Calean Tech

Checklist de IA segura

Doze perguntas para responder antes de colocar uma IA para trabalhar com dados da empresa.

Use antes de liberar uma ferramenta de IA para a equipe, ou antes de ligar uma IA aos dados da empresa. Cada “não sei” é um item de trabalho.

Dados

- [ ] Sabemos quais dados a IA vai ler, e de onde eles vêm?
- [ ] Dados pessoais e sigilosos estão fora, ou mascarados?
- [ ] O fornecedor usa os nossos dados para treinar os modelos dele? Isso está escrito no contrato?

Acesso

- [ ] A IA enxerga só o que a pessoa que pergunta pode enxergar?
- [ ] As credenciais da integração são temporárias e guardadas em cofre, nunca no código?
- [ ] Existe um dono nomeado para cada uso de IA?

Uso

- [ ] A equipe sabe o que pode e o que não pode colar numa IA?
- [ ] Há uma ferramenta aprovada, para ninguém precisar usar a conta pessoal?
- [ ] Respostas que viram decisão passam por revisão humana?

Registro

- [ ] Guardamos quem perguntou o quê, e quando?
- [ ] Conseguimos desligar a integração em minutos, se algo der errado?
- [ ] Revisamos este checklist pelo menos a cada seis meses?