Data-Driven Decision Making com IA

rocketseat.com.br

Por Mayra Melo

Por que se preocupar com dados?

- *Dados são ativos valiosos: informações estratégicas, clientes, processos internos.*
- *Vazamentos podem causar prejuízos financeiros e reputacionais.*
- *IA online (ChatGPT, Claude, Perplexity) processa dados fora da empresa* **Risco de exposição.**

Exemplo prático:

Enviar uma planilha de clientes para um chatbot sem anonimização → risco de vazamento de informações pessoais.

Data Governance

Conjunto de práticas, políticas e regras para gerenciar dados dentro de uma organização.

Objetivos:

Qualidade
Dados corretos e confiáveis.

Segurança
Acesso controlado.

Conformidade legal
GDPR, LGPD, HIPAA.

Uso ético
Evitar discriminação ou vieses.

Regra de governança

“Dados de clientes nunca podem ser enviados para ferramentas externas sem anonimização.”

Principais riscos ao usar IA externa

- Vazamento de dados sensíveis
- Violação de compliance
- Risco reputacional
- Dependência de terceiros

Tipos de dados que exigem cuidado

- Dados PII (Personally Identifiable Information)
- Dados financeiros
- Segredos comerciais
- Dados sensíveis especiais - saúde, política e outros

Boas práticas para desenvolvedores

1. **Anonimização**: remover nomes, CPFs, emails.

2. **Agregação**: usar dados em grupos (ex.: “média de vendas por região” em vez de transações individuais).

3. **Uso de dados fictícios**: criar datasets simulados para testes de IA.

4. **Revisão de termos de uso**: entender o que a ferramenta faz com os dados enviados.

5. **Logs e monitoramento**: controlar quem envia dados para IA externa.

Quando é seguro usar IA online?

1. **Dados completamente anonimizados ou sintéticos.**
2. **Consultas sem informações sensíveis ou confidenciais.**
3. **Cenários de teste e prototipagem sem conexão com dados reais.**

Ferramentas e Técnicas de proteção

- **Tokenização:** substitui dados reais por tokens.
- **Máscaras de dados:** ex.: CPF 123.456.789-00 → XXX.XXX.XXX-XX
- **Ambientes sandbox internos:** IA hospedada dentro da empresa.
- **Consentimento:** obter autorização de usuários se necessário.

Check-list de Data Governance

- Os dados são confidenciais?
- Os dados foram anonimizados?
- Existe risco de vazamento se enviados?
- Estou violando alguma política interna ou lei?
- Posso criar dados fictícios para teste?