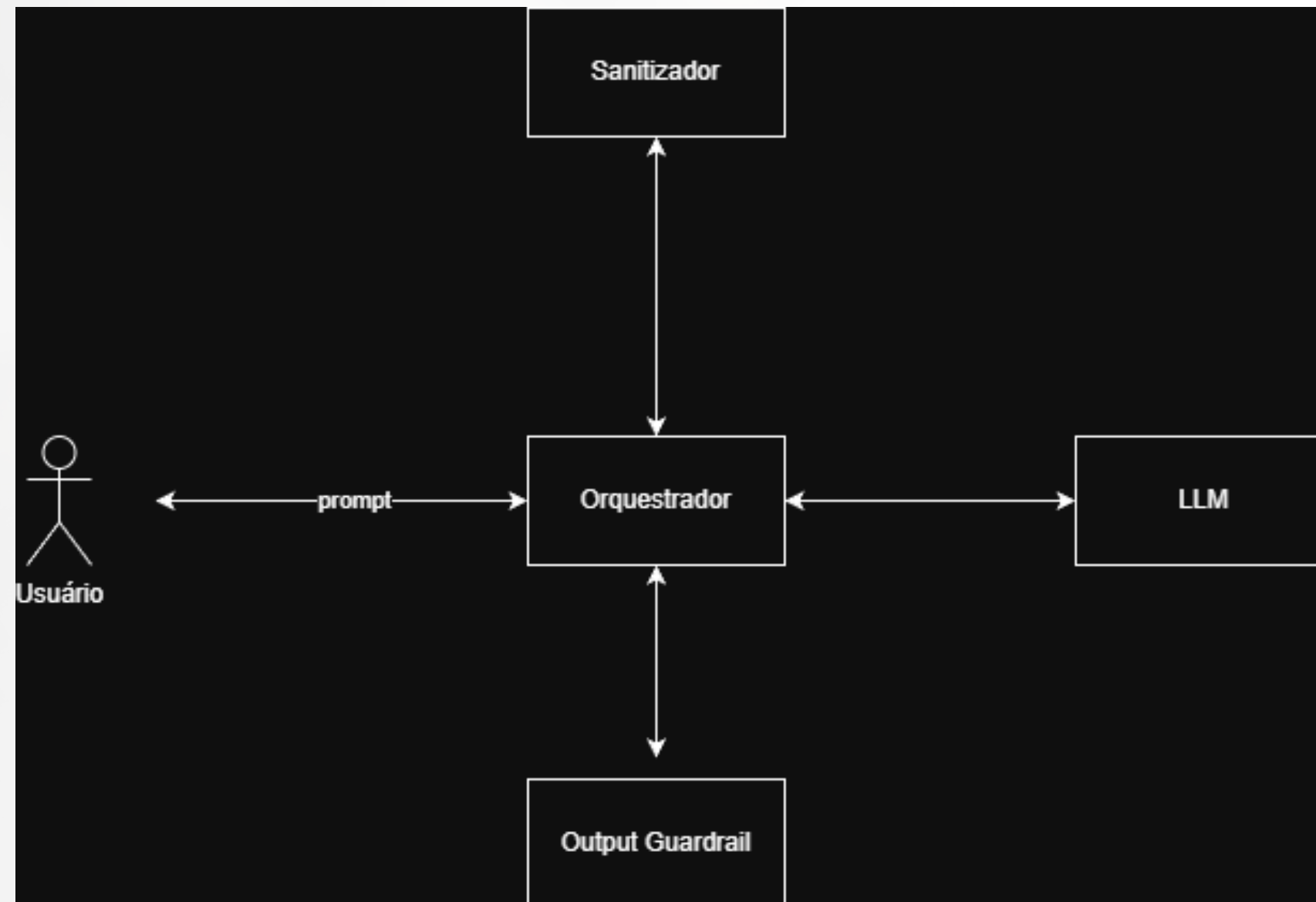


# PLANEJAMENTO E IMPLEMENTAÇÃO

Grupo: Segurança de prompts em modelos de LLMS

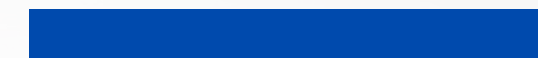
Juan Gustavo, Lucas Emanuel, Lucas Messias, Joás Vitor e  
João Victor



# ARQUITETURA

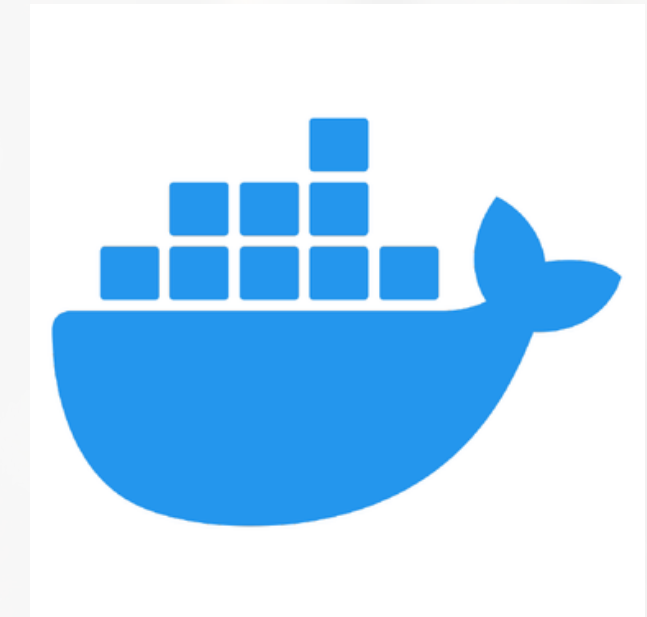
Composta por 4 entidades:

- Usuário (prompt)
- orquestrador
- sanitizador
- Serviço de LLM
- Output guardrail



# TECNOLOGIAS

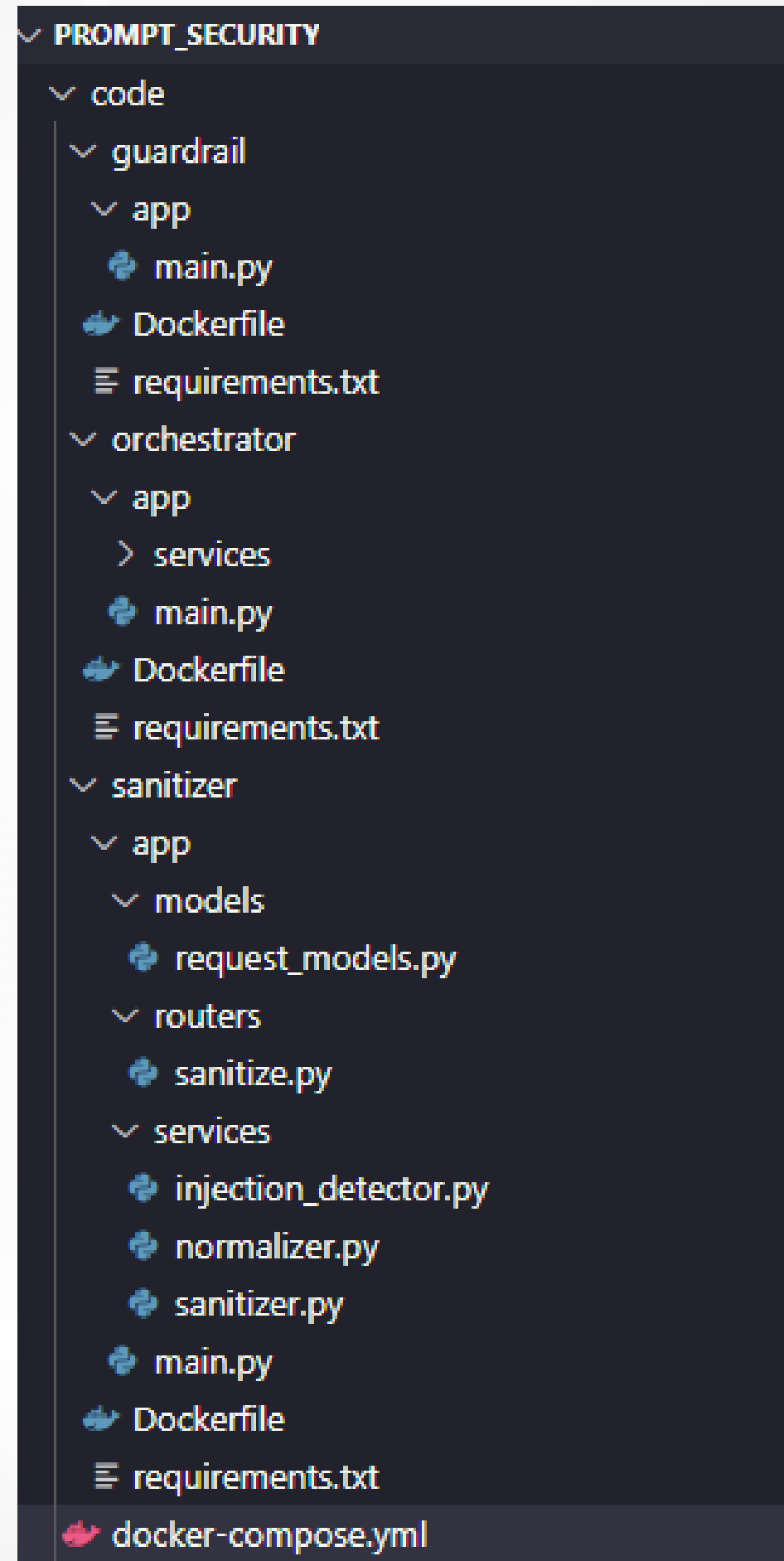
- Python
- FastApi/Uvicorn
- OpenAi Api
- Docker
- Draw.io



# ESTRUTURA DO PROJETO

Foi montado o código inicial das entidades envolvidas no projeto

Foi montado o arquivo Dockerfile e docker-compose para automatizar a criação da estrutura do projeto



A top-down view of a desk with various items: a laptop in the upper center, a cup of coffee in the upper left, a pen in the center, a pair of glasses in the lower center, several paper clips on the left, and a large green leaf in the bottom left corner. The background is a light, neutral color.

**OBRIGADO**