|  |
| --- |
| ANÁLISE DE FRAUDE EM CARTÕES DE CRÉDITO Licenciatura em Engenharia Informática | 2024/2025 | 3º ano  Laboratório de Análise de Dados | Prof. Fátima Leal  Gabriela Almeida | 47004 João Faria | 48057 Luís Meireles | 47799 Mónica Fino | 47366 Paulo Brochado | 47406 Tiago Mesquita | 47558 |

### ÍNDICE

[**Introdução 3**](#_heading=h.3rdcrjn)

[**Contextualização do Dataset 4**](#_heading=h.ktxp7cbj5jqh)

[**Objetivo do Projeto 4**](#_heading=h.ktxp7cbj5jqh)

[**Tecnologias Utilizadas 5**](#_heading=h.ktxp7cbj5jqh)

[**Visão Geral do Programa 5**](#_heading=h.ktxp7cbj5jqh)

[**Análise de Fraudes 7**](#_heading=h.ktxp7cbj5jqh)

[**Estatísticas Avançadas 8**](#_heading=h.ktxp7cbj5jqh)

[**Relatórios e Configurações – Gerar Relatório 9**](#_heading=h.ktxp7cbj5jqh)

[**Relatórios e Configurações – Configurações Avançadas 11**](#_heading=h.ktxp7cbj5jqh)

[**Relatórios e Configurações – Padronização e Normalização 11**](#_heading=h.ktxp7cbj5jqh)

[**Dados 13**](#_heading=h.ktxp7cbj5jqh)

[**Machine Learning 14**](#_heading=h.ktxp7cbj5jqh)

[**Conclusão 17**](#_heading=h.927it0515gle)

# Introdução

O presente projeto, desenvolvido no âmbito da unidade curricular Laboratório de Analise de Dados, tem como principal objetivo a aplicação prática de técnicas de análise de dados e algoritmos de aprendizagem automática, utilizando a linguagem de programação Python.

A realização do projeto divide-se em duas fases complementares: Na primeira fase, é realizada uma análise estatística exploratória de um conjunto de dados escolhido, com o intuito de compreender a sua estrutura, características e padrões relevantes. Esta análise inclui o uso de medidas estatísticas, visualizações gráficas, criação de novas variáveis e normalização dos dados, culminando num painel de controlo gráfico e numa reflexão crítica dos resultados obtidos.

Na segunda fase, são aplicados e comparados diversos modelos de *Machine Learning*, deforma a resolver um problema de revisão ou de classificação. Esta etapa inclui também a análise de desempenho dos modelos, técnicas de redução de dimensionalidade, validação cruzada, e eventualmente algoritmos de recomendação e ferramentas automáticas, com o objetivo de validar os métodos escolhidos.

Este relatório descreve todo o processo de desenvolvimento do trabalho, desde a seleção do conjunto de dados até à análise final dos modelos aplicados, incluindo as decisões técnicas tomadas, os desafios enfrentados e as aprendizagens adquiridas ao longo do projeto.

# Contextualização do Dataset

O *dataset* utilizado neste projeto foi obtido a partir da plataforma *Kaggle* e é amplamente conhecido por ser utilizado em estudos sobre deteção de fraude em transações financeiras. Este conjunto de dados representa transações realizadas com cartões de crédito por titulares europeus ao longo de dois dias, em setembro de 2013. O *dataset* contém 284.807 registos, distribuídos por 31 variáveis. Todas as variáveis presentes no *dataset* classificam-se como Quantitativa Contínua, exceto a variável *class*, que é uma variável Qualitativa nominal.

O principal objetivo deste *dataset* é servir como base para o desenvolvimento e avaliação de modelos de Machine Learning capazes de identificar transações fraudulentas de forma automática, um problema real e crítico enfrentado por instituições financeiras em todo o mundo.

# Objetivo do Projeto

O principal objetivo deste projeto é desenvolver uma análise detalhada e um modelo preditivo para a deteção de fraudes com cartão de crédito, com base num conjunto de dados real e anonimizado. O trabalho está dividido em duas fases que se complementam.

Na primeira etapa, a análise estatística, é realizada uma exploração do *dataset* previamente escolhido de forma a compreender a sua estrutura, distribuição das variáveis, relações entre atributos e identificação de padrões relevantes. Inclui o cálculo de medidas estatísticas, normalização dos dados e criação de visualizações gráficas que suportem a análise crítica do fenómeno.

Na segunda etapa, a aplicação de modelos de *Machine Learning*, com as informações obtidas na fase anterior, são aplicados e comparados vários algoritmos de *Machine Learning* com o objetivo de construir um modelo que permita classificar automaticamente transações como legítimas ou fraudulentas. São exploradas técnicas como regressões, SVM, árvores de decisão, redes neurais e métodos de ensemble, com atenção à avaliação do desempenho, tempos de execução, validação cruzada e métricas como precisão, recall e F1-score.

Dado a elevada desproporção da variável alvo (*class*), o projeto aborda estratégias para lidar com este desafio, garantindo que os modelos conseguem identificar com eficácia as transações fraudulentas, mesmo quando estas representam uma minoria dos dados.

# Tecnologias Utilizadas

* Python – linguagem principal do projeto
* Streamlit – responsável pela interface do utilizador
* Pandas – ferramenta utilizada para a análise e manipulação dos dados
* Numpy – ferramenta para manipulação de matrizes
* Matplotlib – responsável pela visualização dos dados
* Seaborn – complemento para a biblioteca matplotlib
* Scikit-sklearn – útil para a criação de e aplicação de algoritmos de *Machine Learning*

# Visão Geral do Programa

A página principal do nosso programa mostra ao utilizador informações sobre a missão do projeto, os tipos comuns de fraude, as variáveis utilizadas no modelo e ficheiro CSV, como prevenir fraudes e tecnologias e estratégias para prevenção de fraudes.

A missão do projeto é ajudar empresas a detetarem fraudes financeiras com ajuda da Inteligência Artificial e análise de dados. O projeto também oferece soluções para a monitorização, prevenção e identificação de atividades suspeitas.

Os tipos comuns de fraudes dividem-se em:

* Fraude em Cartão de Crédito – utilização não autorizada do cartão de crédito para compras
* *Phishing* – enganar utilizadores para fornecerem informações sensíveis
* Roubo de identidade – falsificação de identidade para acesso financeiro ilícito
* Transações Falsificadas – manipulação ou falsificação de transações bancárias.

Quanto às variáveis utilizadas no modelo CSV, foram utilizadas as seguintes variáveis:

* *Time* – tempo decorrido desde a primeira transação no *dataset*
* V1-V28 – conjunto de variáveis anonimizadas resultantes de PCA (28 componentes principais)
* *Amout* – montante da transação
* *Class* – identificação do tipo de transação (0: legítima, 1: fraudulenta)
* *Hour* – hora do dia em que a transação ocorreu
* *Rolling\_Mean\_Amount* – média móvel do valor da transação (janela de 5 transações)
* *Std\_Amout* – desvio padrão do valor da transação (janela de 5 transações)
* *Delta\_Amout* – diferença entre o valor atual e o valor anterior da transação
* *Amount Category* – categoria do valor da transação (ex.: Muito Baixo, Baixo, Médio, etc.)
* *Time\_Diff* – diferença de tempo entre transações consecutivas
* *Transacao\_Noturna* – indica se a transação ocorreu durante a noite (1: Sim, 0: Não)
* *Num\_Transacoes\_1h* – número de transações realizadas na mesma hora
* *Freq\_Valor\_Transacao* – frequência de transações com o mesmo valor
* *Delta\_Media\_Valor* – Diferença entre o valor da transação e a média móvel
* *Region* – Região geográfica associada à transação

Focando na prevenção de fraudes, esta atividade envolve um conjunto de boas práticas e tecnologias que ajudam a proteger empresas e consumidores. São indicadas as seguintes recomendações:

* Ativar alertas de transação, utilizar a autenticação multifator e monitorização contínua
* Não partilhar informações pessoais, verificar remetentes suspeitos e utilizar autenticação de dois fatores
* Utilizar verificação biométrica, não reutilizar palavras-passe e ativar bloqueios automáticos
* Implementar monitorização de transações em tempo real e análises de comportamento.

Pensando nas empresas, o programa indica quais tecnologias e estratégias que podem ser utilizadas para reforçar a segurança:

* *Machine Learning* e Inteligência Artificial: modelos que analisam padrões e detetam anomalias
* Autenticação Multifator (MFA) – verificação em duas etapas para acessos financeiros
* Monitorização em Tempo Real - identificação de transações suspeitas à medida que ocorrem
* Criptografia Avançada – proteção de dados sensíveis contra acessos não autorizados
* Análises de Comportamento – identificação de padrões incomuns de uso do sistema

# Análise de Fraudes

Nesta secção da aplicação, foi implementado um painel de visualização interativo dedicado à análise das fraudes detetadas no *dataset*. Esta componente permite ao utilizador aplicar filtros personalizados, nomeadamente por intervalo de tempo e por região geográfica da Europa, proporcionando uma exploração mais dirigida dos dados. No âmbito da apresentação do projeto, optou-se por analisar os resultados considerando todas as regiões e todas as horas do dia, de forma a obter uma visão global do fenómeno.

O gráfico apresentado na Figura 1 consiste num gráfico de barras que ilustra a distribuição do número de fraudes ao longo das 24 horas do dia. A análise revela dois picos de atividade fraudulenta significativos: às 2h e às 11h da manhã. O pico registado às 2h pode ser associado a um período de baixa vigilância humana, o que pode favorecer a ocorrência de fraudes. Já o pico das 11h coincide com um horário de elevada atividade comercial, o que pode ser estrategicamente explorado pelos criminosos para disfarçar operações ilícitas entre o volume de transações legítimas.

Uma imagem com texto, captura de ecrã, Retângulo, Tipo de letra

Os conteúdos gerados por IA podem estar incorretos.Uma imagem com diagrama, Gráfico, file, Tipo de letra

Os conteúdos gerados por IA podem estar incorretos.O gráfico apresentado na Figura 2 mostra a percentagem de fraudes por região europeia, permitindo identificar possíveis disparidades geográficas. Os resultados indicam que a distribuição é relativamente equilibrada entre as regiões, embora se destaque a região Norte, onde se observa uma ligeira predominância de fraudes. Esta tendência pode estar relacionada com a alta adoção de meios de pagamento digitais nessa zona, aumentando a exposição a potenciais ataques.

Figura 2

Figura 1

Adicionalmente, foi incluída uma visualização sobre o valor monetário das fraudes (Figura 3). A análise indica que a maioria das fraudes envolve valores inferiores a 120€, o que pode ser uma estratégia para evitar alertas automáticos dos sistemas bancários. Contudo, foi identificada uma exceção notável, com uma transação fraudulenta superior a 2000€. Através da análise espacial-temporal com recurso a um *heatmap* (Figura 4), foi possível identificar que esta fraude de elevado valor ocorreu às 2h da manhã, na região Leste, reforçando a hipótese de que horários com menor controlo facilitam a concretização de fraudes mais significativas.

Uma imagem com texto, captura de ecrã, quadrado, Retângulo

Os conteúdos gerados por IA podem estar incorretos.Esta análise interativa não só facilita a compreensão da distribuição das fraudes no tempo e no espaço, como também oferece um suporte visual fundamental para a tomada de decisões em cenários reais de combate a fraudes.

Figura 4

Uma imagem com texto, captura de ecrã, file, Retângulo

Os conteúdos gerados por IA podem estar incorretos.

Figura 3

# Estatísticas Avançadas

Na interface da aplicação desenvolvida, foi implementada a secção dedicada à apresentação de Estatísticas Avançadas, permitindo ao utilizador explorar de forma aprofundada o comportamento das variáveis do *dataset*. Esta funcionalidade visa apoiar a análise descritiva com métricas estatísticas clássicas, fundamentais para compreender a distribuição e variabilidade dos dados.

No topo da página, são apresentadas as seguintes medidas estatísticas: média, mediana, variância e desvio padrão. Estas medidas oferecem uma perspetiva clara sobre a tendência central e a dispersão dos dados, o que é essencial na preparação e normalização dos mesmos para futuras etapas de modelação.

Uma imagem com texto, captura de ecrã, Gráfico, file

Os conteúdos gerados por IA poderão estar incorretos.Adicionalmente, foi incluída a matriz de correlação, que permite identificar relações lineares entre as variáveis. A análise dessa matriz revela que não existe uma correlação linear forte entre nenhuma das variáveis e a ocorrência de fraudes. Esta ausência de correlação direta é um comportamento comum em problemas de deteção de anomalias, nos quais as variáveis que indicam fraude não se distinguem facilmente por padrões simples.

Figura 5

Uma imagem com diagrama, captura de ecrã, file

Os conteúdos gerados por IA poderão estar incorretos.Para complementar a análise estatística, foi desenvolvido um *violin plot* que representa as fraudes em função do calor das transações e faz regiões. Este tipo de gráfico combina elementos de *boxplot* com a distribuição de densidade dos dados, oferecendo uma visão rica e intuitiva da variação dos valores.

Figura 6

A análise deste gráfico mostra que, em todas as regiões geográficas, a maioria das transações fraudulentas ocorreu com valores baixos, o que pode refletir uma tentativa de passar despercebido aos mecanismos de controlo. No entanto, observa-se também a ocorrência de algumas fraudes com valores elevados, especialmente na região Oeste, o que pode indicar zonas de maior risco ou fragilidade em determinados contextos de uso de cartões.

# Relatórios e Configurações – Gerar Relatório

A funcionalidade Gerar Relatório, inserida na secção Relatórios e Configurações da aplicação, foi desenvolvida com o objetivo de fornecer ao utilizador uma ferramenta prática e flexível para extrair subconjuntos relevantes de dados, de acordo com os critérios de análise definidos durante a exploração do *dataset*.

Neste subtópico, o utilizador pode realizar uma pré-visualização dos dados, selecionando apenas as variáveis de interesse, o que permite focar a análise em atributos específicos sem necessidade de tratar o ficheiro original manualmente. Além disso, é possível aplicar um filtro sobre o tipo de transações, escolhendo entre transações legítimas, fraudulentas ou todas as transições.

Estes filtros oferecem uma grande versatilidade ao utilizador, facilitando, por exemplo, a criação de relatórios dedicados exclusivamente a casos de fraude, ou a análise comparativa entre transações legítimas e fraudulentas.

**Distribuição de Categorias de Montante**

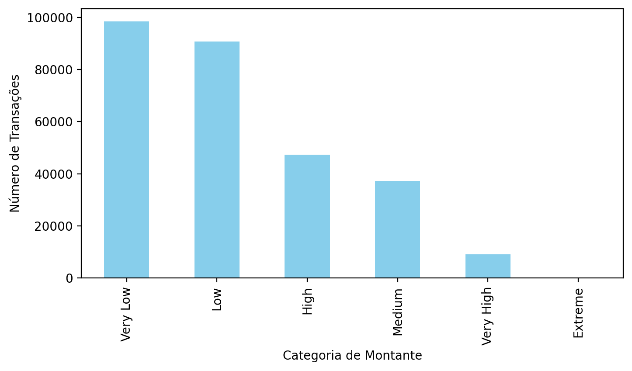
O gráfico apresenta a distribuição das transações de acordo com categorias de valor (*Amout*). Observa-se que a maioria das transações está concentrada nas categorias *Very Low* e *Low*, enquanto as transações de valor elevado, como *Very High* e *Extreme*, são muito menos frequentes. Esta visualização permite perceber rapidamente o perfil típico dos montantes transacionados no *dataset*.

Figura 6

**Proporção de Transações Noturnas –** mostra a percentagem das transações noturnas e diurnas em relação aos filtros que o utilizador escolheu para a sua análise.

**Média Móvel do Montante**

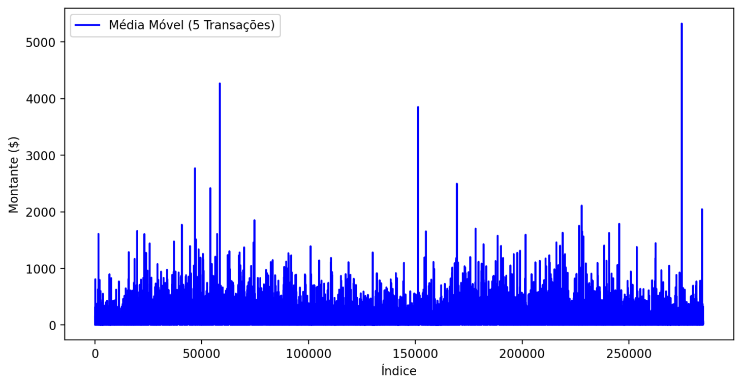
Este gráfico apresenta a média móvel do valor das transações. O objetivo desta visualização é suavizar a variação dos dados e destacar tendências locais nos montantes ao longo do tempo. Apesar da maioria das transações envolver valores baixos, observam-se picos pontuais com montantes significativamente mais elevados, que podem estar associados a anomalias ou potenciais fraudes.

Figura 7

**Diferença de Tempo entre Transições**

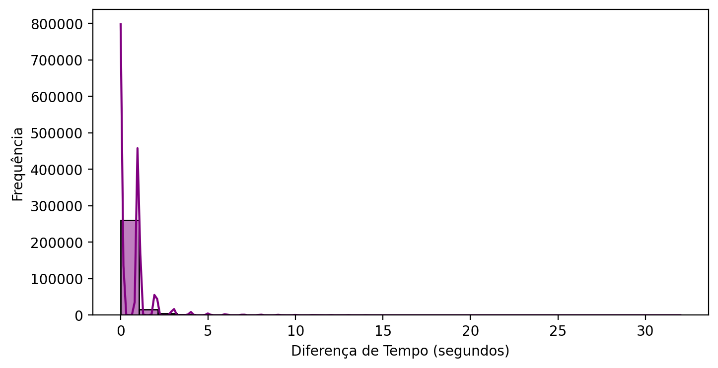
O gráfico mostra a distribuição da diferença de tempo entre transações, medida em segundos. Observa-se que a grande maioria das transações ocorre com intervalos muito curtos, o que indica um fluxo contínuo e intenso de atividades no sistema. A densidade elevada nos primeiros segundos pode refletir o processamento automático de grandes volumes de transações em tempo real.

Figura 8

# Relatórios e Configurações – Configurações Avançadas

A subsecção Configurações Avançadas foi concebida para permitir aos utilizadores uma personalização detalhada dos parâmetros operacionais da aplicação, com destaque na personalização dos critérios de deteção de fraude. Esta componente é estratégica para adaptar o comportamento do sistema às especificidades de diferentes domínios ou políticas internas de risco.

Entre as configurações disponíveis, destaca-se a definição de limites de alerta, onde o utilizador pode ajustar o montante mínimo a partir do qual uma transação é considerada potencialmente suspeita. Este limiar, intervalada entre $10 e $5000, serve como critério inicial para triagem de transações, permitindo um controlo mais fino sobre falsos positivos ou negligência de casos relevantes.

O utilizador pode também selecionar o método de deteção de fraude preferencial. As opções incluem:

* Regra Fixa: baseia-se em limiares definidos manualmente (ex.: valor da transação, horário), sendo mais transparente, mas menos adaptável a novas estratégias de ataque;
* *Machine Learning*: recorre a modelos preditivos treinados sobre padrões históricos, proporcionando maior sensibilidade a anomalias complexas, mas exigindo maior poder computacional e manutenção de modelos.

Outra funcionalidade crucial nesta secção é a Personalização Regional da Monitorização, viabilizada numa seleção com as regiões geográficas existentes na base de dados (*Region*). Esta configuração permite excluir regiões específicas da vigilância ativa ou concentrar os recursos computacionais em áreas com histórico mais denso de fraudes.

# Relatórios e Configurações – Padronização e Normalização

A subsecção Normalização e Padronização da aplicação foi concebida para oferecer ao utilizador uma compreensão prática e visual das técnicas de *rescaling* de dados, essenciais em processos de análise preditiva e deteção automática de fraudes. Este módulo interativo permite aplicar, visualizar e comparar os efeitos da padronização e da normalização em variáveis numéricas do *dataset*.

**Padronização (Z-*score* *Normalization*)**

A padronização transforma os dados de forma que apresentem média zero e desvio padrão igual a um, utilizando a fórmula:

Esta abordagem é especialmente indicada quando os dados seguem uma distribuição aproximadamente normal e quando se pretende preservar *outliers*, o que é crítico na deteção de fraudes, onde valores extremos são frequentemente relevantes. A aplicação permite ao utilizador selecionar uma variável à escolha e observar os seus valores padronizados lado a lado com os originais, sendo também calculadas e apresentadas as estatísticas associadas (média, desvio padrão, etc.).

**Normalização (Min-Max *Scaling*)**

A normalização transforma os valores das variáveis para um intervalo fixo, tipicamente com intervalo entre 0 e 1, através da fórmula:

Esta técnica é recomendada quando os algoritmos requerem valores num intervalo limitado, como acontece em redes neuronais ou algoritmos sensíveis à distância (ex.: KNN, SVM). Tal como na padronização, o utilizador pode aplicar a transformação a qualquer variável numérica e comparar os dados antes e depois da normalização, com apoio de tabelas e histogramas.

**Comparação Visual**

Uma das funcionalidades mais didáticas desta secção é a comparação visual entre os dados originais, padronizados e normalizados. O utilizador pode selecionar duas variáveis à sua escolha, e a aplicação gera gráficos de dispersão (*scatter* *plots*) para cada cenário. Estes gráficos são coloridos de acordo com a classe da transação (fraude ou legítima), permitindo observar de forma clara como a transformação dos dados afeta a separabilidade entre as classes.

Além disso, é apresentada uma visualização adicional da distribuição dos valores antes e depois das transformações, o que facilita a perceção das diferenças de escala, forma e simetria das variáveis.

# Dados

A secção Dados da aplicação constitui o núcleo informativo do sistema, disponibilizando um painel de monitorização estatística e uma descrição detalhada das variáveis envolvidas na análise de transações financeiras com vista à deteção de fraudes. Esta área foi desenhada com o objetivo de oferecer uma visão clara, estruturada e contextualizada sobre o *dataset* em análise, servindo de base para todas as operações analíticas, modelação preditiva e interpretação de resultados.

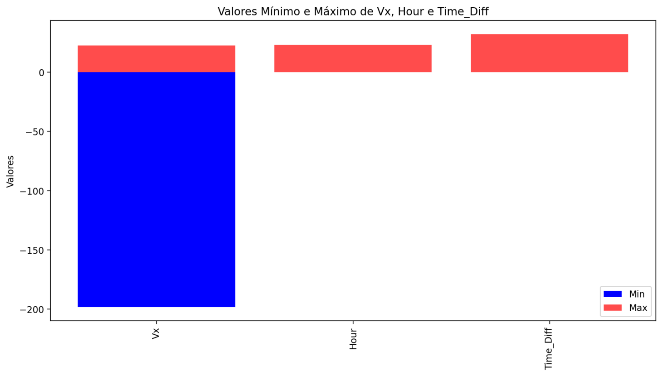
O *dataset* utilizado é composto por transações financeiras associadas a pagamentos com cartão de crédito, contendo aproximadamente 285 mil registos com múltiplas variáveis, tanto originais como derivadas. A variável-alvo *class* é binária (0: legítima, 1: fraudulenta), estando fortemente desproporcionada — com uma proporção de fraudes inferior a 0.2%, o que representa um desafio clássico na área de deteção de anomalias.

A aplicação disponibiliza uma visão agregada das principais métricas descritivas, incluindo:

* Número total de transações;
* Contagem absoluta de fraudes;
* Taxa percentual de fraude;
* Valor médio, mínimo e máximo das transações;
* Desvio padrão do montante das transações.

Estes indicadores são apresentados de forma sumarizada e visualmente acessível, fornecendo uma leitura imediata do volume e dispersão das transações, com impacto direto na calibragem dos modelos de deteção.

A aplicação oferece ainda visualizações comparativas dos valores mínimos e máximos para as variáveis mais relevantes do ponto de vista descritivo e preditivo.

Este gráfico evidencia a amplitude de variação das variáveis *Vx, Hour e Time\_Diff*. A variável *Vx*, resultante da soma dos componentes principais V1 a V28, apresenta valores significativamente mais dispersos, com um mínimo inferior a -200, o que pode indicar *outliers* de interesse na deteção de fraudes. Já *Hour*, com um intervalo fixo de 0 a 23, e *Time\_Diff*, relacionado com a cadência das transações, mostram variações mais controladas, mas ainda assim relevantes para modelação temporal e comportamental.

A diferenciação de cor entre valores mínimos (azul) e máximos (vermelho) ajuda a identificar rapidamente variáveis com amplitude elevada e possíveis anomalias. Esta informação é especialmente útil para compreender a escalabilidade dos dados e ajustar técnicas de normalização ou padronização de forma apropriada.

# Machine Learning

*Machine Learning* é uma subárea da Inteligência Artificial que tem como objetivo permitir que os sistemas informáticos aprendam diretamente a partir dos dados, sem que seja necessário definir explicitamente as regras de decisão. Esta abordagem é especialmente relevante em contextos como a deteção de fraudes financeiras, onde os padrões de comportamento fraudulentos são muitas vezes complexos, variáveis e difíceis de definir manualmente. Com *Machine Learning*, torna-se possível treinar algoritmos que identificam comportamentos anómalos com base em características estatísticas, temporais e comportamentais extraídas das transações.

Existem três paradigmas principais do *Machine Learning*, cada um com diferentes aplicações e requisitos:

**Aprendizado Supervisionado:** Neste tipo de aprendizado, os modelos são treinados com um conjunto de dados rotulado, ou seja, cada exemplo de entrada está associado a uma saída esperada (rótulo). O objetivo do algoritmo é aprender uma função que relacione as variáveis de entrada às suas respetivas saídas.

Algoritmos utilizados na aplicação incluem:

* Regressão Logística
* Árvores de Decisão
* *Random* *Forest*
* *Support Vector Machines* (SVM)
* Redes Neurais (simples)

No âmbito da aplicação desenvolvida, a classificação supervisionada foi utilizada para identificar transações fraudulentas. O conjunto de dados incluía atributos derivados, como a média móvel do montante (*Rolling\_Mean\_Amount*), a diferença entre valores consecutivos (*Delta\_Amount*) e a frequência de transações por montante, permitindo ao modelo aprender padrões associados à classe de fraude.

**Aprendizado Não Supervisionado:** O aprendizado não supervisionado é aplicado quando os dados não estão rotulados. O objetivo é identificar padrões, estruturas ocultas ou agrupamentos naturais nos dados.

Algoritmos aplicáveis:

* *K-means*
* DBSCAN
* Agrupamento Hierárquico
* PCA (*Principal Component Analysis)*
* t-SNE

Na aplicação em questão, o algoritmo de *K-means* foi utilizado de forma exploratória para agrupar transações com base em variáveis como o montante (*Amount*) e componentes principais resultantes de PCA. Esta técnica permitiu identificar subconjuntos de transações com comportamento estatístico semelhante, útil para a deteção de possíveis fraudes em clusters isolados.

**Aprendizado por Reforço:** Embora não tenha sido diretamente implementado na aplicação atual, o aprendizado por reforço representa um paradigma em que o modelo interage com um ambiente dinâmico, recebendo recompensas ou penalizações em função das suas ações. Este tipo de abordagem é promissor em cenários de monitorização contínua e sistemas de prevenção adaptativos.

**Processo de *Machine Learning***

* Preparação dos Dados: importação, limpeza e transformação das variáveis. No código da aplicação, foram geradas novas variáveis, como a hora da transação (*Hour*), o desvio padrão do montante (*Std\_Amount*), entre outras.
* Seleção de Modelo: escolha do algoritmo com base no tipo de problema e na natureza dos dados.
* Treinamento: ajuste do modelo aos dados de treino, utilizando técnicas como validação cruzada.
* Validação: avaliação do modelo com dados não vistos, usando métricas adequadas.
* Ajuste de Hiperparâmetros: otimização dos parâmetros internos do modelo para maximizar o desempenho.
* Implantação: disponibilização do modelo em ambiente produtivo, permitindo classificar novas transações em tempo real.
* Monitoramento: avaliação contínua do desempenho e necessidade de re-treinamento com novos dados.

**Desafios e Considerações em Deteção de Fraudes**

A aplicação de ML à deteção de fraudes apresenta desafios específicos, tais como:

* Desequilíbrio entre classes: A maioria das transações são legítimas, o que exige técnicas como SMOTE (*Synthetic Minority Oversampling Technique*) para balancear o conjunto de dados.
* Adaptação a novas fraudes: Os padrões de fraude mudam constantemente, exigindo modelos que possam ser atualizados regularmente.
* Baixa latência: A deteção precisa ocorrer em tempo quase real, sem comprometer a experiência do utilizador.
* Dados sensíveis: A privacidade e a segurança dos dados devem ser garantidas, principalmente em contextos financeiros.

Na aplicação de Deteção de Fraude, estas questões foram abordadas com a utilização de algoritmos robustos como o *Random Forest*, técnicas de balanceamento de classes (SMOTE) e análise por PCA, permitindo ao sistema classificar transações e avaliar o risco de fraude com base em múltiplas variáveis estatísticas e comportamentais.

**Métricas de Avaliação**

A avaliação dos modelos foi realizada com base em métricas apropriadas ao contexto de classificação desproporcionada, nomeadamente:

* Acurácia: proporção global de classificações corretas.
* Precisão: proporção de verdadeiros positivos entre todas as classificações como fraude.
* *Recall* (Sensibilidade): proporção de fraudes reais corretamente identificadas.
* F1-Score: média harmónica entre precisão e *recall*.
* Matriz de Confusão: permite visualizar os acertos e erros em cada classe.

Estas métricas foram calculadas e apresentadas no ambiente *Streamlit* da aplicação, com gráficos interativos que auxiliam a interpretar os resultados e a ajustar o desempenho do modelo.

# Classificação para Identificar Fraudes

A classificação é uma técnica central em *Machine Learning* aplicada à deteção de fraudes, permitindo distinguir automaticamente entre transações legítimas e fraudulentas com base em padrões aprendidos a partir dos dados históricos. No projeto desenvolvido, utilizámos diversos algoritmos de classificação para identificar fraudes num conjunto de dados real sobre transações com cartões de crédito.

Antes da aplicação dos modelos, foi realizada uma preparação extensa dos dados:

* Criação de novas variáveis: features como *Rolling\_Mean\_Amount*, *Std\_Amount*, *Delta\_Amount*, *Transacao\_Noturna*, entre outras, foram derivadas para enriquecer a capacidade de deteção dos modelos.
* Tratamento de desequilíbrio: dado que as transações fraudulentas representam uma minoria significativa no *dataset*, aplicámos a técnica SMOTE para criar exemplos sintéticos da classe minoritária e equilibrar o conjunto de treino.

Vários algoritmos foram treinados e comparados, com destaque para:

* *Random Forest*: um ensemble de árvores de decisão que mostrou alta robustez e capacidade de generalização. Foi usado tanto com dados originais como com redução de dimensionalidade via PCA.
* Regressão Logística: modelo estatístico que, apesar de simples, oferece uma boa interpretação nas suas decisões e bom desempenho em cenários lineares.
* Árvore de Decisão: útil para visualização das decisões do modelo, permitindo entender as regras que levam à classificação de uma transação como fraude.
* *AdaBoost* e *XGBoost*: algoritmos baseados em *boosting*, que combinam vários modelos fracos para criar um modelo mais forte. O *XGBoost*, em especial, mostrou métricas de *recall* e *F1-Score* superiores.
* SVM (*Support Vector Machines*): testadas com diferentes tipos de *kernel*, foram eficazes na separação das classes em espaços de alta dimensão.
* *Naive Bayes*: uma abordagem probabilística simples, mas eficiente, especialmente útil em cenários com independência entre *features*.
* K-NN (*K-Nearest Neighbors*) e Redes Neuronais: explorados como métodos alternativos, com desempenho variável consoante o número de vizinhos ou configuração das camadas ocultas.

# Ridge e Lasso Regression

A utilização de métodos de regressão, como *Ridge* e *Lasso*, no contexto de deteção de fraudes financeiras, oferece uma abordagem complementar aos algoritmos de classificação tradicionais. Apesar de serem originalmente concebidas para problemas de regressão, estas técnicas podem ser adaptadas a problemas de classificação binária (como distinguir entre transações legítimas e fraudulentas), proporcionando benefícios em termos de interpretação, controlo da complexidade do modelo e seleção de variáveis relevantes.

No projeto desenvolvido, implementado através de uma interface em *Streamlit*, estas técnicas foram testadas com os seguintes passos metodológicos:

* Seleção de Variáveis: As variáveis mais correlacionadas com a variável alvo (indicador de fraude) foram automaticamente identificadas através da análise das correlações absolutas. O número de variáveis utilizadas é escolhido pelo utilizador, permitindo explorar diferentes combinações.
* Normalização dos Dados: Os dados foram normalizados utilizando técnicas de standard *scaling*, essencial para garantir que a penalização aplicada aos coeficientes não favoreça variáveis com maiores magnitudes.
* Divisão do Conjunto de Dados: O conjunto de dados foi dividido em subconjuntos de treino e teste, garantindo a validação cruzada e a medição do desempenho em dados não vistos.
* Ajuste dos Modelos: Foram aplicadas regressões *Ridge* e *Lasso* com diferentes valores do hiperparâmetro de regularização, permitindo observar o impacto da penalização no comportamento dos coeficientes e na capacidade preditiva dos modelos.
* Avaliação de Desempenho: A avaliação baseou-se em métricas como o erro quadrático médio (RMSE) e a análise gráfica da evolução dos coeficientes. Embora não seja o foco principal da regressão medir acurácia classificatória, foi também possível observar o impacto na separação entre transações fraudulentas e não fraudulentas.

Os resultados obtidos com a aplicação das regressões revelam conclusões relevantes no contexto da deteção de fraudes. A regressão *Lasso* demonstra ser particularmente eficaz na redução do número de variáveis utilizadas, ao eliminar automaticamente aquelas que se revelaram menos informativas. Este comportamento resultou em modelos mais simples e interpretáveis, favorecendo a análise explicativa e a compreensão do impacto individual de cada variável. Por outro lado, a regressão *Ridge* destaca-se pela sua capacidade de produzir coeficientes mais estáveis, uma característica especialmente valiosa em cenários com elevada multicolinearidade entre variáveis — como é o caso das componentes principais V1 a V28, provenientes de uma decomposição por Análise de Componentes Principais (PCA).

# Classificar Transação

A funcionalidade de classificação individual de transações representa a etapa final e mais aplicada do sistema de deteção de fraudes, permitindo avaliar, de forma instantânea, se uma determinada transação tem maior probabilidade de ser fraudulenta ou legítima. Esta componente é essencial do ponto de vista operacional, dado que aproxima o modelo analítico da realidade prática, oferecendo suporte direto à tomada de decisão em tempo real.

Na aplicação desenvolvida, essa funcionalidade foi integrada através de uma interface interativa que permite ao utilizador introduzir manualmente os dados de uma transação ou carregar valores externos para análise. Com base nas variáveis previamente selecionadas e utilizadas durante o treino do modelo — como *Amount*, V1, V2, V3, V4 e V10 — o sistema processa os dados e realiza a predição utilizando o algoritmo escolhido (como *Random Forest*, Regressão Logística ou Árvore de Decisão).

As variáveis V1 a V28 correspondem a componentes principais obtidas por transformação PCA sobre os dados originais anonimizados. Embora o significado semântico exato destas variáveis não seja conhecido, estudos demonstraram que as primeiras componentes, como V1, V2, V3, V4 e V10, são aquelas que retêm maior variância e, portanto, mais informação discriminativa. Além disso, análises realizadas no desenvolvimento da aplicação confirmaram que estas variáveis estão entre as mais correlacionadas com a variável-alvo (*Class*) e surgem com elevada importância em modelos de árvore. A sua escolha foi, assim, sustentada tanto por critérios estatísticos como por desempenho empírico.

Antes da classificação, os dados são preparados de forma a garantir compatibilidade com o modelo treinado, o que pode incluir normalização, transformação PCA e verificação de integridade. A predição é então efetuada, apresentando como resultado a classificação da transação, legítima ou fraudulenta, podendo incluir uma probabilidade associada à decisão.

Esta funcionalidade aproxima o modelo do seu propósito prático, permitindo simular decisões em tempo real e aplicar os conhecimentos adquiridos ao longo da análise de dados e treino dos modelos. Funciona também como uma ferramenta de validação do modelo, oferecendo aos utilizadores uma interface acessível para avaliar casos concretos com base em evidência quantitativa.

# Conclusão

O desenvolvimento deste projeto permitiu aplicar, de forma prática e integrada, os conhecimentos adquiridos na unidade curricular de Laboratório de Análise de Dados, articulando técnicas estatísticas, ferramentas de visualização e algoritmos de *Machine Learning* com o propósito de detetar fraudes em transações com cartão de crédito.

Através de uma abordagem estruturada em duas fases, foi possível, numa primeira instância, realizar uma análise exploratória exaustiva do *dataset*, identificando padrões relevantes e características distintivas das transações fraudulentas. A criação de variáveis derivadas e a aplicação de técnicas de normalização e padronização revelaram-se essenciais para preparar os dados para os modelos preditivos.

Na segunda fase, a aplicação e comparação de múltiplos algoritmos supervisionados e não supervisionados permitiu construir modelos robustos, com especial destaque para o *Random Forest* e o SVM, que se evidenciaram pelo seu desempenho na identificação de fraudes. Foram também abordadas limitações associadas à desproporção dos dados, utilizando técnicas como o SMOTE para mitigar este problema e aumentar a capacidade preditiva dos modelos.

A implementação da aplicação interativa em *Streamlit* representou um contributo significativo para a democratização da análise, permitindo ao utilizador final explorar os dados, ajustar parâmetros e gerar relatórios de forma autónoma e intuitiva.

Em suma, o projeto demonstrou a relevância e o potencial da ciência de dados e da aprendizagem automática no combate à fraude financeira, evidenciando a importância de abordagens multidimensionais, adaptáveis e sustentadas por dados rigorosamente analisados. O trabalho realizado constitui não só um exercício técnico e académico, mas também uma simulação realista de um sistema de apoio à decisão com aplicabilidade no contexto empresarial.



upt.pt