



Sua senha sozinha não basta.

Proteja as contas.
Oriente a equipe. Saiba agir.



GESTÃO

TI

COLABORADOR

ENTENDA O RISCO

O golpe pode começar com um login válido.

Uma senha exposta pode abrir caminho para outras contas quando é reutilizada.



CADA PESSOA TEM UMA PARTE

GESTÃO	Oferece os recursos e define as regras.
TI	Configura, acompanha e contém os acessos.
COLABORADOR	Usa os cuidados e avisa quando algo foge do normal.

Toque em um perfil para ir ao conteúdo.

01 / ESCOLHA A PROTEÇÃO

Nem todo método protege do mesmo jeito.

Priorize opções resistentes a páginas falsas, conforme os sistemas e os riscos da empresa.



Chave de acesso (passkey)

Resiste a páginas falsas. Vinculada ao serviço legítimo, com PIN ou biometria. Para uso diário e contas críticas.



Chave física de segurança (FIDO2)

Resiste a páginas falsas. Usa USB ou NFC e se vincula ao serviço legítimo. Priorize contas de administrador.



App autenticador (código temporário)

Boa alternativa quando não houver chave de acesso. O código ainda pode ser capturado em site falso.



SMS ou ligação

Use quando não houver opção melhor. Há riscos de captura do código e transferência fraudulenta da linha.

Só senha? Acrescente proteção. A segunda etapa reduz o risco, mas não elimina todos os golpes.

Comece pelas contas que abrem outras portas.



E-mail corporativo

Ele recebe links de recuperação de outras contas. Protegê-lo é prioridade.



BANCO / FISCAL



ERP / NUVEM



REDES SOCIAIS

DEPOIS DE ATIVAR

1

Guarde a reserva

Gere códigos de recuperação e defina quem os guarda.

2

Registre a implantação

Anote data, sistemas cobertos e responsável.

3

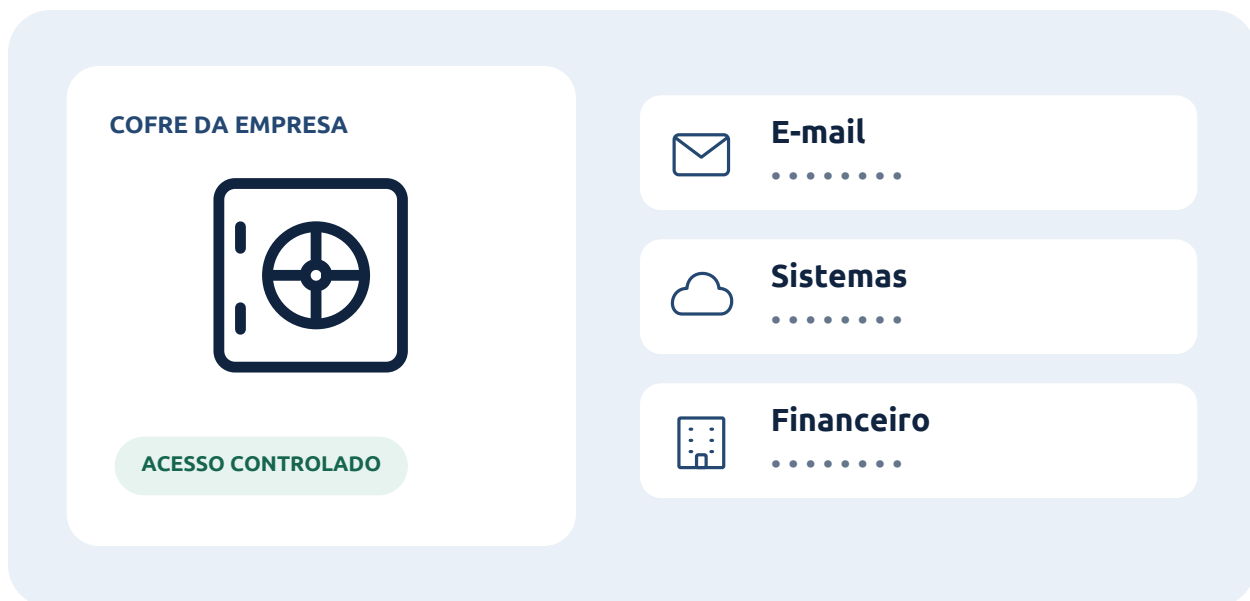
Revise os acessos

Inclua admissão, mudança de função e desligamento.

Fornecedor sem segunda etapa? Considere isso na avaliação e na renovação do contrato.

03 / OFEREÇA UM LUGAR SEGURO

Senha forte precisa de um lugar para ficar.



Adote um gerenciador corporativo.

Use-o para gerar e guardar senhas longas. Proteja o próprio cofre com autenticação forte e acessos autorizados.



Evite

Planilhas abertas, grupos e bilhetes expostos.



Prefira

Cofre aprovado, com controle de acesso.

Exceções precisam de proteção: arquivo criptografado ou anotação trancada, com responsável definido.

Uma conta. Uma senha só dela.

Quanto menos você precisa inventar e decorar, mais fácil é fazer certo.

REPETIR ESPALHA O RISCO

 PESSOAL
.....

 TRABALHO
.....

 BANCO
.....

SEPARAR LIMITA O RISCO

 PESSOAL
.....

 TRABALHO
.....

 BANCO
.....

Gere

Senhas longas e aleatórias no gerenciador.

Não reutilize

Nem entre vida pessoal e trabalho.

Precisa decorar?

Use uma frase longa de palavras sem relação.

Revise

Troque senhas repetidas e ative alertas de vazamento.



Nunca use um exemplo publicado. Evite nomes, datas, sequências de teclado e variações de 123456.

Não foi você? Não aprove.



Solicitação de acesso

Uma tentativa de login pede sua autorização.

NEGAR

Aprovar

EXEMPLO ILUSTRATIVO

1

Negue a solicitação.

Não aceite por pressão ou cansaço.

2

Avise a TI imediatamente.

Pode ser uma tentativa de acesso indevido.



Senha, código de acesso, recuperação ou transação: não repasse.
Confirme pedidos pelo contato que você já conhece.

Quatro cuidados antes do próximo clique.



Trave a tela

Saiu de perto? Bloqueie. Ative também o bloqueio automático.



Atualize

Mantenha sistema e aplicativos atualizados, inclusive no celular.



Abra por conta própria

Para entrar na conta, use o app oficial ou digite o endereço conhecido.



Confira o QR code

Verifique a origem e o destino. Desconfie de adesivos sobrepostos.

Pressa é um sinal de alerta. Mensagem bem escrita também pode ser golpe.

08 / PERCEBEU ALGO ESTRANHO?

Avise agora. A certeza pode vir depois.

Acesso desconhecido, senha que parou de funcionar ou mensagem enviada em seu nome merecem atenção.

1

Interrompa a interação

Não aprove pedidos nem envie mais dados.

2

Acione a TI e a liderança

Use outro canal se o e-mail puder estar comprometido.

3

Preserve o que aconteceu

Não apague mensagens. Registre horário e o que você viu.

**Clicou ou repassou um código?**

Avise também. O relato rápido ajuda a conter danos e deve ser recebido sem constrangimento.

Trocar a senha é só o começo.

Use um equipamento confiável e siga o procedimento de resposta. Registre as ações e seus horários.



Troque e encerre

Altere a senha e encerre as sessões ativas.



Revise a autenticação

Remova fatores, chaves e dispositivos desconhecidos.



Revise a recuperação

Confira telefone, e-mail alternativo e perguntas de segurança.



Corte acessos indevidos

Revise aplicativos autorizados e gere novos códigos de reserva.



Confira o e-mail

Remova encaminhamentos não autorizados que exponham mensagens.



Perdeu o celular ou a chave? Avise a TI e revogue os métodos e dispositivos afetados.

PROTEÇÃO DE DADOS

Se envolver dados pessoais, avalie, comunique e registre.

A LGPD exige medidas adequadas ao risco. A ausência de um controle, por si só, não define uma infração: a avaliação depende do contexto e das exigências aplicáveis.

3 dias úteis

Prazo geral de comunicação, quando ela for exigida.

5 anos

Prazo mínimo de guarda dos registros de incidentes.

AVALIAR

O controlador verifica o impacto nos dados e o risco ou dano relevante às pessoas.

COMUNICAR

Quando exigido, informar ANPD e titulares. A contagem parte da ciência de que o incidente afetou dados pessoais.

REGISTRAR

Guardar os registros por ao menos 5 anos a partir do registro, mesmo sem comunicação.

DEMONSTRAR

Manter evidências de controles, acessos, treinamento e resposta ao incidente.

Regras específicas podem alterar o prazo. Agentes de pequeno porte elegíveis têm prazo em dobro. O operador avisa o controlador sem demora injustificada.

CHECKLIST / 1 DE 2

O que já está funcionando na empresa?

Marque apenas o que está implantado. O que faltar vira uma ação com responsável e prazo.

GESTÃO

- ☐ Método de autenticação definido e documentado.
- ☐ Proteção extra ativa no e-mail e nos sistemas críticos.
- ☐ Gerenciador corporativo disponível para a equipe.
- ☐ Canal de incidentes conhecido por todos.
- ☐ Revisão de acessos na entrada, mudança e saída.

TI

- ☐ Passkey ou chave física nas contas de administrador.
- ☐ Códigos de reserva protegidos, com responsável.
- ☐ Bloqueio automático de tela configurado.
- ☐ Rotina de atualização em funcionamento.
- ☐ Procedimento para sessões, autenticação e recuperação.

CHECKLIST / 2 DE 2

Seu próximo passo começa aqui.

NO DIA A DIA

- ☐ Uso senhas diferentes em contas pessoais e de trabalho.
- ☐ Guardo senhas no gerenciador, sem deixá-las expostas.
- ☐ Não repasso senhas nem códigos de acesso.
- ☐ Nego pedidos de aprovação que não iniciei.
- ☐ Sei a quem avisar e aviso imediatamente.

RESPONSÁVEL PELO ACOMPANHAMENTO

PRAZO PARA CONCLUIR OS ITENS EM ABERTO

PRIMEIRA AÇÃO

Toque nos campos para preencher e salve uma cópia. Alguns visualizadores de celular abrem o PDF apenas para leitura.

Boas práticas. Fontes para conferir.

Edição visual baseada no manual da Prodaz. Texto condensado para leitura rápida e diagramas ilustrativos.

- | | | |
|----|--|---|
| 01 | CERT.br / NIC.br
Cartilha de Segurança para Internet: autenticação. | → |
| 02 | NIST SP 800-63B-4
Diretrizes de autenticação e gestão de autenticadores. | → |
| 03 | ANPD / Resolução nº 15/2024
Comunicação e registro de incidentes com dados pessoais. | → |
| 04 | LGPD / Lei nº 13.709/2018
Segurança, comunicação e sanções: arts. 46, 48 e 52. | → |

CASO CITADO NO MANUAL ORIGINAL

AEPD / 14 de setembro de 2026

Notificação de incidente atribuído a um agente de IA. O relato ainda estava sob análise e não permite, sozinho, afirmar uma tendência.

Toque em cada referência para abrir a fonte. Edição: setembro de 2026.

LEVE PARA A SUA EQUIPE

Transforme a leitura em um cuidado real.



ATIVE

Proteja as contas.



ORIENTE

Combine os cuidados.



AVISE

Não espere a certeza.

Precisa de ajuda para colocar o checklist em prática?

A Prodaz apoia pequenas e médias empresas em proteção de dados e segurança da informação.



CONVERSE COM A PRODAZ

(34) 99969-3656

contato@prodaz.com.br

A primeira conversa não custa nada.

Distribuição gratuita. Material informativo; não substitui orientação jurídica.