



MLOps:

Superando os Desafios para Colocar Modelos de Machine Learning em Produção



PALESTRANTES



Celio Hira Cientista de Dados

Líder técnico em projetos de Engenharia e Ciência de Dados que envolvem a construção de Data Lake em Cloud e implementação de modelos de Machine Learning para Manutenção Preditiva, Forecast de Vendas, Cálculo de Churn dentre outras aplicações.

 [/in/celiohira/](https://www.linkedin.com/in/celiohira/)



Lucas Fantacuci Engenheiro de Software

Atua em projetos de automação de pipeline de entrega contínua de modelos de machine learning, versionamento do código, de dados, de modelos entre outras práticas do MLOps, utilizando tecnologias, tais como Mlflow,,Azure Pipelines, Databricks e Containerização..

 [/in/lucas-sanches-fantacuci/](https://www.linkedin.com/in/lucas-sanches-fantacuci/)



SOMOS A ELEFLOW!

Consultoria de Big Data especializada em gestão e implementação de projetos de dados. Com expertise em:

- Construção de Data Lakes
- Migração para a nuvem
- Implementação e otimização de ferramentas de dados
- Projetos de Governança
- Construção de dashboards
- Modelos de machine learning e Implementação de MLOps

Parceiros :



Em 2021, de acordo com a Gartner, 85% dos projetos de Machine Learning eventualmente falham em trazer os resultados esperados para o negócio.

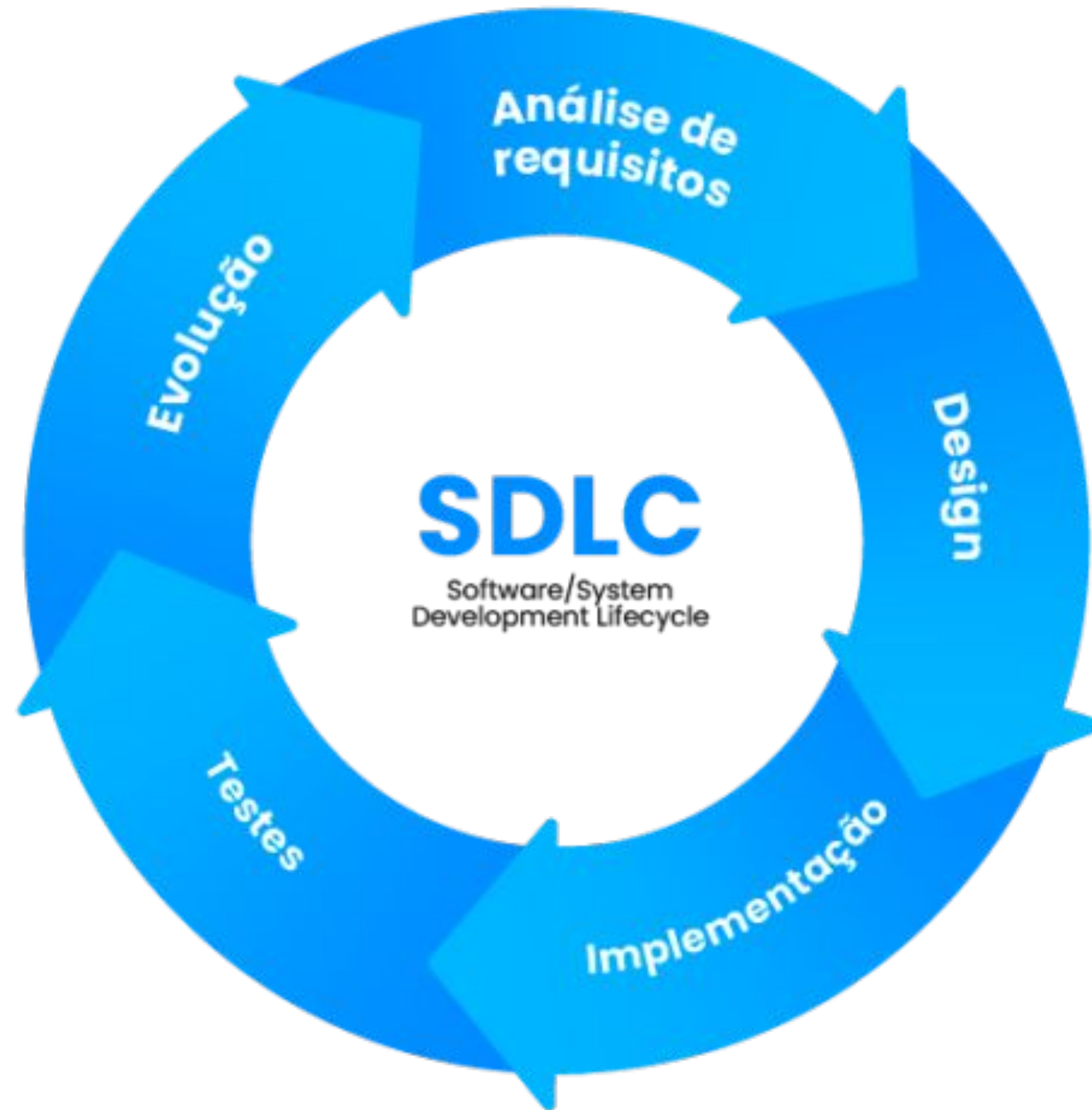
QUAIS SÃO OS DESAFIOS?



Perda inevitável de performance de sistemas de machine learning

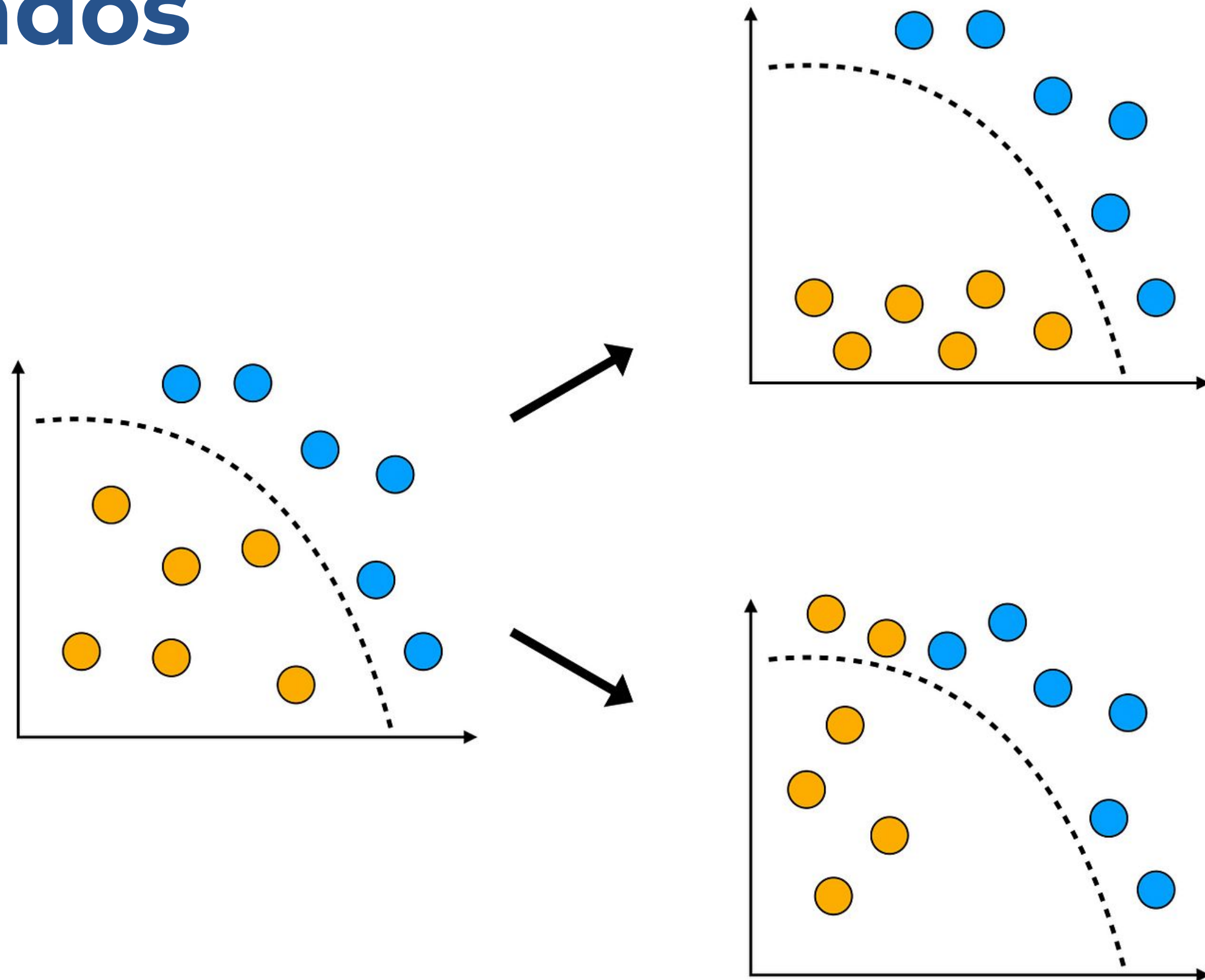


Evolução dos requisitos





Mudança nos padrões dos dados



Dificuldades para publicações de uma nova versão





Muito trabalho manual

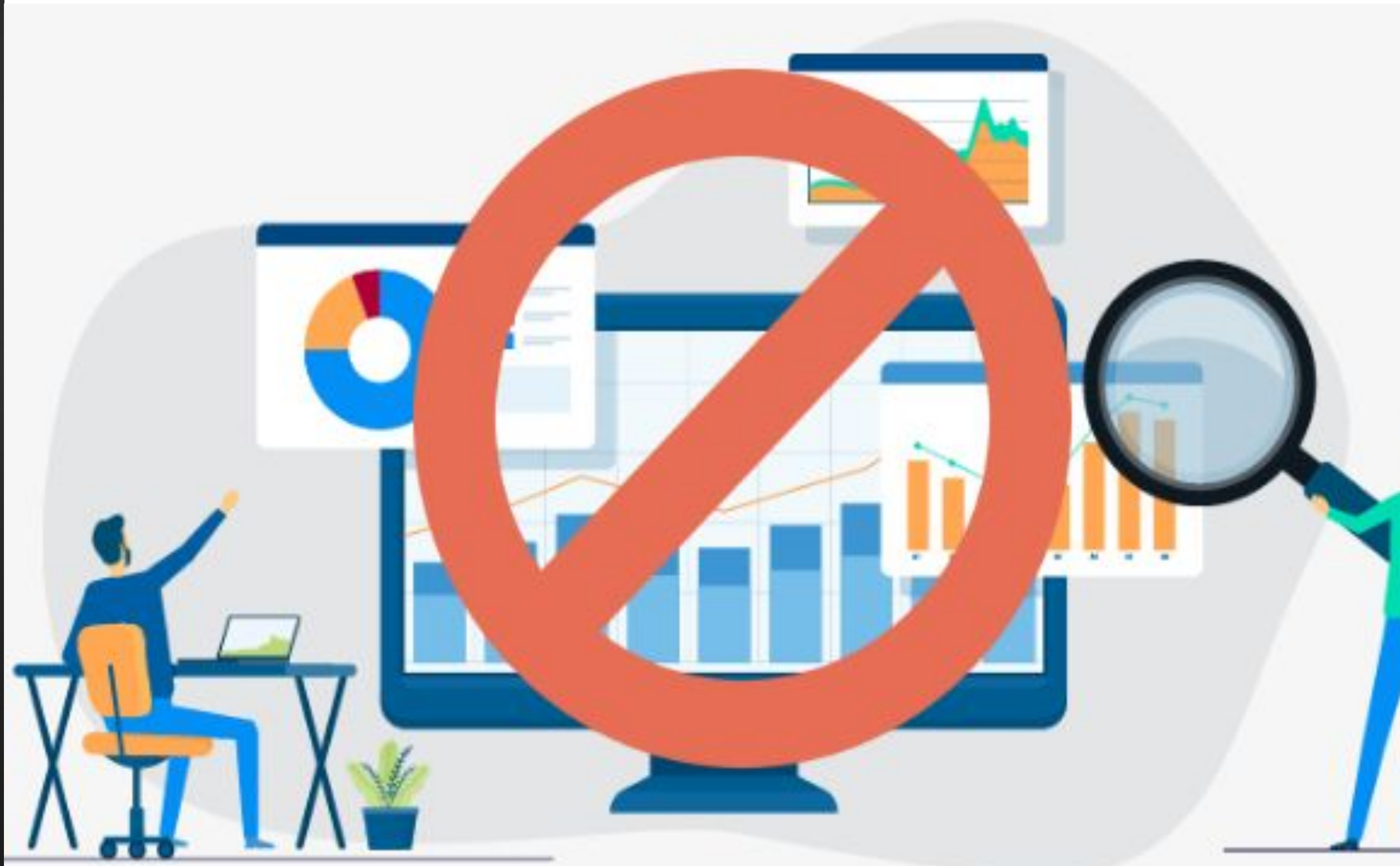




Falta de padronização



Ausência de monitoria

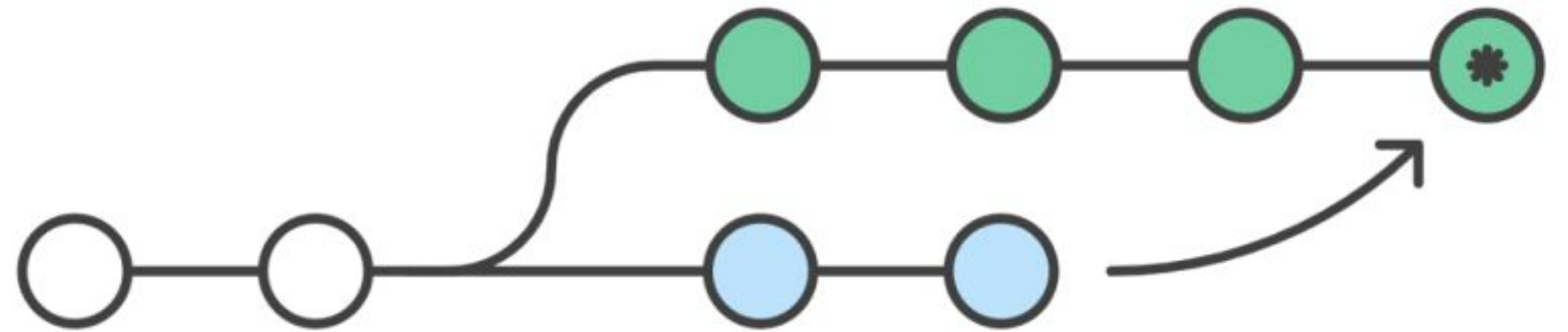


Dificuldades para investigar bugs e problemas





Falta de rastreabilidad





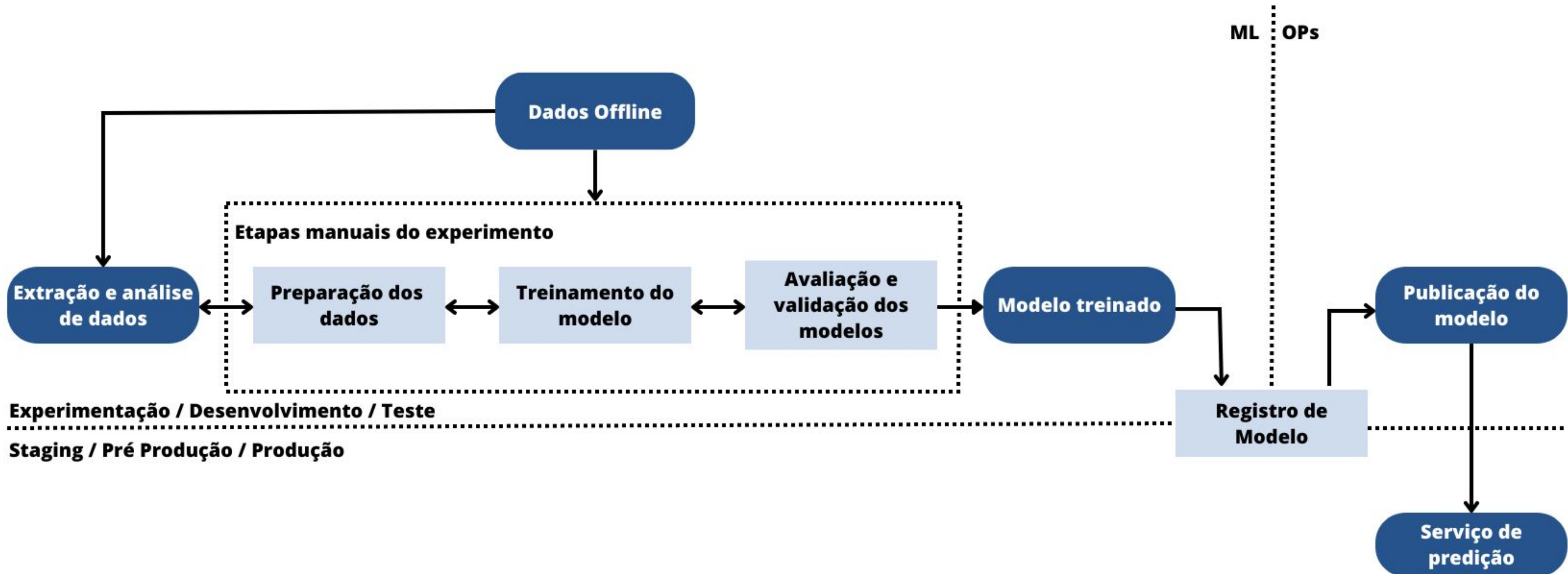
Ambientes inconsistentes

Desenvolvimento

VS

Produção

ML SEM MATURIDADE DE PROCESSO



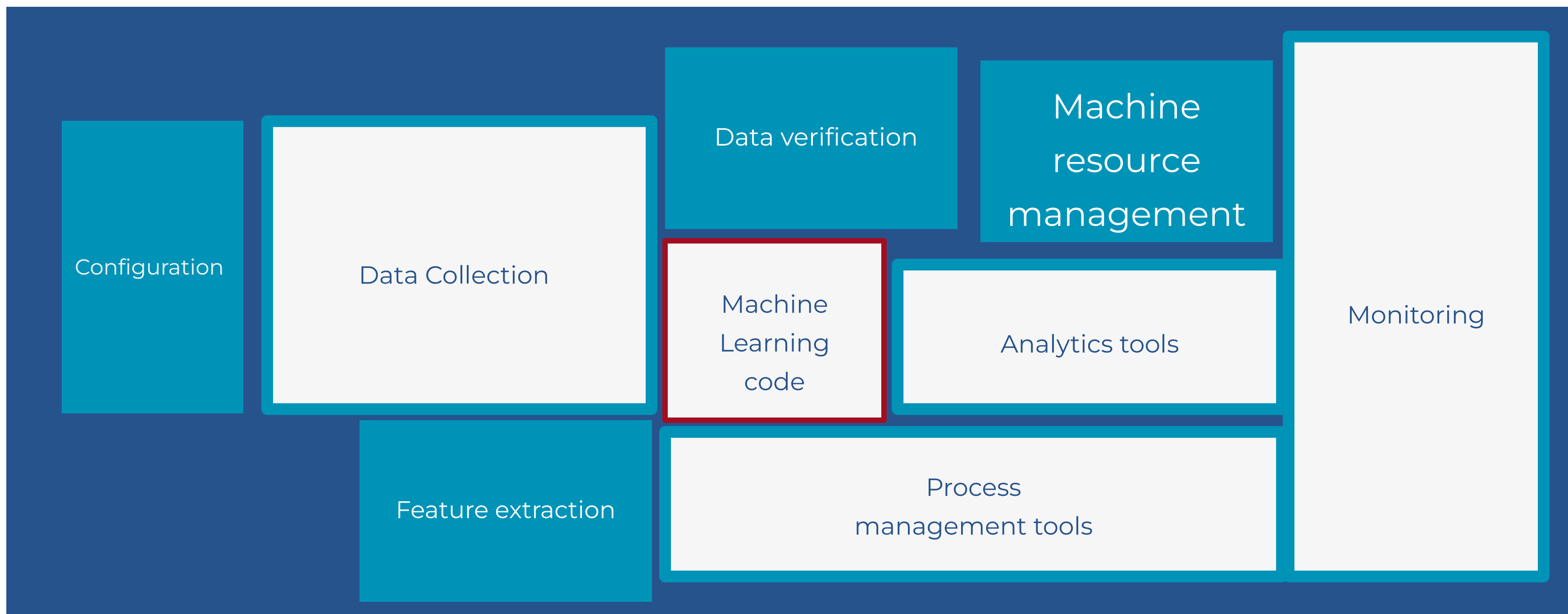
**E POR QUE ENFRENTAMOS
ESSES DESAFIOS?**



O QUE PENSAMOS QUE É UM SISTEMA DE ML

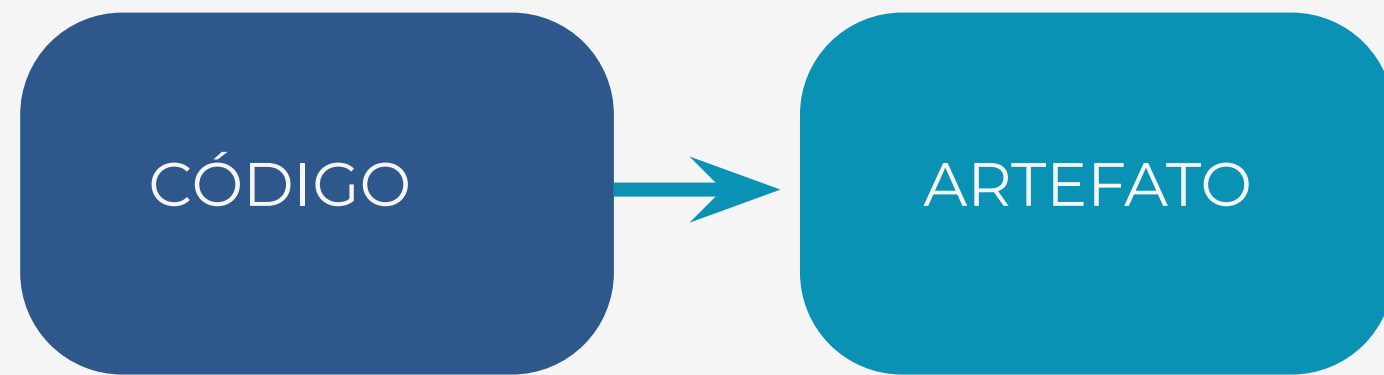
Machine
Learning
code

O QUE É UM SISTEMA DE ML

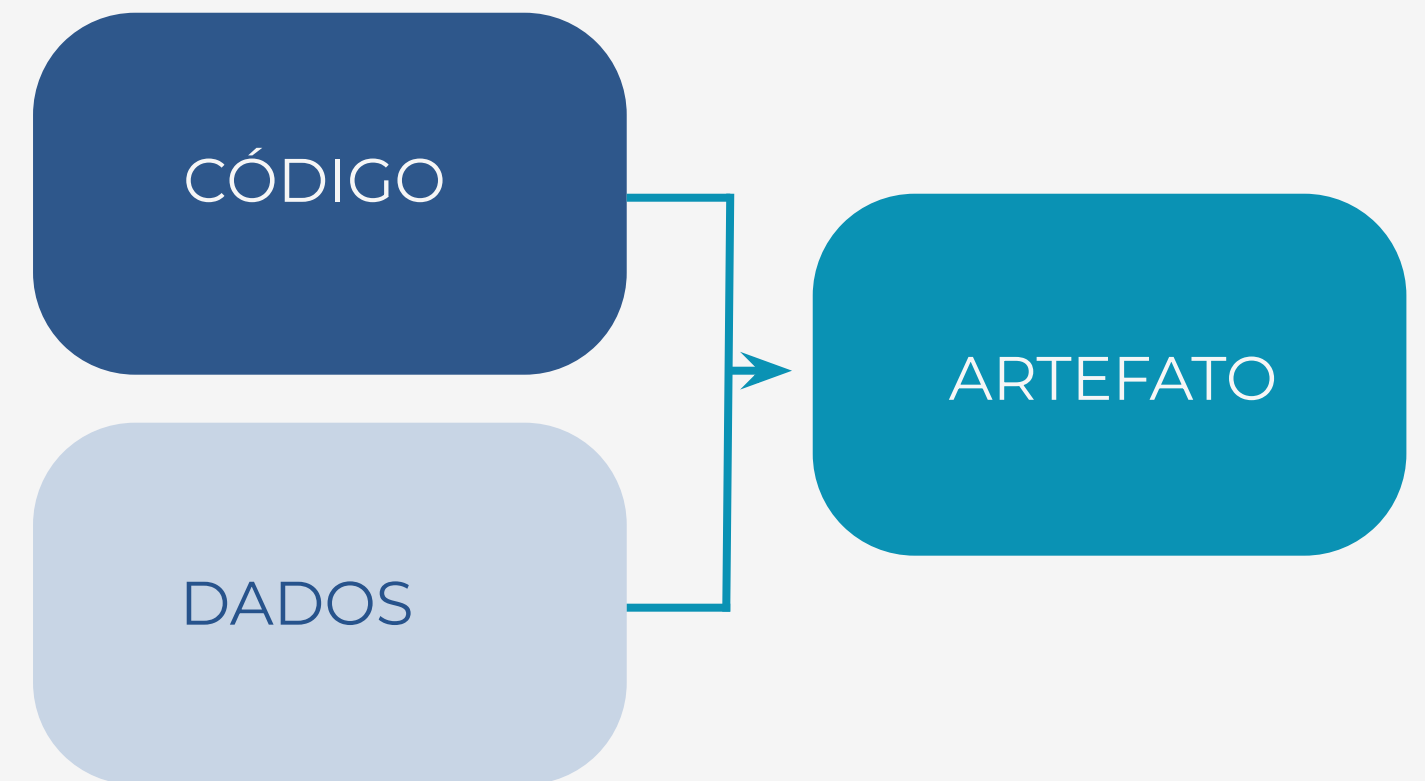


Construção de Sistemas: ML vs Software tradicional

Software tradicional



Machine Learning



Diferenças de Sistemas de ML em pesquisa e em produção

	Pesquisa	Produção
Requisitos	O único requisito é um modelo com uma acurácia no estado da arte	Diferentes stakeholders possuem diferentes requisitos
Prioridade computacional	Treino rápido, alto throughput	Rápida inferência, baixa latência
Dados	Estáticos	Constantemente em mudança

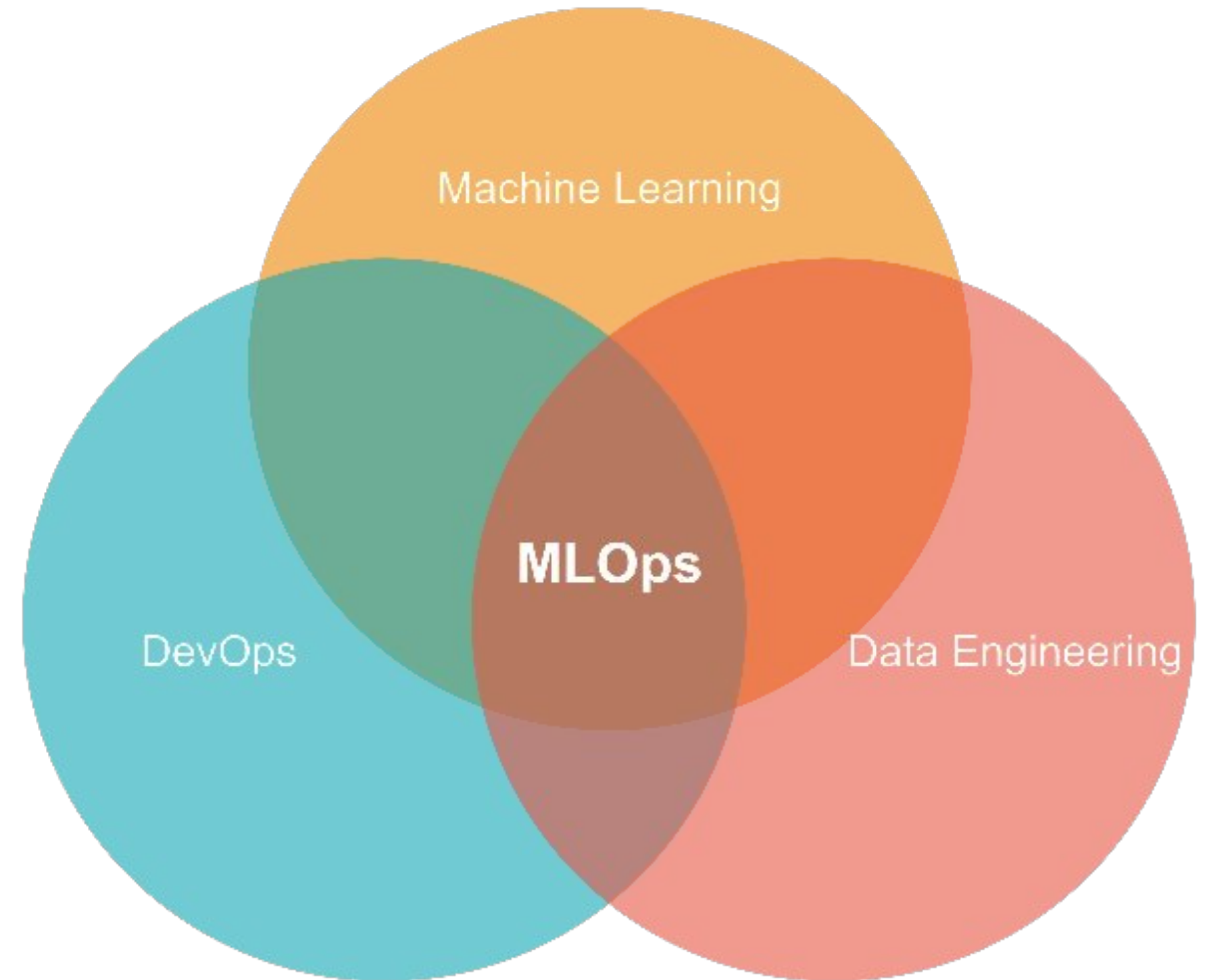
*Tabela retirada do Livro Designing Machine Learning Systems de Chip Huyen de 2022 em sua 1ª edição.

COMO O DEVOPS NÃO É SUFICIENTE, SURGE O MLOPS



MLOps

Conjunto de práticas para gerenciar modelos, dados e códigos de forma a atingir um desempenho estável e eficiente no longo prazo em sistemas de Machine Learning



PRINCÍPIOS MLOPS

Automação

Versionamento

Monitoria

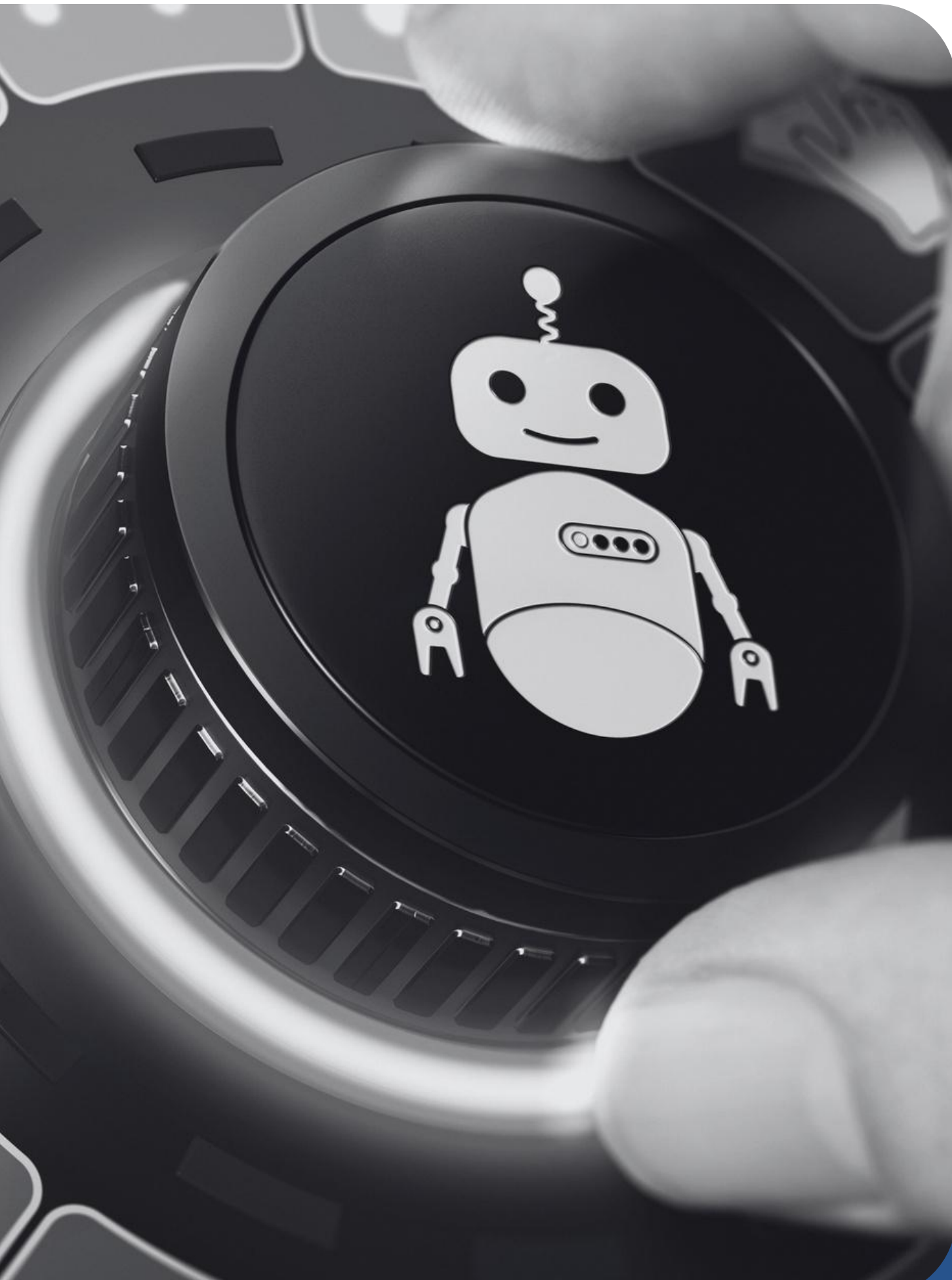
Governança

Reprodutibilidade

Testes

Continuous X

Cultura



Automação

A ideia é agilizar as etapas do ciclo de vida dos modelos de ML de modo a evitar intervenção manual. Inclui:

- Automação dos processos de treinamento, validação, implantação e monitoramento dos modelos
- Implementação de pipelines de dados e CI/CD



Versionamento

Lidar com o versionamento dos dados e dos modelos igualmente ao versionamento dos códigos e artefatos.



Monitoria

O monitoramento é essencial para garantir a qualidade e a confiabilidade dos modelos de ML. Isso inclui monitorar:

- **Dados:** mudanças na distribuição dos dados (data drift) / dados estão no schema esperado?
- **Modelos:** performance do modelo
- **Saúde do sistema como um todo:** código-fonte / pipelines de dados / pipelines de CI/CD

A black and white aerial photograph of a city at night. The image shows a dense urban landscape with numerous skyscrapers and buildings. A prominent feature is a series of bright, vertical light trails that appear to be emanating from the ground and reaching towards the sky, creating a sense of digital connectivity or data flow. The overall atmosphere is futuristic and high-tech.

Reprodutibilidade

Todas as fases do processamento de dados, do treinamento do modelo de ML e da implantação do modelo de ML devem produzir resultados idênticos com a mesma entrada:

- Dados: versionamento de dados
- Modelos: versionamento de modelos
- Código: garantir que as dependências de dev/prod são idênticas / utilização de imagens de containers

Testes

O objetivo é assegurar-se que algo funciona conforme o planejado e tentar descobrir erros o mais cedo possível no ciclo de ML, diminuindo custos e desperdício de tempo.

- **Dados** - validação automática do schema e de estatísticas
- **Código** - testes unitários (partes do código) / testes de integração (disparar a pipeline de ML fim a fim)
- **Modelos** - especificação do modelo / desempenho.



Continuous X (CX)

Integração Contínua (CI)

Entrega Contínua (CD)

Treinamento Contínuo (CT)



Integração contínua

Prática de automatizar a integração de alterações de código, dados e modelos através de testes e validações.

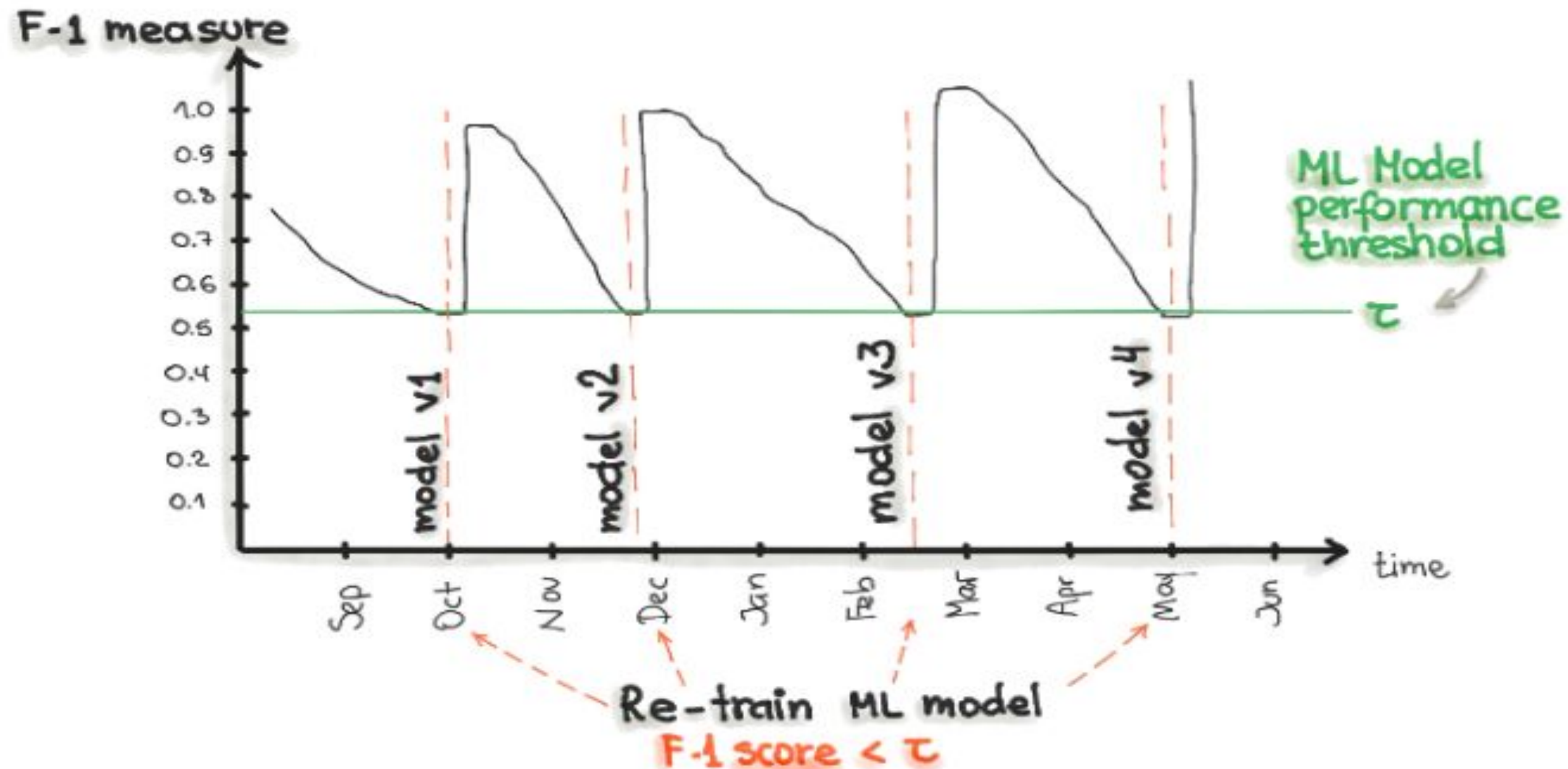


Entrega Contínua

Prática de automatizar o deploy dos artefatos presentes em todo o ciclo de vida de ML.

Treinamento Contínuo

ML MODEL DECAY MONITORING





Governança

Objetivo: Definir regras para o controle de acesso, implementação de políticas e rastreamento de atividades para os processos no fluxo de trabalho de modelos de ML

Racional: O fluxo de trabalho de ML é muito complexo, exigindo bastante automação. Nesse cenário, é muito importante que todas as etapas tenham rastreabilidade, que estejam em conformidade com as políticas de cada empresa e que cada componente tenha um controle de acessos e permissões



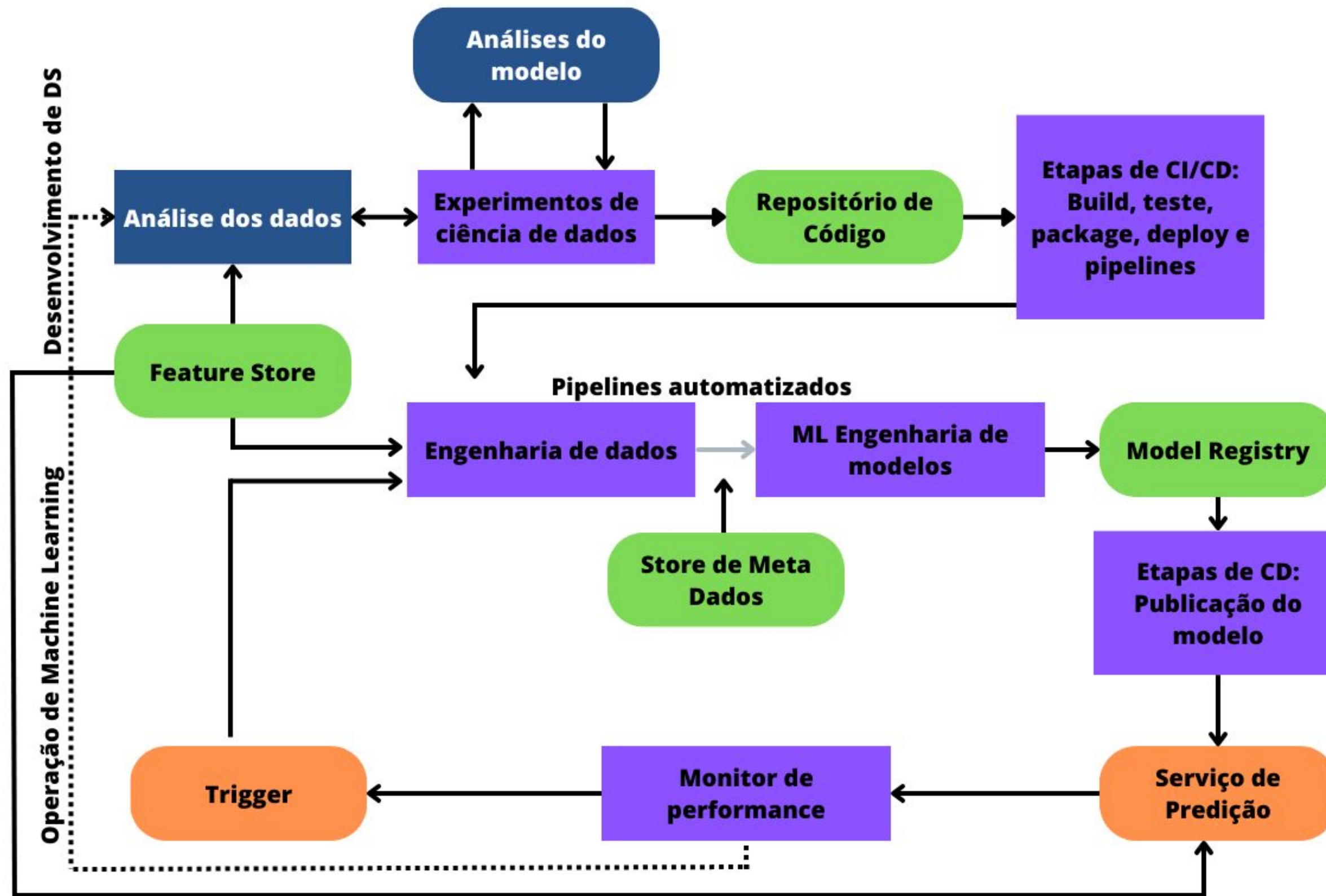
Cultura

As ferramentas / tecnologias são apenas um meio de atingir o objetivo.

É importante que o conjunto de práticas estabelecidos pelo MLOps faça parte da cultura do time que participa do fluxo de trabalho de ML.

O nível de maturidade de MLOps vai estar diretamente associado à cultura de colaboração do time. Um ambiente de colaboração que valorize o aprendizado contínuo nas ferramentas e processos do MLOps vai potencializar o impacto no negócio.

ML COM MATURIDADE USANDO MLOPS



PANORAMA DE FERRAMENTAS E TECNOLOGIAS MLOPS



DATA MANAGEMENT

Data Exploration & Management

Data Labelling

Data Streaming

Data Version Control

Data Generation

Data Privacy

Data Quality Checks

MODELLING

Notebook / Code Management

Data Processing & Visualization

Feature Engineering

Model Training

Experiment Tracking

Model (Hyperparameter) Optimization

Auto ML

Model Management

Model Evaluation

Model Explainability

Frameworks & major libraries

CONTINUOUS DEPLOYMENT

Data Flow Management

Feature Transformation

Monitoring

Model Compliance & Audit

Model Deployment & Serving

Model Validation

Model Compatibility

COMPUTING MANAGEMENT

Computing & Data Infrastructure

Environment Management

Resource Allocation

SCALING

SECURITY & PRIVACY

DADOS

VERSIONAMENTO



PROCESSAMENTO



ARMAZENAMENTO



FEATURE STORE



MACHINE LEARNING

VERSIONAMENTO DE MODELOS / EXPERIMENTOS



AJUSTE DE HYPERPARÂMETROS



MONITORAMENTO



DEPLOYMENT

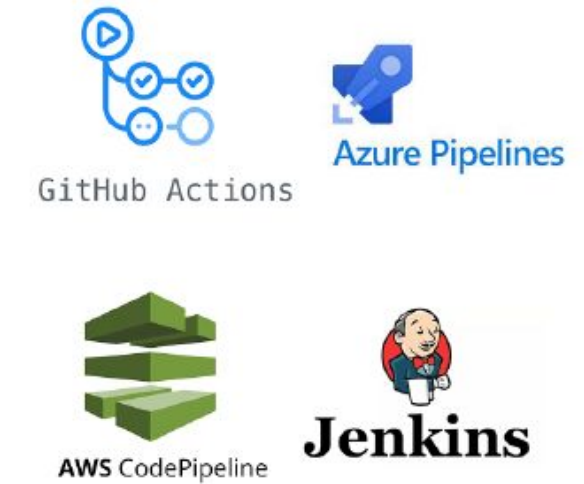


DEV OPS

VERSIONAMENTO DE CÓDIGO



CI/CD



DEPLOYMENT





Considerações finais

- ▶ Projetos de Machine Learning são complexos;
- ▶ MLOps é um conjunto de práticas para gerenciar modelos, dados e códigos de forma a atingir um desempenho estável e eficiente no longo prazo em sistemas de Machine Learning;
- ▶ Não é necessário aplicar todos essas práticas para agregar valor ao negócio. Pode-se aplicar essas práticas de forma incremental;
- ▶ Tudo depende do contexto da cada empresa, de cada caso de uso.



OBRIGADO



 [@eleflowbigdata](https://www.instagram.com/eleflowbigdata)

 [in/eleflow](https://www.linkedin.com/company/eleflow)