Case Prático: Detecção de Atividades Suspeitas de Lavagem de Dinheiro

Nós da CloudWalk buscamos alternativas inovadoras para detectar atividades suspeitas de lavagem de dinheiro e financiamento ao terrorismo. Isso inclui a implementação de soluções tecnológicas avançadas que possam identificar padrões anômalos e classificar transações com base no risco.

A CloudWalk considera diversas técnicas e estratégias para garantir uma detecção eficaz e abrangente. Você, como analista de prevenção à lavagem de dinheiro e financiamento ao terrorismo, deve definir estratégias para implementar essas soluções de maneira eficiente, considerando o uso de diferentes tecnologias, incluindo Large Language Models e outras técnicas de Machine Learning.

Estamos animados para avaliar suas habilidades e sua capacidade de propor soluções práticas para um cenário próximo ao real de compliance e prevenção à lavagem de dinheiro. Abaixo estão as etapas do case e orientações sobre o que esperamos que você demonstre em cada uma delas.

Tarefas do Case

O time de Monitoramento de Prevenção à Lavagem de Dinheiro realizou um mutirão para avaliar a base de dados de determinado período. Considerando que você faz parte do time e utilizando seus conhecimentos e estudos da questão anterior, utilize a base de dados enviada e responda às seguintes tarefas:

1. Análise com Dados Transacionais Simulados

Tarefa: Trabalhe com a amostra de dados transacionais fornecida, que inclui campos como ID do cliente, valor da transação, horário, localização, tipo de pagamento e histórico de transações. Explore esses dados para realizar análises que você consideraria relevantes na identificação de padrões suspeitos de lavagem de dinheiro. De acordo com a sua análise, há algum estabelecimento que tenha apresentado algum indício de suspeita lavagem de dinheiro, financiamento ao terrorismo ou algum possível ato ilícito?

Objetivo: Buscamos entender como você interpreta dados e quais métodos e insights você aplicaria para simular um cenário prático de compliance.

Resolução:

Considerando que o perfil dos clientes na amostra é semelhante, a média das quantias nas transações é de aproximadamente $ 3.106,87, enquanto o desvio padrão é de $ 4.823,95. Dessa forma, foi estabelecido que transações superiores a $ 9.647,90 (duas vezes o valor do desvio padrão) devem ser consideradas suspeitas. Tais transações exigem a aplicação de uma flag para que sejam submetidas a diligências adicionais e monitoramento, com o objetivo de identificar e mitigar riscos elevados, transformando-os em riscos mais baixos.

No primeiro trimestre de 2021, 70,1% das transações, consideradas normais, totalizaram:

- Janeiro: $ 341 mil
- Fevereiro: $ 306 mil
- Março: $ 311 mil

Já as transações suspeitas, que representam 29,9%, somaram:

- Janeiro: $ 66 mil
- Fevereiro: $ 19,4 milhões
- Março: $ 8,7 milhões

Nessa análise, as transações suspeitas estão concentradas no método de pagamento em crédito, com maior frequência em pagamentos com cartões físicos.

---

2. Interpretação e Explicabilidade do Modelo de Machine Learning

Tarefa: Em um ambiente de compliance, é essencial que as previsões sejam interpretáveis. Como você garantiria que o modelo de machine learning seja explicável para a equipe de compliance, especialmente em casos complexos de lavagem de dinheiro? Dica: Inclua técnicas de interpretação de modelos, como SHAP ou LIME, e comente como essas técnicas podem auxiliar a equipe a entender as razões por trás da classificação de uma transação como suspeita.

Objetivo: Avaliar sua capacidade de comunicar decisões do modelo de maneira transparente e explicável, o que ajuda na defesa das decisões e na confiança da equipe.

Resolução: Machine Learning é uma técnica que permite que computadores aprendam com dados, sem serem explicitamente programados para cada tarefa. Em um cenário de combate à lavagem de dinheiro, podemos utilizar ML para analisar **grandes volumes de**

transações financeiras e **identificar padrões** que poderiam ser indicativos de atividades suspeitas como:

- Transações incomuns;
- Transferências entre contas não relacionadas;
- Quantias altas em momentos específicos.

Uma ferramenta que pode ser utilizada para explicar um modelo é a **LIME (Local Interpretable Model-agnostic Explanations)**. Ela melhora a eficiência, a transparência e o controle nas investigações, além de otimizar a precisão do modelo com o tempo.

Como o LIME pode ser útil em casos de lavagem de dinheiro?
O modelo de ML pode indicar que uma transação é suspeita, mas a equipe precisa saber quais características geram essa conclusão. LIME analisa essas características, como:

- O valo da transação;
- O histórico de transações da conta;
- Padrões de horários;
- Relacionamento entre contas (por exemplo, contas de mesmo titular ou de países de alto risco.)

Nisso, a ferramenta complementa com as características das transações:

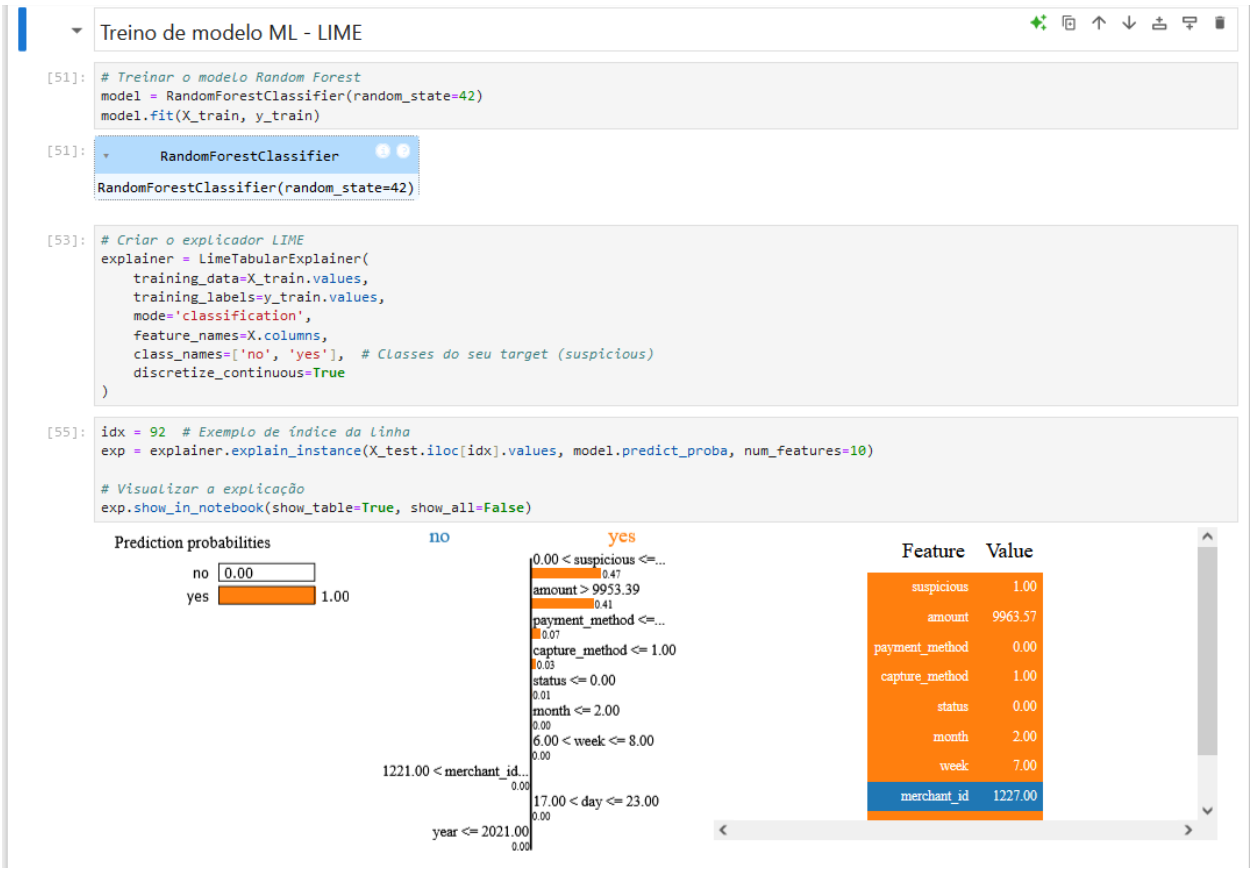
- Valor acima do normal;
- Variação de destino de pagamento;
- Taxa de transações altas em curto período de tempo.

Em uma amostra de transação como suspeita, as variáveis “amount” e “payment_method” têm pesos substanciais para a análise de predição.

- O **valor da transação** foi um dos fatores mais importantes. O modelo considera que, transações com valor acima de $ 9953.39 são mais propensas a serem suspeitas, contribuindo com 47% para a decisão.

- O **método de pagamento** também tem grande peso, com 42% de contribuição. Isso pode indicar que certos métodos de pagamento são mais frequentemente associados a transações suspeitas.

Em suma, o modelo de machine learning pode ajudar a detectar padrões de lavagem de dinheiro automaticamente e o LIME ajuda a explicar o porquê da identificação suspeita, facilitando a interpretação da equipe de compliance.



Observação: para melhor manuseio, o link do script, em repositório, está em anexo no email.

---

3. Escolha de Métricas de Avaliação para Classificação de Risco

Tarefa: Quais métricas de avaliação você usaria para medir o desempenho do modelo de classificação de risco? Justifique o uso de cada métrica, considerando a necessidade de minimizar tanto os falsos positivos quanto os falsos negativos.

Objetivo: Queremos entender sua visão sobre as métricas de avaliação e sua justificativa para o uso de cada uma, especialmente na busca por um equilíbrio ideal entre precisão e recall, crucial para o sucesso em compliance.

Resolução:

Entendimento do Contexto

- O modelo está classificado transações como **suspeitas de fraude** (classe positiva) ou **não suspeitas** (classe negativa).

- No contexto de **fraude**, minimizamos
    - **falsos positivos** (classificar erroneamente uma transação legítima como fraude) e;
    - **falsos negativos** (não identificar uma fraude real).

Métricas de Avaliação Relevantes
Com base nesse contexto, as métricas mais relevantes são:
(Legenda)

- **TP** (Verdadeiro Positivo): Fraudes corretamente identificadas.
- **TN** (Verdadeiro Negativo): Transações não fraudulentas corretamente identificadas.
- **FP** (Falso Positivo): Transações não fraudulentas incorretamente identificadas como fraude.
- **FN** (Falso Negativo): Fraudes não identificadas corretamente.

Precisão

- **Definição:** A precisão mede a proporção de **transações classificadas como fraudulentas que realmente são fraudulentas**.

  Fórmula: Precisão = TP/TP+FP
  Justificativa: A precisão é importante quando o custo de falsos positivos é alto. No caso de fraude, um falso positivo (transação legítima marcada como fraude) pode levar a ações desnecessárias e desconforto para o cliente. Um modelo com alta precisão reduz esse risco.

Recall (Sensibilidade ou Taxa de Verdadeiros Positivos)

- **Definição:** O recall mede a proporção de transações fraudulentas que foram corretamente identificadas pelo modelo.
- **Fórmula:** Recall= TP/TP+FN
- **Justificativa:** O recall é crucial quando o custo de falsos negativos é alto. No caso de fraude, um falso negativo (fraude não detectada) pode resultar em grandes perdas financeiras ou danos à reputação da instituição. Ter um modelo com alto recall é essencial para garantir que a maioria das fraudes seja identificada.

F1-Score

- **Definição:** O F1-score é a média harmônica entre a precisão e o recall. Ele combina as duas métricas em um único número, equilibrando tanto os falsos positivos quanto os falsos negativos.
- **Fórmula:** F1 = 2x (Precisão x Recall / Precisão + Recall)
- **Justificativa:** O F1-score é útil quando há necessidade de um equilíbrio entre precisão e recall, como no caso de fraudes, onde tanto os falsos positivos quanto os falsos negativos precisam ser minimizados. Ele oferece uma métrica única que reflete o desempenho geral do modelo.

```
[135]: dataset.info()

<class 'pandas.core.frame.DataFrame'>
RangeIndex: 9391 entries, 0 to 9390
Data columns (total 16 columns):
 #   Column            Non-Null Count  Dtype
---  ------            --------------  -----
 0   transaction_id    9391 non-null   object
 1   merchant_id       9391 non-null   object
 2   transaction_date  9391 non-null   datetime64[ns]
 3   transaction_time  9391 non-null   object
 4   status            9391 non-null   object
 5   amount            9391 non-null   float64
 6   payment_method    9391 non-null   object
 7   capture_method    9391 non-null   object
 8   card_holder_name  9391 non-null   int32
 9   card_number       9391 non-null   object
 10  year              9391 non-null   int32
 11  month             9391 non-null   int32
 12  week              9391 non-null   UInt32
 13  day               9391 non-null   int32
 14  suspicious        9391 non-null   object
 15  status_code       9391 non-null   int64
dtypes: UInt32(1), datetime64[ns](1), float64(1), int32(4), int64(1), object(8)
memory usage: 999.8+ KB

[137]: dataset['suspicious'] = dataset['suspicious'].astype('int32')

[139]: y_true = dataset['suspicious']
       y_pred = dataset['status_code']

[141]: precision = precision_score(y_true, y_pred)
       recall = recall_score(y_true, y_pred)
       f1 = f1_score(y_true, y_pred)

[151]: # Exibindo os resultados
       print(f'Precision: {precision}')
       print(f'Recall: {recall}')
       print(f'F1-Score: {f1}')

       Precision: 0.6514611546685674
       Recall: 0.32584670231729057
       F1-Score: 0.4344106463878327
```

---

4. Simulação de Relatório de Atividades Suspeitas (SAR)

Tarefa: Usando o LLM (Language Model), crie um relatório SAR para uma transação fictícia suspeita. Estruture o relatório de forma que seja claro para reguladores e intuitivo para o time de compliance, detalhando o contexto e os motivos da suspeita.

Objetivo: Avaliar sua habilidade de criar relatórios de atividades suspeitas que sejam informativos e bem-estruturados. Este exercício mostra como você aplicaria um LLM na criação de relatórios de compliance.

Resolução:

Relatório de Atividade Suspeita (SAR)

Data do Relatório: 08 de dezembro de 2024
Nome do Analista: George Feitosa
Departamento: Compliance
Informações Gerais da Transação

- **ID da Transação**: 125143
- **Data e Hora da Transação**: 16 de fevereiro de 2021, às 14:19
- **Valor da Transação**: $ 9.998,24
- **Método de Pagamento**: Pagamento com cartão de Crédito
- **Contas Envolvidas**:
    - **Número de Cartão**: 509063******2012

2. Descrição da Transação Suspeita
A transação em questão foi uma compra no crédito de $ 9.998,24 realizada de uma conta de origem em nome de um indivíduo que, com base na análise preliminar, não parece ter uma relação clara com o valor ou a natureza da transação.
3. Motivo da Suspeita
A transação foi identificada como suspeita devido aos seguintes fatores:

- **Valor elevado**: A transferência de $ 9.998,24 é significativamente superior ao histórico de transações do cliente, que normalmente realiza transações no valor médio de $ 244,58.
- **Padrão de comportamento incomum**: O cliente realizou um único pagamento, de valor expressivamente mais alto, para uma conta de destino que não consta como beneficiária recorrente nas transações anteriores.
- **Origem da conta**: A conta de origem foi aberta há menos de dois meses, e o cliente tem pouco histórico de movimentação financeira.
- **Conta de Destino**: A conta de destino pertence a uma pessoa física, mas o endereço e as informações cadastrais associadas à conta de destino não correspondem a um padrão de clientes típicos da plataforma.
- **Suspensão de Comunicação**: O cliente não respondeu aos nossos esforços de contato para esclarecimento da transação.

4. Análise Contextual e Circunstancial
O comportamento da transação foge ao padrão do cliente e da plataforma. A conta de origem foi aberta de forma recente, sem histórico substancial de transações, e a movimentação financeira realizada foi de um valor elevado e em um único pagamento para um destinatário desconhecido. Esse tipo de transação é frequentemente associado a tentativas de lavagem de dinheiro ou financiamento de atividades ilícitas, sendo, portanto, necessário que a transação seja investigada mais a fundo.
5. Medidas Tomadas

- **Congelamento da Transação**: A transação foi imediatamente interrompida e os fundos foram bloqueados enquanto aguardam uma investigação mais aprofundada.
- **Contatos com o Cliente**: Foram feitos esforços para entrar em contato com o cliente a fim de obter mais informações sobre a origem e a finalidade da transação. Até o momento, não houve resposta.
- **Análise de Risco**: A transação foi submetida à equipe de compliance para análise de risco detalhada.

6. Ações Recomendadas

- **Investigar a conta de destino**: Verificar se a conta de destino está associada a qualquer outra atividade suspeita ou criminosa.
- **Solicitar informações adicionais ao cliente**: Continuar tentando obter informações mais detalhadas sobre o motivo da transação e a relação do cliente com a conta de destino.
- **Relatar ao COAF (Conselho de Controle de Atividades Financeiras)**: Submeter o caso à autoridade regulatória para investigação adicional sobre possíveis atividades de lavagem de dinheiro ou financiamento ao terrorismo.

7. Conclusão

Dado o alto valor da transação, o comportamento anômalo do cliente, e a falta de informações claras sobre o destino dos fundos, a transação será considerada suspeita até que se obtenham esclarecimentos. Recomendamos que a investigação continue e que a transação seja formalmente reportada ao COAF.

---

5. Proposta de Interface para Monitoramento e Acompanhamento de Alertas

Tarefa: Desenhe ou descreva uma interface básica onde a equipe de compliance possa ver alertas, acompanhar métricas como a taxa de falsos positivos e falsos negativos, e fornecer feedback sobre as previsões do modelo.

Objetivo: Com este exercício, queremos ver como você pensaria em uma interface colaborativa e prática que facilite o monitoramento e o ajuste contínuo do modelo de compliance.

Resolução:

Observação: o link do dashboard segue no corpo do email, assim como o arquivo em repositório.

Questões do Case

Estratégias de Minimização de Risco:

1. Quais práticas você implementaria para segmentar clientes de alto e baixo risco na etapa de onboarding?

   Resolução:

   Análise de risco baseada em dados: Implementar um modelo de avaliação de risco que considere fatores como localização geográfica no país, ocupação (ex:PEPs), histórico transacional, natureza do negócio (média de transações e quantias)

   Classificação Automatizada: Usar algoritmos de *machine learning* para atribuir automaticamente escores de risco com base em critérios objetivos.

2. **Como você trataria casos de clientes com histórico de problemas de conformidade ao serem aceitos novamente?**

   Resolução:

   Revisão Estrita: Realizar uma análise detalhada do histórico de conformidade, identificando se o problema foi isolado, intencional ou sistemático.

   Termos Condicionados: Aceitar o cliente apenas com condições rigorosas, como monitoramento contínuo de transações, limites operacionais e auditorias periódicas.

Experiência do Usuário: 3. Como você equilibraria as exigências de conformidade com uma boa experiência de usuário?

Resolução:

Comunicação Transparente: Informar os clientes de forma clara sobre o motivo de cada etapa do processo e oferecer suporte em tempo real para resolver dúvidas.

Personalização: Adaptar o nível de rigor conforme o perfil do cliente, evitando exigir informações excessivas de clientes de baixo risco.

Validação de Identidade: 4. Quais métodos de validação biométrica considera mais eficazes e por quê?

Resolução:

Reconhecimento Facial com Liveness Check: Combina alta segurança e conveniência, dificultando fraudes com fotos ou vídeos.

Impressões Digitais: Confiável em ambientes que exigem autenticação física.

Porque ambos os métodos têm alta eficácia e ampla adoção por reguladores e experiência de usuário positiva.

Automação e Eficiência Operacional: 5. Quais partes do processo de KYC você acredita que são mais impactantes para automatizar, e quais manteria manuais?

Resolução:

Em automatizações:

- Verificação de identidade (documentos e biometria).
- Busca em bases de dados globais (sanções, PEPs, listas negativas).
- Classificação de risco com base em algoritmos.

Em procedimentos manuais, apenas que carecem de julgamento humano.

- Análise de casos atípicos e investigações aprofundadas.
- Decisões finais em clientes de alto risco, que requerem julgamento humano.

Análise de Dados e Monitoramento Contínuo: 6. Que tipo de dados adicionais você acredita que deveriam ser monitorados durante o relacionamento contínuo com o cliente?

Resolução:

- Mudanças em perfis transacionais: Monitorar desvios significativos no padrão esperado do cliente.
- Atualização de dados cadastrais: Identificar alterações em ocupação, endereço ou status como PEP.
- Eventos externos: Integrar dados de fontes públicas, como notícias sobre envolvimento do cliente em atividades suspeitas.

Tecnologia e Inovação: 7. Como você usaria dados de fontes externas, como redes sociais e processos judiciais, para enriquecer o perfil de risco do cliente?

Resolução:

- Análise de Sentimentos e Reputação: Usar algoritmos de processamento de linguagem natural (NLP) para identificar sinais de risco em postagens públicas.
- Integração com Registros Judiciais: Automatizar consultas a processos judiciais para identificar possíveis envolvimentos em fraudes ou crimes financeiros.
- Privacidade e Consentimento: Garantir conformidade com leis de privacidade, como LGPD, obtendo consentimento explícito para usar esses dados.

Desafios e Problemas Práticos: 8. Quais problemas operacionais considera mais críticos no processo de onboarding e como os resolveria?

Resolução:

- Demora na Verificação de Identidade: Resolver com validação automatizada em tempo real.

- Falsificação de Documentos: Mitigar com tecnologias avançadas de detecção de fraudes em documentos.
- Processo Fracionado: Centralizar o fluxo em uma plataforma única para reduzir erros e aumentar a eficiência.

O que iremos avaliar?

Avaliaremos como você aplicaria IA e Machine Learning para análise de comportamento e transações, considerando métricas, desafios e limitações, além de como mitigaria esses pontos. Também levaremos em conta seu equilíbrio entre conformidade e experiência do usuário, destacando pontos de atrito e soluções. Esperamos entender sua abordagem em validação biométrica e tratamento de falsos positivos, assim como a automação eficiente de processos de KYC, mantendo a segurança nas revisões.

Serão observadas suas sugestões de dados adicionais para monitoramento contínuo e configuração de alertas para clientes de risco moderado. Consideraremos ainda o impacto de atualizações regulatórias no onboarding, a gestão de conformidade entre jurisdições, o uso de dados externos para enriquecer perfis de risco e novos avanços tecnológicos aplicados à AML. Por fim, veremos como lida com desafios operacionais no onboarding e assegura a qualidade dos dados em verificações de AML.

Estamos ansiosos para ver sua abordagem analítica e criativa em cada uma dessas etapas. As respostas a cada item nos ajudarão a entender como você aplica seus conhecimentos na prática e propõe soluções colaborativas para o time de compliance.

Boa sorte!