Análise de Fraudes e Eficiência Operacional para MYK Fintech

A MYK, uma fintech especializada em processamento de transações financeiras, solicitou um estudo para analisar os riscos associados a fraudes e melhorar a eficiência operacional. Este estudo visa identificar os principais indicadores de risco, avaliar o impacto das decisões de recusa na experiência do usuário, analisar vetores de ataque comuns, otimizar o fluxo de transações e quantificar o impacto financeiro das decisões.

Nesta apresentação, abordaremos o entendimento do negócio, análise SWOT, objetivos SMART e resultados detalhados da análise de dados, fornecendo recomendações específicas para cada questão levantada pela empresa.

M **por Mayerikson**

Entendimento do Negócio e Tipos de Fraudes

O que são Fraudes?

Fraude é um crime que busca obter vantagem sobre a vítima, podendo se manifestar como auto fraude, fraude de identidade, falsidade ideológica ou falsificação de comprovantes.

Métodos de Validação

Incluem validação de documentos, biometria, motor de regras, validação de e-mail/celular, verificação do device, geolocalização e validação de aplicativos "de risco".

Dificuldades

Convencer empresas a adotar ferramentas de prevenção (custo/lucro), assertividade nas regras para não impactar clientes legítimos e acompanhar a constante evolução dos golpes.

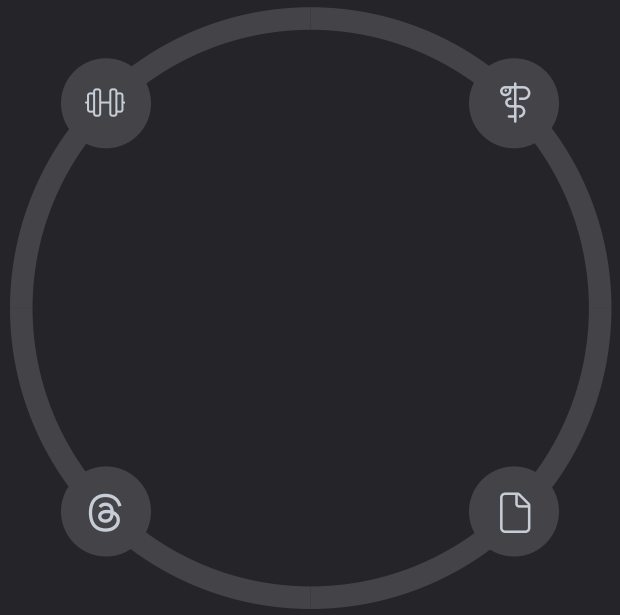
Análise SWOT da MYK Fintech

Forças

- Experiência em processamento de transações
- Reconhecimento da importância de indicadores de risco
- Preocupação com experiência do usuário

Fraquezas

- Possível alto índice de falsos positivos
- Potenciais gargalos no processamento
- Conhecimento incompleto sobre indicadores



Ameaças

- Evolução constante das técnicas de fraude
- Crescente sofisticação de ferramentas maliciosas
- Pressão competitiva para reduzir fricção

Oportunidades

- Implementação de tecnologias avançadas (IA, ML)
- Refinamento dos modelos de pontuação
- Processos de autenticação mais fluidos

Objetivos SMART para Prevenção de Fraudes

Aprimorar Indicadores e Reduzir Falsos Positivos

Implementar sistema refinado de pontuação de risco, reduzir falsos positivos em 30% mantendo ou melhorando detecção de fraudes reais, utilizando machine learning e implementando em 4 meses.

Otimizar Experiência do Usuário

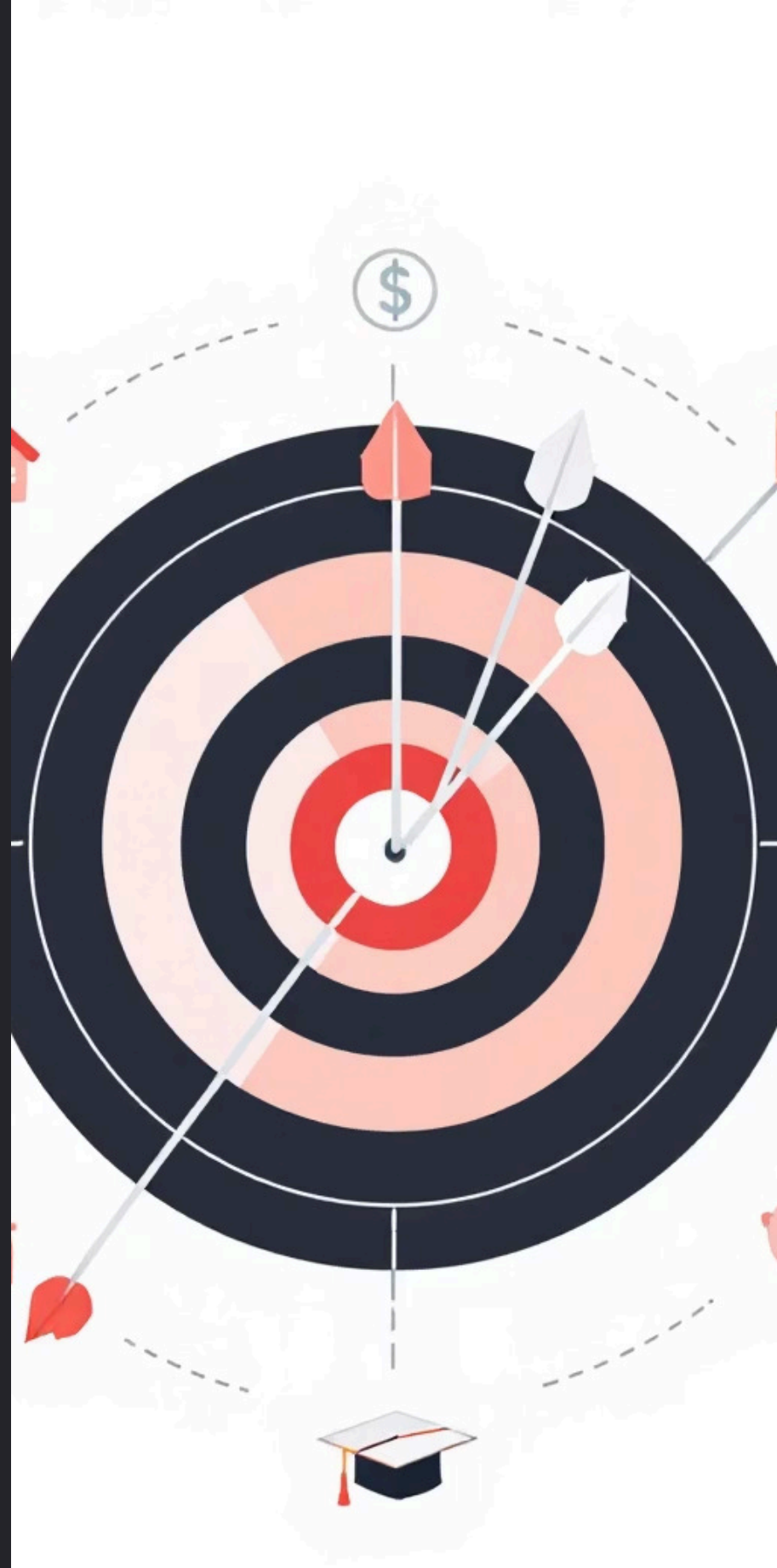
Desenvolver protocolo de comunicação e resolução rápida para transações recusadas, aumentando satisfação do cliente em 25%, com implementação em 3 meses.

Fortalecer Defesas Contra Ataques

Implementar sistema de detecção multicamada para identificar emuladores, adulteração de apps e falsificação de localização, aumentando detecção em 40% em 6 meses.

Otimizar Processamento e Balancear Impacto Financeiro

Redesenhar arquitetura para aumentar capacidade em 50% e desenvolver modelo financeiro para reduzir perdas totais em 25%, com implementação em 5 meses.



Análise de Dados e Modelo Random Forest

Random Forest

Um "time de especialistas" (várias árvores de decisão) que votam juntos para tomar decisões. Cada "especialista" analisa partes diferentes dos dados e características diferentes.

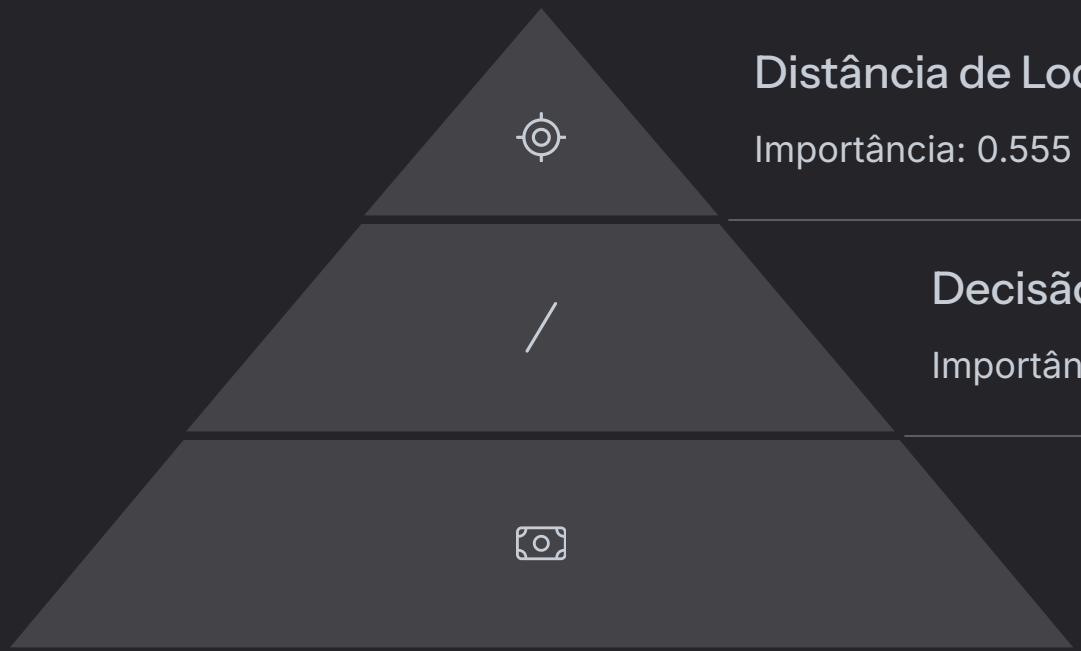
É robusto contra overfitting, lida bem com dados desbalanceados (poucas fraudes) e mostra claramente quais fatores são mais importantes para detectar fraudes.

Matriz de Confusão

Uma "tabela da verdade" que mostra verdadeiros positivos (fraudes detectadas corretamente), falsos positivos (transações normais bloqueadas por engano), falsos negativos (fraudes não detectadas) e verdadeiros negativos (transações normais aprovadas corretamente).

Essencial porque em fraude um falso negativo é muito mais grave que um falso positivo.

Principais Indicadores de Risco e Recomendações



Distância de Localização Frequente

Importância: 0.555

Decisão

Importância: 0.291

Valor da Transação

Importância: 0.136

Para reduzir falsos positivos sem comprometer a segurança, recomendamos: ajustar o limiar de probabilidade para classificação (atualmente 0.5), implementar regras específicas para clientes com bom histórico, criar diferentes níveis de segurança baseados no valor da transação e atualizar o modelo regularmente com dados mais recentes.

O modelo Random Forest demonstra ser eficaz para detecção de fraudes com 66.49% de taxa de detecção. Para implementação, recomenda-se ajustar os limiares por segmento de cliente e valor de transação.

Vetores de Ataque e Estratégias de Defesa

Detecção de Emuladores

Implementar fingerprinting avançado de dispositivos para identificar emuladores com maior precisão, apesar da baixa importância atual (0.000) no modelo.

Verificação de Integridade

Desenvolver sistemas robustos para detectar aplicativos adulterados, implementando verificações de assinatura e integridade do código.

Validação de Localização

Criar verificação cruzada entre GPS, IP e redes móveis para identificar falsificação de localização (importância atual: 0.004).

Análise Comportamental

Implementar sistemas de análise comportamental para identificar padrões suspeitos de uso que possam indicar atividade fraudulenta.

Impacto Financeiro e Estratégias de Otimização

R$272.572

Perda por Fraudes Não Detectadas

1545 transações fraudulentas aprovadas com valor médio de R$176,42

R$376.785

Perda por Recusas Legítimas

3051 transações legítimas recusadas, assumindo 70% de desistência

R$649.357

Custo Total Potencial

Soma das perdas por fraudes e recusas indevidas

Para maximizar a economia, recomendamos: ajustar limiares de decisão baseado no valor da transação (mais rigoroso para transações de alto valor, mais relaxado para baixo valor), implementar análise de custo-benefício balanceando segurança e experiência, segmentar clientes com regras diferenciadas para bons históricos, e estabelecer monitoramento contínuo para acompanhar a evolução dos padrões de fraude.