Checklist de segurança · antes do dado real

> Aplicar ANTES de qualquer dado verdadeiro e ANTES de qualquer usuário além de você. Item sem teste passado = item não cumprido.

- [ ] **1 · Dados fictícios, ainda**
  Teste: nas 3 telas com mais dados, pergunte "se isto vazasse hoje, alguém seria prejudicado?" A resposta precisa ser não.

- [ ] **2 · A última porta está trancada (RLS)**
  Teste: peça à IA da ferramenta: "revise as regras de acesso por linha de todas as tabelas e diga o que um usuário anônimo consegue ler e escrever". Resposta certa: nada, em todas.

- [ ] **3 · A autenticação aponta para o lado certo**
  Teste: deslogado, tente acessar as telas internas pela barra de endereço. Tudo deve barrar em login.

- [ ] **4 · Os papéis funcionam na prática**
  Teste: logado como usuário comum, tente fazer o que só o admin deveria. Cada tentativa deve falhar.

- [ ] **5 · Nenhum segredo na vitrine**
  Teste: pergunte à IA: "existe alguma chave, senha ou segredo exposto no código do cliente? Liste e mova para o lugar seguro."

- [ ] **6 · O mínimo da LGPD**
  Não colete o que não precisa · não guarde dado de terceiros que não sabem que estão ali · dado sensível (saúde, documento, financeiro, cliente/paciente) NÃO entra em protótipo, nunca.

- [ ] **7 · O teste do estranho**
  Mande o link a alguém de fora, sem explicação: "o que você vê sem entrar?" e, como usuário comum, "o que você consegue fazer que parece que não devia?"

- [ ] **E quem aprova?**
  Em organização: segurança da informação / proteção de dados. Sozinho(a): o par mais cético que você tiver. O ponto não é pedir permissão; é não ser a única pessoa que olhou.

Item sem teste passado = item não cumprido. Rode de novo a cada tabela nova. Papéis primeiro, prompt depois.