

5 ARMADILHAS QUE DÃO PREJUÍZO ANTES DO *primeiro cliente*

Pra cada uma: o caso nos Estados Unidos, como é no Brasil com a lei, como checar e o pedido pronto pra IA corrigir. Testa só o teu próprio app.

[] 01 / 05

HOSPEDAGEM · DDoS

Página parada com conta por GB

NOS ESTADOS UNIDOS

A Netlify cobra a banda por GB (hoje, 20 créditos por GB). Em fevereiro de 2024, um site estático parado levou uma conta de **US\$ 104.500** depois de um ataque. A Netlify perdoou depois que o caso viralizou. Hoje o plano grátis pausa o site quando o crédito acaba; nos pagos, a recarga automática cobra no cartão.

NO BRASIL

Nenhuma lei segura essa conta: se o teu cartão é brasileiro, ela vem em dólar, com **IOF de 3,5%** em cima (Decreto 6.306/2007, art. 15-B, VII).

COMO CHECAR

No painel da hospedagem: a recarga automática (auto recharge) está ligada? Tem alerta e teto de gasto? Arquivo pesado (vídeo, áudio, PDF grande) está numa hospedagem que cobra por GB?

PEDIDO PRONTO PRA IA

"Revise a hospedagem do meu site: me diga onde a banda é cobrada por GB, se a recarga automática está ligada e quanto um pico de tráfego me custaria. Mova arquivos pesados para um serviço com limite fixo e coloque o site atrás de uma CDN com proteção contra DDoS. Me mostre antes de mudar."

Fontes: docs.netlify.com (How credits work) · answers.netlify.com (\$104K bill post) · Hacker News, comentário do CEO da Netlify, 27/02/2024 · planalto.gov.br (Decreto 6.306/2007)

[] 02 / 05

ACESSIBILIDADE

Site que não funciona no teclado

NOS ESTADOS UNIDOS

Nos EUA, foram **4.928 processos** de acessibilidade em site em 2025. No 1º semestre de 2025, só 36% dos processados faturavam mais de US\$ 25 milhões: a maioria era empresa menor.

NO BRASIL

A **Lei Brasileira de Inclusão (13.146/2015), art. 63**, obriga a acessibilidade nos sites de empresas com sede ou representação no país, seguindo as diretrizes internacionais, com o símbolo de acessibilidade em destaque.

COMO CHECAR

Usa o teu site só com Tab, Enter e Esc: chega em todos os botões e tu vê onde está o foco? Toda imagem importante tem descrição (texto alternativo)?

PEDIDO PRONTO PRA IA

"Deixe meu site acessível: tudo funcionando só com o teclado e com o foco visível, texto alternativo em cada imagem importante (alt vazio só nas decorativas), contraste do WCAG AA e o símbolo de acessibilidade em destaque. Me mostre a lista antes de aplicar."

Fontes: UsableNet, ADA website lawsuit tracker · planalto.gov.br (Lei 13.146/2015, art. 63)

[] 03 / 05

SUPABASE · LGPD

Banco aberto: a outra face, a lei

NOS ESTADOS UNIDOS

Com o RLS desligado, a chave pública que já vai no JavaScript do site lê a tabela de usuários. Um pesquisador achou isso em **170 de 1.645 apps** do Lovable (10,3%). Virou alerta oficial: CVE-2025-48757, nota 9,3 (crítica).

NO BRASIL

É incidente de segurança na **LGPD**: tu tem o dever de proteger os dados desde a criação do app (art. 46) e, se houver risco ou dano relevante, comunicar a ANPD e os clientes (art. 48) em **3 dias úteis** (Resolução CD/ANPD nº 15/2024).

COMO CHECAR

No painel do Supabase: Advisors > Security. O aviso "RLS Disabled in Public" mostra a tabela aberta.

PEDIDO PRONTO PRA IA

"Liste as tabelas do meu Supabase sem RLS e escreva as regras para cada usuário ver e editar só os próprios dados. Depois monte um registro de incidentes e um modelo de aviso para a ANPD e os clientes, caso algum dado tenha ficado exposto. Me mostre antes de aplicar."

Fontes: nvd.nist.gov (CVE-2025-48757) · mattpalmer.io (statement on CVE-2025-48757) · supabase.com/docs (API keys) · planalto.gov.br (Lei 13.709/2018) · gov.br/anpd (Comunicação de Incidente de Segurança)

[] 04 / 05

SMS · WHATSAPP

Mensagem do lançamento sem aceite

NOS ESTADOS UNIDOS

Nos EUA, a FCC exige **consentimento por escrito** pra mensagem comercial por texto, e a lei (TCPA) prevê **US\$ 500 por mensagem**, e até o triplo se for de propósito. Dez mil SMS: US\$ 5 milhões.

NO BRASIL

Não tem multa por mensagem, e o Não Me Perturbe é só pra ligação de telemarketing de telefonia e crédito consignado. Só que a **LGPD** pede base legal pra usar o número (art. 7º); se a base for o consentimento, ele tem que ser demonstrável e pode ser revogado a qualquer momento (art. 8º). E o **WhatsApp** só deixa mandar com opt-in: sem isso, pode limitar ou banir a conta.

COMO CHECAR

A tua lista de espera tem uma caixa de aceite que a pessoa marca, uma por canal (e-mail, SMS, WhatsApp)? Tu guarda data, hora e o texto do aceite?

PEDIDO PRONTO PRA IA

"Revise o formulário da minha lista de espera: coloque uma caixa de aceite desmarcada para cada canal (e-mail, SMS e WhatsApp), guarde data, hora e o texto aceito, e inclua um jeito fácil de sair em toda mensagem. Me mostre antes de aplicar."

Fontes: fcc.gov (Stop Unwanted Robocalls and Texts) · govinfo.gov (47 U.S.C. § 227(b)(3)) · naomeperturbe.com.br · planalto.gov.br (Lei 13.709/2018) · whatsappbusiness.com/policy

[] 05 / 05

GOOGLE CLOUD · FIREBASE

Função que chama a si mesma

NOS ESTADOS UNIDOS

Uma startup (Milkie Way, 2020) tinha orçamento de US\$ 7 e acordou com uma conta de cerca de **US\$ 72 mil**: um robô no Cloud Run chamava páginas que apontavam umas pras outras, sem fim. O Google avisa: alerta de orçamento **não trava** o gasto.

NO BRASIL

É igual: a conta vem em dólar no cartão, com IOF. Hoje o Firebase tem teto de gasto que pausa o serviço só pra alguns produtos (Firebase AI Logic, App Hosting, Cloud Functions for Firebase e Extensions). O resto, só alerta.

COMO CHECAR

Procura função que chama ela mesma, ou que dispara de novo o gatilho que a acionou (ex.: grava no banco e é acionada por gravação no banco). Ela tem limite de repetições, tempo máximo e número máximo de instâncias?

PEDIDO PRONTO PRA IA

"Procure no meu projeto funções que chamam a si mesmas ou que disparam o próprio gatilho. Em cada uma, coloque limite de repetições, tempo máximo e número máximo de instâncias. Depois me mostre como ligar um teto de gasto ou desligar a cobrança automaticamente quando o orçamento estourar."

Fontes: docs.cloud.google.com (Cloud Billing, budgets) · firebase.google.com/docs (spend caps) · The Register, 10/12/2020

AS 5 DE UMA VEZ

MODELO

Cola no teu agente

"Revise meu app procurando 5 armadilhas de custo e de lei: hospedagem cobrada por GB sem teto, site que não funciona no teclado ou imagem sem texto alternativo, tabela do Supabase sem RLS, mensagem de marketing sem aceite registrado e função que chama a si mesma. Me mostre a lista antes de corrigir."

Depois corrige uma por vez.

Este material é informativo e não é consultoria jurídica. Pro teu caso, fala com um advogado.

Quer aprender a construir com IA sem cair nessas armadilhas, em português?

Lista de espera do **Prosperando com IA**: aliceallgayer.com.br/Lista?de=prosperando