FINANCE TECH
BOOST

Inteligência Artificial e Análise de Dados

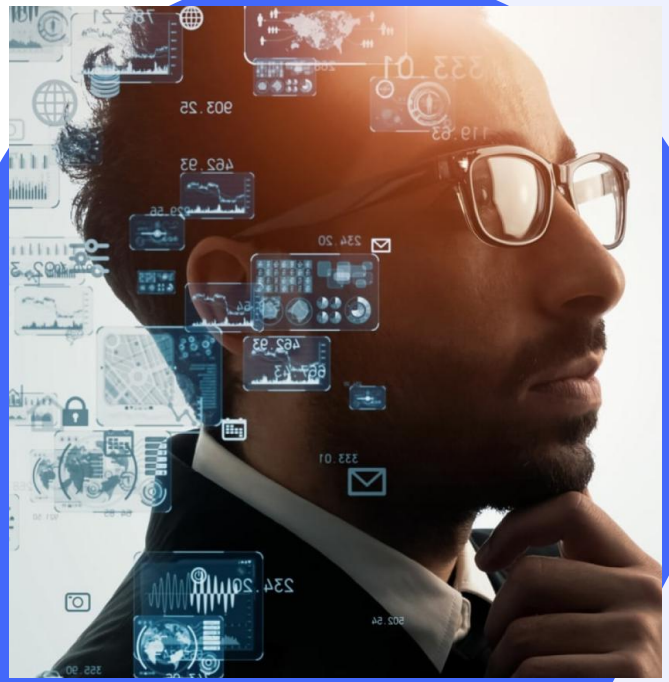
Liderando as Finanças do Futuro

Thiago Diogo e Cleber Brandão

FINANCE TECH
BOOST

Disclaimer

A Responsabilidade pela idoneidade, originalidade e licitude dos conteúdos didáticos apresentados é do especialista.



AGENDA

01 Introdução + Contexto de IA + Panorama atual das fraudes

02 Por que IA? Por que agora?

03 IA e ML aplicados a prevenção a fraudes

04 Arquitetura típica e abordagens

05 Demonstração

06 Estratégias de implementação

Prazer, eu sou Thiago

Founder & CEO
DURANIUM

Staff, Technical Solutions Consultant
Privacy Sandbox
Google

Director
Security, Privacy and Platform
unico

Chief Technology Officer (CTO)
Security, Privacy and Platform
AllowMe
TEMPEST
Protegendo negócios no mundo digital.

Cybersecurity Researcher
AWS Cloud Security & Compliance
NEW YORK UNIVERSITY

Universidade Federal Fluminense
Ciência da Computação e Mestrado em Tecnologia

Massachusetts Institute of Technology
Especialização em Criptografia e Segurança

aws certified Solutions Architect Associate

NYU
Especialização em Security Engineering

Carnegie Mellon University
Especialização em Privacy Engineering

Introdução, contexto e panorama das fraudes

Introdução

Cenário das fraudes no Brasil

O Brasil ocupa posição de destaque mundial em fraudes financeiras. Segundo dados da Federação Brasileira de Bancos (FEBRABAN), as **tentativas de fraude cresceram 73% em 2023**, representando perdas de mais de R$ 2,9 bilhões ao sistema financeiro.

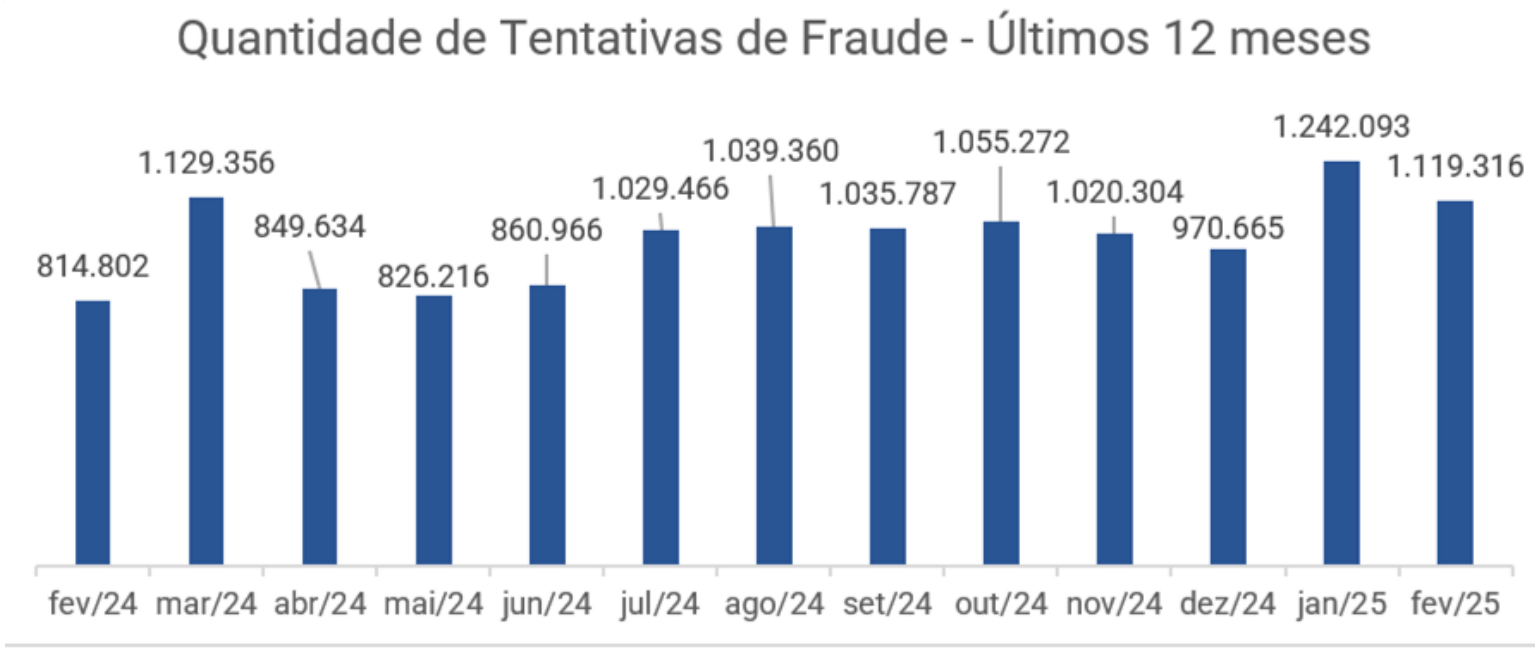
Principais vetores de fraude:

- Engenharia social (40% dos casos)
- Vazamento de dados (25%)
- Ataques cibernéticos diretos (20%)
- Fraudes em cartões (15%)

Fonte: FEBRABAN - Relatório de Tecnologia Bancária 2023

Introdução

Cenário das fraudes no Brasil



Fonte: Serasa Experian

Uma tentativa a cada 2,2 segundos

O movimento dos bancos

Como e para o que os bancos estão usando IA?

Valores percebidos a partir da aplicação de IA[1]

Casos de uso de IA aplicáveis à cibersegurança, prevenção à fraude ou à lavagem de dinheiro e estágio de adoção dos bancos participantes para cada caso[1] (percentual dos bancos)	Não explorado	Em exploração	Em implementação
Cibersegurança, para proteger sistemas e dados contra ataques cibernéticos	20%	10%	70%
Biometria, para reconhecimento de voz, face e outras características biométricas	30%	10%	60%
Visão computacional, para analisar e interpretar imagens e vídeos	35%	25%	40%
Detecção de fraude e lavagem de dinheiro, para identificar transações suspeitas e atividades ilícitas	20%	-	80%
Know Your Customer (KYC) e onboarding, para automatizar e otimizar a verificação de identidade de clientes	15%	20%	65%

FEBRABAN
Federação Brasileira de Bancos

Os bancos entendem que IA pode ser o habilitador de jornadas seguras e simples

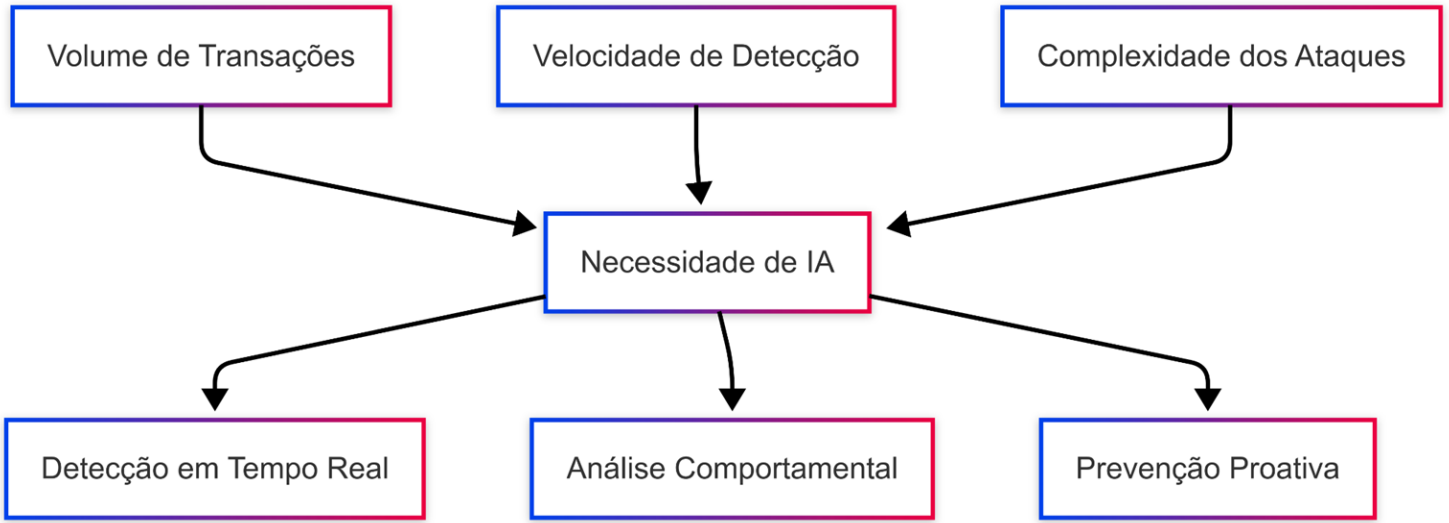
FEBRABAN
Federação Brasileira de Bancos

especialista.

alidade e licitude dos conteúdos didáticos apresentados é do

Por que IA? Por que agora?

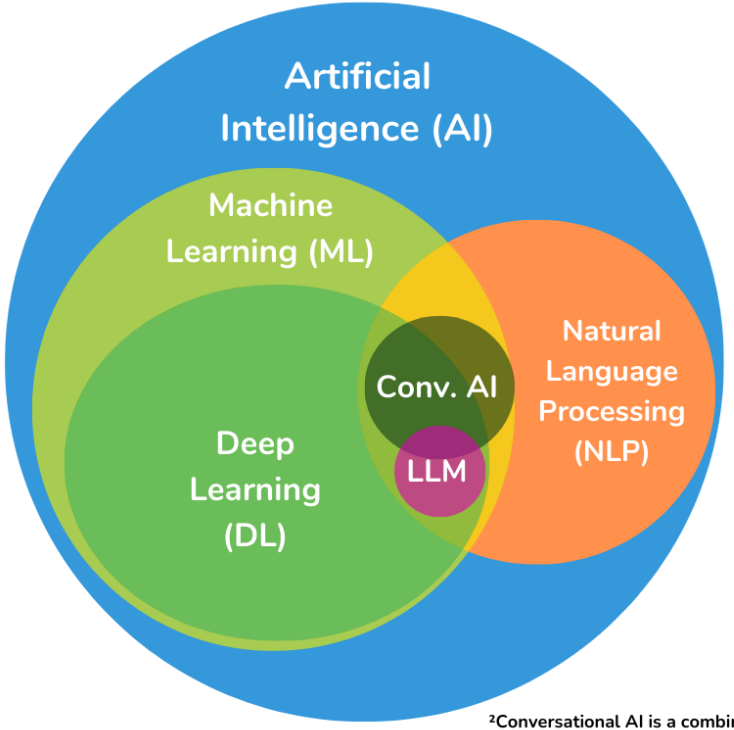
Por que IA é chave para mudar esse cenário?



Porém, cuidado!

AI ≠ GenAI

Porém, cuidado!



- Artificial Intelligence (AI)
- Machine Learning (ML)
- Deep Learning (DL)
- Natual Language Processing (NLP)
- Large Language Model (LLM)[1]
- Conversational AI (Conv. AI)[2]

[1]LLM is an intersection of DL and NLP
[2]Conversational AI is a combination of ML and NLP. It may include DL and LLM, but that isn't always the case.

O Que São LLMs?

- Modelos de linguagem de grande porte (ex: GPT-4, CodeLlama).
- Usados para gerar textos, respostas e código.
- Treinados com grandes volumes de dados.

O Problema: Alucinações

- Falta de conexão com uma base de dados atual
- Geração probabilística, não baseada em fatos
- Ausência de mecanismos de validação interna

Riscos Adicionais da IA

- Vieses nos dados e decisões injustas.
- Uso malicioso da IA para ataques ou fraudes.
- Exposição de dados sensíveis (vazamentos).
- Falta de transparência e explicabilidade.
- Automação excessiva sem supervisão.
- Responsabilidade difusa em decisões automatizadas.
- Violação de privacidade e conformidade regulatória.

Formas de Mitigação (Visão Geral)

- Retrivial-Augmented Generation(RAG).
  - IA consulta bases confiáveis antes de responder.
  - Reduz chance de inventar respostas

- Auto-refinamento (self-checking).
  - IA avalia e revisa sua própria resposta.
  - Detecta inconsistências antes da execução.

- Fine-tuning supervisionado.
  - Reeducação do modelo com dados corretos.
  - Redução de pacotes inventados.
  - Possível impacto na criatividade do código.

Boas Práticas Complementares

- Nunca confiar cegamente no código gerado por IA.
- Verificar pacotes em fontes oficiais.
- Usar ferramentas de análise de dependências.
- Implementar validação automatizada.
- Avaliar explicabilidade e fonte dos dados usados.

Conclusões

- IA é poderosa, mas pode ser enganada.
- Riscos como alucinações e uso malicioso são reais.
- Mitigação depende de práticas seguras e supervisão.

Links e materiais de estudo

- MIT AI Risk Repository

  https://airisk.mit.edu/

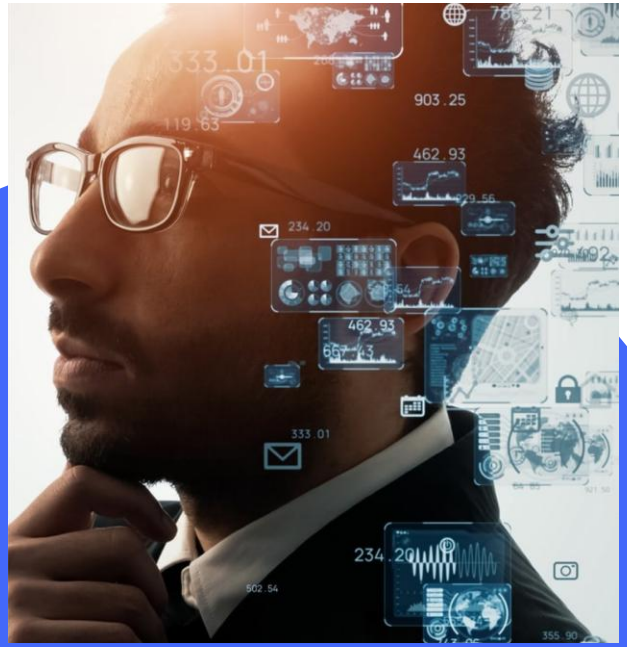
- A Comprehensive Analysis of Package Hallucinations by Code Generating LLMs

  https://arxiv.org/html/2406.10279v1

  Códigos para prática: https://github.com/Spracks/PackageHallucination

- Garak LLM Vulnerability Scanner (nvidia)

  https://garak.ai/



IA e ML aplicados a prevenção a fraudes

O contexto de dados

Entendendo os dados

O volume de dados é assustador enquanto pouca sabedoria é alcançada

O que temos de dados disponíveis?

Entendendo os dados

O cliente...

dados de identificação, idade, cidade do cadastro, tempo de cadastro, cidade da rotina de uso, data do cadastro, tempo de vida dentro do sistema, quantidade de transações aprovadas feitas antes, tempo de vida da senha, usou MFA ou não, etc

A transação...

data, hora, localização, valor, método de pagamento, detalhes do produto/serviço, descontos aplicados, uso de pontos de fidelidade, de qual dispositivo, IP de origem, sistema operacional, histórico de pedidos, frequência, etc

O chargeback...

motivo, data da transação e da solicitação, valores contestados, resultado de processos anteriores, tempo entre transação e solicitação, frequência de solicitações, consistência de códigos de chargeback, discrepância entre valor contestado e transação, etc

E muito mais:

O dispositivo, os dados do contexto do pagamento, os dados do produto/serviço,

Digite seu Tópico aqui

Entendendo os dados

*Exemplos hipotéticos de **correlações** e **padrões**:*

Em 95% das fraudes, o chargeback foi solicitado em exatos **12 min** após a transação...

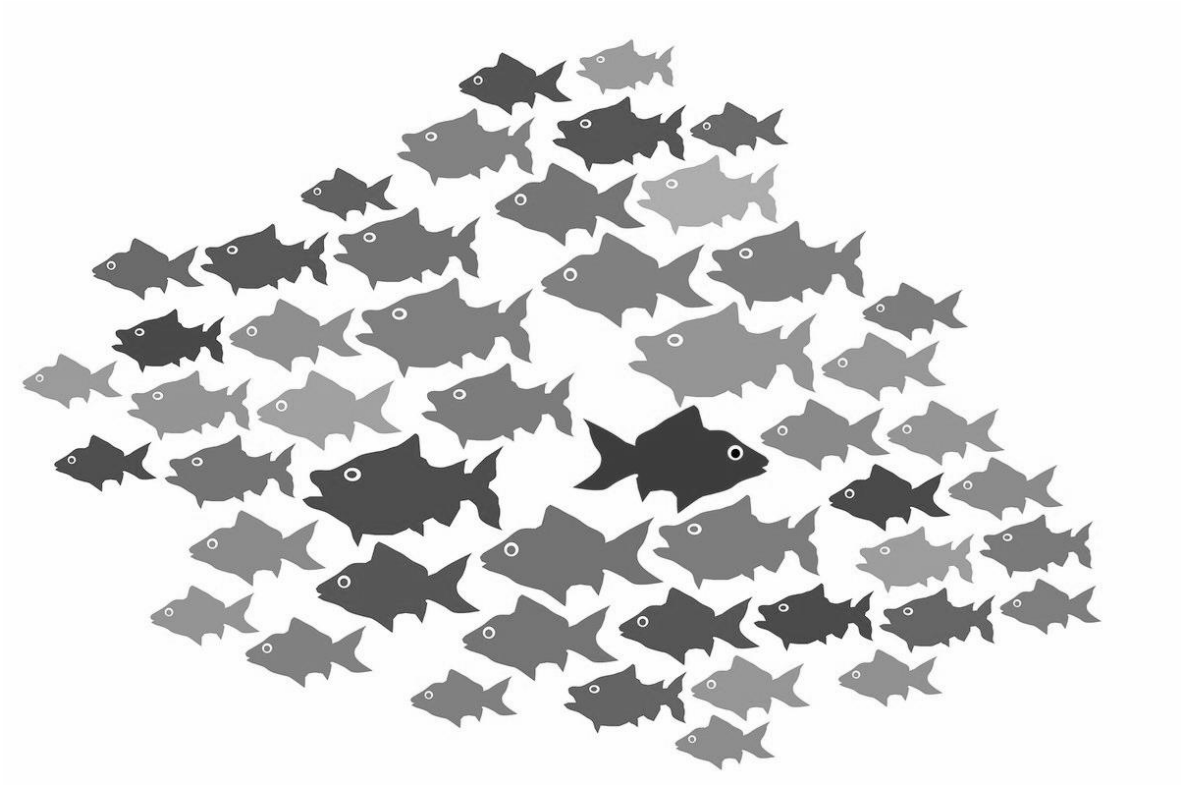
Em nenhum dos chargebacks fraudulentos, o usuário **entrou em contato** via central de atendimento tentando resolver o problema antes

Todas as transações legítimas foram feitas em até **100km do local habitual** do usuário nos últimos 2 meses

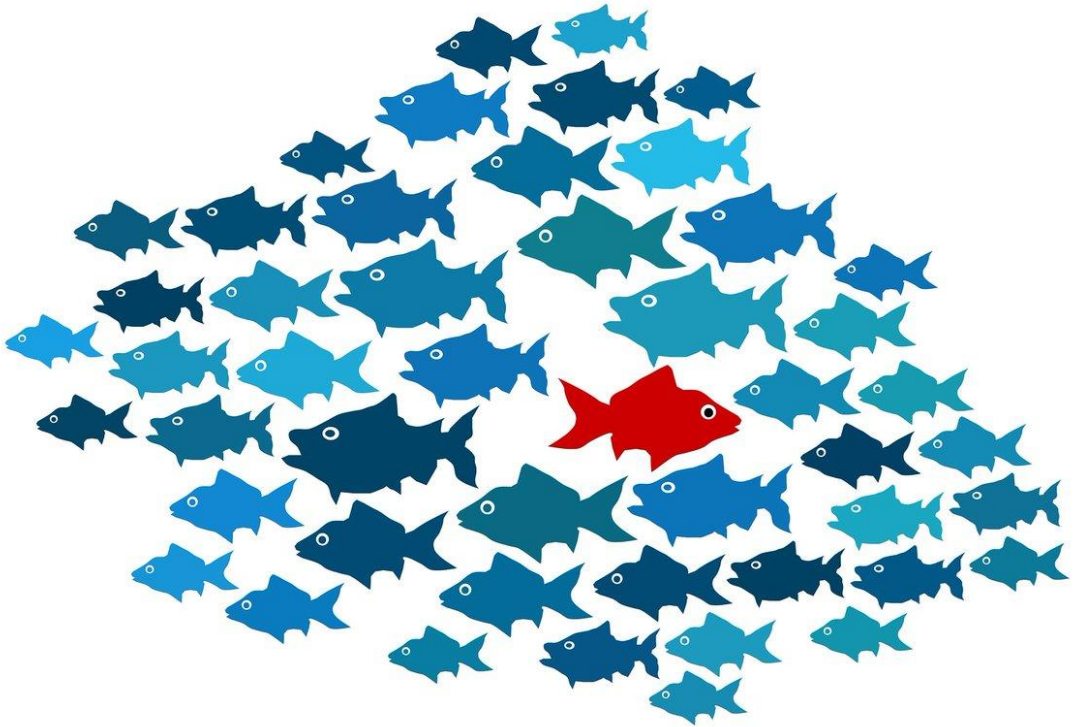
Detectar anomalias

Identificar padrões ou comportamentos incomuns que se desviam do que é considerado normal e esperado, sinalizando uma possível atividade fraudulenta

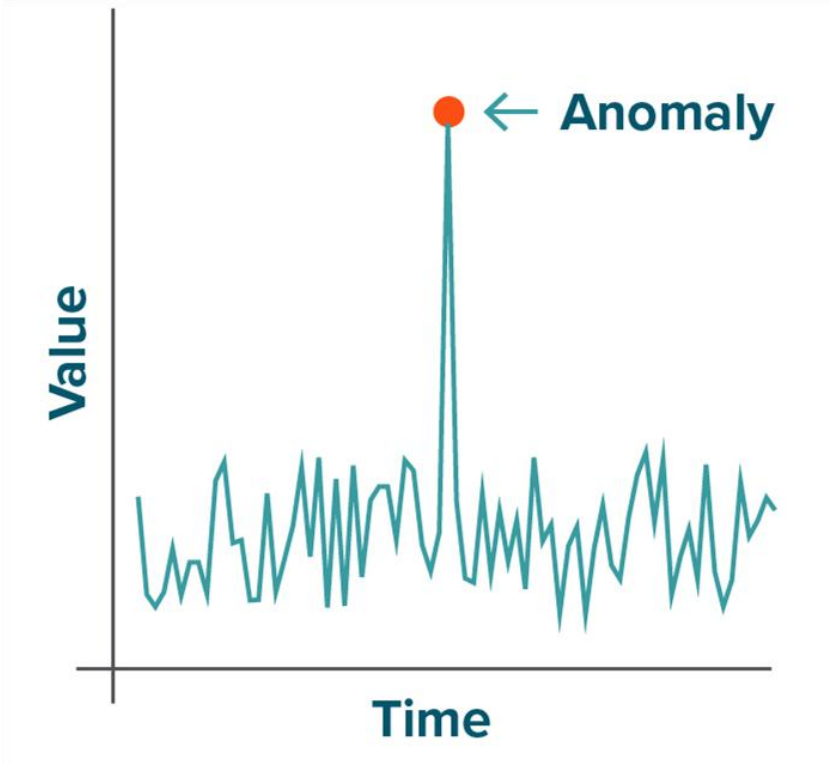
OK, mas como encontrar anomalias?



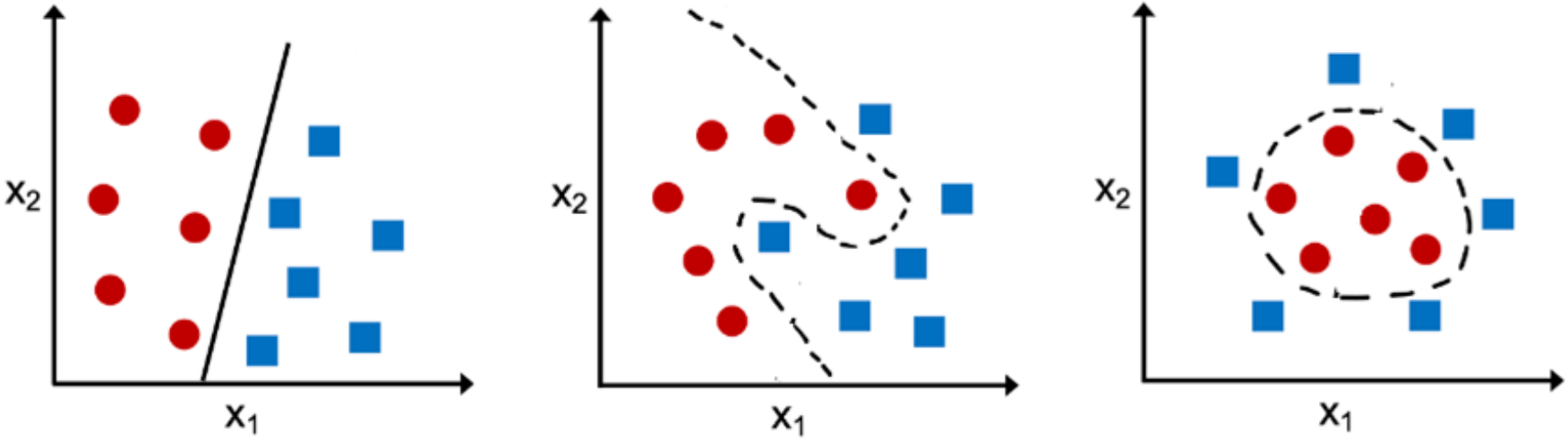
OK, mas como encontrar anomalias?



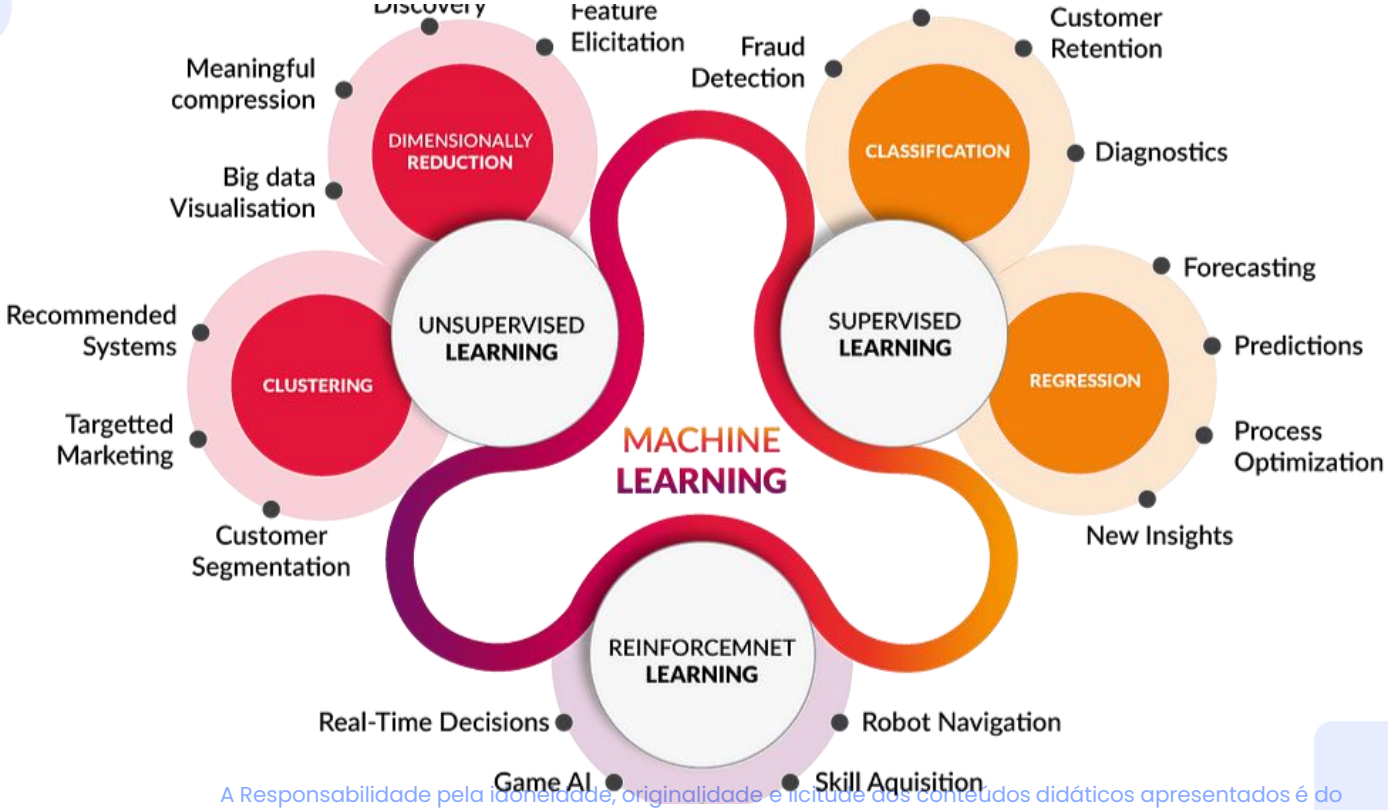
OK, mas como encontrar anomalias?



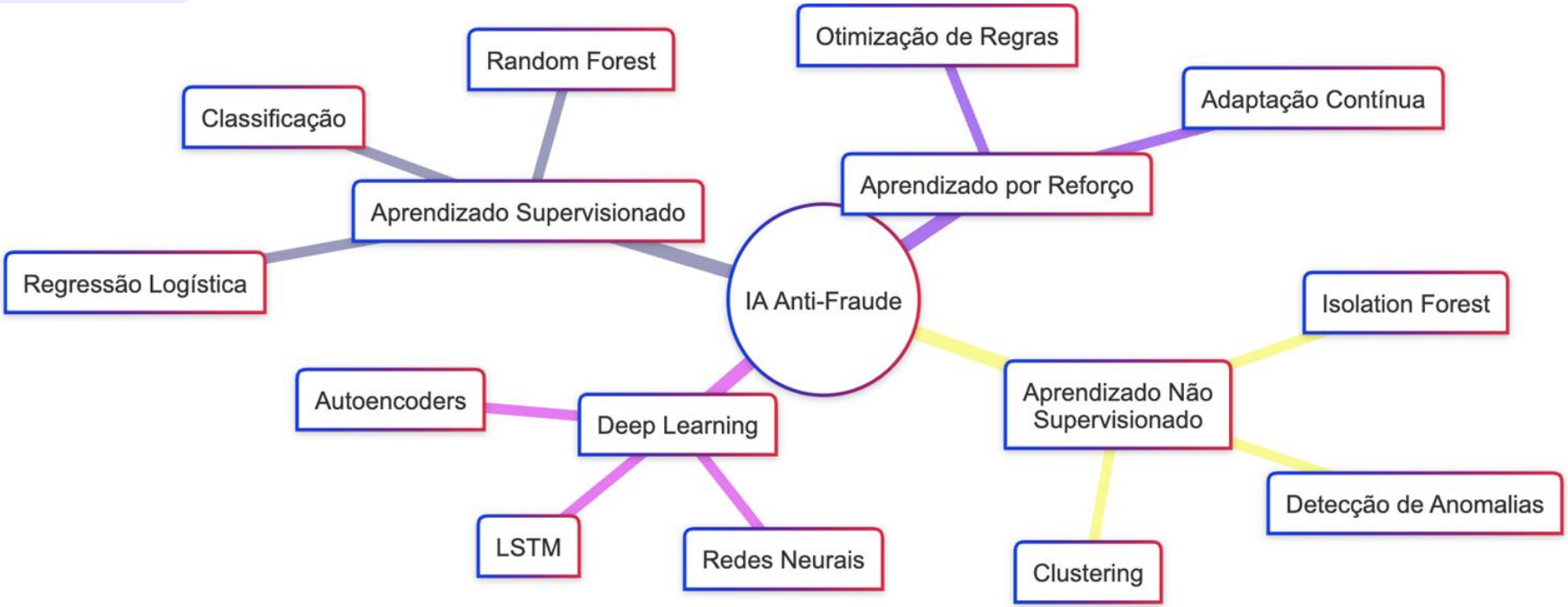
OK, mas como encontrar anomalias?



Modelagens de IA e ML



Aplicando em Prevenção a Fraudes



Aplicando em Prevenção a Fraudes

Detecção de Anomalias

Identifica padrões que desviam significativamente do comportamento normal:

- One-Class SVM: Para dados com poucas amostras fraudulentas
- Isolation Forest: Eficaz para datasets grandes e multi-dimensionais
- Autoencoders: Redes neurais que identificam reconstruções anômalas

Análise Comportamental

Monitora padrões de uso individual:

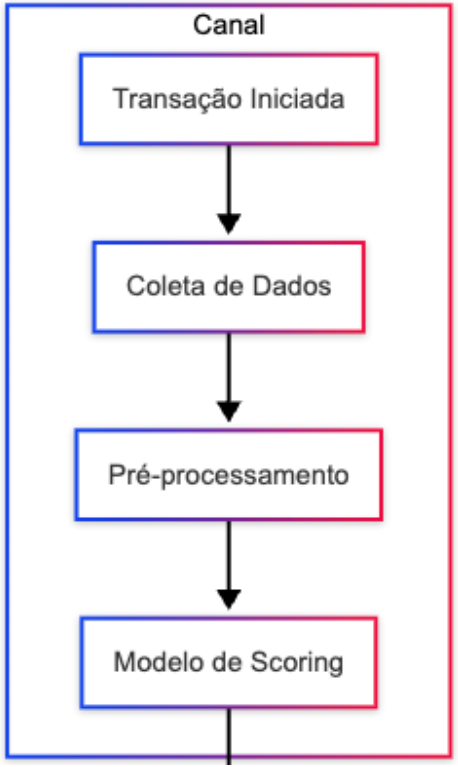
- ➔ Horários habituais de transações
- ➔ Localização geográfica
- ➔ Valores típicos de transferências
- ➔ Dispositivos utilizados

Processamento de Linguagem Natural (NLP)

Analisa comunicações para identificar tentativas de fraude:

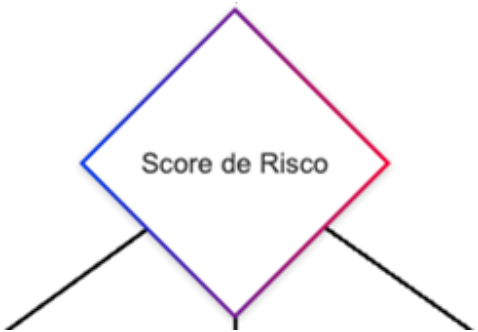
- ➔ Detecção de phishing em e-mails
- ➔ Análise de mensagens suspeitas
- ➔ Identificação de scripts automatizados

Arquitetura Típica



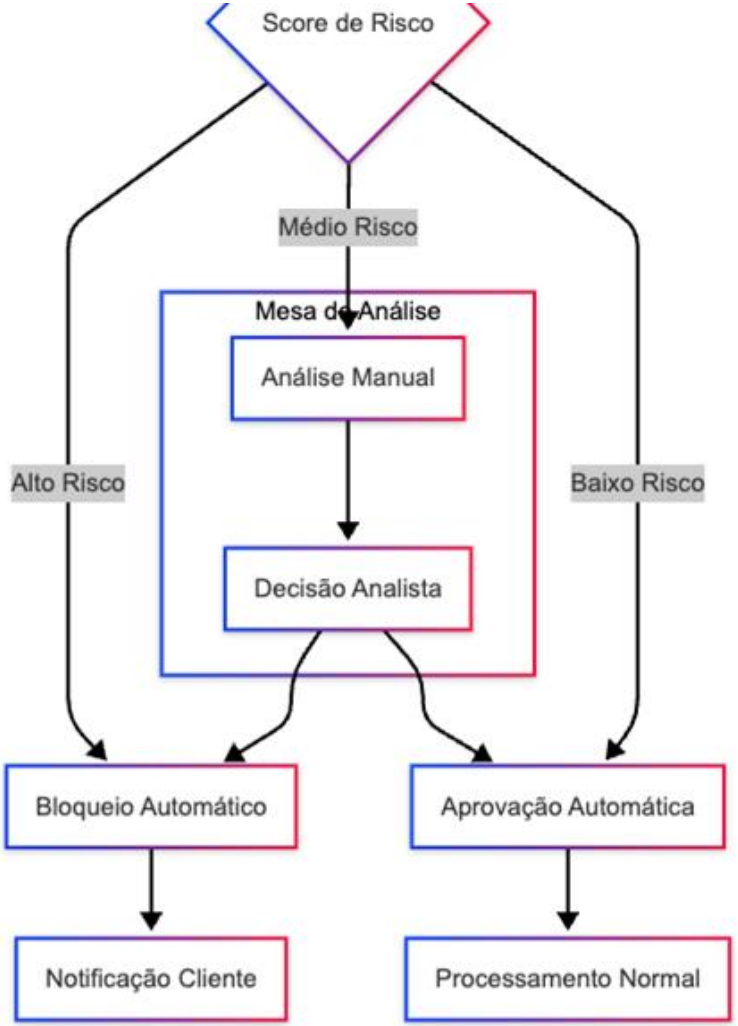
Canais de **aquisição** de transações

Arquitetura Típica



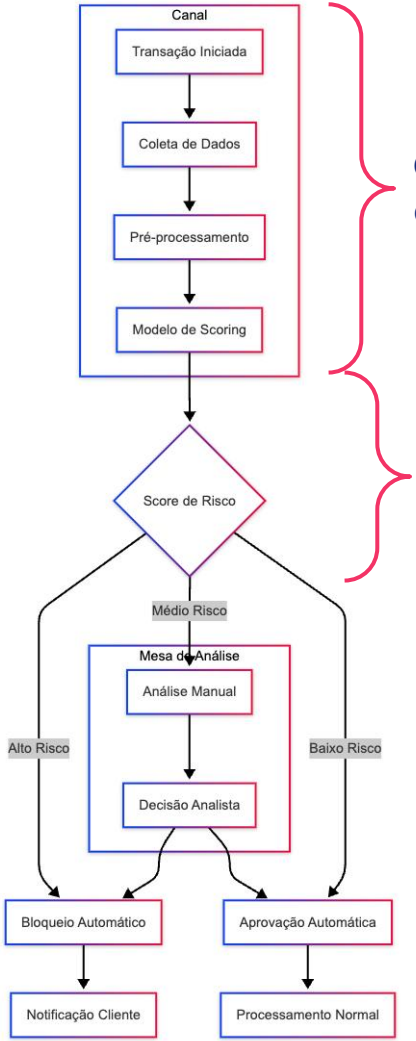
Um **Score de Risco** é calculado com base na abordagem *(regras ou comportamento)*

Arquitetura Típica



Com Base no Score, **uma decisão** é tomada

Arquitetura Típica

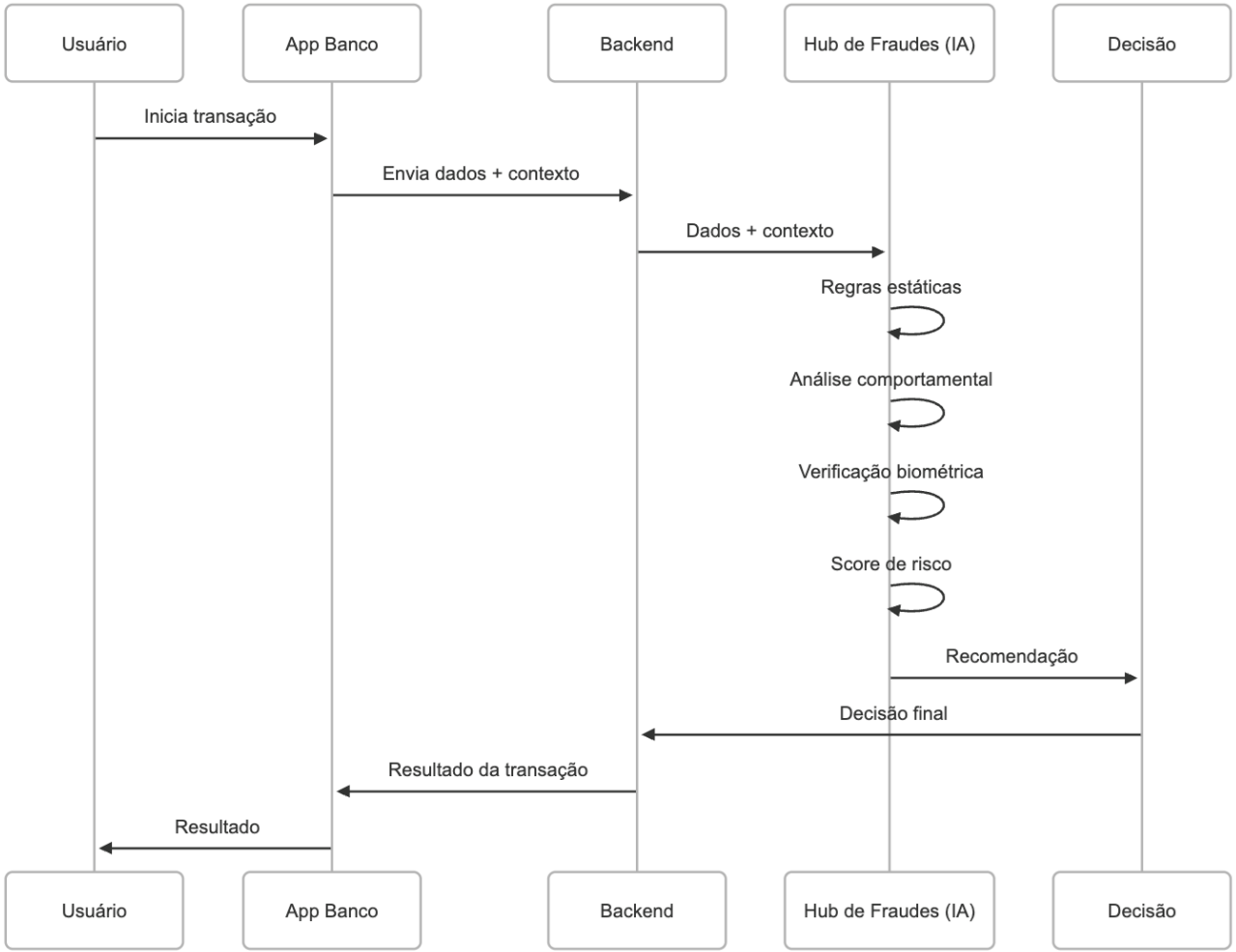


Canal de aquisição de transações

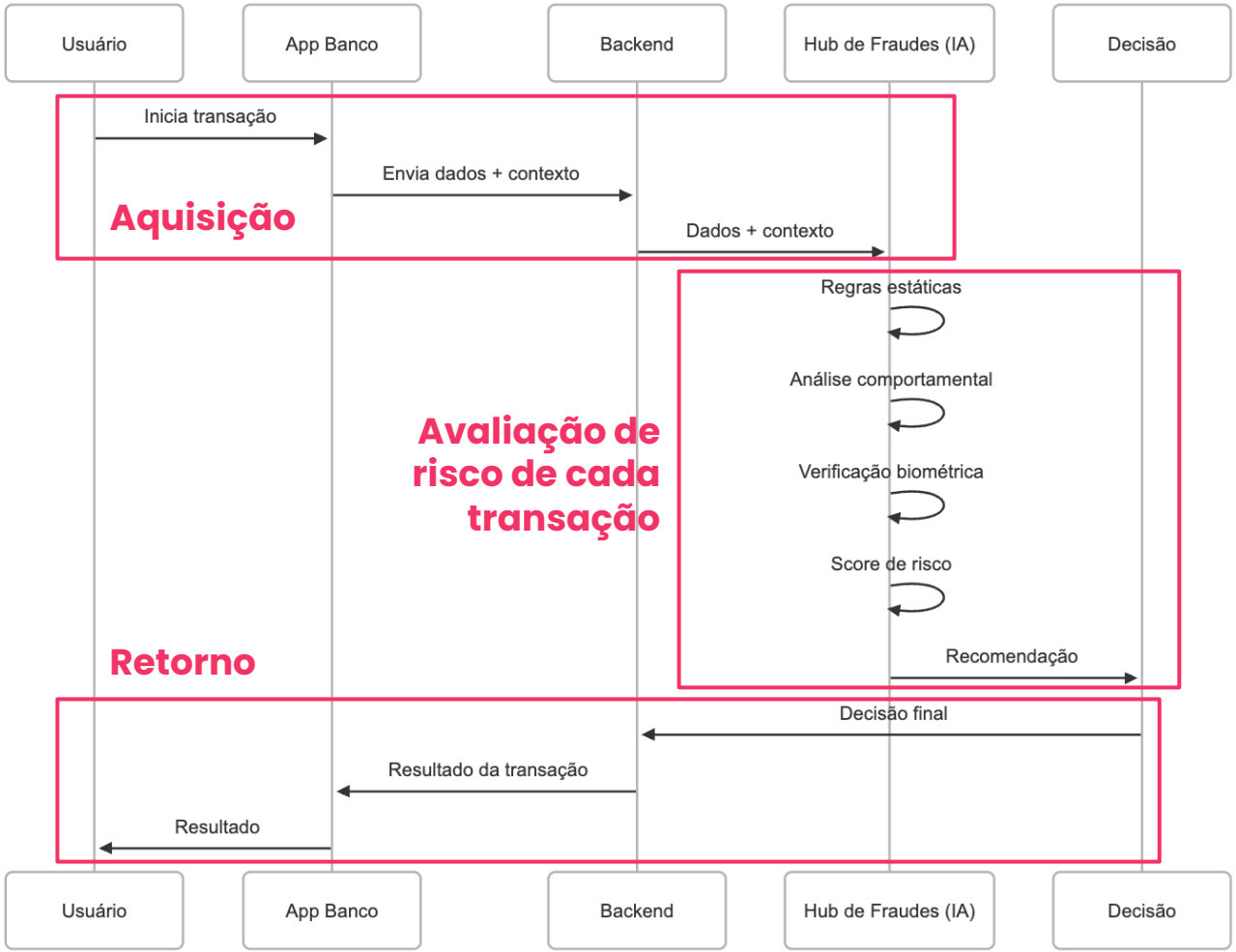
Score de Risco transacional é calculado

Decisão automatizada ou derivação para "Mesa de análise" (manual)

Sequência transacional



Sequência transacional



Calculando o risco de uma transação

Regras
estáticas

Conjunto fixo de condições pré-definidas baseadas em regras if-then

X

Modelos
adaptativos

Algoritmos de ML que aprendem e se ajustam automaticamente aos dados

Abordagens

Aspecto	Regras Estáticas	Modelos Adaptativos
Flexibilidade	❌ Baixa - requer alteração manual	✅ Alta - auto-ajuste contínuo
Implementação	✅ Simples e rápida	❌ Complexa, requer expertise em ML
Manutenção	❌ Alta - revisão manual constante	✅ Baixa - aprendizado automático
Detecção de Novos Padrões	❌ Não detecta automaticamente	✅ Identifica padrões emergentes
Precisão Inicial	⚠️ Boa para fraudes conhecidas	✅ Pode ser superior com dados suficientes
Escalabilidade	⚠️ Limitada pela complexidade das regras	✅ Escala com volume de dados
Taxa de Falsos Positivos	❌ Pode ser alta sem ajustes	✅ Otimização contínua
Adaptação a Mudanças	❌ Manual e lenta	✅ Automática e rápida
Dependência de Dados	✅ Baixa	❌ Alta - requer grandes volumes

Motores de Antifraude

No mercado, existem diversas plataformas chamadas motores de antifraudes – a depender do seu negócio, vale considerar

FINANCE TECH
BOOST

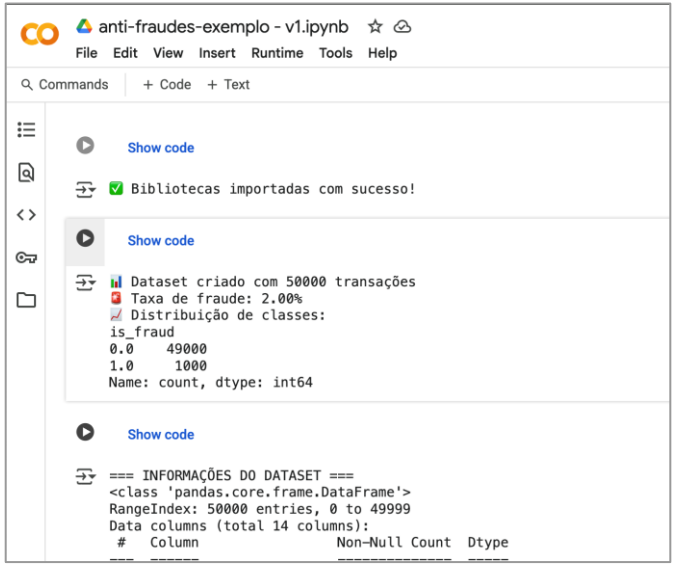
Demonstração

Demonstração

📊 Dados Sintéticos → 🔍 Análise Exploratória → 🤖 4 Modelos de ML → 📈 Avaliação de Performance → ⚡ Sistema Tempo Real → 🚨 Alertas Automáticos

🎯 Objetivos da Demo

- **Implementar 4 algoritmos** diferentes de detecção de fraudes
- **Comparar** performance entre modelos supervisionados e não-supervisionados
- **Simular** um ambiente bancário real com scoring em tempo real
- **Visualizar métricas de negócio** relevantes



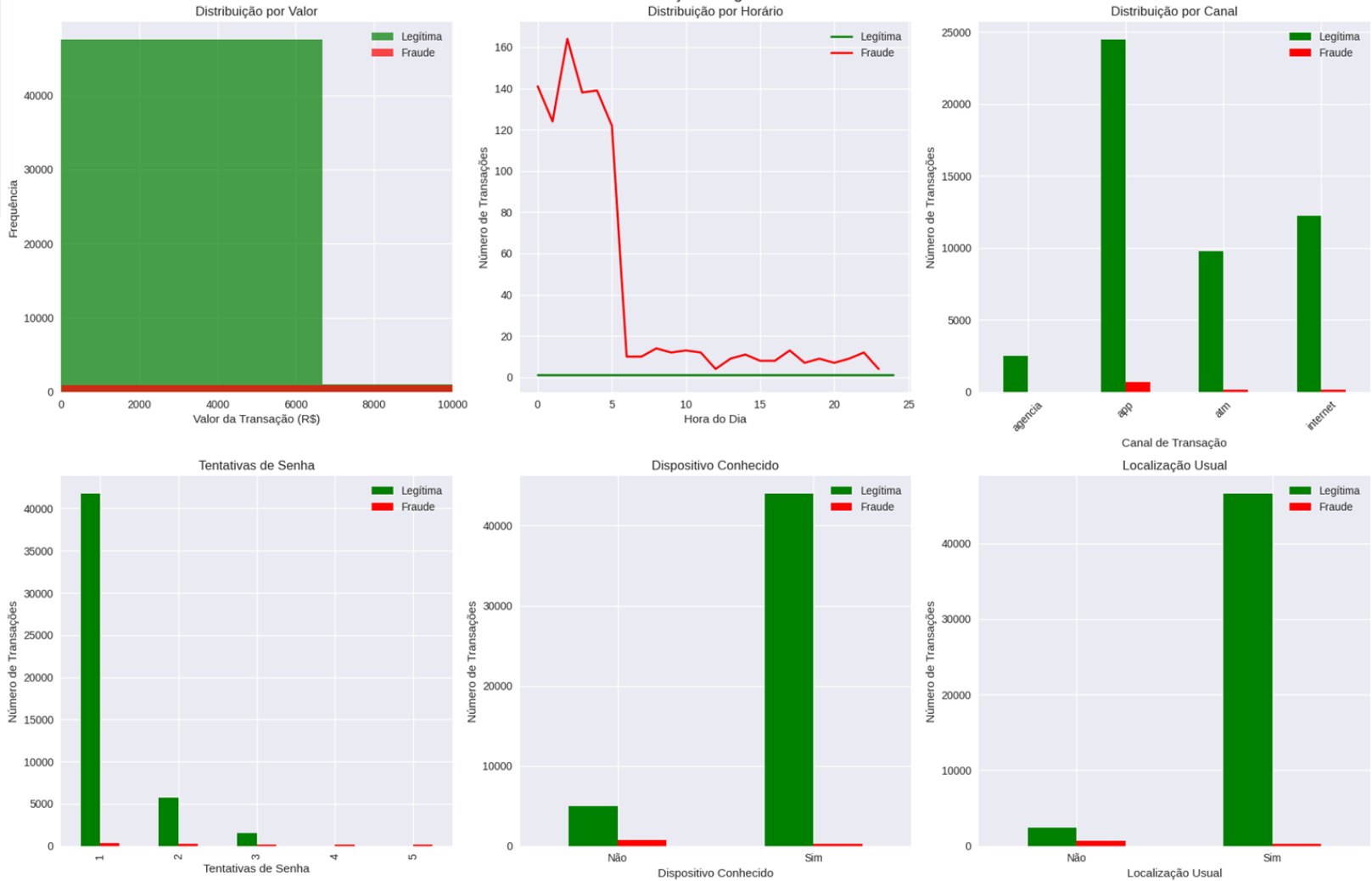
📊 Dataset Realista

- **50.000 transações** simulando padrões brasileiros
- **2% taxa de fraude** (similar ao mercado real)
- **11 features** incluindo valor, horário, canal, dispositivo, localização
- **Padrões comportamentais** distintos entre transações legítimas e fraudulentas

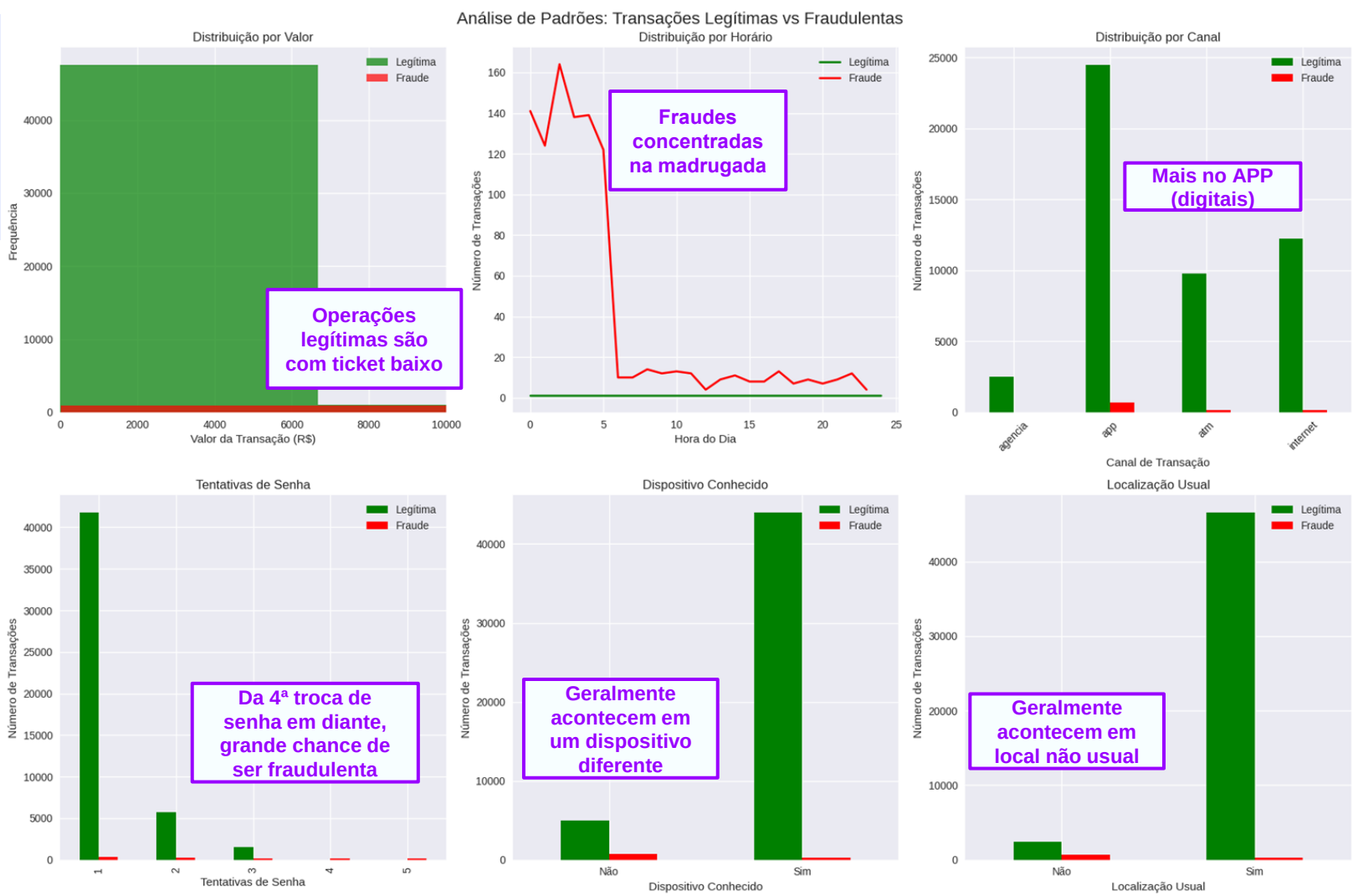
🛠️ Stack Tecnológico

- **Python** + Scikit-learn + Pandas
- **Modelos**: Random Forest, Logistic Regression, Isolation Forest, One-Class SVM
- **Técnicas**: SMOTE para balanceamento, Feature Engineering, Cross-validation
- **Visualização**: Matplotlib, Seaborn, Plotly (interativo)

Comportamento

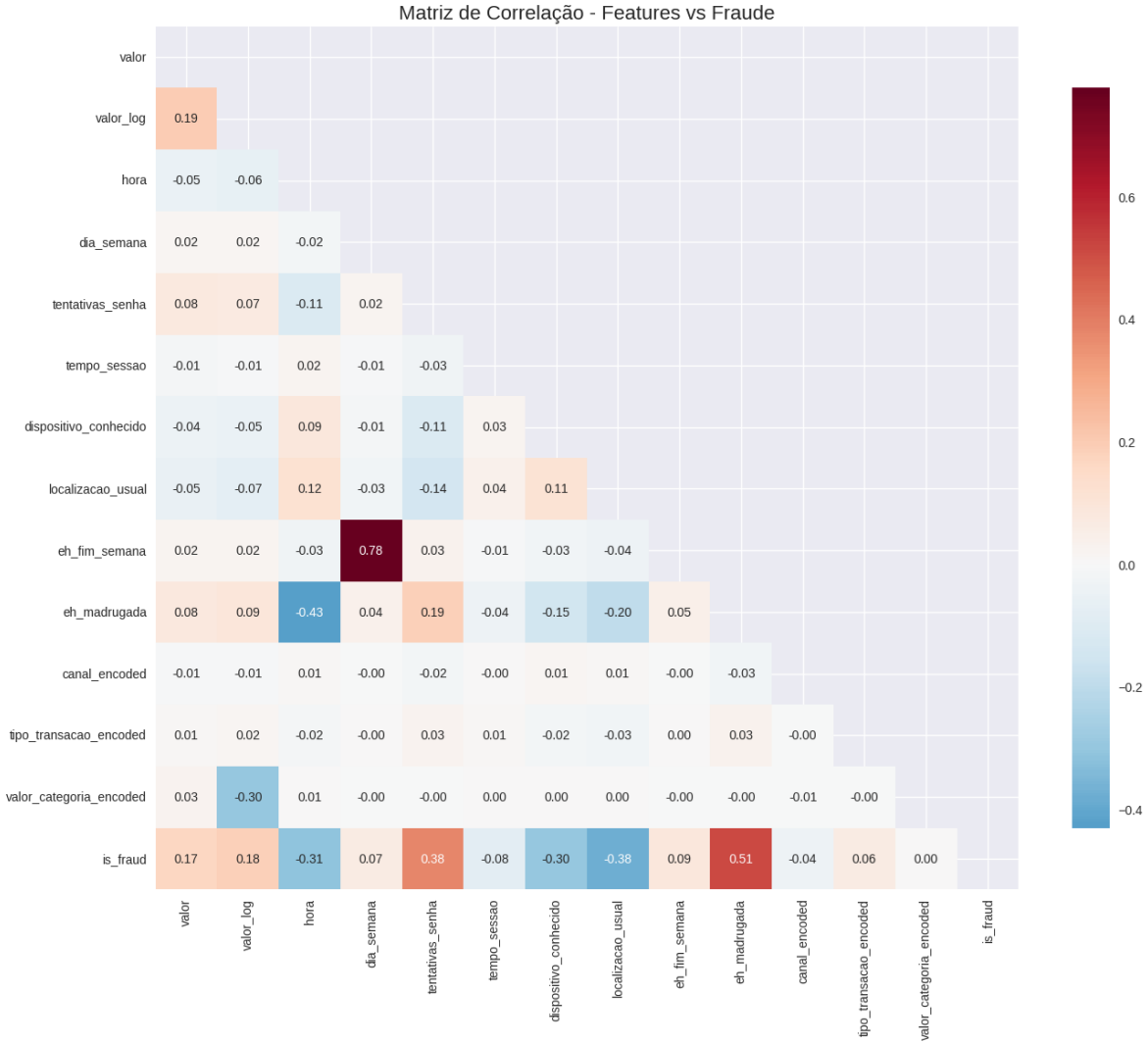


Comportamento



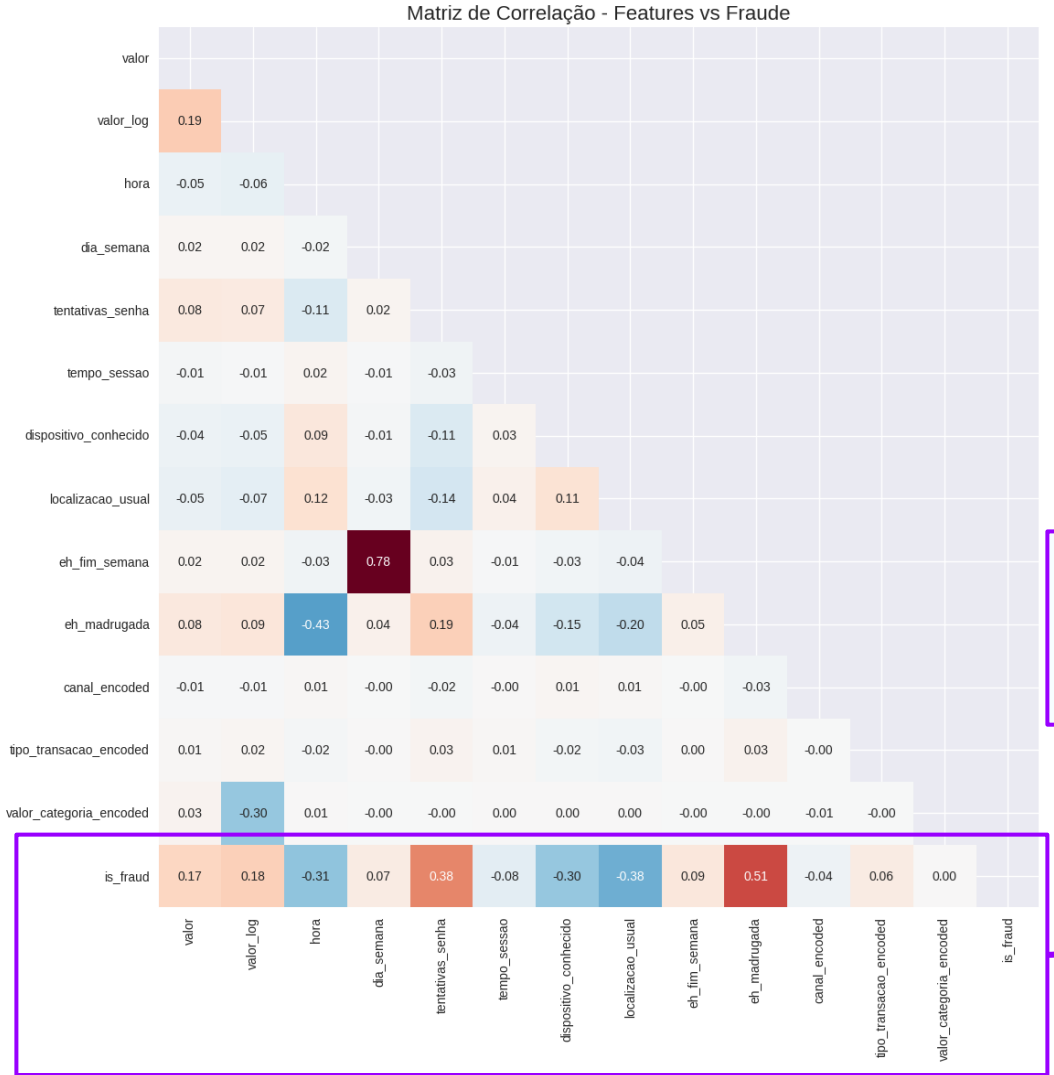
O que influencia a fraude?

Onde se concentra nosso risco transacional?



O que influencia a fraude?

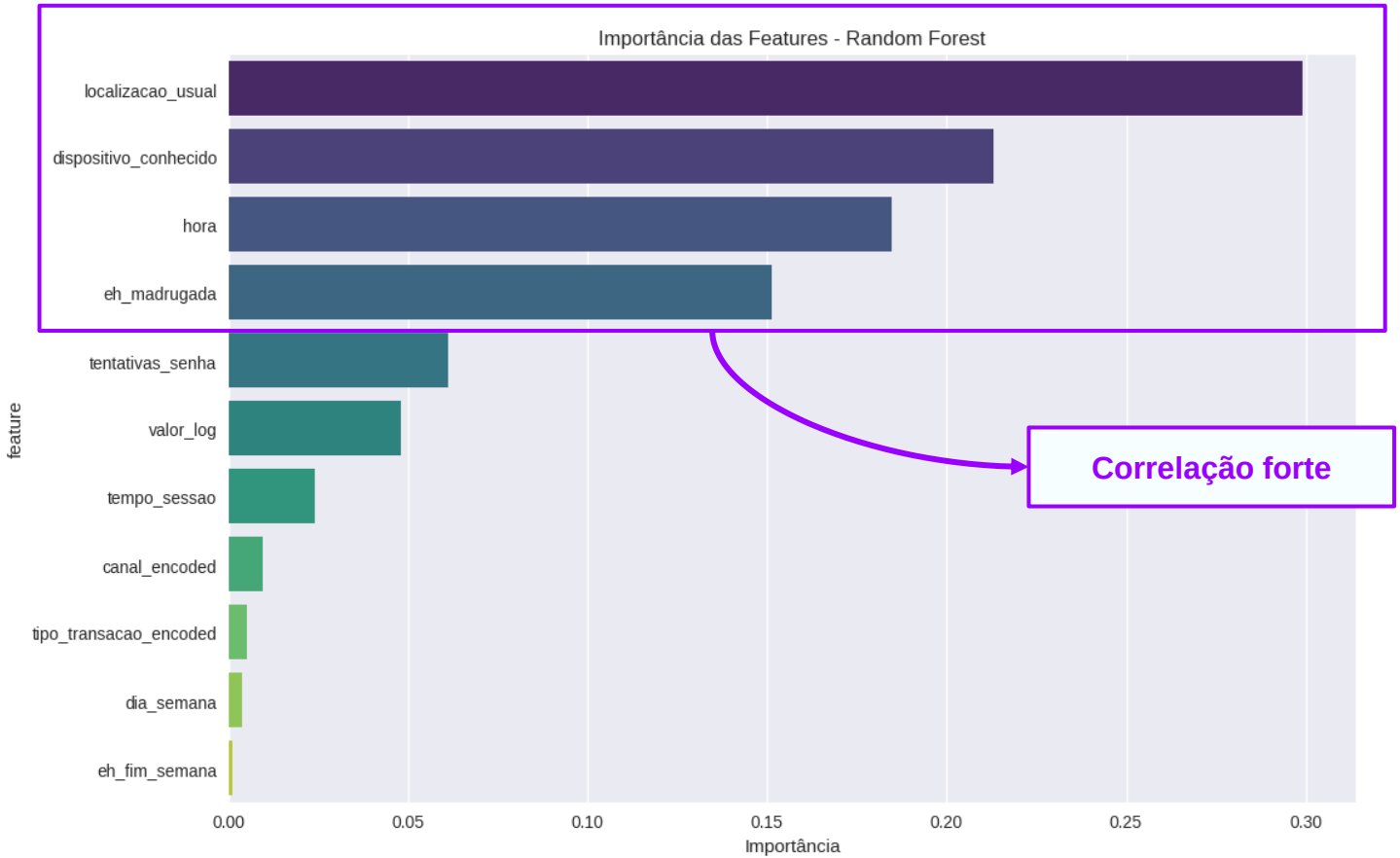
Onde se concentra nosso risco transacional?



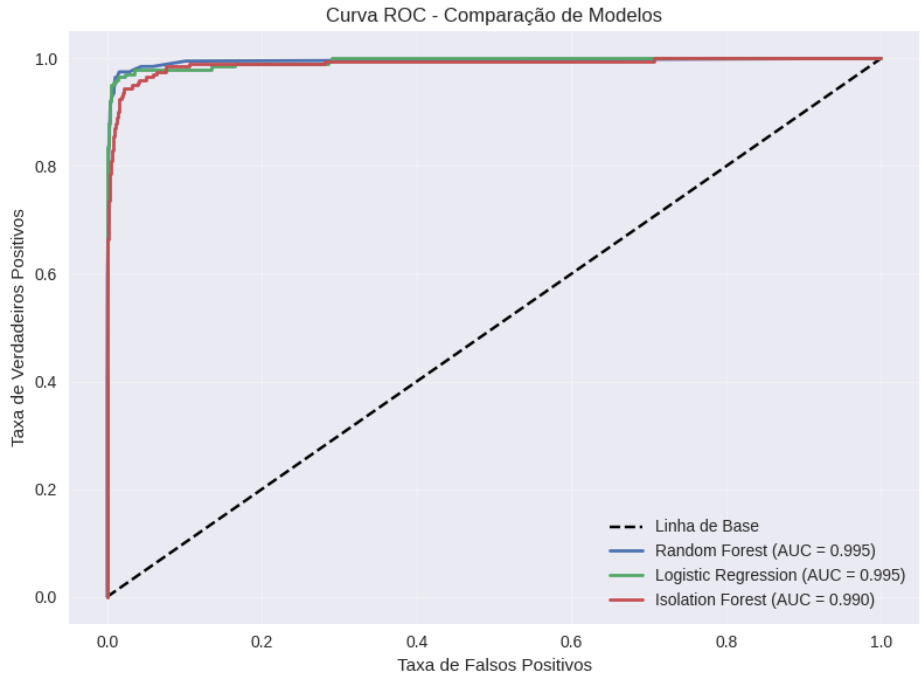
Madrugadas, troca de senha e de um local diferente ao usual...

O que influencia a fraude?

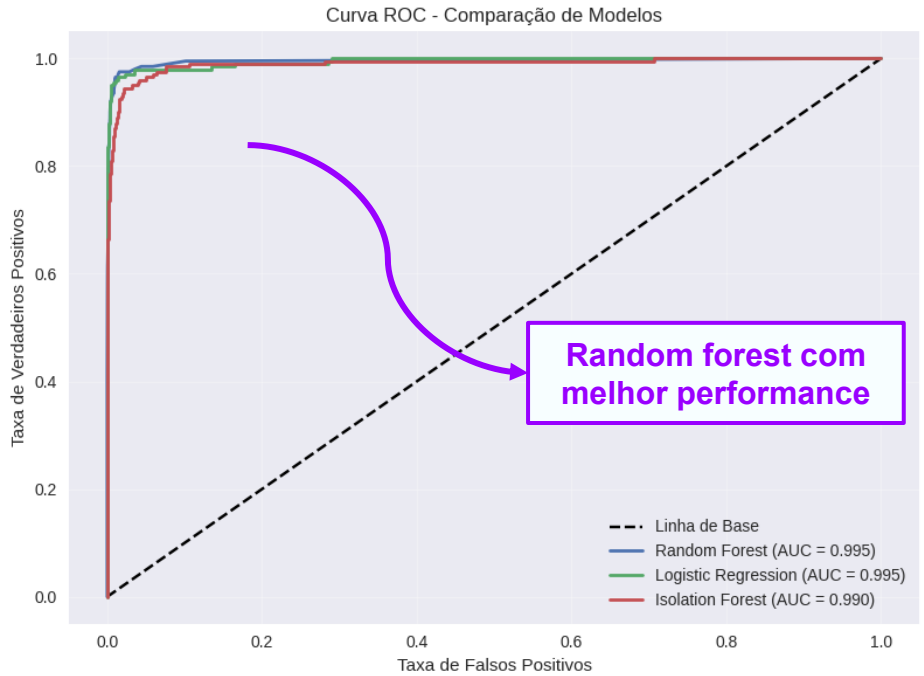
Onde se concentra nosso risco transacional?



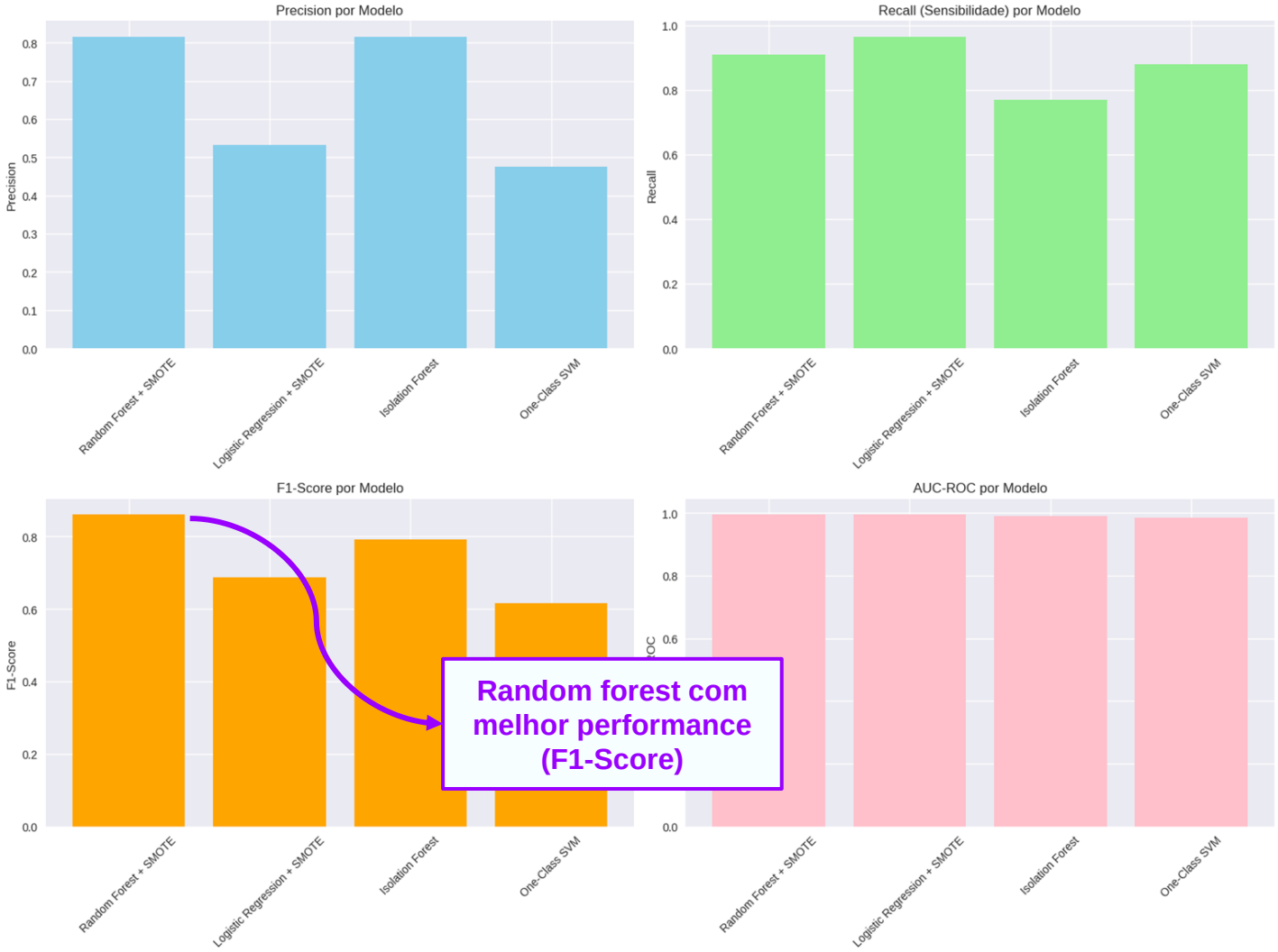
E como avaliar os resultados?



E como avaliar os resultados?



E qual modelo de IA/ML performou melhor nesse exemplo?



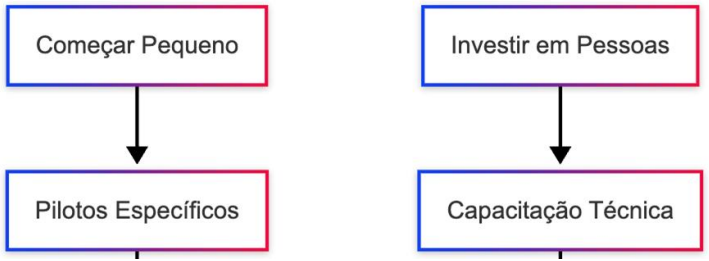
Estratégias de implementação

Estratégia de implementação

Curso: Inteligência Artificial e Análise de Dados

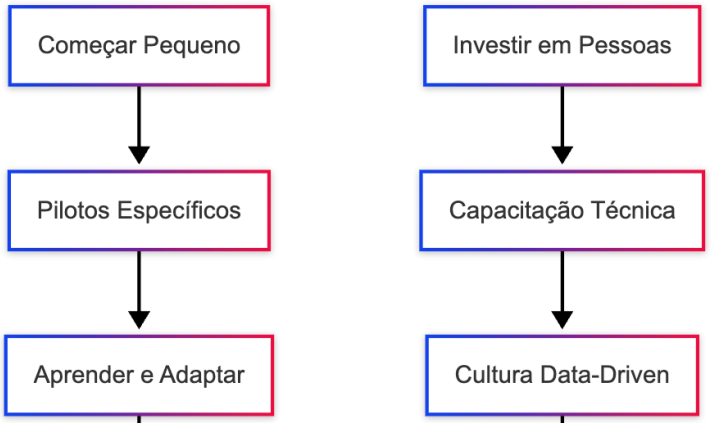
Estratégia de implementação

Curso: Inteligência Artificial e Análise de Dados



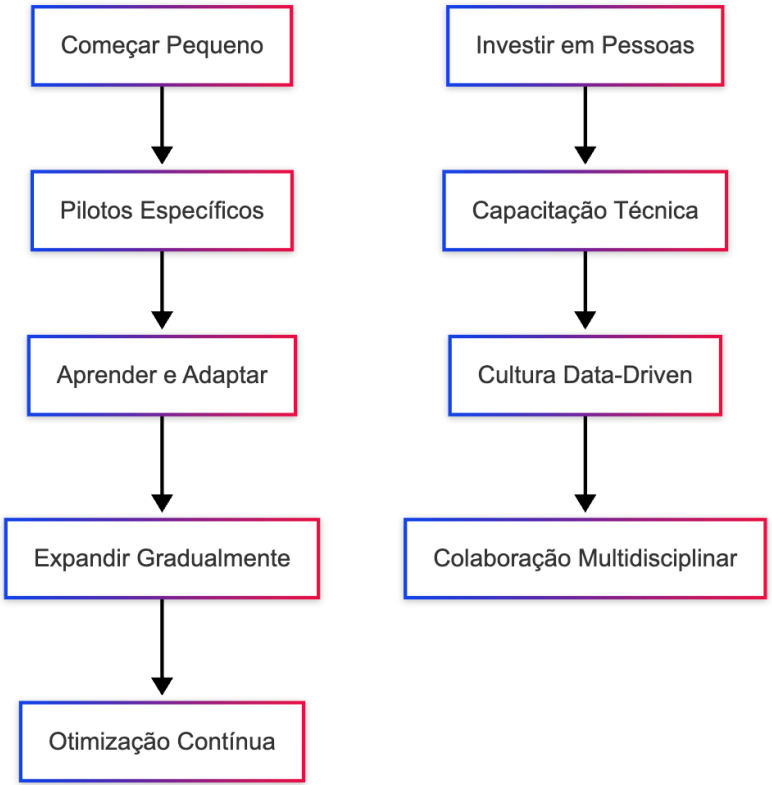
Estratégia de implementação

Curso: Inteligência Artificial e Análise de Dados



Estratégia de implementação

Curso: Inteligência Artificial e Análise de Dados



A Re :icos apresentados é do especialista.

FINANCE TECH
BOOST

Muito Obrigado!

Contato

Thiago Diogo

thiago@duranium.io

https://www.linkedin.com/in/**thiagodiogo**

SCAN ME