INSTITUTO FEDERAL DE SANTA CATARINA

LUCAS DE MATTOS

# APLICAÇÃO DE TÉCNICAS DE *MACHINE LEARNING* NO APOIO À DETECÇÃO DE FRAUDES EM PAGAMENTOS ONLINE

Caçador - SC

07 de Dezembro de 2021

LUCAS DE MATTOS

# APLICAÇÃO DE TÉCNICAS DE *MACHINE LEARNING* NO APOIO À DETECÇÃO DE FRAUDES EM PAGAMENTOS ONLINE

Monografia apresentada ao Curso de Sistemas de Informação do Câmpus Caçador do Instituto Federal de Santa Catarina para a obtenção do diploma de Bacharel em Sistemas de Informação.

Orientador: Profa. Milena Cristina França, Ma.

Coorientador: Prof. Paulo Roberto Cordova, Dr.

Caçador - SC

07 de Dezembro de 2021

Lucas de Mattos
APLICAÇÃO DE TÉCNICAS DE *MACHINE LEARNING* NO APOIO À DETECÇÃO DE FRAUDES EM PAGAMENTOS ONLINE/ Lucas de Mattos. – Caçador - SC, 07 de Dezembro de 2021-
41 p. : il. (algumas color.) ; 30 cm.

Orientador: Profa. Milena Cristina França, Ma.

Monografia (Graduação) – Instituto Federal de Santa Catarina – IFSC
Campus Caçador
Sistemas de Informação, 07 de Dezembro de 2021.

1. *Machine Learning*. 2. Fraudes. 3. Pagamentos Online. 4. Regressão Logística. 5. Árvore de Decisão. I. Profa. Milena Cristina Franca Ma.. II. Instituto Federal de Santa Catarina. III. Campus Caçador. IV. APLICAÇÃO DE TÉCNICAS DE *MACHINE LEARNING* NO APOIO À DETECÇÃO DE FRAUDES EM PAGAMENTOS ONLINE.

LUCAS DE MATTOS

# APLICAÇÃO DE TÉCNICAS DE *MACHINE LEARNING* NO APOIO À DETECÇÃO DE FRAUDES EM PAGAMENTOS ONLINE

Este trabalho foi julgado adequado para obtenção do título de Bacharel em Sistemas de Informação, pelo Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, e aprovado na sua forma final pela comissão avaliadora abaixo indicada.

Caçador - SC, 07 de Dezembro de 2021:

---

Profa. Milena Cristina França, Ma.
Orientadora
Instituto Federal de Santa Catarina

---

Prof. Paulo Roberto Cordova, Dr.
Coorientador
Instituto Federal de Santa Catarina

---

Prof. Cristiano Mesquita Garcia, Me.
Banca Avaliadora
Instituto Federal de Santa Catarina

---

Prof. Samuel da Silva Feitosa, Dr.
Banca Avaliadora
Instituto Federal de Santa Catarina

*Este trabalho é dedicado à minha família,*
*meus colegas, amigos e professores.*

# AGRADECIMENTOS

Agradeço em primeiro lugar a Deus, que me deu forças para continuar nesta jornada até o fim e conseguir concluir este trabalho.

A minha esposa Rafaela, que sempre esteve ao meu lado, nos momentos bons e ruins, sempre me apoiando e incentivando para que eu nunca desistisse.

Agradeço em especial à minha mãe, que me apoiou em todas as minhas decisões ao longo desta jornada e à toda a minha família.

Agradeço também aos meus colegas de graduação, aos meus professores, principalmente aos meus orientadores Profa. Milena e Prof. Paulo e toda a comunidade acadêmica do IFSC câmpus Caçador.

E por fim, todos que me auxiliaram de alguma forma. Muito obrigado!

*"Ainda que eu atravesse pelo vale da sombra*
*e da morte, não temerei mal algum,*
*pois o Senhor está comigo..."*
*(Bíblia Sagrada, Salmos 23:4)*

# RESUMO

O aprendizado de máquina (*Machine Learning*) têm sido usado com bastante frequência em diversas áreas de pesquisa, com o objetivo de automatizar tarefas complexas ou fazer predições. A fraude em pagamentos online é um problema que ainda precisa ser debelado, pois traz consigo diversos impactos negativos, tanto para o comércio eletrônico quanto para os intermediadores de pagamentos, e até mesmo para o governo. Neste projeto é proposto a aplicação de técnicas de *Machine Learning* para auxiliar na detecção de fraudes em pagamentos online. Com o uso do aprendizado de máquina, é possível predizer se uma transação de pagamento online tem potenciais chances de ser fraudulenta ou não. Para tal, foram utilizados os algoritmos de Regressão Logística e de Árvore de Decisão, além da validação do modelo, usando como base as métricas de avaliação da Acurácia, Precisão, Revocação AUC ROC e Matriz de Confusão. O modelo de Regressão Logística apresentou melhor desempenho ao classificar os dados atingindo uma acurácia e precisão de 95%, enquanto que o modelo de Árvore de Decisão apresentou uma acurácia e precisão de 93%. Este trabalho pode ser utilizado como ponto de partida para outros trabalhos no futuro, utilizando como base o modelo gerado a partir das técnicas de *Machine Learning*.

**Palavras-chave**: *Machine Learning*. Fraudes. Pagamentos Online. Regressão Logística. Árvore de Decisão.

# ABSTRACT

Machine Learning has been used quite frequently in several research areas, with the aim of automating complex tasks or making predictions. Online payment fraud is a problem that still needs to be tackled, as it brings with it several negative impacts, both for e-commerce and for payment intermediaries, and even for the government. This project proposes the application of Machine Learning techniques to help detect fraud in online payments. Using machine learning, it is possible to predict whether an online payment transaction has the potential to be fraudulent or not. For this purpose, the Logistic Regression and Decision Tree algorithms were used, in addition to the validation of the model, based on the metrics for evaluating Accuracy, Precision, AUC ROC Recall and Confusion Matrix. The Logistic Regression model performed better when classifying the data, reaching an accuracy and precision of 95%, while the Decision Tree model presented an accuracy and precision of 93%. This work can be used as a starting point for other works in the future, using as a basis the model generated from Machine Learning techniques.

**Keywords**: Machine Learning. Fraud. Online Payment. Logistic Regression. Decision tree.

# LISTA DE ILUSTRAÇÕES

# LISTA DE TABELAS

# LISTA DE ABREVIATURAS E SIGLAS

**AUC ROC** Area Under the ROC Curve and Receiver Operating Characteristic

**CNDL** Confederação Nacional de Dirigentes Lojistas

**FEBRABAN** Federação Brasileira de Bancos

**KDD** Knowledge Discovery in Databases

**MEI** Microempreendedor Individual

**ML** Machine Learning

**SPC** Serviço de Proteção ao Crédito

# SUMÁRIO

# 1 INTRODUÇÃO

No Brasil o *e-commerce* (comércio eletrônico) tem crescido de forma considerável nos últimos anos. Segundo Terra (2021) um estudo de perfil do *e-commerce* brasileiro feito por uma parceria entre PayPal e BigData Corp mostra que a expansão do *e-commerce* brasileiro foi de, aproximadamente, 40% após dois anos de crescimento moderado. Os registros de 2016 são de 9,23% e de 12,5% em 2017. Em 2017 o *e-commerce* brasileiro apontou o seu maior crescimento desde o ano de 2014. Segundo a MeioeMensagem (2021), com as lojas físicas fechadas por conta da pandemia, muitas pessoas recorreram às compras online e, com isso, o *e-commerce* brasileiro registrou um crescimento de 47% no primeiro semestre, sua maior alta em 20 anos, com uma crescente no número de vendas em 2020. A Ebit (2020) estimou um salto de 39% no número de pedidos realizados no Ecommerce, totalizando 90,8 milhões.

Todo esse crescimento do comércio eletrônico e das vendas online trazem consigo um crescimento nas atividades fraudulentas, como apontado na pesquisa realizada pela ConsumidorModerno (2021). Considerando-se a estimativa de que o *e-commerce* brasileiro registrou 250 milhões de pedidos no ano de 2020, a taxa de 2,52% de tentativas de fraude significa que uma tentativa de fraude ocorre no País a cada 5 segundos – ou ainda que a cada 40 compras online, uma tem origem fraudulenta. É certo que tanto usuários fraudadores quanto usuários legítimos usam o *e-commerce*, mas a natureza anônima das compras online não promove um ambiente ideal para que as transações ocorram (MASSA; VALVERDE, 2014).

Segundo o dicionário Aurélio, fraude é o ato de lograr, falsificar produtos, documentos, marcas etc. Qualquer ação ilícita, desonesta, ardilosa que busca enganar ou ludibriar alguém. No contexto deste trabalho e do comércio eletrônico, esses atos podem estar relacionados com a realização de compras não-identificadas por parte de usuários legítimos, clonagem de cartões de crédito, prática de cartel de preços feitos pelos comerciantes, roubos de contas de usuários, utilização dos sites de maneira indevida, entre outros. Segundo uma pesquisa realizada pela AgenciaSenado (2021) a prática de fraudes em pagamentos online já gerou prejuízos ao Brasil de aproximadamente R$ 1 bilhão, além de perdas de poder aquisitivo e abalos emocionais às famílias brasileiras. Foi proposto ao Senado Nacional alterações no Código Penal para fixar a pena de reclusão de quatro a oito anos ao criminoso que praticar fraude por meio de dispositivo eletrônico ou de informática, conectado ou não à internet, com ou sem a violação de mecanismo de segurança, ou com utilização de programa malicioso.

Para diminuir o problema de fraudes em pagamentos online são realizadas análises de fraude, os quais, na maioria das vezes são feitas de forma automática. Segundo a PH3A (2018) para tal procedimento é aplicado um *Quiz* online, que tem por objetivo validar se a identidade corresponde com o documento atrelado ao cartão de crédito do titular, confirmadas todas as informações concedidas pelo comprador e validadas pelo banco emissor do cartão de crédito, a aprovação da compra é imediata. Nesse caso, a análise é apenas automática. Também, em muitos casos, além da análise automatizada é realizada por algumas empresas uma análise manual dos dados, como aponta a pesquisa da PH3A (2018), explicando que, quando a análise automática não é suficiente para determinados casos, a análise manual é acionada. Em linhas gerais, ela é um processo no qual os dados do comprador são verificados e analisados com ainda mais rigor, sendo que esse tipo de análise pode levar até 48 horas. Neste contexto pode ser útil o uso da metodologia do *Knowledge Discovery in Databases (KDD)* para a resolução desse problema. Segundo Bramer (2007) a metodologia do KDD trata-se de um processo de extração de dados que visa a obtenção de informação que não é óbvia, antes desconhecida e com potencial de ser útil. Tudo isso associado a técnicas de *Machine Learning (ML)*, que é uma abordagem normalmente utilizada para a detecção de

padrões em dados, visando a automatização de tarefas complexas ou fazer predições, e vêm se tornando um diferencial em diversas áreas (INAZAWA et al., 2019).

Foram encontrados outros trabalhos que utilizam a técnica de Mineração dos Dados, com o objetivo principal de detectar possíveis fraudes em pagamentos online no Brasil (PACHECO, 2019) (FELIPE, 2012). Algumas outras técnicas de ML também são aplicadas em outras áreas de pesquisa, como por exemplo, nas áreas da saúde pública (BERTOZZO, 2019), empresarial (QUINTÃO; MENDONÇA, 2020) e de ensino (FERREIRA, 2016). Neste trabalho procura-se utilizar técnicas de ML dentro do processo de KDD para auxiliar a identificar de forma mais rápida e assertiva possíveis atividades fraudulentas nos pedidos de pagamentos online. As técnicas abordadas neste trabalho serão aplicadas em um ambiente de teste criado a partir da coleta de dados anônimos, cujo os dados serão extraídos de um *dataset* público.

## 1.1 Problema de Pesquisa

Para o problema de pesquisa, pode ser definida a seguinte questão: "Utilizando como base as técnicas de ML, pode-se realizar o desenvolvimento de um modelo computacional, que visa auxiliar na detecção de possíveis fraudes em pagamentos online?".

## 1.2 Hipótese de Pesquisa

Para a solução do problema podemos apresentar a seguinte hipótese: Com base nas técnicas de ML, é possível realizar o desenvolvimento de um modelo computacional que visa auxiliar na detecção de fraudes em pagamentos online.

## 1.3 Objetivos

### 1.3.1 Objetivo Geral

Este trabalho tem como objetivo geral realizar o desenvolvimento de um modelo computacional aplicando técnicas de ML, no apoio à detecção de fraudes em pagamentos online.

### 1.3.2 Objetivos Específicos

- Identificar as técnicas de ML mais utilizadas para o auxílio na detecção de possíveis fraudes em pagamentos online;
- Fazer a coleta dos dados genéricos a partir de um *dataset* público;
- Realizar a mineração e o balanceamento dos dados coletados;
- Treinar os modelos com base nos dados tratados;
- Aplicar métricas de avaliação nos modelos;
- Desenvolver um protótipo usando o modelo computacional mais adequado.

## 1.4 Justificativa

Podemos ressaltar que, apesar de existirem pesquisas utilizando outras formas para tentar resolver o problema de fraudes em pagamentos online, pode-se afirmar que com base no crescente número de *e-commerces* sendo abertos e de pedidos de pagamento online sendo gerados todos os dias, surgem novos tipos de atividades fraudulentas em pagamentos online, conforme apontado na pesquisa realizada pela Veja (2021). As fraudes se transformam, diminuem em alguns segmentos, mas aumentam em outros. Elas acontecem cada vez mais sem a necessidade da posse física do cartão, por meio de operações em *e-commerce*, sites e aplicativos. A motivação para realizar este trabalho partiu de pesquisas realizadas principalmente por empresas de cartão de crédito e intermediadoras de pagamentos online, identificando novos tipos de fraudes.

Para esta pesquisa será abordado a aplicação do KDD, segundo Goldschmidt (2005) basicamente, uma aplicação de KDD é composta por três tipos de componentes: o problema em que será aplicado o processo de KDD, os recursos disponíveis para a solução do problema e os resultados obtidos a partir da aplicação dos recursos disponíveis em busca da solução do problema. Com a metodologia do KDD podemos analisar os dados e realizar o processamento dos mesmos, isso nos auxilia no tratamento de uma grande quantidade de requisições de pagamentos analisando suas possíveis classificações de existência de fraude. Sem a aplicação da metodologia de KDD, a classificação de existência de fraude, seria um trabalho muito complexo e com grandes chances de classificar requisições de forma errada no ponto de vista humano.

Todos os resultados obtidos neste trabalho, poderão ser utilizados futuramente por empresas que possuem sites ou aplicativos voltados ao comércio eletrônico (*e-commerce*) no auxílio à detecção de possíveis fraudes em pagamentos online, e também será possível reutilizar o *dataset* e os dados coletados ou pré-processados em futuros novos projetos que aparecerem abordando o mesmo tema.

## 1.5 Organização do texto

O restante deste texto está organizado da seguinte forma: No Capítulo 2 é apresentada a fundamentação teórica que traz os principais tipos de fraudes praticados no Brasil, bem como as principais técnicas de ML utilizadas neste trabalho. No Capítulo 3 é apresentado o estado da arte da área pesquisada, onde buscou-se observar na bibliografia os principais trabalhos que abordam o mesmo tema. No Capítulo 4 são discutidos os procedimentos metodológicos e a empregabilidade das técnicas de ML. No Capítulo 5 são apresentados os resultados da pesquisa e as métricas de avaliação que foram aplicadas sobre os modelos afim de selecionar o modelo computacional mais adequado. Por fim, no Capítulo 6 são apresentadas as considerações finais acerca deste trabalho e como ele pode ser utilizado em outros trabalhos no futuro.

# 2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo serão apresentados os principais tópicos relacionados ao problema da fraude em pagamentos online e seus impactos na sociedade, bem como os principais métodos e formas de tentar solucioná-lo. Além disso, serão abordadas as principais técnicas e algoritmos de *Machine Learning (ML)*, bem como, a Mineração dos Dados dentro do processo de *Knowledge Discovery in Databases (KDD)*, e as formas de classificação de um modelo que será aplicado no auxílio à detecção de possíveis fraudes em pagamentos online.

## 2.1 Fraudes em pagamentos online

A fraude em pagamentos online é uma dificuldade enfrentada não somente por comerciantes que possuem *sites* ou aplicativos voltados ao comércio eletrônico, mas também, por instituições bancárias e é um problema a ser resolvido. A fraude dentro do contexto deste trabalho e do comércio eletrônico, pode estar relacionada à compras não identificadas por parte dos usuários legítimos, clonagem de cartões de crédito, roubos de contas de usuários ou clonagem de *sites* de venda. O ato do indivíduo praticar fraude, está atrelado a fatores de decisões racionais relacionado com ganhos financeiros. Segundo o autor Becker (1993), a teoria do Método Simples do Crime Racional aborda as decisões acerca de uma atitude criminosa e afirma que são tomadas de forma racional, levando em consideração a obtenção do retorno desta ação, o risco de ser descoberto e a punição aplicada. Entretanto, Mead et al. (2009) colocam em evidência que a disposição de obter ganhos financeiros e o autodomínio de um indivíduo, geram um comportamento heterogêneo com relação à sua honestidade.

A Federação Brasileira de Bancos (FEBRABAN), realiza pesquisas em diversos bancos nacionais e internacionais que possuem atividades no Brasil, com o objetivo de proporcionar medidas de combate à fraudes em pagamentos ou transações eletrônicas. Através dessas pesquisas é possível extrair e analisar informações relevantes acerca das fraudes em pagamentos online.

O comércio eletrônico brasileiro e as instituições bancárias, sofrem impactos negativos e relativamente grandes com relação as fraudes em transações online. A Confederação Nacional de Dirigentes Lojistas (CNDL), conduziu um estudo em 2019 constatando que, pelo menos 46% dos internautas brasileiros foram vítimas de algum tipo de golpe financeiro nos últimos 12 meses anteriores à pesquisa, significando um público alvo com cerca de 12,1 milhões de pessoas. Estimou-se que o prejuízo total decorrente dessas fraudes nos 12 meses anteriores à pesquisa, chegou a cerca de R$ 1,8 bilhão (FEBRABAN, 2020).

Outra pesquisa foi realizada pelo Serviço de Proteção ao Crédito (SPC), nesse estudo foi constatado que o Microempreendedor Individual (MEI) foi público mais afetado com golpes em transações online no ano de 2018. O estudo revela que 33% dos empresários receberam cheques falsificados ou roubados e 25% receberam transações com cartões de crédito ou débito clonados, esses foram os tipos de fraudes mais sofridas pelos micro e pequenos empresários ao longo de 2018. Cerca de 11% das micro empresas tiveram algum prejuízo financeiro no Brasil (SPC, 2019).

Existem algumas campanhas de conscientização para uma navegação segura, técnicas de efetuar análise de dados nas compras e transações online que são criadas pela própria FEBRABAN, a mesma afirma que a investigação das fraudes no comércio eletrônico se faz necessária para que o ciclo de impunidade dos fraudadores seja interrompido (FEBRABAN, 2020).

### 2.1.1 Tipos de fraudes

A *internet* trouxe consigo a possibilidade das empresas oferecerem e venderem seus produtos de forma rápida e prática, mas isso também trouxe alguns perigos para as pessoas que utilizam essa tecnologia, pois, existem muitas atividades fraudulentas por trás das transações financeiras realizadas na *internet*. As mais utilizadas pelos fraudadores são detalhadas a seguir.

- ***Phishing:*** O *Phishing* é um dos maiores perigos encontrados na *internet*. Essa fraude consiste em clonar *sites* de venda reais e a partir disso criar um site muito semelhante, porém ilícito, com o objetivo de fazer com que os usuários coloquem suas informações como documentos, informações de cartão de crédito, senhas de acesso e informações bancárias. Este tipo de fraude ocorre principalmente com o envio de *e-mails* contendo links de acesso aos sites falsos. Com isso, os *crackers* [1] conseguem realizar compras online com as informações roubadas dos utilizadores (ACFE, 2008).
- ***Pharming:*** O *Pharming* é diferente do *Phishing*, na medida em que, o usuário não precisa clicar em um link para que seja redirecionado para *sites* falsos. O *Pharming* explora vulnerabilidades em sites ou aplicações, a fim de permitir que um *cracker* redirecione os usuários para um *site* ou aplicativo falso, possibilitando que o fraudador receba informações e dados dos usuários e com isso possa efetuar transações online utilizando as informações roubadas (ACFE, 2008).

A FEBRABAN desenvolveu cartilhas a fim de prevenir situações de *Phishing* e *Pharming*, onde os donos de sites ou aplicativos de venda e instituições bancárias são aconselhados a tomar algumas medidas de segurança, como utilizar redes de *internet* seguras, possuir sistemas antifraude e analisar os dados de transações financeiras dos usuários. No entanto, se faz necessário buscar alternativas que possam auxiliar a predizer se uma transação online tem potenciais chances de ser fraudulenta. E uma dessas alternativas se dá através da utilização do aprendizado de máquina (*Machine Learning*).

Uma das formas mais empregadas para resolver problemas em diversas áreas de conhecimento é a utilização de técnicas ou algoritmos de ML dentro do processo de KDD. As técnicas ou algoritmos de *Machine Learning*, podem fornecer métodos de classificação de dados, e com isso o computador pode aprender alguns padrões, sendo útil na predição de fraudes em pagamentos online, ou no auxílio à resolução de problemas em diversas aplicações.

## 2.2 Knowledge Discovery in Databases (KDD)

Em 1989 o termo KDD foi formalizado, devido ao conceito ampliado de buscar conhecimento a partir de bases de dados. O KDD possui diversas definições. Para os autores (FAYYAD; PIATETSKY-SHAPIRO; SMYTH, 1996) ele é um processo não trivial, iterativo e interativo, que visa identificar padrões compreensíveis, novos, válidos e com um potencial grande de serem utilizados a partir de um conjunto de dados. É de responsabilidade do analista de dados e do especialista de domínio, orientar a execução do processo de KDD. Basicamente uma aplicação de KDD possui três componentes: (a) o problema em que será aplicado o processo de KDD; (b) os recursos disponíveis para a solução do problema; e (c) os resultados obtidos a partir da aplicação dos recursos (GOLDSCHMIDT; PASSOS; BEZERRA, 2015).

[1] Cracker: Indivíduo que utiliza de técnicas e recursos tecnológicos para roubar dados de empresas ou usuários na *internet*.

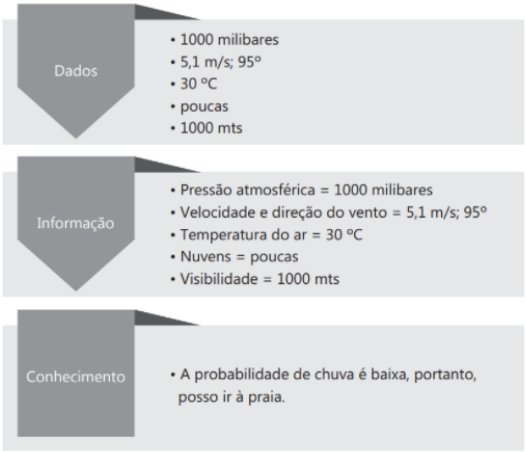
As etapas operacionais do processo de KDD se dividem em três estágios principais, que são:

- **Pré-processamento:** Esta etapa compreende captar, organizar e tratar os dados.
- **Mineração dos Dados:** Onde são definidos alguns algoritmos a serem aplicados a fim de obter conhecimento útil.
- **Pós-processamento:** Tem como principal característica o tratamento do conhecimento obtido na Mineração dos dados, tendo como objetivo facilitar a avaliação e a interpretação no que diz respeito ao conhecimento descoberto (GOLDSCHMIDT; PASSOS; BEZERRA, 2015).

### 2.2.1 Mineração dos Dados

A Mineração dos Dados é a principal etapa dentro do processo de KDD, onde, a partir dos dados busca-se obter conhecimentos novos e úteis, por isso alguns autores até classificam a Mineração dos Dados como sinônimo do processo de KDD (GOLDSCHMIDT; PASSOS; BEZERRA, 2015). Na Figura 1, podemos ver um exemplo de transformação de dados em conhecimento útil.

Figura 1 – Exemplo da diferença entre dados, informação e conhecimento.




Fonte: Castro e Ferrari (2016)

A etapa de Mineração dos Dados dentro do processo do KDD corresponde em aplicar algoritmos capazes de extrair conhecimento a partir dos dados pré-processados. Ainda nesta etapa serão discutidas algumas técnicas de análise descritiva, agrupamento, predição, associação e detecção de anomalias. E por fim é realizado a avaliação ou validação do conhecimento, que visa identificar os conhecimentos úteis e não triviais obtidos (CASTRO; FERRARI, 2016). Dentro da etapa de Mineração dos Dados são realizadas diversas atividades, como a análise exploratória dos dados e aplicação de algoritmos de *Machine Learning*.

#### 2.2.1.1 Machine Learning (ML)

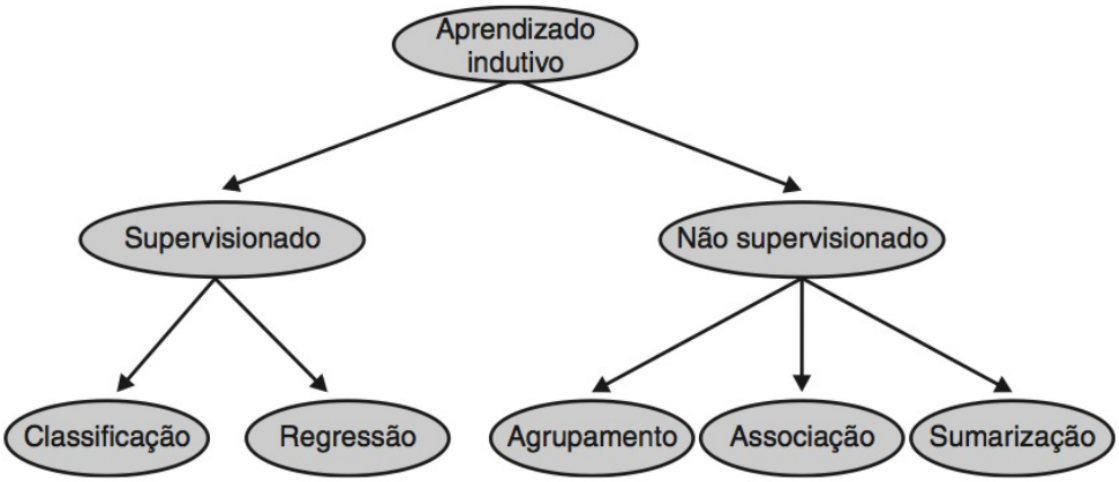
Na literatura foram encontradas diversas definições de *Machine Learning*, uma delas é a apresentada por Mitchell (1997) que define ML como a capacidade de melhorar o desempenho na realização de alguma tarefa por meio da experiência. O ML, visa gerar um modelo que resgata a essência dos dados, podendo assim, realizar predições com dados que o modelo ainda não conhece.

O aprendizado de máquina (*Machine Learning*), faz parte da Mineração dos Dados que é uma das últimas etapas dentro do processo de KDD. Esta etapa consiste em programar os computadores para

que eles aprendam com experiências passadas, e para isso, eles empregam um princípio de inferência denominado indução, onde a máquina consegue obter conclusões genéricas a partir de um conjunto particular de exemplos. Com isso, os algoritmos de ML aprendem a induzir uma função ou hipótese capaz de resolver um problema, utilizando como base os dados obtidos, que representam as instâncias do problema a ser resolvido (FACELI et al., 2011).

Os algoritmos de ML têm sido bastante utilizados em diversas tarefas, que podem ser classificadas mediante à diferentes critérios. Um desses algoritmos remete-se ao paradigma que irá lidar com a tarefa. Ele divide as tarefas de aprendizado em: a) Preditivas e b) Descritivas. As tarefas preditivas e descritivas fazem parte do aprendizado indutivo, no qual são realizadas as generalizações com base nos dados, para que em seguida, obtenha-se os aprendizados supervisionados (preditivos) e não supervisionados (descritivos). As tarefas supervisionadas são divididas de forma genérica, em classificação e regressão e as não supervisionadas são divididas em agrupamento, associação e sumarização (FACELI et al., 2011). Essa hierarquia de aprendizado pode ser observada com mais detalhes na Figura 2.

Figura 2 – Hierarquia de aprendizado.




Fonte: Faceli et al. (2011)

Neste trabalho será utilizado o modelo de aprendizado supervisionado, no qual, serão utilizados algoritmos de classificação para predizer se a transação eletrônica possui potenciais características de fraude. Os dados a serem analisados estão relacionados a diversos fatores dentro do processo de compra, como, por exemplo, o tempo que o usuário permaneceu no site ou aplicativo de compra, dados pessoais que ele inseriu na plataforma, dados de cartão de crédito, dados bancários, chaves de pix, entre outros.

#### 2.2.1.1.1 Classificação

A classificação das coisas acontece quase sempre na vida cotidiana. Para o autor Bramer (2007), a classificação consiste na divisão de objetos de forma que cada um seja atribuído a um de um número de categorias, mutuamente exaustivas e exclusivas conhecidas como classes. Isso significa que cada objeto deve pertencer a apenas uma classe e ser atribuído precisamente a uma única classe. Podemos citar como exemplos de algoritmos, a Árvore de Decisão, a Regressão Logística, Classificação Bayesiana, Redes Neurais, entre outros.

Os algoritmos mais utilizados para predizer se uma transação financeira online tem grande potencial de ser fraudulenta, são: a Árvore de Decisão, a Regressão Logística e o algoritmo dos vizinhos mais próximos (k-NN). Segundo o estudo realizado por Adepoju et al. (2019), esses são os métodos que possuem mais assertividade quando se trata de classificar uma transação online em categoria de fraude ou não fraude. São utilizados como base para este trabalho os algoritmos da Regressão Logística e da Árvore de Decisão, além das métricas de acurácia, precisão, revocação, *Area Under the ROC Curve and Receiver Operating Characteristic (AUC ROC)* e Matriz de Confusão para avaliação dos modelos.

#### 2.2.1.1.2 Regressão Logística

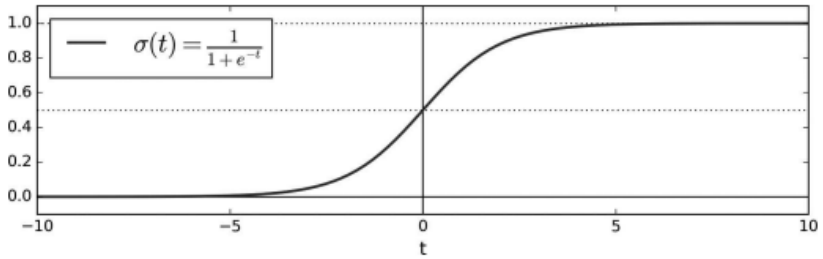
A Regressão Logística é uma técnica estatística, seu principal objetivo é construir um determinado modelo que permite a predição de valores, onde é empregada uma variável categórica a partir de um conjunto de observações. A partir desse modelo gerado é possível calcular ou prever a probabilidade de um evento ocorrer, dado uma observação aleatória.

A Regressão Logística é um algoritmo comumente utilizado em problemas de classificação, pois uma de suas características é produzir um valor correspondente à capacidade de pertencer a uma determinada classe, por exemplo, um determinado e-mail tem 30% de chances de ser spam. Quando a probabilidade estimada pelo algoritmo é maior do que 50%, o modelo consegue prever que a instância pertence a uma determinada classe que é chamada de classe positiva, identificada como 1. Caso contrário, se a probabilidade for menor do que 50% o modelo prevê que a instância pertence à classe negativa, identificada como 0. Isso faz com que o algoritmo se transforme em um classificador binário. Para estimar as probabilidades, o modelo realiza uma soma ponderada das características de entrada, o resultado desse cálculo é a logística (GERON, 2019).

A logística é basicamente uma função sigmóide, que irá resultar em um número entre 0 e 1. Sua definição é mostrada na Equação 2.1 e na Figura 3.

$$\sigma(t) = \frac{1}{1 + exp(-t)} \tag{2.1}$$

Figura 3 – Função Logística.




Fonte: Geron (2019)

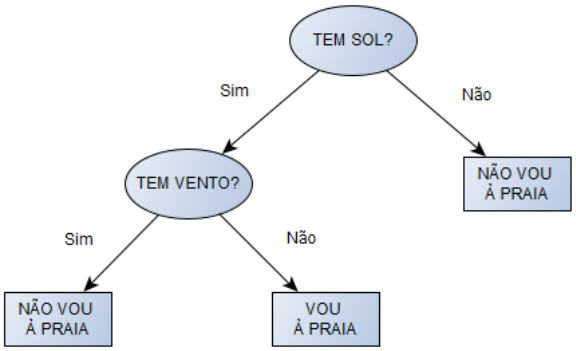
A partir da classificação binária dos dados, o algoritmo prevê 1 se p=$\theta^r$.x for positivo, e se for negativo ele prevê 0. Com isso é possível treinar um modelo que irá conseguir predizer novos valores a partir de novas instâncias de dados aleatórias. O treinamento do modelo tem como objetivo definir o vetor do parâmetro $\theta$, sendo assim o modelo irá estimar probabilidades altas quando a previsão for 1 (positiva) e baixas probabilidades quando a previsão for 0 (negativa) (GERON, 2019). Essa ideia é incorporada pela função de custo, levando em conta uma única instância **y** mostrada na Equação 2.2.

$$c(\theta) = \begin{cases} -log(p) & se \quad y = 1, \\ -log(1-p) & se \quad y = 0. \end{cases} \tag{2.2}$$

#### 2.2.1.1.3 Árvore de Decisão

Uma Árvore de Decisão utiliza a estratégia dividir para conquistar para resolver problemas de classificação. O algoritmo da Árvore de Decisão consiste em dividir um problema complexo em um problema mais simples e de forma recursiva, aplicando a mesma estratégia consecutivamente. As soluções dos subproblemas vão sendo combinadas, na forma de uma árvore, para que assim possa produzir uma solução do problema complexo (FACELI et al., 2011). Na Figura 4, pode-se ver um exemplo simples de Árvore de Decisão, aplicado à um problema de decisão para ir à praia, onde cada retângulo representa uma classe e cada elipse representa um teste em um determinado atributo.

Figura 4 – Exemplo de Árvore de Decisão.




Fonte: Elaborada pelo autor.

Essa é a ideia por trás dos algoritmos que tem base em Árvores de Decisão, como: ID3 (QUINLAN, 1979), ASSISTANT (CESTNIK; BRATKO; KONONENKO, 1987), CART (BREIMAN et al., 1984), C4.5 (QUINLAN, 1993). De modo formal, uma Árvore de Decisão é um grafo acíclico direcionado, em que cada nó é um nó de divisão com dois ou mais sucessores, ou um nó folha. Um nó folha é rotulado com uma função, a qual, é a constante que minimiza a função de custo. Em problemas de classificação essa constante é a moda, já em problemas de regressão, a constante que minimiza a função de custo do erro médio quadrático é a média, quanto que para a função de custo do desvio absoluto é a mediana (FACELI et al., 2011).

Conforme a Árvore de Decisão vai sendo construída, ela pode ser usada para a classificação de novos dados, então é possível obter uma classe ou um valor de resposta a cada observação. Através do conjunto de perguntas na árvore, cada uma das novas observações vai chegar em um dos nós terminais da árvore, se tornando a classe dominante. A classe dominante é a classe que possui a maior quantidade de observações no nó atual. Por exemplo, um nó com 5 observações da classe 1, duas observações da classe 2 e 0 observações da classe 3, terá a classe 1 como classe dominante (BREIMAN et al., 1984).

# 3 ESTADO DA ARTE DA ÁREA PESQUISADA

O processo de pesquisa e seleção dos trabalhos relacionados, foi realizado com base em um mapeamento sistemático sobre as pesquisas com propostas para resolver o problema de fraudes em pagamentos online utilizando técnicas de ML. Esta revisão resultou na identificação e seleção dos principais trabalhos de pesquisa relacionados ao tema deste trabalho. Outro objetivo deste mapeamento sistemático foi verificar os métodos utilizados para auxiliar na detecção de fraudes em pagamentos online de maneira que possam ser aplicados neste projeto de forma satisfatória.

## 3.1 Mapeamento Sistemático da Literatura

Na etapa de Mapeamento Sistemático da Literatura se faz necessário realizar as tarefas de definição de questões de pesquisa e *strings* de busca, realizar uma pesquisa de estudos iniciais mais relevantes, seleção dos documentos encontrados na pesquisa e extração dos dados selecionados. Foi utilizada a ferramenta Parsifal [1] para registrar o processo de definição da *string* de busca, buscar e salvar os artigos, bem como realizar as classificações necessárias com base nos critérios selecionados.

Para realizar a pesquisa foi utilizada a seguinte questão: Como as técnicas de *Machine Learning* têm sido aplicadas na identificação de fraude em pagamentos online? A partir desta pergunta foram extraídas as palavras que nos auxiliaram a montar a *string* de busca e realizar as consultas nas bases de dados selecionadas. Podemos ver as palavras selecionadas juntamente com os seus sinônimos na Tabela 1.

Tabela 1 – Tabela com palavras-chave e sinônimos.

| **Palavra-chave** | **Sinônimos** |
|---|---|
| Detection | Classification |
| Machine Learning | Data mining,<br>Incremental learning,<br>Online learning |
| Payment fraud | Payment cheating,<br>Payment scam |

Fonte: Elaborada pelo autor.

São listadas na Tabela 2 as bases de dados onde foram pesquisados os artigos juntamente com a string de busca utilizada e o número de artigos que foram retornados da busca. Podemos notar que, a mesma string de busca foi utilizada para pesquisar nas três bases de dados.

Tabela 2 – Tabela com as bases de dados e artigos.

| **Base de Dados** | **Artigos** | **String de Busca** |
|---|---|---|
| ACM Digital Library | 17 | ("detection"OR "classification") AND ("machine learning" OR "data mining"OR "incremental learning"OR "ML"OR "online learning") AND ("payment fraud"OR "payments cheating"OR "payments scam") |
| IEEE Digital Library | 7 | |
| Scopus | 16 | |

Fonte: Elaborada pelo autor.

[1] https://parsif.al/

### 3.1.1 Critérios de Inclusão

Foram definidos os seguintes critérios de inclusão:

- Nova tecnologia para detectar fraudes em pagamentos online;
- Processo, método, técnica ou algoritmo para detectar fraudes em pagamentos online;
- Sistema para detecção de fraude em pagamentos online.

Os 13 artigos selecionados se adequaram em um ou mais critérios de inclusão dentre os apresentados. Podemos ver na Tabela 3 os artigos selecionados junto com os seus respectivos autores:

Tabela 3 – Tabela com os artigos selecionados e seus autores.

| ID | Título do artigo | Autor(a)/Autores |
|---|---|---|
| A1 | Feature engineering strategies based on a One-point Crossover for fraud detection on Big Data Analytics | Soleh, M. and Djuwitaningrum, E.R. and Ramli, M. and Indriasari, M. |
| A2 | Classification-based fraud detection for payment marketing and promotion | He, S. and Zheng, J. and Lin, J. and Tang, T. and Zhao, J. and Liu, H. |
| A3 | LAW: Learning Automatic Windows for Online Payment Fraud Detection | Wang, C. and Wang, C. and Zhu, H. and Cui, J. |
| A4 | Fraud detection on payment transaction networks via graph computing and visualization | Sun, Q. and Tang, T. and Zheng, J. and Lin, J. and Zhao, J. and Liu, H. |
| A5 | The benefits of using artificial intelligence in payment fraud detection: A case study | Soviany, C. |
| A6 | Design and development of financial fraud detection using machine learning | Prasad, J.R. and Saikumar, S. and Subbarao, B.V. |
| A7 | An Automated Feature Engineering Method for Online Payment Fraud Detection | Wang, C. and Wang, C.-Q. |
| A8 | Electronic payment fraud detection using supervised and unsupervised learning | Pracidelli, L.P. and Lopes, F.S. |
| A9 | Unsupervised Machine Learning for Card Payment Fraud Detection | Parreno-Centeno, M. and Ali, M.A. and Guan, Y. and Moorsel, A. |
| A10 | Automatic Machine Learning algorithms for fraud detection in digital payment systems | Kolodiziev, O. and Mints, A. and Sidelov, P. and Pleskun, I. and Lozynska, O. |
| A11 | Comparative Evaluation of Credit Card Fraud Detection Using Machine Learning Techniques | Adepoju, O. and Wosowei, J. and Lawte, S. and Jaiman, H. |
| A12 | Study on Machine Learning Techniques with Conventional Tools for Payment Fraud Detection | Vidanelage, H.M.M.H. and Tasnavijitvong, T. and Suwimonsatein, P. and Meesad, P. |
| A13 | Fraud detection within bankcard enrollment on mobile device based payment using machine learning | Zhou, H. and Chai, H.-F. and Qiu, M.-L. |

Fonte: Elaborada pelo autor.

Todos os artigos selecionados dizem respeito à formas de detecção de fraudes em pagamentos online, utilizando Mineração de Dados dentro do processo de KDD e técnicas de ML.

### 3.1.2 Critérios de Exclusão

Foi aplicada a pesquisa inicial nas bases de dados utilizando a *string* de busca, excluindo os artigos que se enquadraram nos critérios de exclusão mostrados na Tabela 4.

Tabela 4 – Tabela com os critérios de exclusão.

| **Critério de Exclusão** | **Nº de artigos recusados** |
|---|---|
| O estudo apresenta resultados fora da área de pesquisa | 15 |
| O estudo é duplicado | 6 |
| O estudo é uma versão antiga de outro estudo | 4 |
| O estudo não é um estudo primário | 2 |

Fonte: Elaborada pelo autor.

A pesquisa teve no início um total de 40 artigos, que foram extraídos das três bases de dados. Depois de ter aplicado os critérios de exclusão restaram apenas 13 artigos. Dos 40 artigos, 15 deles foram eliminados pelo critério de O estudo apresenta resultados fora da área de pesquisa, indicando que o estudo aborda uma área diferente da proposta. Pelo critério de "O estudo é duplicado", foram eliminados 6 artigos, ainda 4 artigos foram eliminados pelo critério de "O estudo é uma versão antiga de outro estudo", caracterizando que o artigo foi baseado em um estudo já ultrapassado. Por fim, 2 artigos foram eliminados pelo critério de "O estudo não é um estudo primário", isso significa que o artigo comumente se trata de uma revisão sistemática.

## 3.2 Análise dos trabalhos selecionados

Na última etapa do Mapeamento Sistemático da Literatura foram extraídos os dados dos artigos selecionados. As técnicas de ML mais utilizadas na maioria dos trabalhos são, a Árvore de Decisão (A1-A2-A5-A6-A7-A10-A12-A13), que busca predizer possíveis fraudes financeiras com base em técnicas e algoritmos de classificação, rede neural (A3-A4-A8-A9-A12), onde são abordadas técnicas de regressão e classificação, floresta aleatória (A6-A13), que apresentam formas de resolver problemas de classificação e a Regressão Logística (A6-A11), onde os principais métodos utilizados são algoritmos de classificação. Outras técnicas foram utilizadas em menor frequência, sendo, regressão do vetor de suporte (A6-A2), que busca predizer fraudes com algoritmos de regressão e Naïve Bayes (A11), buscando através do algoritmo de Naïve Bayes predizer possíveis fraudes financeiras.

Também foram identificadas as formas com que os autores abordam o problema e quais conclusões obtiveram com os resultados. Os que utilizaram algoritmos de classificação para resolução da problemática, definiram que estas são as melhores técnicas para resolver problemas de decisão. Já os que utilizaram algoritmos de regressão afirmaram que ficaram insatisfeitos com os resultados obtidos com relação aos problemas de decisão, embora tenham conseguido atingir os objetivos da pesquisa.

# 4 METODOLOGIA

Para este trabalho, foi adotada uma pesquisa aplicada voltada à obtenção do conhecimento e com o objetivo de empregá-la no auxílio à resolução do problema de fraudes em pagamentos online. Este projeto teve início com uma pesquisa exploratória aplicada à bibliografia, nesta pesquisa foi realizado um Mapeamento Sistemático da Literatura para obter o conhecimento dos principais métodos, técnicas ou algoritmos que auxiliam na predição de fraudes em pagamentos online, por meio do aprendizado de máquina (*Machine Learning*).

Após a pesquisa realizada, foi obtido um *dataset* contendo os dados das transações online, onde os dados estavam adequadamente anonimizados. Após a obtenção do *dataset* foram realizados os processos de limpeza, seleção, transformação e mineração dos dados, e por fim, a aplicação das técnicas de ML. Os dados utilizados neste trabalho foram obtidos por meio de um repositório público chamado Kaggle [1]. Para a realização das tarefas mencionadas acima foi utilizado a linguagem de programação Python, juntamente com as bibliotecas Pandas [2] e Scikit-Learn [3] e o ambiente de desenvolvimento Google Colab [4].

A seguir, são apresentados os passos para desenvolvimento e avaliação do trabalho. Para que seja possível realizar a seleção correta dos dados e o modelo consiga obter um bom desempenho durante o seu treinamento, devem ser aplicadas algumas técnicas de Mineração dos Dados, como por exemplo, a análise exploratória e o balanceamento dos dados, os quais são explicados nas seções 4.1 e 4.2. Ainda no processo de criação de um modelo de ML, deve-se mencionar a capacidade de realizar testes do modelo como descrito na seção 4.3, bem como suas métricas de avaliação mostradas na seção 4.4.

## 4.1 Análise Exploratória dos Dados

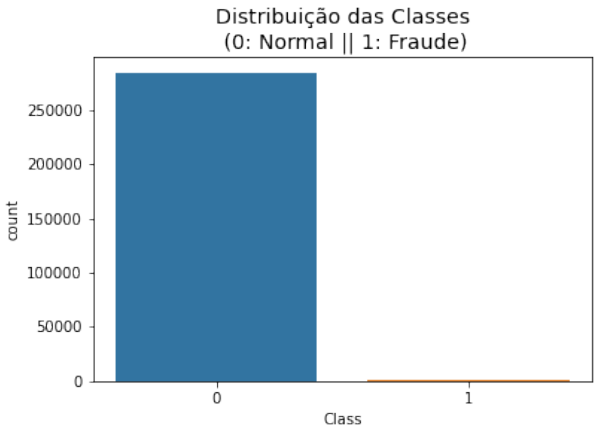
A análise exploratória dos dados, por muitas vezes, é exigida dentro do processo do KDD. Ela deve acontecer para que o pesquisador ou cientista de dados consiga obter o maior número possível de observações acerca dos dados que estão sendo trabalhados, sendo essas, padrões e dentro de cada padrão muitas variáveis (atributos, entradas). O objetivo da análise exploratória dos dados é captar e/ou explorar informações a partir desses dados, utilizando técnicas estatísticas (JHONSON, 1998).

O *dataset* utilizado neste trabalho possuía no total 31 colunas e 284.807 entradas. Foi constatado que o mesmo não possuía nenhum dado nulo ou faltante. Além disso, a maioria das variáveis estavam padronizadas com exceção das colunas Class, Time e Amount.

[1] https://https://www.kaggle.com/mlg-ulb/creditcardfraud
[2] https://pandas.pydata.org/
[3] https://scikit-learn.org/stable/
[4] https://colab.research.google.com/?hl=pt_BR

A partir da análise exploratória dos dados, foi possível constatar que apenas 0,17% das transações eram de origem fraudulenta, isso caracteriza um desbalanceamento dos dados como pode ser visto na Figura 5. Dentro de um *dataset* que possui 284.807 transações, praticamente 99% das transações são de origem legítima, logo se faz necessário realizar um balanceamento dos dados.

Figura 5 – Análise dos dados de transações.



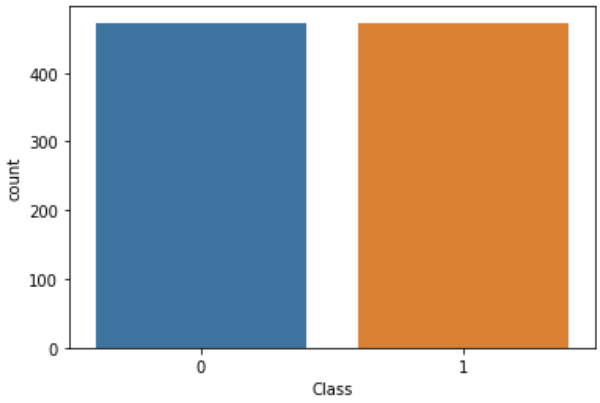

Fonte: Elaborada pelo autor.

## 4.2 Balanceamento dos Dados

Pode-se dizer que um conjunto de dados é considerado desbalanceado, quando há uma desproporção muito grande no número de exemplos de uma ou mais classes com relação às demais. É possível observar, por exemplo, um estudo de caso de uma central telefônica, onde o número de trotes é muito menor do que o número de ligações legítimas, ou seja, existe uma grande desproporção entre o número de exemplos da classe de ligações legítimas e a classe das chamadas falsas. Em situações assim, os algoritmos de ML não conseguem realizar uma classificação satisfatória dos dados, pois os exemplos das classes com menor proporção não são classificados corretamente, sendo assim, ocorre que o algoritmo poderá classificar os dados que não são legítimos de forma errada (BRAGA, 2011).

No procedimento de balanceamento dos dados, foi construído um novo *dataset* com 50% dos dados originários de transações fraudulentas e os outros 50% com dados originários de transações legítimas. Os dados de transações fraudulentas foram mantidos e os dados de transações legítimas foram escolhidos de forma aleatória, o restante dos dados dessa classe foram excluídos. Esse método de balanceamento se chama subamostragem aleatória (*undersampling*), onde os exemplos que irão compor o novo *dataset* são escolhidos de forma aleatória. Após a aplicação do balanceamento dos dados, a quantidade de exemplos selecionados para a classe de fraude (1) e para a classe de não-fraude (0) foi de 473, como pode ser observado na Figura 6.

Figura 6 – *Dataset* após o balanceamento dos dados.




Fonte: Elaborada pelo autor.

## 4.3 Treino e Teste

Antes de aplicar as técnicas de aprendizado de máquina, o *dataset* (100%) foi dividido em duas partes, uma parte para treino (70%) e a outra para teste (30%). Assim foi necessário para evitar problemas de *Overfitting*. O *Overfitting* acontece quando o modelo treinado se ajusta muito bem ao conjunto de dados anteriormente observado, mas, se mostra ineficaz para prever novos resultados com base em dados novos (DOMINGOS, 2012). Antes de ser realizado a divisão, os dados são misturados para que a sequência deles não interfira no processo de treinamento do modelo. Após a base de dados ser dividida dessa forma, é possível treinar o modelo para predizer se uma transação tem potenciais chances de ser fraudulenta com base em novos dados de entrada.

É possível observar na Figura 7 a divisão do *dataset*, onde o valor 0.7 atribuído à variável *"train_size"* corresponde aos 70% do *dataset* reservado para treino.

Figura 7 – Divisão do dataset em treino e teste.

```
[ ]  1 #dividindo o dataset
     2 X_train, X_test, y_train, y_test = train_test_split(X,y, train_size=0.7)
```

Fonte: Elaborada pelo autor.

## 4.4 Validação do Modelo

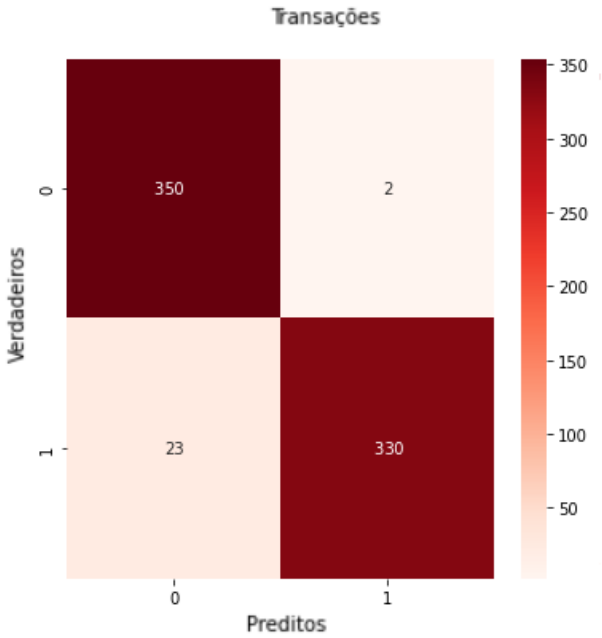
Para realizar a validação do modelo, foram empregadas métricas de avaliação de desempenho nos algoritmos de ML. As métricas comumente utilizadas são a acurácia, a precisão e a revocação, além de outras como a AUC ROC e a matriz de confusão.

### 4.4.1 Matriz de Confusão

A matriz de confusão, na maioria das vezes, é representada em forma de tabela que permite a visualização dos erros e acertos do algoritmo, bem como, os falsos-negativos (quando o algoritmo classifica algo verdadeiro como falso) e os falsos-positivos (quando o algoritmo classifica algo falso como verdadeiro). Em um problema de classificação onde o algoritmo é um classificador binário, a matriz de confusão terá duas colunas (Verdadeiro e Falso) ou (0 ou 1).

Na Figura 8 pode ser observada a matriz de confusão das transações, onde a diagonal principal contém as predições verdadeiras-positivas e verdadeiras-falsas. Já na diagonal oposta estão dispostos os falsos-positivos e os falsos-negativos que representam as classificações que o algoritmo fez de forma incorreta. No *dataset* utilizado com as transações fraudulentas e não-fraudulentas, se faz necessário identificar os casos onde existam falsos-positivos, pois se o algoritmo definir uma transação fraudulenta como sendo legítima, logo ele não estará cumprindo com o seu objetivo principal que é predizer transações fraudulentas com a maior precisão possível. No caso do algoritmo classificar transações legítimas como sendo fraudulentas, o problema não será tão grave, pois já que a transação é legítima a empresa não teria prejuízos financeiros com estornos ou *cashbacks*.

Figura 8 – Matriz de confusão das transações online.




Fonte: Elaborada pelo autor.

### 4.4.2 Métricas de Desempenho

As métricas de avaliação de desempenho mais comuns, utilizadas em problemas de classificação são: a acurácia, a precisão, a revocação, entre outras. Ainda podem ser utilizadas outras métricas como a AUC ROC, tais métricas podem assumir outros nomes dependendo de como são empregadas (BRAMER, 2007).

A acurácia é uma métrica que mede a quantidade de classificações corretas do modelo com relação ao número total de exemplos, também chamados de instâncias. Sua fórmula se dá pela soma da quantidade de verdadeiros-negativos VN e a quantidade de verdadeiros-positivos VP, divididos pela quantidade total de exemplos preditos pelo modelo, como é mostrado na Equação 4.1 (BRAMER, 2007). É ideal que um modelo obtenha o maior valor de acurácia possível, pois isso mostra que o algoritmo está acertando cada vez mais.

$$\text{Acurácia} = \frac{VN + VP}{T} \tag{4.1}$$

A revocação é uma métrica calculada em relação a cada classe, onde em cada verificação o algoritmo busca trazer a frequência de cada exemplo encontrado em uma determinada classe. Na Equação

4.2, pode ser observado a presença da variável que representa os falsos-negativos FN, quando menor o valor desta variável, maior será o valor da revocação e consequentemente maior será a taxa de acerto do algoritmo.

$$\text{Revocação} = \frac{VP}{VP + FN} \tag{4.2}$$

A precisão, embora muito parecida com a métrica da revocação, pois seu cálculo também se dá em relação a cada classe, é uma métrica que busca encontrar dentre os exemplos classificados como sendo de uma determinada classe, quantos realmente pertencem a essa classe. Para realizar este cálculo é inserido na sua função a variável que representa os Falsos-Positivos FP, como é mostrado na Equação 4.3.

$$\text{Precisão} = \frac{VP}{VP + FP} \tag{4.3}$$

Além das métricas apresentadas acima, outra métrica que também é bastante utilizada para avaliar o desempenho de modelos classificadores é a AUC ROC, ou também conhecida como área sob a curva. A curva AUC é derivada da curva ROC, então deve-se compreender inicialmente a curva ROC (YANG; BERDINE, 2017).

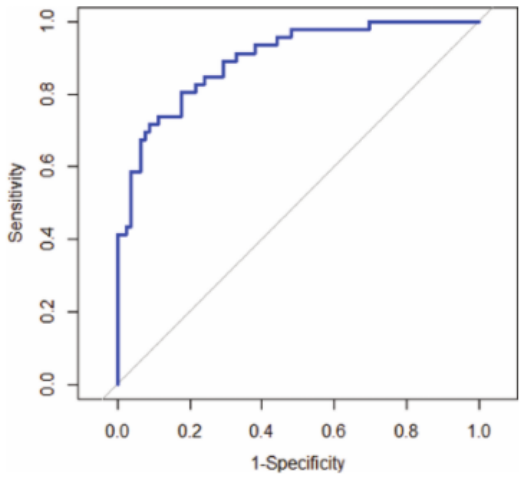
A curva ROC (*Receiver Operating Characteristic*), busca avaliar o quão bom o modelo pode distinguir entre duas classes, podendo ser elas 0 ou 1, ou positivo e negativo. A ROC possui dois parâmetros: Taxa de Verdadeiro Positivo TVP e Taxa de Falso Positivo TFP, os quais são mostrados com detalhes nas Equações 4.4 e 4.5.

$$\text{TVP} = \frac{VP}{VP + FN} \tag{4.4}$$

$$\text{TFP} = \frac{FP}{FP + VN} \tag{4.5}$$

A curva AUC (*Area Under the ROC Curve*), é praticamente uma forma de resumir a curva ROC em um único valor calculando a área sob a curva. O valor da AUC pode variar entre 0,0 e 1,0 como pode ser observado na Figura 9 e o limiar entre a classe, ou seja, seu ponto central é de 0,5. Sendo assim, se o valor da AUC ficar acima do limite limiar, o algoritmo classifica em uma determinada classe e se ficar abaixo ele classifica em outra classe.

Figura 9 – Exemplo de curva AUC.




Fonte: Yang e Berdine (2017).

## 4.5 Desenvolvimento do Protótipo

Com base nas técnicas de Regressão Logística e da Árvore de Decisão, aplicadas sobre os dados de transações online, foi desenvolvido um protótipo para predição de fraudes em pagamentos online, utilizando a linguagem *Python* juntamente com algumas bibliotecas usadas para trabalhar com algoritmos de ML.

Para a utilização do modelo de ML, foi desenvolvida uma aplicação *web* que permite receber novos dados de entrada, interagir com o modelo de *ML* e apresentar resultados em tempo real através de uma interface gráfica. A aplicação foi desenvolvida utilizando uma biblioteca do *Python* chamada *Streamlit*[1]. Esta biblioteca é compatível com diversos *frameworks* de *ML*, como por exemplo, o Scikit Learn[2] utilizado neste trabalho.

[1] https://streamlit.io/
[2] https://scikit-learn.org/stable/

# 5 RESULTADOS

Neste capítulo serão descritos os modelos de Regressão Logística e da Árvore de Decisão utilizados neste trabalho, além de sintetizar os principais resultados obtidos através da aplicação desses modelos nos dados de transações online.

O *dataset* utilizado neste trabalho possui 30 colunas, sendo essas, contendo variáveis representadas como V1,V2,V3,V4...V27 e V28, com exceção das variáveis Class, Time e Amount. Nesse caso, para que possamos fazer com que o algoritmo ganhe desempenho no processo de classificar os dados, podemos em cada execução ajustar os *hyperparameters* que são os parâmetros padrões utilizados pelas bibliotecas do *Python*, assim conseguimos otimizar os algoritmos de *ML* para que consigam obter maior desempenho em suas predições.

## 5.1 Modelo de Regressão Logística

Para este modelo, foram estabelecidos os parâmetros padrões da biblioteca Scikit Learning, com exceção da variável "*random_state*", que traz valores aleatórios para as variáveis em cada iteração do modelo. O objeto classificador foi criado e armazenado na variável "model_lr", como mostra a Figura 10.

Figura 10 – Criação do classificador usando Regressão Logística.

```
4 #2. Instanciar o modelo
5 model_lr = LogisticRegression(random_state=42)
```

Fonte: Elaborada pelo Autor.

Em seguida, após a criação do objeto classificador, o modelo foi treinado com os parâmetros definidos anteriormente na divisão do *dataset*. Na Figura 11 é possível observar o treinamento do modelo utilizando o método *fit* e as variáveis pré-definidas.

Figura 11 – Treinamento do modelo de Regressão Logística.

```
8 #3. Fit do modelo
9 model_lr.fit(X_rand, y_rand)
```

Fonte: Elaborada pelo Autor.

Após a realização do treinamento do modelo, foi definido as novas variáveis de entrada como teste para verificar se o modelo tem potencial para predizer se uma transação é fraudulenta ou não-fraudulenta. Este processo consiste em utilizar o método *predict*, passando como parâmetro a variável de teste *X_test*, como pode ser observado na Figura 12.

Figura 12 – Predição da Regressão Logística.

```
11 #5. Fazer previsões em cima dos novos dados
12 y_pred_lr = model_lr.predict(X_test)
```

Fonte: Elaborada pelo Autor.

## 5.2 Modelo da Árvore de Decisão

No modelo de Árvore de Decisão, também foram estabelecidos os parâmetros padrões da biblioteca Scikit Learning, com exceção da variável *max_depth* na qual é definido o número máximo de arestas que a árvore irá possuir. A Figura 13 mostra a criação do objeto classificador, que é armazenado na variável *model_tree*.

Figura 13 – Criação do classificador usando Árvore de Decisão.

```
#2. Instanciar o modelo e escolher os hyperparametros
model_tree = DecisionTreeClassifier(max_depth=12)
```

Fonte: Elaborada pelo Autor.

Em seguida, na Figura 14 pode ser observado o treinamento do modelo de Árvore de Decisão utilizando o método *fit*, juntamente com os parâmetros de teste definidos na divisão dos dados.

Figura 14 – Treinamento do modelo de Árvore de Decisão.

```
#3. Fit do modelo
model_tree.fit(X_rand, y_rand)
```

Fonte: Elaborada pelo Autor.

Após o treinamento do modelo, o classificador da Árvore de Decisão recebeu um novo conjunto de dados de teste para predizer a qual classe eles pertencem. Pode-se observar na Figura 15 essa etapa do processo, onde foi atribuído ao classificador o método *predict* junto com os dados de teste e armazenado na variável *y_pred_tree*.

Figura 15 – Treinamento do modelo de Árvore de Decisão.

```
#Fazer previsões em cima dos novos dados
y_pred_tree = model_tree.predict(X_test)
```

Fonte: Elaborada pelo Autor.

## 5.3 Avaliação do Modelo

O modelo de Regressão Logística foi avaliado utilizando as métricas mencionadas na seção 4.4. Pode-se observar na Figura 16 que o modelo obteve em seu melhor resultado uma média de precisão de 95% após duas execuções, a revocação e a acurácia também apresentaram uma taxa de 95%, isso mostra que o modelo teve um bom desempenho ao realizar predições com base em novos dados.

Figura 16 – Métricas aplicadas à Regressão Logística.

```
Utilizando Regressão Logística:

              precision    recall  f1-score   support

           0       0.94      0.96      0.95       252
           1       0.95      0.93      0.94       221

    accuracy                           0.95       473
   macro avg       0.95      0.95      0.95       473
weighted avg       0.95      0.95      0.95       473
```

Fonte: Elaborada pelo Autor.

Assim como o modelo de Regressão Logística, o modelo da Árvore de Decisão foi avaliado seguindo as mesmas métricas de avaliação de desempenho. O modelo obteve no seu primeiro resultado uma precisão de 85%, e ainda uma revocação e acurácia de 89%, como pode ser observado na Tabela 5. Contudo o algoritmo da Árvore de Decisão não obteve seu melhor modelo.

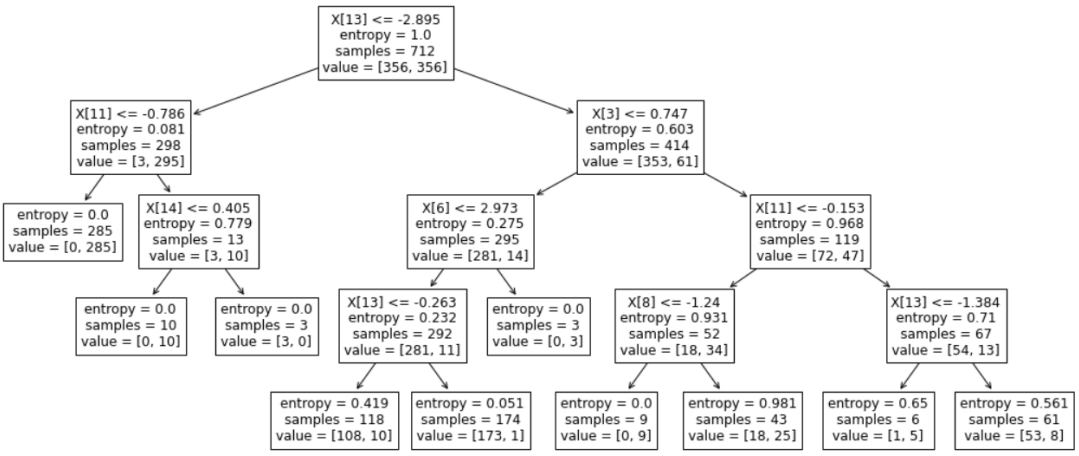
Tabela 5 – Tabela com as métricas obtidas na Árvore de Decisão.

| **Nº Execução** | **Alterações** | **Precisão** | **Revocação** | **Acurácia** | **Classe** |
|---|---|---|---|---|---|
| 1 | - | 85% | 89% | 89% | "Não-fraude" |
| | | 82% | 89% | | "Fraude" |
| 2 | "max_depth"= 4 | 89% | 90% | 91% | "Não-fraude" |
| | | 83% | 89% | | "Fraude" |
| 3 | Inclusão do critério de Entropia | 94% | 92% | 93% | "Não-fraude" |
| | | 92% | 93% | | "Fraude" |

Fonte: Elaborada pelo autor.

Após a avaliação da primeira execução do modelo da Árvore de Decisão, foi diminuído o tamanho das arestas da árvore, atribuindo o valor 4 à variável *max_depth* e acrescentado o critério de entropia, que serve para estimar a aleatoriedade da classe a ser predita. Em seguida, pode-se observar na Figura 17 o modelo da Árvore de Decisão que foi gerada, onde as arestas são os retângulos que possuem um valor definido por X[n] e os retângulos que não possuem outras divisões são chamados de nós-folha.

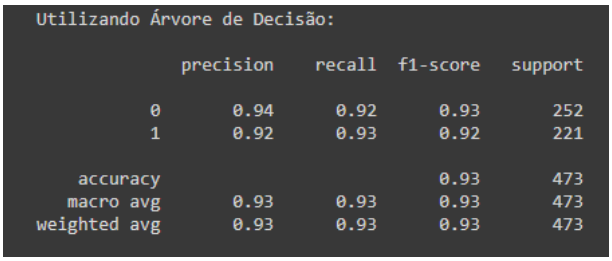
Figura 17 – Árvore de Decisão após a segunda execução.




Fonte: Elaborada pelo Autor.

Após a alteração dos *hyperparameters* do modelo, o mesmo obteve uma média de precisão e revocação de 93%, além da acurácia também de 93%, como é mostrado na Figura 18.

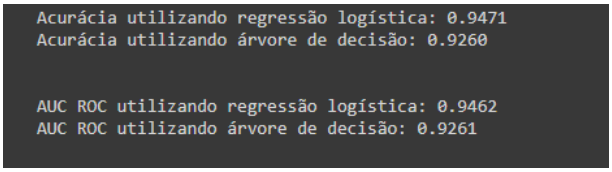
Figura 18 – Métricas de avaliação após a segunda execução.




Fonte: Elaborada pelo Autor.

Para que se possa extrair uma informação correta acerca da avaliação das métricas de desempenho, muitas vezes se faz necessário comparar uma técnica com a outra, assim a avaliação do modelo se torna mais precisa. Após o treinamento do modelo e avaliação utilizando as métricas mencionadas acima, foi aplicado a métrica de avaliação de desempenho AUC ROC, como pode ser observado na Figura 19, onde o algoritmo de Regressão Logística obteve uma taxa de 94% e o algoritmo da Árvore de Decisão 92%. Sendo assim, pode ser definido que esses foram os melhores modelos obtidos, pois os valores da acurácia e da curva AUC ROC são muito parecidos.

Figura 19 – Resultado da avaliação dos modelos.




Fonte: Elaborada pelo Autor.

Em uma breve comparação entre os modelos da Árvore de Decisão e da Regressão Logística, podemos notar através da Tabela que o modelo de Regressão Logística obteve um desempenho maior com relação ao modelo de Árvore de Decisão, levando em consideração a média dos valores obtidos pela acurácia de 93% e da precisão 92%, sendo que para o modelo de Árvore de Decisão a média da acurácia foi de 89% e da precisão 85%.

Tabela 6 – Tabela com o resultado da avaliação dos modelos.

| **Regressão Logística** | | | **Árvore de Decisão** | | |
|---|---|---|---|---|---|
| Nº de execuções | Acurácia | AUC ROC | Nº de execuções | Acurácia | AUC ROC |
| 2 | 95% | 95% | 3 | 93% | 93% |

Fonte: Elaborada pelo Autor.

## 5.4 Desenvolvimento da aplicação

A aplicação foi desenvolvida utilizando a linguagem *Python* juntamente com a biblioteca *Streamlit*, seu objetivo é realizar predições de fraude ou não-fraude em tempo real utilizando técnicas de ML. Pode-se observar na Figura 20 que o aplicativo apresenta de forma gráfica os dados inseridos pelo usuário, bem como o resultado da predição realizada pelo algoritmo de ML.

Figura 20 – Interface do aplicativo de predição.


Fonte: Elaborada pelo Autor.

Para que o usuário possa definir os parâmetros de entrada, foi criado uma interface no aplicativo com um conjunto de elementos da biblioteca Streamlit, chamados de *Sliders*, que podem ser manipulados. A medida que o usuário manipula esses controles, o aplicativo recebe novos valores de entrada e realiza predições com base nesses novos dados. Os controles possuem valores mínimos e máximos pré-definidos, como pode ser observado na Figura 21. Os valores mínimos e máximos definidos em cada variável, foram extraídos por meio de uma análise estatística do *dataset*.

Figura 21 – Interface de entrada de dados do aplicativo.


Fonte: Elaborada pelo Autor.

Esta aplicação foi desenvolvida para mostrar de forma gráfica como o algoritmo de ML classifica as transações com base em novos dados de entrada, no entanto, para que o modelo seja empregado em um ambiente real é recomendado ofertar o modelo em forma de *webservice*, para que outro aplicativo ou sistema possa consumir este serviço como um detector de fraudes em pagamentos online.

# 6 CONCLUSÕES

Neste trabalho, buscou-se observar a problemática das fraudes em pagamentos online e como ela traz impactos negativos, seja na sociedade como um todo, no ambiente tecnológico, no ambiente governamental ou nos setores financeiros das empresas que possuem comércio eletrônico no Brasil. As fraudes financeiras praticadas na *internet*, também causam impactos negativos na vida financeira de consumidores que buscam ou optam por adquirir seus produtos na *internet*, e é um problema que deve ser combatido.

Através de um Mapeamento Sistemático da Literatura, pôde-se observar os principais métodos ou técnicas para tentar resolver este problema. Os principais estudos levantados, mostram que é possível utilizar a mineração de dados e técnicas de *Machine Learning* para auxiliar na detecção de fraudes em pagamentos online. Ainda através desses estudos, foi possível identificar que a fraude em pagamentos online trata-se de um problema de classificação, dentro do âmbito computacional. Para obter conhecimento mais apurado sobre determinadas técnicas e algoritmos de *Machine Learning*, foi necessário buscar na literatura as principais formas de resolver problemas de classificação, como por exemplo, o algoritmo de Regressão Logística e da Árvore de Decisão utilizados neste trabalho.

A hipótese apresentada neste trabalho de que é possível desenvolver um modelo computacional, que busca prever fraudes em pagamentos online utilizando técnicas de ML, pode ser alcançada. O modelo que se apresentou mais eficaz com relação à precisão ao realizar a classificação dos dados em fraude ou não-fraude, foi o algoritmo da Regressão Logística, segundo as métricas de avaliação aplicadas ao modelo.

Este trabalho pode ser utilizado como base ou ponto de partida para novos trabalhos, podendo ser reaproveitado o modelo de ML desenvolvido para predição, bem como o aplicativo desenvolvido para prever fraudes em pagamentos online com base em novos dados de entrada. Também podem ser utilizadas muitas outras técnicas que venham a contribuir com a melhoria do modelo. Além disso, é possível ofertar o modelo em forma de *webservice*, sendo assim, através de uma integração com outro aplicativo ou sistema este serviço pode ser usado como um detector de transações fraudulentas.

# REFERÊNCIAS


ACFE. *Report To the Nations on Occupational Fraud and Abuse*. 2008. Disponível em: <https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/2008-rttn.pdf>. Acesso em: 27 mai 2021. Citado na página 17.

ADEPOJU, O. et al. *Comparative Evaluation of Credit Card Fraud Detection Using Machine Learning Techniques*. [S.l.]: Scopus, 2019. Citado na página 20.

AGENCIASENADO. *Projetos aumentam punição para quem praticar fraude em canais eletrônicos*. 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/09/28/projetos-aumentam-punicao-para-quem-praticar-fraude-em-canais-eletronicos>. Acesso em: 12 abr 2021. Citado na página 13.

BECKER, G. S. *The Economic Way of Looking at Behavior*. [S.l.]: Journal of Political Economy, 1993. v. 101. 385–409 p. Citado na página 16.

BERTOZZO, R. J. Aplicação de machine learning em dataset de consultas médicas do sus. In: RICHARD (Ed.). *Trabalho Conclusão do Curso submetido ao curso de Sistemas de Informação, Universidade Federal de Santa Catarina, Florianópolis*. [S.l.: s.n.], 2019. Citado na página 14.

BRAGA, C. L. d. C. A. P. *Aprendizado supervisionado com conjunto de dados desbalanceados*. [S.l.: s.n.], 2011. Citado na página 27.

BRAMER, M. *Principles of data mining*. [S.l.]: Springer, 2007. v. 180. Citado 3 vezes nas páginas 13, 20 e 29.

BREIMAN, L. et al. *Classification and Regression Trees*. [S.l.]: Chapman and Hall/CRC, 1984. v. 1. Citado na página 22.

CASTRO, L. N. de; FERRARI daniel G. *Introdução à Mineração de Dados: Conceitos básicos, algoritmos e aplicações*. [S.l.]: Saraiva, 2016. v. 1. Citado na página 18.

CESTNIK, B.; BRATKO, I.; KONONENKO, I. *ASSISTANT 86: A Knowledge-Elicitation Tool for Sophisticated Users*. [S.l.]: DBLP, 1987. v. 1. Citado na página 22.

CONSUMIDORMODERNO. *Índice de tentativas de fraude no e-commerce brasileiro cresce em 2019*. 2021. Disponível em: <https://www.consumidormoderno.com.br/2020/03/13/tentativas-de-fraude-crescem-em-2019/>. Acesso em: 12 abr 2021. Citado na página 13.

DOMINGOS, P. A few useful things to know about machine learning. *Communications of the ACM, ACM New York, NY, USA*, v. 55, n. 10, p. 78–87, 2012. Citado na página 28.

EBIT, W. *WEBSHOPPERS - E-BIT. 42. ed.* 2020. Disponível em: <https://ebit.com.br/webshoppers>. Acesso em: 04 abr 2021. Citado na página 13.

FACELI, K. et al. *Inteligência Artificial-Uma abordagem de aprendizado de máquina*. [S.l.]: GEN | Grupo Editorial Nacional, 2011. v. 1. Citado 3 vezes nas páginas 19, 21 e 22.

FAYYAD, U.; PIATETSKY-SHAPIRO, G.; SMYTH, P. *From Data Mining to Knowledge Discovery: An Overview. Knowledge Discovery and Data Mining*. [S.l.]: AAAI Press, 1996. Citado na página 17.

FEBRABAN. *A importância do binômio prevenção-investigação nas fraudes eletrônicas*. 2020. Disponível em: <https://noomis.febraban.org.br/especialista/renato-opice-blum/a-importancia-do-binomio-prevencao-investigacao-nas-fraudes-eletronicas>. Acesso em: 27 mai 2021. Citado na página 16.

FELIPE, J. J. *Mineração de dados para detecção de fraudes em transações eletrônicas*. Dissertação (Dissertação de Mestrado) — Universidade Federal de Minas Gerais, 2012. Citado na página 14.

FERREIRA, L. D. Técnicas de aprendizado de máquina aplicadas à identificação de perfis de aprendizado em um ambiente real de ensino. In: LUCAS (Ed.). *Monografia apresentada ao Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos.* [S.l.: s.n.], 2016. Citado na página 14.

GERON, A. *Mãos à Obra Aprendizado Máquina com Scikit-Learn e TensorFlow.* [S.l.]: Alta Books, 2019. v. 1. Citado 2 vezes nas páginas 20 e 21.

GOLDSCHMIDT, E. P. R. *Data Mining: Um guia prático.* [S.l.]: Elsevier, 2005. v. 1. Citado na página 15.

GOLDSCHMIDT, R.; PASSOS, E.; BEZERRA, E. *Data Mining: Conceitos, técnicas, algoritmos, orientações e aplicações.* [S.l.]: Elsevier, 2015. v. 2. Citado 2 vezes nas páginas 17 e 18.

INAZAWA, P. et al. *Machine Learning: Desafios para um Brasil competitivo.* [S.l.]: Revista Computação Brasil, 2019. v. 39. Citado na página 14.

JHONSON, D. W. W. R. A. *Applied multivariate statistical analysis.* [S.l.]: Prentice-Hall, 1998. v. 4. Citado na página 26.

MASSA, D.; VALVERDE, R. A fraud detection system based on anomaly intrusion detection systems for e-commerce applications. In: DANIEL, R. (Ed.). [S.l.]: Canadian Center of Science and Education, 2014. p. 117–138. ISSN 1913-8989. Citado na página 13.

MEAD, N. L. et al. *Too Tired to Tell the Truth: Self-Control Resource Depletion and Dishonesty.* [S.l.]: Journal of Experimental Social Psychology, 2009. v. 45. 594–597 p. Citado na página 16.

MEIOEMENSAGEM. *E-commerce cresce 47% - www.meioemensagem.com.br.* 2021. Disponível em: <https://www.meioemensagem.com.br/home/marketing/2020/08/27/e-commerce-cresce-47-maior-alta-em-20-anos.html>. Acesso em: 04 abr 2021. Citado na página 13.

MITCHELL, T. M. *Machine Learning.* [S.l.]: McGraw-Hill, 1997. v. 1. Citado na página 18.

PACHECO, J. C. *Modelos para detecção de fraudes utilizando técnicas de Aprendizado de Máquina.* Dissertação (Dissertação de Mestrado) — Fundação Getulio Vargas escola de economia de São Paulo, 2019. Citado na página 14.

PH3A. *Como é feita análise de fraude em uma compra com cartão de crédito?* 2018. Disponível em: <https://blog.ph3a.com.br/como-e-feita-analise-de-fraude-em-uma-compra-com-cartao-de-credito>. Acesso em: 12 abr 2021. Citado na página 13.

QUINLAN, J. R. *Induction of Decision Trees.* [S.l.]: Centre for Advanced Computing Sciences., 1979. v. 1. Citado na página 22.

QUINLAN, J. R. *C4.5: Programs for Machine Learning.* [S.l.]: Morgan Kaufmann Publishers Inc., 1993. v. 1. Citado na página 22.

QUINTÃO, M. M. F.; MENDONÇA, M. C. Machine learning na melhoria de processos internos: Estudos de caso na indÚstria de varejo brasileira. In: FLORA (Ed.). *Projeto de Graduação apresentado ao Curso de Engenharia de Produção, Universidade Federal do Rio de Janeiro, Rio de Janeiro.* [S.l.: s.n.], 2020. Citado na página 14.

SPC. *Cheques falsificados ou roubados e cartão de crédito clonado foram principais fraudes sofridas por micro e pequenas empresas em 2018, apontam CNDL/SPC Brasil.* 2019. Disponível em: <https://www.spcbrasil.org.br/pesquisas/pesquisa/5977>. Acesso em: 27 mai 2021. Citado na página 16.

TERRA. *Pesquisa mostra que e-commerce cresceu quase 40% no Brasil em um ano.* 2021. Disponível em: <https://www.terra.com.br/noticias/dino/pesquisa-mostra-que-e-commerce-cresceu-quase-40-no-brasil-em-um-ano,866200188360481 85f689ea3bb91d2c7d7q6snyz.html>. Acesso em: 12 abr 2021. Citado na página 13.

VEJA. *Como funcionam as novas fraudes com cartão de crédito*. 2021. Disponível em: <https://veja.abril.com.br/economia/como-funcionam-as-novas-fraudes-com-cartao-de-credito/>. Acesso em: 09 abr 2021. Citado na página 15.

YANG, S.; BERDINE, G. The receiver operating characteristic (roc) curve. *The Southwest Respiratory and Critical Care Chronicles*, v. 5, p. 34, 05 2017. Citado 2 vezes nas páginas 30 e 31.