Ratio Sistemas Educacionais

Educação · Tecnologia · Segurança

Manual de Segurança Digital para Estudantes e Professores

Boas práticas, proteção de dados, prevenção de golpes
e uso seguro da tecnologia no ambiente educacional

Estudantes · Professores · Orientadores · Coordenadores

2026

Apresentação

Este manual foi elaborado para ser um recurso prático, claro e confiável sobre segurança digital no ambiente educacional. Ele não é um tratado técnico nem um manual de TI — é um guia voltado a pessoas comuns que usam tecnologia no dia a dia do estudo e do ensino.

Objetivo

Oferecer orientações acessíveis, baseadas em boas práticas reconhecidas internacionalmente, para que estudantes, professores e profissionais da educação possam proteger suas contas, arquivos, identidade e privacidade digital. O foco é a prevenção cotidiana: hábitos simples que reduzem significativamente o risco de incidentes.

Público-Alvo

• Estudantes do ensino médio, técnico e superior
• Professores e instrutores de todas as disciplinas
• Orientadores, coordenadores e supervisores pedagógicos
• Gestores e profissionais de suporte educacional
• Qualquer pessoa inserida em um ambiente escolar ou acadêmico

Escopo

O conteúdo abrange os riscos digitais mais comuns no contexto educacional: senhas e autenticação, golpes por e-mail e mensagem, segurança de dispositivos, uso de redes Wi-Fi, armazenamento em nuvem, privacidade de dados, plataformas educacionais, uso responsável de inteligência artificial e conduta em caso de incidente. Não inclui técnicas ofensivas, exploração de vulnerabilidades ou qualquer instrução que possa ser usada para causar dano.

Natureza deste Material

• Educacional — voltado à prevenção e à formação de bons hábitos digitais
• Defensivo — não contém instruções ofensivas ou de exploração de sistemas
• Independente — pode ser usado individualmente, em sala de aula ou em oficinas
• Atualizado — alinhado às diretrizes do CERT.br, NIST e CISA (2024)
• Livre de juridiquês — linguagem clara, sem excesso de termos legais

Como usar este manual

Cada capítulo é independente: você pode ler na ordem, começar pelo tema mais urgente ou usar capítulos isolados em atividades de formação. Ao final de cada capítulo há um checklist prático e

perguntas de revisão que podem ser usadas em dinâmicas de grupo ou autoavaliação. O Glossário (ao final) explica os termos técnicos usados ao longo do texto.

Este material é produzido pela Ratio como recurso educacional de acesso livre para instituições de ensino, professores e estudantes.

Sumário

Introdução

A escola e a universidade são ambientes onde dados pessoais, documentos acadêmicos, contas institucionais e informações de centenas de pessoas circulam diariamente. Entender os riscos digitais presentes nesse contexto é o primeiro passo para agir com mais segurança.

Imagine um estudante que envia seu trabalho de conclusão de curso por e-mail para um endereço ligeiramente errado — ou que perde o pendrive onde guardou a única cópia de seu projeto. Imagine um professor que recebe uma mensagem urgente pedindo sua senha de acesso ao sistema da instituição, e fornece por engano. Ou uma coordenadora que clica em um link recebido no grupo do WhatsApp da escola e tem seu celular comprometido.

Esses não são cenários hollywoodianos. São situações cotidianas, documentadas e recorrentes. Segundo o relatório anual do CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), o phishing — golpe que engana a vítima para que forneça dados — permanece entre as ameaças mais frequentes registradas no país. A grande maioria dos incidentes digitais não exige hackers sofisticados: basta um descuido, uma senha fraca ou um link malicioso.

O ambiente educacional tem características que o tornam especialmente vulnerável: alta rotatividade de usuários, dispositivos compartilhados, redes abertas, uso de plataformas diversas e, muitas vezes, pouca cultura de segurança digital entre os usuários. Ao mesmo tempo, é um ambiente com alto potencial de transformação: uma boa formação em segurança digital chega, por meio de estudantes e professores, a famílias, comunidades e organizações inteiras.

Dados do contexto brasileiro (CERT.br, 2023)

- O CERT.br registrou mais de 1,2 milhão de notificações de incidentes em 2023
- Fraudes e phishing responderam por uma parcela significativa dos casos
- Dispositivos móveis são cada vez mais alvo de golpes via SMS e WhatsApp
- A maior parte dos incidentes envolve erro humano, não falha técnica complexa
- Fonte: CERT.br — Estatísticas de Incidentes de Segurança (nic.br/cert)

O que este manual não é

Este manual não é um curso de hacking. Não ensina a invadir sistemas, explorar vulnerabilidades ou contornar proteções. Não foi escrito para especialistas em segurança da informação — embora eles possam usá-lo como material de referência para formações.

O que este manual é

- Um guia prático de proteção cotidiana para o ambiente educacional

- Uma referência acessível baseada em boas práticas reconhecidas internacionalmente
- Um recurso que pode ser usado individualmente, em sala de aula ou em oficinas
- Um documento que respeita a inteligência do leitor sem exigir formação técnica
- Um material que trata segurança digital como hábito, não como paranoia

■ Segurança digital é comportamento, não só ferramenta

> Instalar um antivírus ou usar uma rede privada virtual (VPN) ajuda, mas não substitui hábitos seguros. A maioria dos incidentes acontece porque alguém clicou em algo suspeito, reutilizou uma senha ou deixou uma sessão aberta em computador público. Ferramenta sem comportamento correto tem eficácia limitada.

Ao longo deste manual, você encontrará explicações claras, exemplos do dia a dia educacional, checklists práticos e orientações sobre o que fazer quando algo der errado. O objetivo não é criar medo — é criar preparo.

Capítulo 1

O que é segurança digital

Objetivo: compreender o que significa segurança digital, conhecer os conceitos fundamentais de risco, ameaça, vulnerabilidade e incidente, e entender por que esses temas dizem respeito a qualquer pessoa que usa tecnologia no ambiente educacional.

1.1 Conceito geral

Segurança digital — ou segurança da informação aplicada ao ambiente digital — é o conjunto de práticas, comportamentos e medidas técnicas que protegem dados, sistemas e comunicações contra acessos não autorizados, modificações indevidas ou indisponibilidade. Em linguagem simples: é garantir que as informações certas estejam disponíveis para as pessoas certas, no momento certo, e que ninguém mais possa acessá-las ou alterá-las sem permissão.

Segurança digital não é exclusividade de empresas ou governos. Qualquer pessoa que usa um e-mail, armazena fotos no celular, faz login em plataformas de ensino ou envia arquivos pela internet está lidando com informações que precisam ser protegidas. No ambiente educacional, isso inclui notas, provas, planos de aula, documentos pessoais, dados de alunos e muito mais.

1.2 A tríade da segurança da informação

O modelo mais consolidado para entender segurança da informação é a chamada tríade CIA (do inglês Confidentiality, Integrity, Availability), traduzida como Confidencialidade, Integridade e Disponibilidade. Cada pilar representa uma dimensão distinta do que significa proteger uma informação.

Pilar	Significado	Exemplo no ambiente educacional
Confidencialidade	Somente quem tem permissão pode acessar a informação.	A lista de notas de uma turma deve ser vista apenas pelo professor e pela coordenação.
Integridade	A informação deve ser precisa e não pode ser alterada sem autorização.	Um aluno não deve conseguir alterar sua própria nota no sistema.
Disponibilidade	A informação deve estar acessível quando quem tem permissão precisar dela.	O professor deve conseguir acessar o sistema de presenças na hora da aula.

1.3 Risco, ameaça, vulnerabilidade e incidente

Quatro termos são essenciais para pensar sobre segurança digital. Eles se relacionam, mas têm significados distintos:

Vocabulário fundamental

• Ameaça: qualquer coisa que possa causar dano — um vírus, um golpista, um funcionário descuidado ou até uma queda de energia.

• Vulnerabilidade: uma fraqueza que pode ser explorada por uma ameaça — uma senha fraca, um sistema desatualizado, um usuário sem treinamento.

• Risco: a combinação de ameaça + vulnerabilidade. Risco = probabilidade de algo ruim acontecer × impacto se acontecer.

• Incidente: quando o risco se concretiza — uma conta invadida, um arquivo apagado, dados vazados.

1.4 Acidente, descuido e ataque — diferenças importantes

Nem todo incidente é um ataque. É importante distinguir três origens diferentes para agir de forma proporcional:

• Acidente: falha técnica sem intenção — um disco rígido que para de funcionar, um servidor que cai por problema de energia.
• Descuido: erro humano sem intenção maliciosa — clicar em um link suspeito por distração, enviar um arquivo para o destinatário errado, esquecer o login aberto em computador público.
• Ataque: ação intencional de terceiro para causar dano — phishing, invasão de conta, ransomware.

No ambiente educacional, a esmagadora maioria dos incidentes decorre de descuido — não de ataques sofisticados. Isso é uma boa notícia: comportamentos simples e consistentes reduzem muito o risco.

Exemplo Prático — Risco em sala de aula

Uma professora usa o computador do laboratório para projetar conteúdo e se esquece de encerrar a sessão do e-mail institucional ao sair. O próximo usuário — um aluno — tem acesso à caixa de entrada dela, que contém informações de avaliações e dados de outros alunos. Não há ataque aqui: há vulnerabilidade (sessão aberta) e descuido (não fazer logout). O impacto pode ser sério mesmo sem intenção.

1.5 Por que a educação é um ambiente de risco digital

Escolas e universidades concentram características que elevam o risco digital:

• Alta rotatividade de usuários em dispositivos compartilhados
• Uso de redes Wi-Fi abertas ou de segurança limitada
• Grande volume de dados pessoais de menores de idade
• Plataformas diversas com diferentes níveis de segurança

• Pressão de prazos que leva a comportamentos descuidados
• Baixa cultura de segurança digital entre boa parte dos usuários
• Pouca política institucional de segurança em muitas escolas

Checklist — Conceitos básicos que todo usuário deve conhecer

- ■ Sei o que são confidencialidade, integridade e disponibilidade
- ■ Entendo a diferença entre ameaça, vulnerabilidade, risco e incidente
- ■ Sei distinguir acidente, descuido e ataque
- ■ Reconheço que a maior parte dos incidentes vem de descuido humano
- ■ Entendo que segurança digital é responsabilidade de todos, não só da TI

Erros comuns de entendimento

✗ "Segurança digital é coisa de especialista" — qualquer usuário tem responsabilidade sobre suas próprias práticas.

✗ "Não tenho nada importante para proteger" — dados pessoais, senhas e arquivos acadêmicos são valiosos para golpistas.

✗ "Se eu tiver antivírus, estou protegido" — ferramentas ajudam, mas não substituem comportamento seguro.

✗ "Isso não acontece comigo" — incidentes são democráticos: afetam pessoas de todos os níveis técnicos.

Perguntas de Revisão

1. Explique com suas palavras o que significa a tríade Confidencialidade, Integridade e Disponibilidade.

2. Qual é a diferença entre ameaça e vulnerabilidade? Dê um exemplo de cada para o contexto escolar.

3. Por que descuidos humanos são mais comuns que ataques sofisticados em ambientes educacionais?

4. Cite duas características do ambiente educacional que aumentam o risco digital.

Com esses conceitos em mente, os próximos capítulos abordam as situações práticas mais comuns — começando por onde a maioria dos incidentes começa: as senhas.

Capítulo 2

Senhas e autenticação

Objetivo: aprender a criar senhas fortes e únicas, entender como gerenciadores de senha facilitam a vida com mais segurança, e adotar a autenticação em dois fatores (MFA) como proteção essencial para contas pessoais e institucionais.

2.1 Por que senhas importam tanto

A senha é, em geral, a única barreira entre uma conta e um invasor. Quando alguém obtém sua senha — seja por adivinhação, vazamento ou golpe — tem acesso a tudo que você armazena, envia e recebe naquela conta. No ambiente educacional, isso pode significar: e-mails institucionais, notas, arquivos de alunos, comunicações internas e dados pessoais.

Segundo o relatório Have I Been Pwned (haveibeenpwned.com), que agrega dados de vazamentos públicos, bilhões de combinações de e-mail e senha já foram expostas. As senhas mais comuns encontradas em vazamentos seguem sendo "123456", "password" e variações simples — o que mostra que o problema não é técnico, mas comportamental.

2.2 O que torna uma senha forte

Uma senha forte tem três características principais: comprimento, complexidade e imprevisibilidade. O NIST (Instituto Nacional de Padrões e Tecnologia dos EUA) recomenda priorizar o comprimento — senhas longas são geralmente mais seguras do que senhas curtas com símbolos aleatórios.

Característica	Recomendação	Exemplo fraco	Exemplo forte
Comprimento	Mínimo 12–16 caracteres	Maria123	MariaGosta!DeChocolate42
Variedade	Maiúsculas, minúsculas, números, símbolos	professor	Prof@SS0r!2024
Imprevisibilidade	Evite nomes, datas e palavras do dicionário	nascimento2001	xK#9mL!qRt2@
Unicidade	Uma senha diferente para cada serviço	mesma senha em tudo	senha única por site

2.3 Senhas únicas — por que reutilizar é perigoso

Quando você usa a mesma senha em vários serviços e uma deles sofre um vazamento, todos os outros ficam expostos. Esse ataque chama-se "credential stuffing": o invasor pega listas de senhas vazadas e testa automaticamente em outros serviços. Uma senha única por serviço limita

o dano a um único vazamento.

■ Verificação de vazamentos

Você pode verificar se seu e-mail já apareceu em algum vazamento público acessando o site haveibeenpwned.com — serviço gratuito mantido pelo pesquisador de segurança Troy Hunt. Se seu e-mail aparecer, troque as senhas dos serviços listados imediatamente.

2.4 Gerenciadores de senha

Memorizar dezenas de senhas únicas e longas é humanamente impossível. A solução são os gerenciadores de senha: aplicativos que armazenam e geram senhas seguras, protegidos por uma única senha mestra forte. Você precisa lembrar apenas de uma senha — o gerenciador cuida do resto.

Gerenciadores de senha recomendados (gratuitos e auditados)

- Bitwarden — código aberto, gratuito, multiplataforma, auditado por terceiros
- KeePassXC — local (sem nuvem), código aberto, altamente controlável
- Proton Pass — integrado ao ecossistema Proton, versão gratuita disponível
- Nota: gestores embutidos em navegadores (Chrome, Firefox) também ajudam, mas têm limitações em comparação com soluções dedicadas

2.5 Autenticação em dois fatores (MFA)

Mesmo uma senha forte pode ser comprometida — por vazamento, phishing ou engenharia social. A autenticação multifator (MFA ou 2FA) adiciona uma segunda camada de verificação: além da senha, o sistema exige algo que somente você possui (como um código temporário no celular).

Segundo a Microsoft, contas com MFA ativo resistem a mais de 99% dos ataques automatizados de invasão de conta. Isso não significa invulnerabilidade, mas a proteção adicional é substancial.

Tipo de MFA	Como funciona	Segurança	Recomendado para
App autenticador	Código de 6 dígitos gerado localmente (TOTP)	Alta	Contas importantes — e-mail, banco, AVA
SMS / ligação	Código enviado por mensagem de texto	Média	Melhor que nada; evite para contas críticas
Chave física (hardware)	Dispositivo USB/NFC que confirma presença física	Muito alta	Contas institucionais sensíveis
E-mail de confirmação	Código ou link enviado ao e-mail	Média	Só se o e-mail também tiver MFA

2.6 Erros comuns com senhas

Erros comuns — Senhas e autenticação

✗ Usar a mesma senha em e-mail pessoal, e-mail institucional e redes sociais

✗ Incluir nome, data de nascimento ou nome da escola na senha

✗ Anotar a senha em papel colado no monitor ou em bloco de notas sem proteção

✗ Compartilhar senha com colegas "por praticidade"

✗ Não ativar MFA por considerar inconveniente

✗ Usar variações previsíveis da mesma senha: senha1, senha2, senha3

✗ Responder a perguntas de segurança com respostas reais e fáceis de descobrir

Exemplo Prático — Login no laboratório

João, estudante do terceiro ano, acessa o AVA da escola no computador do laboratório usando seu login e senha. Ao terminar, fecha apenas a aba do navegador — sem fazer logout. A próxima aluna a usar o computador abre o mesmo navegador, clica em "voltar" e encontra a sessão de João ainda ativa. Não houve ataque: apenas ausência do hábito de encerrar sessões em dispositivos compartilhados.

Checklist — Senhas e autenticação

- ■ Todas as minhas senhas têm ao menos 12 caracteres
- ■ Uso senhas diferentes para cada serviço importante
- ■ Utilizo um gerenciador de senha para organizar meus acessos
- ■ Meu e-mail principal tem autenticação em dois fatores ativada
- ■ Meu acesso ao AVA/LMS institucional usa MFA, se disponível
- ■ Nunca compartilho senhas com colegas ou familiares
- ■ Faço logout em dispositivos compartilhados ao terminar de usar
- ■ Já verifiquei se meu e-mail aparece em algum vazamento conhecido

Perguntas de Revisão

1. Quais são as três características de uma senha forte segundo as recomendações atuais do NIST?
2. Por que reutilizar a mesma senha em vários serviços é perigoso? O que é "credential stuffing"?
3. Qual é a função principal de um gerenciador de senha?
4. Explique o que é autenticação multifator e por que ela é mais segura do que apenas uma senha.
5. O que você deve fazer imediatamente ao descobrir que sua senha foi vazada em um incidente?

Ter senhas fortes e MFA ativo é a base da proteção digital. O próximo capítulo aborda o principal vetor de entrada para invasões: os golpes de engenharia social.

Capítulo 3

Golpes comuns e engenharia social

Objetivo: reconhecer os principais golpes digitais que afetam estudantes e professores, entender como a engenharia social manipula a confiança das pessoas, e desenvolver o hábito de verificar antes de clicar, responder ou fornecer informações.

3.1 O que é engenharia social

Engenharia social é a arte de manipular pessoas para que revelem informações confidenciais ou realizem ações prejudiciais — sem precisar "hackear" sistemas. O alvo não é a tecnologia; é o ser humano. Golpistas exploram emoções como urgência, medo, curiosidade, ganância ou confiança para fazer a vítima agir sem pensar.

No ambiente educacional, a engenharia social pode se disfarçar de mensagem da direção, aviso urgente sobre notas, e-mail do sistema de biblioteca, comunicado sobre bolsas ou até uma solicitação de colega "precisando de ajuda urgente".

3.2 Phishing

Phishing é o golpe digital mais comum. O nome vem do inglês "fishing" (pescar): o golpista "lança uma isca" esperando que alguém morda. Geralmente chega como e-mail, mas pode aparecer em mensagens de texto, aplicativos de chat e até ligações telefônicas.

Como um phishing típico funciona

- 1. Você recebe um e-mail com aparência legítima (logotipo, linguagem formal)
- 2. A mensagem cria urgência: "Sua conta será suspensa em 24 horas"
- 3. Há um link para um site falso que imita o site real
- 4. Você digita usuário e senha no site falso
- 5. O golpista captura suas credenciais e acessa sua conta real

3.3 Smishing e vishing

Smishing é phishing via SMS ou WhatsApp. Vishing é phishing por voz (ligação telefônica). Ambos usam as mesmas táticas de urgência e confiança, mas em canais diferentes. No Brasil, golpes via WhatsApp têm crescido expressivamente, incluindo variantes que se passam por instituições de ensino, serviços públicos ou até contatos conhecidos.

3.4 Golpes mais comuns no ambiente educacional

Golpe	Como funciona	Sinal de alerta
Falso aviso de suspensão de conta	E-mail ou mensagem urgente pedindo que você clique num link para "reativar" acesso ao AVA, e-mail ou sistema da escola.	Urgência exagerada, link com URL estranha, remetente suspeito.
Falsa bolsa ou benefício	Mensagem oferecendo bolsa, auxílio ou desconto, pedindo dados pessoais ou pagamento de taxa.	Oferta inesperada, pedido de dados bancários ou documentos.
Pedido falso de código MFA	"Enviei um código por engano para o seu número, pode me passar?" — na verdade, é o código de recuperação da sua conta.	Nunca compartilhe códigos MFA com ninguém, por nenhum motivo.
Falsa coleta de dados acadêmicos	Formulário disfarçado de pesquisa institucional pedindo nome, CPF, matrícula e senha.	Formulário não oficial, pedindo senha — nenhuma pesquisa legítima pede senha.
Golpe do "professor"	Mensagem no WhatsApp se passando por professor pedindo que o aluno compre vale-presente ou transfira dinheiro.	Pedido de dinheiro por mensagem — ligue para confirmar antes de qualquer ação.

3.5 Como reconhecer um golpe

Golpes bem-feitos podem ser difíceis de identificar à primeira vista. Mas quase todos têm ao menos um dos sinais abaixo:

- Urgência artificial: "Responda agora", "Sua conta será bloqueada em 2 horas"
- Remetente suspeito: o domínio do e-mail não corresponde à instituição real (ex.: contato@univesidade-oficial.com.br versus univesidade-oficial.edu.br)
- Link diferente do que parece: passe o mouse sobre o link antes de clicar e verifique o endereço real no rodapé do navegador
- Erros de português ou formatação estranha
- Pedido de senha, código MFA ou dados pessoais — nunca forneça por e-mail ou mensagem
- Oferta boa demais para ser verdade
- Pressão para não comentar com ninguém

■ A regra de ouro contra golpes

Antes de clicar em qualquer link, abrir qualquer anexo ou fornecer qualquer informação em resposta a uma mensagem inesperada: PARE. Respire. Questione. Se houver dúvida, acesse o serviço diretamente pelo navegador (não pelo link recebido) ou ligue para a instituição pelo número oficial. Golpistas contam com a pressa e a confiança da vítima.

3.6 Engenharia social no ambiente escolar

Além dos golpes digitais, a engenharia social pode acontecer de forma presencial ou híbrida no ambiente educacional:

• Colega que pede para usar seu login "por um momento"
• Pessoa desconhecida que faz perguntas detalhadas sobre a rotina da escola
• Solicitação de dados de alunos por e-mail não verificado
• Pedido de acesso a sistema administrativo por telefone, sem processo formal

Exemplo Prático — Pedido de código no WhatsApp

Ana recebe uma mensagem de um número desconhecido: "Olá Ana, sou da secretaria da faculdade. Houve um problema no seu cadastro e precisamos do código que você acabou de receber por SMS para confirmar sua identidade." O código que Ana recebeu é, na verdade, o código de verificação em dois fatores do e-mail dela. Se Ana enviar o código, o golpista acessa sua conta. Secretarias legítimas nunca solicitam códigos de verificação por mensagem.

Checklist — Proteção contra golpes

■ Sempre verifico o remetente completo antes de clicar em links de e-mail
■ Nunca forneço senha, código MFA ou dados pessoais por mensagem ou telefone
■ Quando recebo mensagem urgente de instituição, acesso o site diretamente
■ Não clico em links de promoções ou bolsas inesperadas sem verificar
■ Sei que nenhuma instituição legítima pede senha por e-mail ou mensagem
■ Reporto mensagens suspeitas ao setor responsável da minha instituição

Erros comuns — Golpes e engenharia social

✗ Clicar em links sem verificar o endereço real de destino
✗ Confiar no visual de um e-mail (logotipo e formatação são fáceis de copiar)
✗ Compartilhar código de verificação com quem "pediu por engano"
✗ Ignorar sinais de alerta por pressão de tempo ou medo da consequência
✗ Não reportar o golpe por vergonha — relatar ajuda a proteger outros

Perguntas de Revisão

1. O que é engenharia social e por que ela é eficaz mesmo contra pessoas inteligentes?
2. Descreva como funciona um ataque de phishing típico em três etapas.
3. Quais são os cinco principais sinais de alerta de um e-mail ou mensagem fraudulenta?
4. Por que nunca se deve compartilhar um código de verificação MFA com outra pessoa?
5. O que você deve fazer ao receber uma mensagem urgente pedindo que clique em um link para evitar suspensão da sua conta?

Saber reconhecer golpes é metade da proteção. A outra metade está em adotar comportamentos seguros com e-mail, links e anexos — tema do próximo capítulo.

Capítulo 4

E-mail, links e anexos

Objetivo: desenvolver um comportamento seguro ao lidar com e-mail, saber verificar links antes de clicar e entender os riscos associados a anexos recebidos de fontes desconhecidas ou suspeitas.

4.1 O e-mail como principal vetor de ataques

O e-mail continua sendo o canal mais explorado para golpes e distribuição de malware. Isso ocorre porque é universal, permite personificação fácil e chega diretamente à caixa de entrada do usuário. No ambiente educacional, estudantes e professores recebem centenas de e-mails por semana — muitos legítimos, alguns não.

4.2 Como verificar o remetente

O nome exibido em um e-mail não é o remetente real. Qualquer pessoa pode configurar um e-mail para exibir o nome "Secretaria Acadêmica" ou "Suporte Institucional". O que importa é o endereço de e-mail completo, especialmente o domínio (a parte após o @).

Como verificar o remetente real

- Clique no nome do remetente para expandir e ver o endereço completo
- Verifique se o domínio confere com o da instituição: @universidade.edu.br vs @universidade-edu.com
- Desconfie de domínios públicos (Gmail, Hotmail) para comunicações institucionais
- E-mails de serviços como banco, AVA ou plataforma educacional devem vir do domínio oficial desses serviços
- Em dúvida: não clique. Acesse o serviço diretamente pelo navegador.

4.3 Urgência artificial — como identificar

Mensagens legítimas raramente exigem ação imediata sob pena de perda grave. Frases como "Sua conta será excluída em 24 horas", "Você foi selecionado, responda agora" ou "Ação necessária imediatamente" são táticas clássicas para fazer você agir sem pensar. Quanto maior a urgência imposta pelo remetente, maior deve ser a sua cautela.

4.4 Como verificar links antes de clicar

- Passe o cursor sobre o link (sem clicar) e observe o endereço real que aparece na barra de status do navegador ou rodapé do cliente de e-mail

- O domínio principal é a parte logo antes do último ponto antes da barra (ex.: em "login.universidade.edu.br/aluno", o domínio é "universidade.edu.br")
- Desconfie de encurtadores de URL (bit.ly, tinyurl) em e-mails institucionais
- HTTPS não garante que o site é legítimo — apenas que a conexão é criptografada
- Em caso de dúvida, copie o texto do link e cole em um verificador como o VirusTotal (virustotal.com) antes de acessar

4.5 Riscos de anexos

Anexos maliciosos são um dos métodos mais usados para distribuir malware. Qualquer tipo de arquivo pode ser malicioso, mas alguns formatos são especialmente explorados:

Tipo de arquivo	Risco	Conduta recomendada
.exe, .msi, .bat, .cmd	Alto — executam código diretamente	Nunca abra sem contexto absolutamente seguro
.docx, .xlsx, .pptx com macros	Médio-alto — macros podem executar código	Desative macros automáticas; habilite apenas se necessário e de fonte confiável
.pdf	Médio — pode conter scripts ou exploits	Mantenha o leitor de PDF atualizado; desconfie de PDFs de remetentes desconhecidos
.zip, .rar	Variável — pode conter qualquer arquivo	Verifique o remetente; escaneie antes de abrir
.jpg, .png, .mp4	Baixo — raramente explorado	Ainda assim, verifique o remetente se o contexto for estranho

4.6 Comportamento seguro com e-mail

- Não abra e-mails em HTML de remetentes completamente desconhecidos
- Se esperava um arquivo de alguém, confirme por outro canal antes de abrir
- Mantenha o cliente de e-mail e o sistema operacional atualizados
- Use a visualização em texto puro se disponível para e-mails suspeitos
- Reporte e-mails suspeitos ao suporte de TI da instituição

Exemplo Prático — Trabalho acadêmico com malware

Carlos, professor de história, recebe um e-mail de um endereço desconhecido com o assunto "Trabalho Final — Entrega atrasada". O e-mail tem um arquivo .docx anexado. Carlos abre o arquivo; uma janela pede para "Habilitar edição" e "Habilitar conteúdo" — isso ativa macros maliciosas que instalam um programa de acesso remoto no computador dele. Nunca habilite macros em documentos de remetentes desconhecidos.

Checklist — E-mail, links e anexos

- ■ Verifico o endereço completo do remetente, não apenas o nome exibido
- ■ Passo o cursor sobre links antes de clicar para ver o destino real
- ■ Nunca abro anexos executáveis (.exe, .bat) recebidos por e-mail
- ■ Desativo macros automáticas em documentos do Office
- ■ Não forneço dados pessoais ou senhas em resposta a e-mails
- ■ Reporto e-mails suspeitos ao suporte da instituição

Erros comuns — E-mail e links

- ✗ Confiar no visual do e-mail (logotipo e layout são facilmente copiados)
- ✗ Clicar em links sem verificar o destino real
- ✗ Abrir anexos sem confirmar com o remetente por outro canal
- ✗ Habilitar macros em documentos solicitados por mensagem
- ✗ Ignorar alertas do antivírus ou do próprio cliente de e-mail

Perguntas de Revisão

1. Por que o nome exibido no remetente de um e-mail não é confiável por si só?
2. Como verificar o destino real de um link antes de clicar nele?
3. Quais tipos de anexo representam maior risco e por quê?
4. O que significa "urgência artificial" e como ela é usada em golpes?

Com hábitos seguros de e-mail, você elimina grande parte do risco digital. O próximo capítulo aborda os dispositivos que usamos no dia a dia.

Capítulo 5

Segurança de dispositivos

Objetivo: adotar práticas essenciais de segurança para notebooks, desktops, celulares e tablets usados no ambiente educacional, incluindo bloqueio de tela, atualizações, backup e cuidados em dispositivos compartilhados.

5.1 Por que dispositivos precisam de proteção

Um dispositivo sem proteção adequada é uma porta de entrada para qualquer pessoa que o acesse — fisicamente ou pela rede. No ambiente educacional, dispositivos carregam e-mails, documentos, senhas salvas, histórico de navegação e acesso a plataformas institucionais. Perder um celular ou ter um notebook roubado pode expor muito mais do que apenas arquivos pessoais.

5.2 Bloqueio de tela e autenticação no dispositivo

O bloqueio de tela é a primeira linha de defesa física de um dispositivo. Um celular sem bloqueio, deixado sobre uma mesa ou perdido, dá acesso imediato a todas as contas, arquivos e aplicativos.

Configurações de bloqueio recomendadas

- Celular: PIN de 6+ dígitos, padrão complexo ou biometria (digital/face) como complemento — não como única proteção
- Notebook/desktop: senha de login forte; bloqueio automático após 2–5 minutos de inatividade
- Tablet: mesmas recomendações do celular
- Nunca use PIN 0000, 1234 ou datas de nascimento como bloqueio de tela
- Ative bloqueio remoto e localização nos celulares (ex.: "Find My" no iOS, "Encontre meu dispositivo" no Android)

5.3 Atualizações de sistema e aplicativos

Atualizações de sistema operacional e aplicativos corrigem vulnerabilidades conhecidas. Um sistema desatualizado é um alvo mais fácil porque os problemas que ele tem já são públicos — e ferramentas de exploração desses problemas estão disponíveis para qualquer pessoa.

A CISA (Agência de Segurança Cibernética dos EUA) mantém um catálogo público de vulnerabilidades conhecidas exploradas ativamente. A maioria delas tem correção disponível — o problema é que usuários e instituições demoram para aplicar atualizações.

■ Mantenha tudo atualizado

Ative atualizações automáticas sempre que possível: sistema operacional (Windows, macOS, iOS, Android, Linux), navegadores (Chrome, Firefox, Safari, Edge), aplicativos de produtividade (Office, PDF reader, e-mail), e plugins de navegador (se ainda os usa). Atualizações de segurança não devem ser adiadas por semanas.

5.4 Backup — proteção contra perda de dados

Backup é cópia de segurança dos seus dados em local diferente do original. É a única proteção confiável contra ransomware, falha de hardware, roubo ou acidente. A regra de referência é a 3-2-1:

Regra	O que significa	Exemplo prático
3	Mantenha 3 cópias dos dados importantes	Original no notebook + cópia na nuvem + cópia em HD externo
2	Use 2 tipos de mídia diferentes	Nuvem (Google Drive / OneDrive) + HD externo físico
1	Mantenha 1 cópia fora do local principal (offsite)	Nuvem é automaticamente "offsite"; HD em casa de familiar também

5.5 Antivírus e antimalware

Softwares de proteção contra malware são úteis, mas não são infalíveis. O Windows inclui o Defender, que oferece proteção básica adequada para a maioria dos usuários sem custo adicional. Sistemas macOS e Linux têm menor incidência de malware, mas não são imunes.

Importante: nenhum antivírus substitui comportamento seguro. Um usuário que clica em tudo pode ser infectado mesmo com o melhor software de proteção instalado.

5.6 Cuidados em dispositivos compartilhados

• Nunca salve senhas no navegador de computadores de laboratório ou públicos
• Sempre faça logout de todas as contas ao terminar de usar
• Verifique se a sessão encerrou de fato — fechar a aba não é logout
• Limpe o histórico de navegação se usou contas pessoais
• Não conecte pendrives ou HDs externos de procedência desconhecida
• Desconfie de software instalado em computadores compartilhados que você não reconhece

Exemplo Prático — TCC perdido por falta de backup

Fernanda estava na reta final do TCC quando o HD do notebook parou de funcionar. O único arquivo do trabalho estava no dispositivo — sem backup em nuvem ou pendrive. Perdeu seis meses de trabalho. Um serviço de nuvem gratuito (Google Drive, OneDrive) com sincronização automática teria evitado completamente a situação. Dados sem backup são dados que podem sumir a qualquer momento.

Checklist — Segurança de dispositivos

- ■ Meu celular tem bloqueio de tela com PIN de 6+ dígitos ou biometria
- ■ Meu notebook/desktop tem senha de login e bloqueio automático por inatividade
- ■ Tenho atualizações automáticas ativadas no sistema operacional
- ■ Meus aplicativos principais estão atualizados
- ■ Tenho backup dos meus arquivos importantes (regra 3-2-1 ou similar)
- ■ Não salvo senhas em computadores compartilhados
- ■ Faço logout completo após usar dispositivos de laboratório ou públicos
- ■ Tenho "localizar dispositivo" ativado no meu celular

Erros comuns — Dispositivos

- ✗ Não ter bloqueio de tela no celular por "ser inconveniente"
- ✗ Adiar atualizações de sistema indefinidamente
- ✗ Guardar arquivos importantes apenas no dispositivo, sem backup
- ✗ Salvar senhas no navegador de computadores compartilhados
- ✗ Conectar pendrives encontrados ou de origem desconhecida
- ✗ Deixar sessões abertas ao encerrar uso de computador público

Perguntas de Revisão

1. Qual é a primeira linha de defesa física de um dispositivo?
2. Por que atualizações de segurança não devem ser adiadas?
3. Explique a regra de backup 3-2-1 com um exemplo do contexto educacional.
4. Quais cuidados você deve ter ao usar um computador de laboratório compartilhado?

Dispositivos seguros são o alicerce da proteção digital pessoal. O próximo capítulo aborda as redes que conectam esses dispositivos.

Capítulo 6

Wi-Fi, redes e internet

Objetivo: entender os riscos das redes Wi-Fi abertas e domésticas, saber como proteger a conexão no ambiente escolar e fora dele, e adotar comportamentos seguros ao navegar em redes desconhecidas.

6.1 Redes Wi-Fi abertas

Redes Wi-Fi abertas — sem senha, presentes em cafeterias, bibliotecas, shoppings, aeroportos e muitas instituições de ensino — são convenientes, mas apresentam riscos específicos. Em uma rede aberta, o tráfego não criptografado pode ser capturado por qualquer pessoa conectada à mesma rede.

Isso não significa que redes abertas são sempre perigosas ou que você não deve usá-las. Significa que você deve saber o que fazer e o que evitar enquanto estiver conectado a elas.

Ação	Em rede aberta	Observação
Acessar sites HTTPS	Relativamente seguro	O conteúdo é criptografado entre você e o servidor
Acessar sites HTTP	Evitar	Tráfego legível por terceiros na rede
Fazer login em contas	Apenas com HTTPS	Verifique o cadeado no navegador
Transações bancárias/financeiras	Evitar	Use rede móvel (4G/5G) se possível
Trabalhar com documentos sensíveis	Usar VPN ou evitar	VPN criptografa todo o tráfego
Verificar e-mails	Com cautela + HTTPS	Evite em redes completamente abertas sem HTTPS

6.2 Rede doméstica — configurações básicas

A rede Wi-Fi de casa é mais segura do que uma rede pública, mas também precisa de configuração adequada. Muitos roteadores chegam de fábrica com senhas padrão amplamente conhecidas.

Configurações básicas do roteador doméstico

- Troque a senha de administrador do roteador (nunca deixe "admin/admin")
- Use WPA2 ou WPA3 como protocolo de segurança Wi-Fi — evite WEP e WPA
- Crie uma senha de Wi-Fi forte (12+ caracteres, não o endereço de casa)
- Mantenha o firmware do roteador atualizado (verificar periodicamente)
- Crie uma rede de convidados (guest network) para dispositivos de visitas
- Desative o WPS se não precisar dele — é uma vulnerabilidade conhecida

6.3 VPN — o que é e quando usar

Uma VPN (Virtual Private Network, Rede Privada Virtual) cria um túnel criptografado entre seu dispositivo e um servidor remoto, protegendo o tráfego de rede de observadores na mesma rede. Não é obrigatória no uso doméstico normal, mas pode ser útil em redes públicas.

■ VPN: não é solução mágica

Uma VPN protege seu tráfego de quem está na mesma rede, mas não te torna anônimo na internet, não substitui senhas fortes e não protege contra phishing. O provedor da VPN pode ver seu tráfego — use serviços auditados e confiáveis (Mullvad, ProtonVPN) se precisar.

6.4 Comportamento seguro em redes desconhecidas

- Verifique se está no HTTPS: o cadeado fechado na barra do navegador confirma criptografia
- Prefira usar dados móveis (4G/5G) para acessar contas importantes fora de casa
- Desative o Wi-Fi quando não estiver usando para evitar conexões automáticas
- Nunca se conecte a redes com nomes genéricos como "Free WiFi" sem confirmar com o estabelecimento que é a rede oficial
- Evite transações financeiras ou acesso a dados sensíveis em redes públicas

Exemplo Prático — Rede falsa em biblioteca

Rodrigo está na biblioteca da universidade e vê duas redes disponíveis: "Biblioteca-UFXYZ" e "Biblioteca_UFXYZ" (com underscore). Ele se conecta na segunda sem perceber a diferença. A rede falsa foi criada por alguém para capturar tráfego. Rodrigo acessa o sistema da universidade via HTTP (sem HTTPS) — suas credenciais de login são capturadas. Sempre confirme o nome exato da rede com a instituição.

Checklist — Wi-Fi e redes

- ■ Meu roteador doméstico usa WPA2 ou WPA3 com senha forte
- ■ Troquei a senha de administrador do roteador do padrão de fábrica
- ■ Em redes públicas, acesso apenas sites com HTTPS
- ■ Não faço transações financeiras em redes Wi-Fi abertas
- ■ Verifico o nome exato da rede antes de conectar em lugares públicos
- ■ Desativo o Wi-Fi quando não estou usando

Erros comuns — Redes

- ✗ Deixar a senha de administrador do roteador como padrão de fábrica
- ✗ Conectar automaticamente em qualquer rede aberta disponível
- ✗ Usar WEP como protocolo de segurança (quebrado desde os anos 2000)
- ✗ Fazer login em contas importantes via HTTP em rede pública
- ✗ Ignorar avisos de certificado SSL no navegador

Perguntas de Revisão

1. Qual é o principal risco de usar redes Wi-Fi abertas?
2. Quais configurações básicas você deve verificar no roteador doméstico?
3. O que é uma VPN e em que situações ela é recomendada?
4. Como identificar se um site está usando HTTPS?

Capítulo 7

Arquivos, nuvem e documentos acadêmicos

Objetivo: entender como armazenar, compartilhar e proteger arquivos com segurança, com foco em documentos acadêmicos — TCCs, planos de aula, avaliações, listas de alunos e outros arquivos críticos do dia a dia educacional.

7.1 O risco de perder documentos acadêmicos

Arquivos acadêmicos representam horas, semanas ou meses de trabalho. Um TCC perdido por falha de HD, um plano de aula apagado por acidente, uma prova formatada no último computador disponível — são situações reais e evitáveis com hábitos simples de organização e backup.

Além da perda acidental, há o risco de exposição: uma lista de notas enviada para o grupo errado, uma prova compartilhada sem restrição de acesso, um formulário com dados de alunos acessível a qualquer pessoa com o link.

7.2 Armazenamento em nuvem — boas práticas

Serviços de nuvem como Google Drive, OneDrive e Dropbox oferecem sincronização automática, histórico de versões e acesso multiplataforma. São excelentes para backup, mas precisam de configuração adequada de permissões.

Serviço	Armazenamento gratuito	Integração	Observação
Google Drive	15 GB	Google Workspace / Gmail	Comum em escolas com G Suite for Education
Microsoft OneDrive	5 GB (15 GB com Edu)	Microsoft 365	Integrado ao pacote Office institucional
Dropbox	2 GB	Diversas plataformas	Plano gratuito limitado; bom histórico de versões
iCloud	5 GB	Ecossistema Apple	Conveniente para usuários de iPhone/Mac

7.3 Permissões de compartilhamento

O maior risco de segurança no uso da nuvem não é invasão técnica: é compartilhamento excessivo. Quando você gera um link "qualquer pessoa com o link pode acessar", qualquer pessoa que receba esse link — incluindo quem você não pretendia — pode acessar o arquivo.

Regras de compartilhamento seguro

- Use "restrito" ou "somente pessoas específicas" como padrão
- Compartilhe "somente leitura" quando o destinatário não precisa editar
- Evite links "qualquer pessoa com o link" para documentos sensíveis
- Revise periodicamente quem tem acesso aos seus arquivos compartilhados
- Remova o compartilhamento quando a colaboração terminar
- Para documentos com dados de alunos, nunca use links públicos

7.4 Versionamento e recuperação de arquivos

Serviços de nuvem mantêm histórico de versões dos arquivos. Isso permite recuperar versões anteriores se um arquivo for acidentalmente editado ou excluído. Saiba como acessar esse recurso no serviço que você usa — pode salvar horas de retrabalho.

7.5 Pendrives e HDs externos

- Pendrives são convenientes, mas fáceis de perder — nunca guarde neles a única cópia de algo importante
- Não conecte pendrives encontrados em lugares públicos — é uma técnica de distribuição de malware conhecida
- Considere criptografar pendrives com dados sensíveis (VeraCrypt é gratuito e confiável)
- HDs externos são ótimos para backup local (regra 3-2-1)
- Ejetar corretamente o pendrive antes de remover evita corrupção de arquivos

Exemplo Prático — Prova distribuída acidentalmente

A professora Camila cria a prova do semestre em um documento do Google Drive e gera um link de compartilhamento para enviar para a coordenação. Ela usa a opção "qualquer pessoa com o link pode ver". Depois, esse link é repassado por e-mail para toda a equipe pedagógica. Um aluno que estava copiado por engano nesse e-mail acessa a prova antes da aplicação. Usar "compartilhado apenas com pessoas específicas" teria evitado completamente o problema.

Checklist — Arquivos, nuvem e documentos

- ■ Tenho backup dos meus arquivos acadêmicos importantes em pelo menos dois locais
- ■ Uso sincronização automática com a nuvem para trabalhos em andamento
- ■ Compartilho documentos com permissões restritas por padrão
- ■ Nunca uso links públicos para documentos com dados de alunos
- ■ Conheço como recuperar versões anteriores dos meus arquivos na nuvem
- ■ Não guardo a única cópia de arquivos importantes em pendrive

Erros comuns — Arquivos e nuvem

- ✗ Guardar o TCC ou projeto final apenas no notebook, sem backup
- ✗ Compartilhar documentos com dados de alunos via link público
- ✗ Não revogar compartilhamentos após o fim da colaboração
- ✗ Usar pendrive encontrado sem verificação
- ✗ Depender de um único dispositivo para guardar trabalhos importantes

Perguntas de Revisão

1. Qual é o principal erro de configuração que torna documentos na nuvem inseguros?
2. Explique a regra de backup 3-2-1 aplicada a um documento de TCC.
3. Que cuidado especial deve ser tomado ao compartilhar documentos com dados de alunos?
4. Por que pendrives encontrados em lugares públicos representam risco?

Capítulo 8

Privacidade e dados pessoais

Objetivo: compreender o que são dados pessoais, entender os riscos de exposição em redes sociais e formulários, conhecer os princípios básicos da LGPD no contexto educacional e adotar práticas que protejam a privacidade de alunos, professores e da instituição.

8.1 O que são dados pessoais

Dado pessoal é qualquer informação que identifica ou pode identificar uma pessoa natural. A Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018) brasileira define e protege esses dados, estabelecendo obrigações para quem os coleta, armazena ou processa.

Categoria	Exemplos	Observação
Dados de identificação	Nome, CPF, RG, matrícula, e-mail, telefone	Os mais comuns e frequentemente coletados
Dados sensíveis (LGPD)	Saúde, biometria, origem racial, religião, opção sexual	Exigem proteção reforçada e consentimento explícito
Dados de localização	Endereço residencial, geolocalização de fotos	Podem revelar rotinas e expor a riscos físicos
Dados acadêmicos	Notas, frequência, histórico, avaliações psicopedagógicas	Dados de menores exigem consentimento dos responsáveis
Dados comportamentais	Histórico de navegação, uso de plataformas, preferências	Coletados automaticamente por serviços digitais

8.2 Exposição em redes sociais

Redes sociais são projetadas para encorajar o compartilhamento. O que você posta pode revelar muito mais do que pretende: sua localização, rotina, renda, vínculos familiares, crenças e vulnerabilidades. No ambiente educacional, isso se aplica a estudantes, professores e à própria imagem da instituição.

- Revise as configurações de privacidade das suas redes sociais periodicamente
- Limite quem pode ver suas postagens, stories e informações de perfil
- Metadados de fotos (EXIF) podem conter localização GPS — desative essa função nas configurações da câmera do celular
- Pense antes de postar: uma publicação deletada pode já ter sido capturada e compartilhada
- Evite postar fotos que identifiquem rotinas, endereços ou padrões de deslocamento

8.3 Dados de alunos — responsabilidade especial

Professores e gestores escolares lidam com dados de pessoas menores de idade, o que exige cuidado redobrado. A LGPD estabelece que dados de crianças e adolescentes merecem proteção especial e que seu tratamento deve ter consentimento dos responsáveis.

Boas práticas com dados de alunos

- Não compartilhe listas com nomes e notas de alunos em grupos públicos de WhatsApp
- Não publique fotos de alunos (especialmente menores) sem autorização formal
- Use comunicação oficial da instituição para dados acadêmicos, não grupos informais
- Não armazene dados de alunos em serviços pessoais (e-mail pessoal, Drive pessoal) sem política institucional que autorize
- Ao descartar documentos físicos com dados de alunos, use fragmentação

8.4 LGPD no contexto educacional — pontos essenciais

A LGPD impõe obrigações a qualquer organização que colete ou processe dados pessoais no Brasil, incluindo escolas e universidades. Não é necessário ser especialista jurídico para entender os princípios básicos:

Princípios da LGPD relevantes para educadores

- Finalidade: colete dados apenas para fins específicos e legítimos (ex.: frequência e rendimento — não para marketing)
- Necessidade: colete apenas os dados estritamente necessários
- Transparência: informe ao aluno (ou responsável) quais dados são coletados e para quê
- Segurança: adote medidas técnicas para proteger os dados coletados
- Prevenção: antecipe riscos antes que incidentes ocorram
- Responsabilização: a instituição responde pelos dados que coleta

■ A LGPD não é apenas para TI

A proteção de dados é responsabilidade de todos que lidam com informações pessoais — não apenas do setor de tecnologia. Um professor que posta a lista de notas em grupo público, um coordenador que envia dados de alunos por e-mail sem criptografia, ou uma secretaria que descarta prontuários sem fragmentar — todos têm responsabilidade sobre os dados que manipulam.

8.5 Cuidado com formulários e coleta de dados

- Antes de preencher um formulário online, verifique quem o criou e se a finalidade é legítima

- Nenhuma pesquisa ou cadastro legítimo pede senha ou código de verificação
- Formulários do Google Forms ou Microsoft Forms podem ser criados por qualquer pessoa
- Desconfie de formulários que pedem CPF, dados bancários ou documentos sem justificativa clara

Exemplo Prático — Lista de notas no grupo de WhatsApp

O professor Marcos cria um grupo no WhatsApp com todos os alunos da turma para comunicados e envia as notas finais diretamente no grupo, com nomes e pontuações de todos. Isso expõe dados pessoais (desempenho acadêmico) de todos os alunos para todos os membros do grupo, sem consentimento. Além de ser uma prática que pode violar a LGPD, pode constranger alunos e gerar conflitos. O correto é usar o sistema oficial da instituição para divulgar notas.

Checklist — Privacidade e dados pessoais

- ■ Reviso as configurações de privacidade das minhas redes sociais
- ■ Não compartilho dados de alunos em grupos públicos ou informais
- ■ Peço autorização antes de fotografar e publicar imagens de alunos
- ■ Uso canais oficiais da instituição para comunicar dados acadêmicos
- ■ Verifico a finalidade antes de preencher formulários online
- ■ Fragmento documentos físicos com dados pessoais antes de descartar

Erros comuns — Privacidade e dados

- ✗ Enviar lista de notas com nomes de alunos em grupos de WhatsApp
- ✗ Publicar fotos de alunos menores sem autorização dos responsáveis
- ✗ Armazenar dados de alunos em serviços pessoais sem política institucional
- ✗ Preencher formulários suspeitos com CPF ou dados pessoais
- ✗ Ignorar a LGPD por acreditar que só se aplica a grandes empresas

Perguntas de Revisão

1. O que é um dado pessoal sensível segundo a LGPD? Dê dois exemplos.
2. Por que dados de alunos menores exigem proteção especial?
3. Quais são os cinco princípios da LGPD mais relevantes para educadores?
4. Que cuidados você deve ter antes de preencher um formulário online?

Capítulo 9

Plataformas educacionais e contas institucionais

Objetivo: usar com segurança os sistemas e plataformas do ambiente educacional — AVA, e-mail institucional, sistemas de gestão, Google Classroom, Microsoft Teams e similares — com atenção especial a permissões, compartilhamento e saída segura de contas.

9.1 E-mail institucional — usos e cuidados

O e-mail institucional é o canal oficial de comunicação acadêmica. Ele carrega o nome da instituição e, por isso, tem responsabilidades específicas: o que você envia por esse endereço representa formalmente a instituição ou o seu vínculo com ela.

- Use o e-mail institucional exclusivamente para fins acadêmicos e profissionais
- Não cadastre o e-mail institucional em serviços pessoais ou newsletters
- Ative MFA no e-mail institucional sempre que o sistema permitir
- Não encaminhe dados sigilosos de alunos para e-mails pessoais
- Ao desligar da instituição, transfira arquivos importantes antes do encerramento da conta

9.2 AVA e LMS — Ambientes Virtuais de Aprendizagem

Plataformas como Moodle, Google Classroom, Microsoft Teams for Education, Blackboard e Canvas concentram dados acadêmicos sensíveis: avaliações, rubricas, feedbacks, frequências e comunicações. Acesso indevido a essas plataformas pode comprometer a integridade acadêmica.

Plataforma	Tipo	Cuidados específicos
Moodle	LMS institucional (servidor próprio)	Configurar permissões por papel (aluno/professor/admin); backup periódico do servidor
Google Classroom	SaaS (Google)	Gerir quem pode ingressar nas turmas; revisar permissões de apps de terceiros
Microsoft Teams Edu	SaaS (Microsoft)	Controlar gravação de aulas; gerir canais e permissões de equipe
Blackboard / Canvas	SaaS ou on-premises	Verificar política de dados do fornecedor; usar SSO institucional

9.3 Compartilhamento indevido em plataformas

Um dos riscos mais comuns em plataformas educacionais é o compartilhamento inadvertido de conteúdo ou acesso:

- Turmas no Google Classroom configuradas como "qualquer pessoa com o link pode ingressar" permitem entrada de pessoas externas
- Links de reunião do Teams ou Meet publicados em redes sociais permitem invasão de aula (zoom bombing)
- Materiais de avaliação publicados como "visível para todos" no AVA antes da aplicação comprometem a integridade da prova
- Permissões de edição concedidas a alunos em espaços que deveriam ser somente de leitura

9.4 Saída segura de contas em computadores públicos

Este é um dos descuidos mais frequentes no ambiente educacional. Um login esquecido em laboratório, biblioteca ou computador da secretaria dá acesso completo à conta para o próximo usuário.

Procedimento de saída segura — sempre faça os três passos

- 1. Clique em "Sair" / "Logout" / "Encerrar sessão" na plataforma ou e-mail
- 2. Feche todas as abas e janelas do navegador
- 3. Se possível, limpe os dados de navegação (histórico, cookies, senhas)
- Verificação: abra uma nova aba e tente acessar a plataforma — deve pedir login. Se não pedir, você ainda está logado.
- Nunca confie apenas em "fechar a aba" — isso não encerra a sessão.

9.5 Senhas e acessos de contas acadêmicas

- Nunca compartilhe sua matrícula e senha do sistema acadêmico com colegas, mesmo para "ajudar" alguém a ver a própria situação
- Não autorize terceiros a acessarem sua conta institucional, mesmo que pareça inofensivo
- Se suspeitar que sua conta foi comprometida, troque a senha imediatamente e avise o suporte da instituição
- Use senhas diferentes para a conta institucional e para serviços pessoais

Exemplo Prático — Zoom bombing em aula remota

A professora Lúcia divulga o link da reunião do Google Meet no grupo público da escola no Facebook para facilitar o acesso dos alunos. Desconhecidos entram na aula, interrompem com conteúdo inapropriado e forçam o encerramento da sessão. Links de aula devem ser enviados apenas aos alunos matriculados, por canal oficial — não publicados em grupos abertos.

Checklist — Plataformas e contas institucionais

- ■ Tenho MFA ativo no e-mail institucional (se a plataforma permite)
- ■ Faço logout completo ao terminar de usar plataformas em computadores compartilhados
- ■ Não compartilho minha senha ou matrícula com ninguém
- ■ Configuro turmas e reuniões com acesso restrito a participantes autorizados
- ■ Não publico links de reunião em grupos públicos ou redes sociais
- ■ Não encaminho dados de alunos para e-mail pessoal

Erros comuns — Plataformas educacionais

- ✗ Não fazer logout em laboratórios por "falta de tempo"
- ✗ Compartilhar senha de acesso ao sistema com colegas
- ✗ Publicar links de aula em grupos públicos do Facebook ou WhatsApp
- ✗ Configurar turmas com acesso aberto sem verificação de identidade
- ✗ Usar o mesmo e-mail institucional para cadastros pessoais

Perguntas de Revisão

1. Quais são os três passos para uma saída segura de conta em computador público?
2. Por que nunca se deve compartilhar a senha de acesso ao sistema acadêmico?
3. O que é "zoom bombing" e como preveni-lo?
4. Quais cuidados específicos você deve ter ao configurar uma turma no AVA?

Capítulo 10

IA, produtividade e segurança

Objetivo: entender os riscos de privacidade ao usar ferramentas de inteligência artificial generativa no contexto educacional, saber quais dados nunca devem ser inseridos nessas ferramentas e adotar um uso responsável e crítico da IA no estudo e no ensino.

10.1 IA generativa no ambiente educacional

Ferramentas de inteligência artificial generativa — como assistentes de texto, geradores de imagem e ferramentas de síntese — tornaram-se presentes no dia a dia de estudantes e professores. Elas podem auxiliar na pesquisa, na escrita, na revisão e na criação de materiais didáticos. Mas seu uso inadequado cria riscos específicos de privacidade e segurança.

10.2 Riscos ao inserir dados sensíveis em ferramentas de IA

A maior parte das ferramentas de IA generativa envia os dados digitados para servidores externos, onde são processados e, em muitos casos, podem ser usados para treinar ou melhorar os modelos. Isso significa que informações inseridas nessas ferramentas podem sair do seu controle.

Categoria de dado	Exemplo	Risco de inserir em IA pública
Dados pessoais de alunos	Nome, CPF, matrícula, notas	Violação de privacidade e potencial infração à LGPD
Documentos institucionais sigilosos	Atas de reunião, contratos, avaliações internas	Exposição de informações confidenciais da instituição
Provas e avaliações inéditas	Questões que ainda serão aplicadas	Comprometimento da integridade acadêmica
Comunicações privadas	E-mails internos, conversas de chat institucional	Exposição de comunicações que não são públicas
Senhas e credenciais	Senhas, tokens, chaves de API	Risco crítico — nunca insira credenciais em ferramentas de IA

■ Regra simples para IA e dados sensíveis

Se você não publicaria essa informação em uma rede social pública, não a insira em uma ferramenta de IA pública. Essa heurística simples protege dados pessoais, institucionais e acadêmicos do risco de exposição inadvertida.

10.3 Política de dados das ferramentas de IA

Diferentes ferramentas têm políticas distintas sobre como tratam os dados inseridos pelos usuários. Algumas oferecem opções de "não usar meus dados para treinamento" — verifique as configurações do serviço que você usa. Ferramentas com versões corporativas ou educacionais (como o Microsoft Copilot com conta institucional) geralmente têm políticas mais restritivas de uso dos dados.

Boas práticas antes de usar uma ferramenta de IA

- Leia o resumo da política de privacidade do serviço
- Verifique se há opção para desativar o uso dos seus dados para treinamento
- Prefira ferramentas com versão institucional/corporativa para dados sensíveis
- Em caso de dúvida, anonimize os dados antes de inserir (substitua nomes por "Aluno A", "Professor B")
- Nunca insira senhas, CPFs, dados bancários ou credenciais

10.4 Revisão crítica de respostas de IA

Ferramentas de IA generativa podem produzir respostas incorretas, desatualizadas ou fabricadas — fenômeno chamado de "alucinação". No contexto educacional, isso tem implicações diretas:

- Referências bibliográficas geradas por IA frequentemente não existem — sempre verifique a existência das fontes antes de citar
- Dados estatísticos e fatos históricos gerados por IA podem estar errados — confirme em fontes primárias
- A IA não substitui o pensamento crítico: use como ferramenta de apoio, não como fonte definitiva
- Em avaliações e trabalhos acadêmicos, verifique a política da instituição sobre uso de IA antes de utilizá-la

10.5 Uso responsável de IA no estudo e no ensino

- Para esboços e brainstorming: adequado, com revisão posterior
- Para resumo de textos próprios: adequado, sem dados sensíveis
- Para explicação de conceitos: útil, mas confirme em fontes confiáveis
- Para trabalhos com dados reais de alunos ou instituição: evite ferramentas públicas
- Para avaliações e provas: verifique política institucional antes

Exemplo Prático — Plano de aula com dados de alunos

O professor André quer usar uma ferramenta de IA para criar um plano de aula diferenciado. Para contextualizar, cola no prompt os nomes e dificuldades específicas de dez alunos da turma, incluindo um aluno com laudo de dislexia. Esses dados pessoais e de saúde de menores foram enviados para um servidor externo sem consentimento dos responsáveis. O correto seria descrever o perfil da turma de forma anonimizada: "tenho alunos com dificuldade em leitura" em vez de dados nominais.

Checklist — IA e segurança de dados

- ■ Nunca insiro nomes, CPF ou dados pessoais de alunos em ferramentas de IA públicas
- ■ Não insiro documentos institucionais sigilosos em ferramentas de IA
- ■ Verifico a existência de referências bibliográficas geradas por IA
- ■ Anonimizo dados antes de inserir em ferramentas de IA quando necessário
- ■ Conheço a política da minha instituição sobre uso de IA em avaliações

Erros comuns — IA e privacidade

- ✗ Inserir listas com nomes e notas de alunos para "personalizar" um plano de aula
- ✗ Usar respostas de IA em trabalhos acadêmicos sem verificar a veracidade
- ✗ Citar referências geradas por IA sem confirmar que existem
- ✗ Inserir rascunhos de contratos ou atas institucionais em chatbots públicos
- ✗ Acreditar que "a IA é privada" sem verificar a política de dados do serviço

Perguntas de Revisão

1. Por que inserir dados pessoais de alunos em ferramentas de IA públicas pode violar a LGPD?
2. O que é "alucinação" em IA e por que isso é importante para educadores?
3. Qual é a regra simples para decidir se um dado pode ser inserido em uma ferramenta de IA pública?
4. Como você pode usar IA de forma útil sem comprometer dados sensíveis?

Capítulo 11

O que fazer em caso de incidente

Objetivo: saber como agir com calma e eficácia diante de incidentes digitais comuns — conta invadida, clique em link suspeito, perda de dispositivo, vazamento de dados — com foco nas ações imediatas corretas e nos erros que pioram a situação.

11.1 A importância de agir rápido e corretamente

Em um incidente digital, o tempo e a qualidade das primeiras ações determinam a extensão do dano. Entrar em pânico, ignorar o problema ou tomar atitudes erradas pode transformar um incidente controlável em um desastre maior. Este capítulo oferece um guia prático para as situações mais comuns.

11.2 Conta invadida ou comprometida

Ações imediatas — Conta invadida

- 1. Troque a senha imediatamente pelo portal oficial do serviço (não clique em links recebidos por e-mail — acesse diretamente)
- 2. Ative ou verifique o MFA se ainda não estiver ativo
- 3. Encerre todas as sessões ativas (a maioria dos serviços tem opção "sair de todos os dispositivos")
- 4. Verifique se e-mails de encaminhamento ou regras suspeitas foram criados na sua caixa
- 5. Verifique se a senha de recuperação (e-mail ou telefone) foi alterada
- 6. Se for conta institucional: avise imediatamente o suporte de TI
- 7. Notifique contatos próximos que podem ter recebido mensagens falsas enviadas pela conta comprometida

11.3 Clicou em link suspeito ou abriu anexo malicioso

- Desconecte o dispositivo da rede Wi-Fi imediatamente (isso pode interromper comunicação de malware com servidores externos)
- Não desligue o computador abruptamente — isso pode dificultar análise posterior
- Avise o suporte de TI da instituição com detalhes do ocorrido
- Se tiver antivírus, execute uma verificação completa do sistema
- Troque as senhas de contas importantes de outro dispositivo limpo
- Monitore suas contas nos dias seguintes por atividade suspeita

■ Não entre em pânico — analise o que aconteceu

Nem todo clique em link suspeito resulta em infecção. Muitos links de phishing apenas tentam capturar credenciais — se você não digitou nada no site, o risco é menor. Avalie o que aconteceu, anote os detalhes e relate ao suporte.

11.4 Perda ou roubo de dispositivo

Ação	Celular	Notebook/Desktop
Localizar remotamente	Use "Encontre meu dispositivo" (Android) ou "Find My" (iOS)	Windows: "Encontrar meu dispositivo" no conta Microsoft; macOS: Find My
Bloquear remotamente	Bloqueio remoto via Google/Apple — impede acesso mesmo sem SIM	Não disponível nativamente sem configuração prévia
Apagar remotamente	Apagamento remoto se não houver recuperação possível	BitLocker (Windows) protege dados mesmo sem acesso remoto
Revogar acessos	Faça logout de todas as contas pelo navegador de outro dispositivo	Mesma ação — especialmente e-mail e plataformas acadêmicas
Comunicar	Registre boletim de ocorrência (necessário para seguro e cancelamento de linha)	Avise TI da instituição se havia dados institucionais no dispositivo

11.5 Vazamento acidental de dados

Vazamento acidental é quando você envia dados para a pessoa errada, publica algo que não deveria ou compartilha um link com permissão excessiva sem perceber. Exemplos: enviar lista de notas para o grupo errado, compartilhar um Drive com permissão pública, postar print com dados visíveis.

- Revogue o acesso imediatamente (remova o compartilhamento, apague a publicação)
- Notifique as pessoas cujos dados foram expostos
- Se envolve dados de alunos menores, avise a coordenação e, se necessário, os responsáveis
- Registre o ocorrido internamente — transparência é melhor do que silêncio
- Se o vazamento for significativo, a instituição pode ter obrigação de notificar a ANPD (Autoridade Nacional de Proteção de Dados)

11.6 Quem avisar — dentro e fora da instituição

Situação	Quem avisar
Conta institucional comprometida	Suporte de TI da instituição — imediatamente
Malware em computador institucional	TI da instituição — isole o equipamento antes
Dados de alunos expostos	Coordenação pedagógica + DPO da instituição (se houver)
Golpe financeiro	Banco + Polícia Civil (Delegacia de Crimes Digitais ou BO online)
Ameaça ou assédio online	Direção da instituição + polícia se houver risco físico
Incidente em conta pessoal	Suporte do serviço afetado + familiares se necessário

11.7 O que NÃO fazer em um incidente

Erros que pioram incidentes digitais

✗ Ignorar o problema esperando que "se resolva sozinho"

✗ Pagar resgate em casos de ransomware sem consultar especialista (pagamento não garante recuperação e financia criminosos)

✗ Apagar evidências do incidente antes de reportar ao suporte

✗ Culpar-se publicamente antes de entender o que aconteceu

✗ Não avisar contatos que podem ter recebido mensagens fraudulentas da conta

✗ Continuar usando o dispositivo comprometido sem verificação

✗ Trocar a senha no mesmo dispositivo suspeito (use outro dispositivo)

Exemplo Prático — Conta de e-mail institucional comprometida

A coordenadora Beatriz percebe que colegas estão recebendo e-mails estranhos enviados pelo endereço dela, pedindo cliques em links. Ela age imediatamente: acessa o portal do e-mail de outro computador, troca a senha, encerra todas as sessões ativas, verifica se há regras de encaminhamento desconhecidas (encontra e remove uma), ativa MFA e avisa o TI da instituição. Em seguida, envia uma mensagem a todos os contatos alertando sobre os e-mails falsos. A agilidade e a sequência correta de ações limitaram o dano.

Checklist — Resposta a incidentes

- ■ Em caso de conta comprometida: troco senha + encerro sessões + ativo MFA
- ■ Sei como bloquear meu celular remotamente em caso de perda
- ■ Sei a quem reportar incidentes na minha instituição
- ■ Não pago resgates sem consultar especialista
- ■ Após incidente, monitoro minhas contas por atividade suspeita
- ■ Documento o que aconteceu para apoiar a análise posterior

Perguntas de Revisão

1. Quais são as cinco primeiras ações ao descobrir que sua conta de e-mail foi comprometida?
2. O que você deve fazer imediatamente após clicar em um link suspeito?
3. Por que não é recomendado pagar resgate em casos de ransomware?
4. Quem você deve notificar se dados de alunos foram acidentalmente expostos?

Capítulo 12

Checklist final de boas práticas

Este capítulo reúne os checklists consolidados do manual em três perfis: estudante, professor e instituição/sala de aula. Use como autoavaliação periódica ou como ferramenta de diagnóstico em atividades de formação.

12.1 Checklist do Estudante

Revise cada item abaixo. Marque o que você já pratica e identifique o que ainda precisa implementar:

Senhas e autenticação

- ■ Uso senhas diferentes para cada serviço importante
- ■ Minhas senhas têm ao menos 12 caracteres
- ■ Uso um gerenciador de senhas
- ■ Tenho MFA ativo no e-mail principal e no AVA institucional
- ■ Nunca compartilho senhas com colegas

Golpes e e-mail

- ■ Verifico o remetente completo antes de clicar em links
- ■ Nunca forneço senhas ou códigos MFA por mensagem ou telefone
- ■ Sei reconhecer os sinais de urgência artificial em golpes
- ■ Não abro anexos de remetentes desconhecidos
- ■ Reporto e-mails suspeitos ao suporte da instituição

Dispositivos e redes

- ■ Meu celular tem bloqueio de tela ativo
- ■ Faço logout em computadores de laboratório ao terminar
- ■ Tenho backup dos meus trabalhos acadêmicos importantes
- ■ Não faço transações sensíveis em redes Wi-Fi abertas
- ■ Meu sistema operacional está atualizado

Privacidade e IA

- ■ Revejo configurações de privacidade das minhas redes sociais
- ■ Não insiro dados pessoais reais em ferramentas de IA públicas
- ■ Verifico referências geradas por IA antes de usar em trabalhos
- ■ Conheço a política da instituição sobre uso de IA em avaliações

12.2 Checklist do Professor

Contas e acesso

- ■ Tenho MFA ativo no e-mail institucional
- ■ Uso senhas fortes e únicas para sistemas acadêmicos
- ■ Faço logout de plataformas ao usar computadores compartilhados
- ■ Não acesso sistemas institucionais em redes Wi-Fi abertas sem VPN

Dados de alunos

- ■ Não compartilho dados de alunos em grupos públicos de WhatsApp
- ■ Não publico fotos de alunos menores sem autorização dos responsáveis
- ■ Uso canais oficiais para comunicar notas e informações acadêmicas
- ■ Compartilho documentos com permissões restritas por padrão na nuvem
- ■ Fragmento documentos físicos com dados de alunos antes de descartar

Plataformas e materiais

- ■ Configuro turmas e reuniões com acesso restrito a participantes
- ■ Não publico links de reunião em grupos ou redes sociais públicas
- ■ Mantenho backup de planos de aula e materiais didáticos
- ■ Verifico permissões de compartilhamento em documentos do Drive/OneDrive
- ■ Não insiro avaliações inéditas em ferramentas de IA públicas

12.3 Checklist da Instituição / Gestores

Política institucional

- ■ A instituição tem política formal de segurança da informação
- ■ Há responsável designado para proteção de dados (DPO ou similar)
- ■ Professores e funcionários recebem formação básica em segurança digital
- ■ Existe canal claro para reporte de incidentes de segurança

Infraestrutura e sistemas

- ■ Computadores dos laboratórios têm configuração de logout automático
- ■ A rede Wi-Fi da escola usa WPA2 ou WPA3
- ■ Sistemas acadêmicos têm suporte a MFA para professores e gestores
- ■ Há política de backup para dados acadêmicos críticos
- ■ Softwares e sistemas operacionais são mantidos atualizados

Dados de alunos e LGPD

- ■ A coleta de dados de alunos é documentada com finalidade definida
- ■ Há política clara sobre compartilhamento de dados de alunos
- ■ Formulários de coleta de dados incluem aviso de privacidade
- ■ Dados de alunos menores contam com consentimento dos responsáveis
- ■ A instituição tem plano de resposta a incidentes de segurança

12.4 Pontuação e diagnóstico

Use a tabela abaixo para interpretar seus resultados após preencher os checklists relevantes ao seu perfil:

Percentual de itens marcados	Diagnóstico	Próximo passo sugerido
Menos de 50%	Atenção necessária	Priorize os capítulos mais relevantes e implemente os itens pendentes
50% a 75%	Base razoável, com lacunas	Identifique os grupos de itens não marcados e trabalhe neles
75% a 90%	Boas práticas consolidadas	Refine os detalhes e revise anualmente
Acima de 90%	Excelente postura de segurança	Compartilhe as práticas com colegas e contribua para a cultura da instituição

Segurança digital é um processo contínuo, não um estado permanente. Revisitar esses checklists periodicamente — especialmente após mudanças de plataforma, cargo ou rotina — é parte de uma postura saudável de proteção.

Glossário

Definições dos principais termos técnicos usados neste manual, em linguagem acessível. Os termos estão organizados em ordem alfabética.

Antivírus / Antimalware

Software que detecta, bloqueia e remove programas maliciosos de um dispositivo. Funciona comparando arquivos com uma base de assinaturas conhecidas e monitorando comportamentos suspeitos. Não substitui boas práticas, mas é uma camada adicional útil de proteção.

Atualização de segurança

Correção de software lançada pelo fabricante para resolver vulnerabilidades conhecidas. Manter sistemas e aplicativos atualizados é uma das medidas mais eficazes de proteção, pois elimina falhas que já têm exploração conhecida.

Autenticação

Processo de verificar a identidade de um usuário antes de conceder acesso a um sistema. Pode ser por senha (algo que você sabe), token ou dispositivo (algo que você tem), ou biometria (algo que você é).

Backup (cópia de segurança)

Cópia de dados armazenada em local separado do original, criada para permitir recuperação em caso de perda, dano ou ataque. A regra de referência é a 3-2-1: 3 cópias, em 2 tipos de mídia, com 1 fora do local principal.

CERT.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Órgão do NIC.br responsável por tratar incidentes e disseminar boas práticas de segurança na internet brasileira. Publica estatísticas anuais e cartilhas gratuitas (cert.br).

Criptografia

Técnica matemática que transforma dados em formato ilegível para quem não possui a chave de decifração. O HTTPS usa criptografia para proteger a comunicação entre o navegador e os servidores.

Dado pessoal

Qualquer informação que identifica ou pode identificar uma pessoa natural. Inclui nome, CPF, e-mail, telefone, endereço, matrícula, foto, dados de localização e muito mais. A LGPD regula o tratamento desses dados no Brasil.

Dado pessoal sensível

Categoria especial de dado pessoal que exige proteção reforçada pela LGPD: dados sobre saúde, biometria, origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, orientação sexual ou dado genético.

Engenharia social

Conjunto de técnicas psicológicas usadas para manipular pessoas a revelar informações confidenciais ou realizar ações prejudiciais. Explora emoções como urgência, medo, curiosidade e confiança. Não requer conhecimento técnico avançado e é responsável pela maioria dos incidentes digitais.

HTTPS

Versão segura do protocolo HTTP, que usa criptografia TLS para proteger a comunicação entre navegador e servidor. Identificado pelo ícone de cadeado no navegador. Garante que a conexão é criptografada, mas não garante que o site é confiável ou legítimo.

Incidente de segurança

Evento que viola ou ameaça violar políticas de segurança, causando comprometimento de confidencialidade, integridade ou disponibilidade de dados ou sistemas. Inclui invasões, vazamentos, infecções por malware e perdas de dispositivo.

LGPD

Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Lei brasileira que regula a coleta, armazenamento e tratamento de dados pessoais por pessoas físicas ou jurídicas. Estabelece direitos dos titulares e obrigações de quem trata dados, inclusive instituições de ensino.

Malware

Termo genérico para qualquer software criado com intenção maliciosa: vírus, trojans, spyware, adware, ransomware e outros. Pode infectar dispositivos via anexos de e-mail, downloads, pendrives ou exploração de vulnerabilidades.

MFA / 2FA (Autenticação multifator)

Método de autenticação que exige dois ou mais fatores independentes para verificar a identidade do usuário. Os fatores podem ser: algo que você sabe (senha), algo que você tem (token, celular), algo que você é (biometria). Reduz drasticamente o risco de invasão de contas.

Nuvem (computação em nuvem)

Modelo de armazenamento e processamento de dados em servidores remotos acessados pela internet, em vez de armazenamento local. Exemplos: Google Drive, OneDrive, Dropbox. Oferece acesso multiplataforma e backup automático, mas exige configuração adequada de permissões.

Phishing

Tipo de golpe digital em que o atacante se passa por entidade confiável (banco, escola, serviço online) para induzir a vítima a fornecer dados sensíveis (senhas, dados de cartão) ou clicar em links maliciosos. Pode chegar por e-mail, SMS (smishing) ou telefone (vishing).

Privacidade

Direito de controlar quais informações pessoais são coletadas, por quem e para qual finalidade. No contexto digital, envolve configurações de redes sociais, permissões de aplicativos, coleta de dados por serviços e tratamento de dados pessoais.

Ransomware

Tipo de malware que criptografa os arquivos da vítima e exige pagamento (resgate) para fornecer a chave de decriptação. Extremamente destrutivo para instituições sem backup adequado. A melhor proteção é manter backups atualizados e sistemas corrigidos.

Smishing

Variante de phishing executada via SMS ou aplicativos de mensagem como WhatsApp. O atacante envia mensagem com link malicioso ou solicitação de dados se passando por banco, serviço de entrega, instituição de ensino ou pessoa conhecida.

Spoofing (falsificação)

Técnica de forjar a identidade de um remetente — fazendo um e-mail parecer ter vindo de um endereço legítimo, ou uma página web parecer ser o site oficial de um serviço. Usado em ataques de phishing e engenharia social.

VPN (Rede Privada Virtual)

Tecnologia que cria um túnel criptografado entre o dispositivo do usuário e um servidor remoto, protegendo o tráfego de rede de observadores na mesma rede local. Útil em redes Wi-Fi públicas. Não garante anonimato total nem substitui outras práticas de segurança.

Vulnerabilidade

Fraqueza em um sistema, processo ou comportamento que pode ser explorada por uma ameaça para causar dano. Pode ser técnica (software desatualizado, configuração incorreta) ou humana (falta de treinamento, descuido).

WPA2 / WPA3

Protocolos de segurança para redes Wi-Fi. WPA2 é o padrão amplamente adotado e considerado seguro para uso doméstico e institucional. WPA3 é a versão mais recente, com melhorias de segurança. Evite WEP e WPA (versões antigas e vulneráveis).

Referências

Fontes consultadas na elaboração deste manual. Todas as afirmações facturais relevantes são sustentadas pelas fontes listadas abaixo — preferencialmente documentos oficiais, cartilhas governamentais e publicações de organizações reconhecidas na área de segurança digital.

CERT.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de Segurança para Internet. Versão 6.0. NIC.br / CGI.br, 2012 (atualizada). Disponível em: cartilha.cert.br

CERT.br

Estatísticas de Incidentes de Segurança reportados ao CERT.br — 2023. NIC.br, 2024. Disponível em: cert.br/stats

NIST — National Institute of Standards and Technology

NIST Special Publication 800-63B: Digital Identity Guidelines — Authentication and Lifecycle Management. Grassi, P.A. et al. NIST, 2017 (rev. 2020). Disponível em: pages.nist.gov/800-63-3/sp800-63b.html

CISA — Cybersecurity and Infrastructure Security Agency

Known Exploited Vulnerabilities Catalog. CISA, atualização contínua. Disponível em: cisa.gov/known-exploited-vulnerabilities-catalog

CISA

Phishing Guidance: Stopping the Attack Cycle at Phase One. CISA / NSA / FBI / MS-ISAC, 2023. Disponível em: cisa.gov

Microsoft

Your Pa$$word doesn't matter. Alex Weinert, Microsoft Identity Security. Microsoft Tech Community Blog, 2019. Disponível em: techcommunity.microsoft.com

Microsoft

One simple action you can take to prevent 99.9 percent of account attacks. Alex Weinert, Microsoft Security Blog, 2019. Disponível em: microsoft.com/security/blog

Have I Been Pwned

Hunt, Troy. Have I Been Pwned — serviço de verificação de vazamentos de credenciais. Disponível em: haveibeenpwned.com

Brasil — Presidência da República

Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

ANPD — Autoridade Nacional de Proteção de Dados

Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. ANPD, 2021. Disponível em: gov.br/anpd

ANPD

Guia de Boas Práticas — Lei Geral de Proteção de Dados (LGPD). ANPD, 2023. Disponível em: gov.br/anpd

EFF — Electronic Frontier Foundation

Surveillance Self-Defense: Tips, Tools and How-tos for Safer Online Communications. EFF, atualização contínua. Disponível em: ssd.eff.org

Verizon

2023 Data Breach Investigations Report (DBIR). Verizon Business, 2023. Disponível em: verizon.com/business/resources/reports/dbir

VirusTotal

VirusTotal — serviço gratuito de análise de arquivos e URLs suspeitos. Google LLC. Disponível em: virustotal.com

Bitwarden

Bitwarden — gerenciador de senhas de código aberto. Disponível em: bitwarden.com

KeePassXC

KeePassXC — gerenciador de senhas local, código aberto. Disponível em: keepassxc.org

---

Nota: os endereços de URL listados eram acessíveis no momento da elaboração deste material. Links podem mudar; em caso de acesso falho, busque o título do documento diretamente no site da organização responsável.