Perdomlabs

Checklist de Governança de IA + LGPD

24 pontos pra auditar como sua empresa usa IA hoje.

Como usar: marque o que sua empresa **já faz hoje**. Cada item **não** marcado é uma lacuna de governança — risco de vazamento, custo descontrolado ou exposição à LGPD. No fim há um guia de pontuação.

1. INVENTÁRIO E VISIBILIDADE (SHADOW AI)

- [ ] **1.** Você sabe quais ferramentas de IA (ChatGPT, Copilot, Claude, Gemini...) seus times usam hoje — inclusive as não oficiais?
- [ ] **2.** Existe um inventário das integrações de IA nos seus produtos e sistemas (APIs, agentes, RAG)?
- [ ] **3.** Há uma política de uso de IA escrita e comunicada aos funcionários?

2. IAM E ACESSOS

- [ ] **4.** As chaves de API de IA são individuais e rastreáveis — não compartilhadas entre pessoas?
- [ ] **5.** O acesso a modelos e dados segue o princípio do menor privilégio?
- [ ] **6.** As chaves de API ficam num cofre de segredos (não em código, .env commitado ou planilha)?
- [ ] **7.** Existe rotação e revogação de chaves quando alguém sai ou troca de função?

3. AMBIENTES E DADOS

- [ ] **8.** Há separação entre ambientes (dev, staging, produção) para experimentos com IA?
- [ ] **9.** Dado real de cliente é mantido fora de testes/prompts, ou anonimizado antes do uso?
- [ ] **10.** Existe regra clara de quais dados podem ser enviados a modelos de terceiros — e quais nunca?

4. CUSTO E ESCOLHA DE MODELO

- [ ] **11.** Você tem visibilidade do custo mensal de IA por time ou projeto?
- [ ] **12.** Há alertas e limites de gasto (budget) configurados nas plataformas de IA?
- [ ] **13.** A escolha do modelo é por caso de uso (custo × qualidade) — não o mais caro por padrão?
- [ ] **14.** Há otimização de prompts e contexto pra reduzir tokens desperdiçados?

5. SEGURANÇA E GUARDRAILS

- [ ] **15.** Existe prevenção contra vazamento de dado sensível/PII em prompts (filtros, DLP)?
- [ ] **16.** Seu time sabe reconhecer e mitigar prompt injection?
- [ ] **17.** Ações de agentes em operações críticas passam por aprovação humana?
- [ ] **18.** Há logs de quem usou IA, com quê e quando (trilha de auditoria)?

6. LGPD E CONFORMIDADE

- [ ] **19.** Há base legal definida para o tratamento de dados pessoais via IA?
- [ ] **20.** Os contratos com fornecedores de IA cobrem tratamento de dados (DPA) e sub-processadores?
- [ ] **21.** Você sabe se o fornecedor usa seus dados/prompts para treinar modelos — e desativou isso?
- [ ] **22.** Existe processo para atender direitos do titular (acesso, exclusão) quando há IA envolvida?

7. CAPACITAÇÃO DO TIME

- [ ] **23.** Os funcionários receberam treinamento sobre uso seguro e produtivo de IA?
- [ ] **24.** Os desenvolvedores sabem manter a qualidade do código gerado por IA (complexidade, revisão)?

Quantos você marcou?

20–24	Maturidade alta. Foco em refinar e auditar continuamente.
12–19	Há base, mas com lacunas que já representam risco real. Priorize IAM, custo e LGPD.
0–11	Exposição significativa. Vale um diagnóstico estruturado antes que um incidente force a conversa.

Quer ajuda pra fechar essas lacunas?

A Perdomlabs faz um Diagnóstico de Governança de IA e implementa as correções junto do seu time.

perdomlabs.com · **contato@perdomlabs.com**

© Perdomlabs · perdomlabs.com