e veja qual e-mail ou telefone cada um utiliza para recuperar o acesso. Guarde essa organização sem incluir senhas em um arquivo desprotegido. Uma conta usada para recuperar várias outras concentra consequências se for invadida ou perdida.

Comece a proteção por esses acessos centrais: senha diferente, verificação adicional e dados de recuperação atualizados. A recuperação depende das regras e das provas exigidas pelo serviço; saber seu nome de usuário não garante que ele devolverá a conta.

> Exemplo hipotético: Mário percebe que três serviços enviam a recuperação para um e-mail antigo ao qual não consegue mais entrar. Ele procura atualizar os cadastros enquanto ainda tem acesso.

Confira hoje quais e-mails e telefones seus serviços utilizam para recuperação.

Acessar a fonte [4]: Autenticação — pp. físicas 11, 14 e 19

Conheça também meus livros · livros.regys.com.br

02 Uma senha vazada não precisa abrir todas as contas

Use uma senha diferente para cada conta.

Exclusiva	Não reutilizada em outro serviço
Longa	Difícil de adivinhar
Sem pistas	Evite nomes e datas pessoais

Repetir a mesma senha facilita que o vazamento de um serviço seja usado em outro. Crie senhas longas e diferentes, sem sequências óbvias ou informações pessoais fáceis de descobrir. Siga também os requisitos apresentados pelo serviço.

Um gerenciador pode ajudar a criar e guardar essas senhas. Se souber que uma senha foi exposta, troque-a pelo canal oficial e substitua o mesmo segredo onde ele tiver sido repetido. Não faça a troca seguindo um link de alerta que você não conferiu.

> Exemplo hipotético: Depois de um aviso legítimo de exposição, Elisa troca a senha daquela conta e as de outras em que havia usado a mesma combinação.

Comece pelas contas centrais e elimine a reutilização de senhas.

Acessar a fonte [4]: Autenticação — pp. físicas 7–10 e 16 • Acessar a fonte [2]: Geração de senhas — seção Gerar uma nova senha

03 Organize senhas sem deixá-las à vista

Guardar senhas exige proteger também o lugar onde elas ficam.

Gerenciador	Proteja a entrada e a recuperação
Papel	Guarde em local seguro
Arquivo comum	Evite lista desprotegida de senhas

Um gerenciador de senhas organiza credenciais e pode oferecer geração de combinações diferentes. Confira a origem, a proteção de acesso e as opções de recuperação. Se houver senha principal, proteja-a com cuidado; outros mecanismos devem ser conferidos na ajuda do gerenciador escolhido.

Se optar por anotar senhas em papel, guarde-o em local protegido. Uma lista visível ao lado do aparelho ou uma foto enviada em grupo expõe as contas. O objetivo é conseguir recuperar seu acesso sem deixar o conjunto disponível a outras pessoas.

> Exemplo hipotético: Celina decide usar um gerenciador. Antes de transferir suas contas, consulta as instruções de recuperação e guarda a informação de emergência em local protegido.

Escolha um método que consiga usar e proteger, inclusive numa emergência.

Acessar a fonte [4]: Autenticação — pp. físicas 9 e 12 • Acessar a fonte [2]: Geração de senhas — introdução e seção Gerar uma nova senha • Acessar a fonte [3]: Proteção das senhas guardadas — introdução e seção Crie uma Senha Principal

04 Ative uma segunda etapa e cuide dos códigos

A verificação em duas etapas acrescenta proteção ao acesso.

Configurar	Use a área de segurança da conta
Confirmar	Aprove apenas acessos iniciados por você
Reserva	Guarde códigos de recuperação

Muitos serviços combinam a senha com uma confirmação adicional. Consulte as opções: chave de segurança, aplicativo gerador de códigos ou mensagem, conforme disponibilidade. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) recomenda preferir chave física ou aplicativo a mensagens de texto.

Nenhum código deve ser repassado a um suposto atendente por ligação ou conversa. Recuse pedidos de aprovação de entrada que você não iniciou. Se o serviço fornecer códigos de reserva, guarde-os protegidos e separados da única forma de entrar.

> Exemplo hipotético: Lúcia recebe uma solicitação de aprovação sem estar tentando entrar. Ela recusa e abre a área de segurança pelo aplicativo conhecido para conferir os acessos.

Autorize somente uma entrada que você reconhece e iniciou.

Acessar a fonte [4]: Autenticação — pp. físicas 4–6 e 12

05 Entenda a chave de acesso antes de criar uma

Crie chaves de acesso somente em dispositivos pessoais que você controla.

Disponibilidade	Depende do serviço e do aparelho
Desbloqueio	Pode autorizar a entrada na conta
Recuperação	Confira antes de perder o dispositivo

Alguns serviços oferecem chave de acesso, também chamada passkey, como alternativa à senha. Em aparelhos compatíveis, a entrada pode usar o desbloqueio do dispositivo. O funcionamento e a recuperação variam conforme o serviço e onde a chave está guardada.

No exemplo da Conta do Google, criar essa chave em computador compartilhado é arriscado: outra pessoa que desbloqueie o aparelho poderá entrar. Sair da conta no navegador não basta para desfazer a chave criada. Confira como remover acessos antes de vender ou emprestar o dispositivo.

> Exemplo hipotético: Num computador emprestado, Pedro recusa a criação de uma chave de acesso. Ele consulta a ajuda do serviço para usar um meio que não deixe acesso permanente ali.

Leia os requisitos e o procedimento de remoção antes de criar a chave.

Acessar a fonte [1]: Chaves de acesso — seções Verificar os requisitos da chave de acesso e Configurar chaves de acesso

06 Estar conectado também é uma autorização

Revise dispositivos e serviços que continuam com acesso à sua conta.

Dispositivos	Há algum que você não reconhece?
Serviços	O acesso concedido ainda é necessário?
Avisos	Confira pela própria área de segurança

Algumas contas permanecem abertas depois de você fechar o aplicativo. Consulte na área de segurança os dispositivos conectados e os acessos recentes, quando disponíveis. Ao perder ou trocar um aparelho confiável, remova a autorização conforme a ajuda do serviço.

Entrar em outro aplicativo usando uma conta existente também concentra acessos. Revise os serviços autorizados e remova os que não utiliza mais. Se receber um alerta, confira diretamente no serviço; não use o link da mensagem como única prova de que houve uma invasão.

> Exemplo hipotético: Ao trocar de celular, Teresa encontra o aparelho antigo na lista de dispositivos da conta. Ela segue o procedimento oficial para retirar aquela autorização.

Revise aparelhos antigos e acessos concedidos que deixaram de ser necessários.

Acessar a fonte [4]: Autenticação — pp. físicas 15–16 e 20

07 Prepare a recuperação antes de perder o celular

Atualize alternativas de acesso enquanto ainda consegue entrar.

Contato	E-mail e telefone precisam estar atuais
Reserva	Proteja códigos e meios alternativos
Troca	Confira o novo acesso antes de apagar o antigo

Confirme se você ainda controla o e-mail e o número cadastrados. Quando o serviço permitir alternativas, configure-as e entenda seu uso. Guardar o único código de reserva dentro da conta bloqueada não ajuda a recuperá-la.

Antes de trocar de aparelho, siga a documentação para transferir ou substituir os mecanismos de autenticação. Não apague o dispositivo antigo até conferir o acesso necessário no novo. Se códigos de reserva forem perdidos ou expostos, substitua-os conforme o serviço.

> Exemplo hipotético: Antes de restaurar o celular antigo, José confirma a entrada no novo e revisa os métodos de recuperação. Só depois remove as autorizações antigas.

Tenha uma alternativa que não dependa apenas do aparelho que pode perder.

Acessar a fonte [4]: Autenticação — pp. físicas 6 e 19–20

08 Se houver suspeita, procure o caminho oficial

Reaja pelo serviço oficial e use um aparelho confiável para proteger o acesso.

Conferir	Abra diretamente a área de segurança
Conter	Troque o segredo exposto e reveja acessos
Recuperar	Use o atendimento oficial se perdeu a entrada

Uma mensagem de alerta pode ser verdadeira ou uma tentativa de obter sua senha. Abra o serviço diretamente e verifique. Se houve acesso indevido, altere a senha, confira a verificação em duas etapas e retire autorizações desconhecidas pelos recursos disponíveis.

Se suspeitar de programa malicioso no aparelho, faça a troca de senhas em outro que considere seguro, ou depois de resolver o problema. Se perdeu a entrada, siga a recuperação oficial. Evite promessas de recuperar qualquer conta mediante pagamento e entrega de códigos.

> Exemplo hipotético: Após um acesso que não reconhece, Helena usa outro aparelho de confiança para entrar no serviço, proteger a conta e revisar os dispositivos conectados.

Destino oficial, aparelho confiável e recuperação preparada: mantenha os três.

Acessar a fonte [4]: Autenticação — pp. físicas 12, 16 e 20 • Acessar a fonte [5]: Computadores — p. física 17

Referências bibliográficas

Fontes em ordem alfabética. Os números identificam os links usados no texto. Os títulos originais e as datas de consulta constam de cada referência.

[1] GOOGLE. **Fazer login com uma chave de acesso em vez de uma senha**. Central de Ajuda do Google, [s.d.]. Disponível em: https://support.google.com/accounts/answer/13548313?hl=pt-BR. Acesso em: 20 out. 2026.

[2] MOZILLA. **Como gerar uma senha segura no Firefox**. Suporte Mozilla, [s.d.]. Disponível em: https://support.mozilla.org/pt-BR/kb/como-gerar-uma-senha-segura-no-firefox. Acesso em: 20 out. 2026.

[3] MOZILLA. **Use uma senha principal para proteger contas e senhas armazenadas**. Suporte Mozilla, [s.d.]. Disponível em: https://support.mozilla.org/pt-BR/kb/use-senha-principal-para-proteger-contas-e-senhas. Acesso em: 20 out. 2026.

[4] NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Autenticação**. NIC.br, novembro de 2022, 2022. Disponível em: https://cartilha.cert.br/fasciculos/autenticacao/fasciculo-autenticacao.pdf. Acesso em: 20 out. 2026.

[5] NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Computadores**. NIC.br, abril de 2024, 2024. Disponível em: https://cartilha.cert.br/fasciculos/computadores/fasciculo-computadores.pdf. Acesso em: 20 out. 2026.

Sobre esta cartilha

Para conferir antes de compartilhar

1

QUEM ESTÁ ENVOLVIDO?

Identifique as pessoas, instituições e responsabilidades de cada situação. Um exemplo não descreve todos os integrantes de um grupo nem permite generalizar uma conduta.

2

QUE TIPO DE REGISTRO É ESSE?

Uma lei estabelece regras; uma pesquisa apresenta resultados e limites; uma notícia relata um acontecimento. Exemplos hipotéticos ajudam a explicar uma ideia, mas não comprovam fatos reais.

3

QUAL É A AVALIAÇÃO?

Diferencie o que a fonte documenta da explicação ou recomendação desta cartilha. Confira o contexto, a data e os limites do documento antes de tirar conclusões ou compartilhar.

Sobre a pesquisa e as interpretações

Esta cartilha é um material educativo baseado em pesquisa documental e fontes identificadas. Explicações e orientações de leitura não substituem os documentos citados nem uma análise de cada caso. O objetivo é ajudar o leitor a conferir informações e participar com consciência.

O que esta seleção permite concluir

Guia de organização de acessos, sem garantir recuperação de conta ou comparar a segurança de produtos. Requisitos, opções e atendimento são definidos por cada serviço. Fontes consultadas em 20/10/2026. Nomes de menus e recursos variam entre versões e serviços. As orientações reduzem riscos, sem garantir proteção absoluta. Exemplos são fictícios.

Recorte editorial: 20 de outubro de 2026. Normas, serviços e conhecimentos podem mudar. Confira a fonte indicada antes de aplicar uma orientação.

Organização: Régys Borges da Silveira

1ª edição · Revisão editorial: 20 de outubro de 2026.

Produção com apoio de inteligência artificial (IA). Ilustrações geradas por IA, sem valor documental. Edição distribuída em formato digital; consulte as fontes pelos links do texto e das referências.

Distribuição gratuita, sem cadastro. Materiais de terceiros mantêm suas condições de uso.

Conheça os demais volumes da coleção

CONTINUE A EXPLORAR

A leitura continua

Conheça os livros de Régys Borges da Silveira e encontre sua próxima leitura.

Explore os livros →

livros.regys.com.br

Lendo no papel?

Aponte a câmera do celular para o QR code. No PDF, toque no botão ou no endereço acima.

Este convite registra apenas a cartilha de origem e uma contagem agregada de acessos, sem identificar você.