CURSO DE CIÊNCIA DA COMPUTAÇÃO – TCC	
( ) PRÉ-PROJETO (X) PROJETO	ANO/SEMESTRE: 2023/2

IDENTIFICAÇÃO AUTOMÁTICA DE PERDAS NÃO TÉCNICAS EM SISTEMAS DE DISTRIBUIÇÃO ELÉTRICA UTILIZANDO APRENDIZADO DE MÁQUINA

Mônica Luíza Doege

Profª. Andreza Sartori – Orientadora

Ms. Johnny Deschamps – Coorientador

1 INTRODUÇÃO

O sistema de geração e distribuição de energia elétrica no Brasil enfrenta problemas de diversas naturezas, tais como: sociais, econômicos, políticos, ambientais e tecnológicos. De fato, a crise de energia elétrica no Brasil tomou força nos últimos anos e, como ponto principal, tem-se a forte dependência de hidrelétricas e a escassez de chuvas no país. Com essa falta de planejamento e organização geral quem mais sofre é a população. Com isso, como resultados surgem a possibilidade de racionamento e apagões, bem como o aumento significativo das tarifas de energia elétrica (BORGES, 2021). Segundo Corsini (2022), os dados da Associação Brasileira dos Comercializadores de Energia (Abraceel) apontam que a tarifa de energia elétrica residencial teve um crescimento médio anual de 16,3% entre os anos de 2015 e 2021.

A crise hidrelétrica se tornou um adicional em problemas já presentes no sistema, como as perdas de energia. As perdas de energia elétrica se referem a energia gerada que é passada pelo sistema de distribuição, mas não chega a ser comercializada. Essas perdas podem ser divididas em duas categorias: Perdas Técnicas (PT) e Perdas Não Técnicas (PNT) (ANEEL, 2023). Segundo Piotrowski *et al.* (2021), as Perdas Técnicas (PT), ocorrem durante o processo de transporte e transformação de energia elétrica em energia térmica, mais conhecido como Efeito Joule. Já as Perdas Não Técnicas (PNT) são resultado da falta de faturamento da energia elétrica distribuída. Entre as causas mais comuns, estão presentes: o furto de energia, fraude na medição ou fornecimento de energia, falha ou falta na conferência dos medidores e erro no faturamento.

De acordo com dados da ANEEL (2023), em 2022 a taxa de perdas não técnicas no Brasil ficou por volta de 14%, dando um prejuízo de mais de R$ 6 bilhões. Conforme levantamento realizado pela Associação Brasileira de Distribuidores de Energia Elétrica (ABRADEE), a energia perdida por furto ou desvio em 2022 seria suficiente para abastecer os estados de Santa Catarina, Paraná, Mato Grosso do Sul e Espírito do Santo. O valor dessas perdas é pago tanto pelas distribuidoras de energia quanto pelo consumidor final, com uma média de 10% desse custo sendo repassado para o consumidor. O cálculo das PNT é determinado pela diferença entre a energia entregue pela distribuidora de energia e a quantidade de energia contabilizada e paga pelos consumidores. Com essa diferença, é realizado o rateio do valor a pagar pelo consumidor e pela distribuidora. As PNT também impactam a possibilidade de crescimento e melhorias dentro das distribuidoras, na qual o valor pago poderia ser revertido em geração de energia renovável. Além de prejuízo, esse tipo de prática traz riscos a população, como aumento de possibilidade de curto-circuito, incêndio e choques elétricos (CEMIG, 2023).

Conforme apontado por Deschamps (2023), Gerente da Divisão Comercial da Centrais Elétricas de Santa Catarina (CELESC) de Blumenau, atualmente em Blumenau a detecção de PNT é realizada de forma manual pelos técnicos. Estes profissionais analisam os dados de consumo em busca de padrões atípicos e, posteriormente, realizam visitas de inspeção para investigar cada caso identificado. Esse processo de análise é demorado e custoso para a distribuidora de energia, e está sujeito a falhas. Além disso, parte do preço é pago pela população blumenauense, causando aumento nas tarifas de energia elétrica. Neste contexto, esse trabalho tem como objetivo disponibilizar uma solução automatizada para a detecção de PNT, utilizando uma base de dados fornecida pela distribuidora de energia de Blumenau (CELESC) por meio de técnicas de aprendizado de máquina.

1.1 OBJETIVOS

O objetivo deste trabalho é disponibilizar um protótipo para a identificação automática de perdas não técnicas em sistemas de distribuição elétrica por meio de técnicas de aprendizado de máquina.

Os objetivos específicos são:

a) identificar os padrões que definem Perdas Não Técnicas;
b) validar a acurácia do modelo encontrado;
c) utilizar dados reais para o treinamento, validação e teste do modelo gerado.

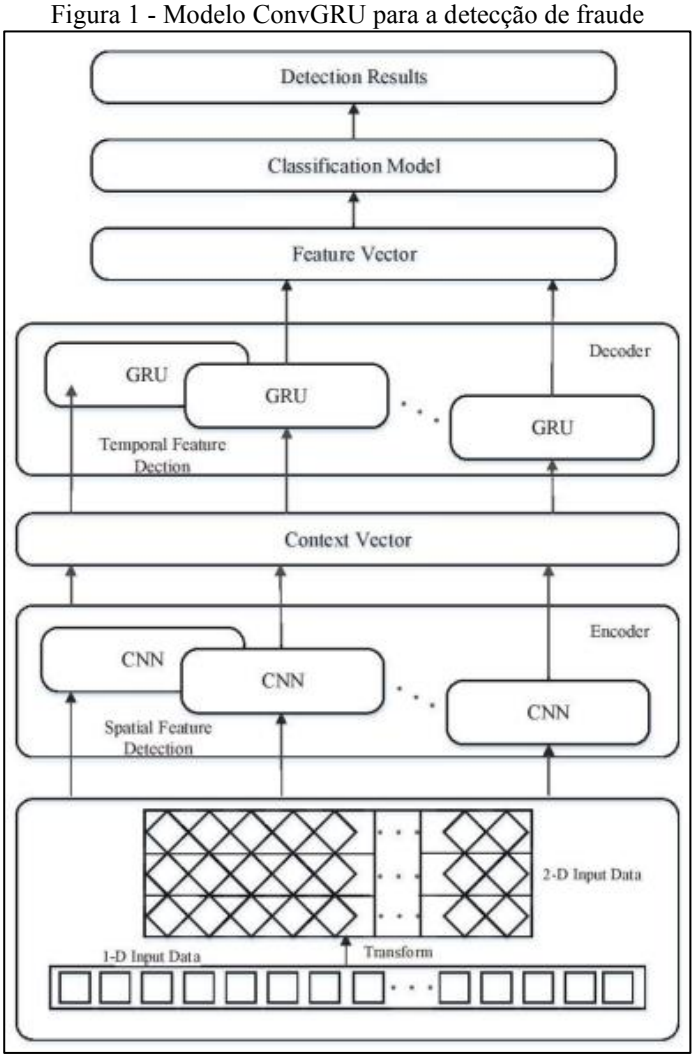
2 TRABALHOS CORRELATOS

Nesta seção serão apresentados três trabalhos correlatos. O primeiro trabalho relata um modelo utilizando rede neural convolucional de unidade recorrente fechada juntamente com o algoritmo de *K-means* para detectar roubo de energia elétrica (NIU; ZHANG, 2021). O trabalho de Markovska *et al*. (2023) apresenta um modelo utilizando rede neural convolucional temporal com *Self-Attention* para a deteção de roubo de energia. Por fim, o terceiro trabalho implementou uma solução para fraudes de energia elétrica em uma infraestrutura com medição avançada, utilizando máquina de vetores de suporte (KORBA; KARABADJI, 2019).

2.1 A DATA-DRIVEN METHOD FOR ELECTRICITY THEFT DETECTION COMBING CONVGRU AND K-MEANS CLUSTERING

O trabalho de Niu e Zhang (2021) utiliza um modelo de rede neural artificial chamado *Convolutional Gated Recurrent Unit* (ConvGRU) para a detecção de roubo de energia elétrica. Essa técnica está dividida em duas partes: primeiro tem-se a Rede Neural Convolucional (*Convolutional Neural Network* - CNN), que é separada da parte da *Gated Recurrent Unit* (GRU). A CNN foi utilizada para extrair as características espaciais entre diferentes dados do usuário, e a GRU é utilizada para aprender as características temporais internas de consumo de energia. Este modelo foi organizado de maneira codificadora-decodificadora (encoder-decoder). Como apresentado na Figura 1, a CNN é a codificadora (encoder), que é responsável pela extração de características espaciais e redução da dimensão da entrada em 2D. A GRU é a decodificadora (decoder), que executa a extração de características temporais nas características intermediárias processadas na parte convolucional.

Figura 1 - Modelo ConvGRU para a detecção de fraude



Fonte: Niu e Zhang (2021).

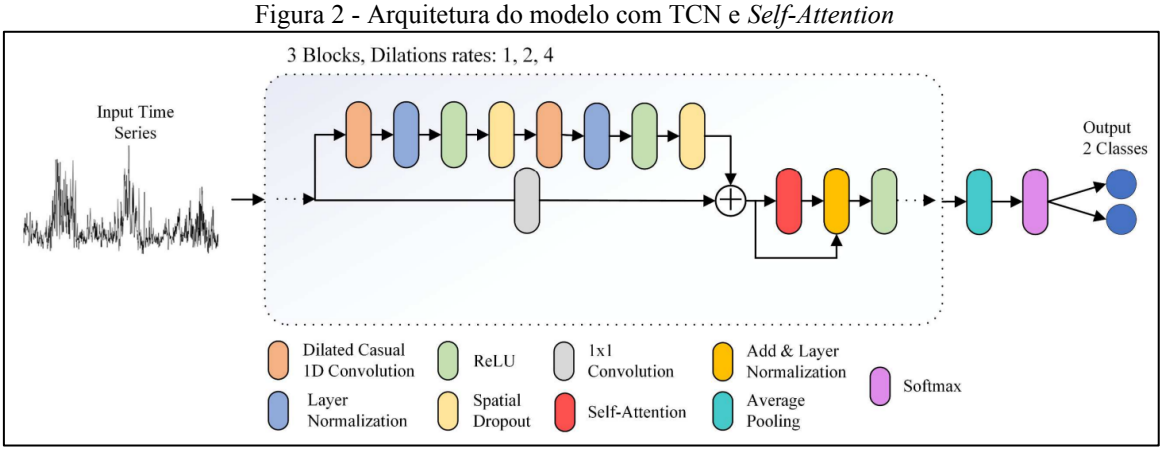
O conjunto de dados utilizado foi disponibilizado pela *Sustainable Energy Authority Of Ireland* (SEAI), que contém relatórios de consumo de energia a cada meia hora. O conjunto contém registros de mil unidades consumidoras irlandesas durante o período de 504 dias. Como esses dados foram cedidos pelos próprios usuários, o projeto partiu do princípio de que todos eram consumidores regulares. A partir disso, foi selecionado 20% dessa base de dados e foi alterado os valores, para representar consumidores não regulares.

Como técnica de pré-processamento foi utilizado o *K-means*. Como na base de dados utilizada existiam diversos tipos de consumidores, como casas residenciais até indústrias, o *K-means* foi utilizado para fazer uma separação inicial e agrupá-los em clusters. Para calcular esse agrupamento foi utilizado distância Euclidiana. Sem a técnica de *K-means*, o modelo atingiu uma acurácia de 96.7%. O modelo de ConvGRU, juntamente com a técnica de *K-means*, atingiu 98.8% de acurácia, com taxa de falso negativo igual a 4% e taxa de positivo verdadeiro de 96%, o que demonstra alto índice de detecções de roubo de corretas. No trabalho apresentado, os autores destacam a relevância do pré-processamento dos dados utilizados e que estes foram importantes para alcançar os resultados obtidos.

2.2 ELECTRICITY THEFT DETECTION BASED ON TEMPORAL CONVOLUTIONAL NETWORKS WITH SELF-ATTENTION

Markovska *et al*. (2023) utilizaram uma Rede Neural Convolucional Temporal (*Temporal Convolutional Nerworks* - TCN) com *Self-Attention* para detectar roubo de energia elétrica. O modelo proposto, apresentado na Figura 2, possui três camadas de TCN, representados pelas cores laranja e cinza, e três taxas de dilatação diferentes. Duas TCNs estão representadas em Laranja e a terceira TCN está representada em Cinza. A TCN representada em cinza é uma *skip connection*, que se conecta diretamente com a entrada e com o último resultado da etapa de *Spatial Dropout*. *Skip connections* são utilizadas para prevenir o problema de gradiente de desaparecimento, onde o gradiente se torna muito pequeno durante a retropropagação. A saída de cada TCN é passada pela camada de *Self-Attention*, representada em vermelho na Figura 2. Por fim, foi utilizado a função de ativação *Softmax* para classificar os dados gerados nos processos anteriores.

Figura 2 - Arquitetura do modelo com TCN e *Self-Attention*



Fonte: Marakovska *et al*. (2023).

O conjunto de dados utilizado foi disponibilizado pela *State Grid Corporation of China* (SGCC), que contém o valor de consumo de energia diário, separado por hora, e a identificação de cada consumidor. O conjunto de dados contém 42.372 registros/unidades consumidoras, de janeiro de 2014 a outubro de 2016. Destes, cerca de 8% são consumidores irregulares. Na fase de preparação dos dados foi utilizado interpolação de Hermite, que é uma técnica de interpolação polinomial que preserva a monotonicidade dos dados para garantir a continuidade da sua primeira derivada. Para a normalização foi utilizado a técnica de Min-Max, método que dimensiona os dados para um intervalo entre 0 e 1. Dado o pequeno número de consumidores irregulares, foi realizado um balanceamento dos dados, criando registros irregulares utilizando como base os dados já existentes. O modelo proposto alcançou uma acurácia de 94,66%, F1-Score de 95% e AUC de 0.946, conseguindo alcançar valores acima dos outros modelos de pesquisas relacionadas.

2.3 SMART GRID ENERGY FRAUD DETECTION USING SVM

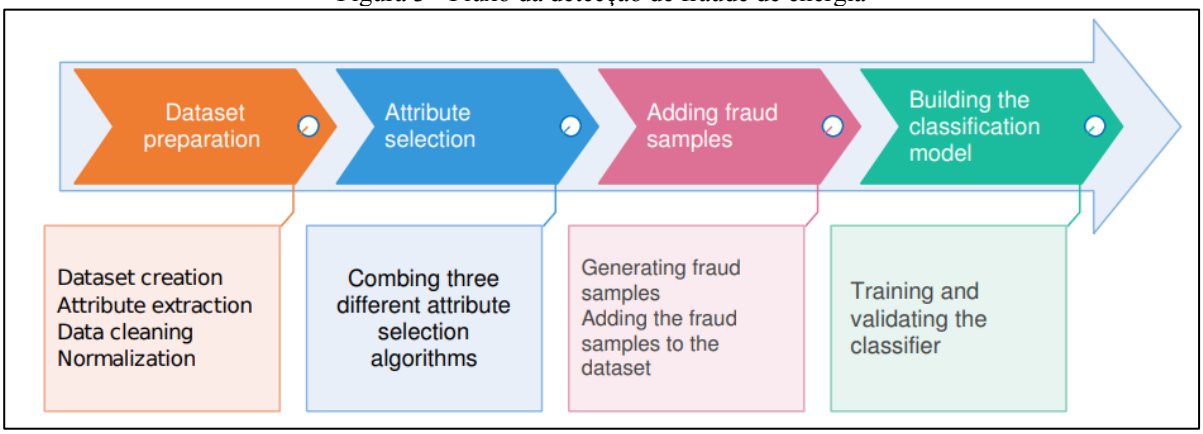
O trabalho proposto por Korba e Karabadji (2019) tinha como objetivo detectar fraudes na infraestrutura de medição avançada (*Advanced Metering Insfrastructure* - AMI). AMI é um sistema automático de medição de energia elétrica quecoleta dados de forma remota. No trabalho, os autores abordam três cenários específicos de fraude:

a) em que a unidade consumidora diminui o valor da medição em uma certa porcentagem;
b) em que a unidade consumidora zera o valor da medição durante um período específico;
c) em que a unidade consumidora diminui o valor da medição por certa porcentagem apenas durante um período determinado.

O conjunto de dados utilizados foi disponibilizado pelo *Irish Smart Energy Trial*, que contém dados de cinco mil consumidores, com as seguintes colunas: *Meter ID*, *Encoded date/time* e *Energy Consumption* (KWh). A Figura 3 apresenta o modelo desenvolvido, o qual apresenta 4 etapas. Após a etapa de extração de atributos e normalização dos dados (*Dataset Preparation*), foram utilizados três algoritmos de seleção de atributos (*Attribute*

Selection), que são: Ganho de Informação, Razão de Ganho e Incerteza Simétrica. Como o trabalho foca em três cenários de irregularidades, foram criados registros com esses cenários e estes foram adicionados ao conjunto de dados original (*Adding fraud samples*). Como técnica de classificação foi utilizado o *Support Vector Machine* (SVM), com kernel polinomial. Como resultado, o modelo obteve uma acurácia de 91,062%.

Figura 3 - Fluxo da detecção de fraude de energia



Fonte: Korba e Karabadji (2019).

Korba e Karabadji (2019) concluíram que o modelo proposto atingiu resultados satisfatórios para os cenários propostos. Os autores citaram trabalhos relacionados e fizeram comparações com os resultados, como por exemplo um trabalho que utilizou Redes Neurais Artificias. Apesar deste trabalho ter uma taxa de classificação correta maior, esse modelo conseguiu uma taxa de falso positivo mais baixa, cerca de 9%, o que demonstra que o modelo teve uma boa performance em detectar corretamente as fraudes.

3 PROPOSTA DO PROTÓTIPO

Nesta seção serão apresentados a justificativa, os principais Requisitos Funcionais (RF) e Requisitos Não Funcionais (RNF), a metodologia a ser utilizada e o cronograma a ser seguido no decorrer do trabalho.

3.1 JUSTIFICATIVA

O Quadro **1** apresenta um comparativo das principais características dos três trabalhos correlatos selecionados.

Quadro 1 - Comparativo dos trabalhos correlatos

Características \ Trabalhos Correlatos	Niu e Zhang (2021)	Marakovska *et al* (2023)	Korba e Karabadji (2019)
Quantidade de unidades consumidoras observadas	1.000	42.372	5.000
Dados presentes no *dataset*	Relatórios de consumo de energia a cada meia hora e identificação	Valores do consumo diário separado por hora e identificação	*Meter ID*, *Encoded date/time* e *Energy Consumption* (KWh)
Pré-processamento dos dados	Distância Euclidiana + *K-means*	Interpolação de Hermite + técnica de Min Max	Análise manual das características + normalização
Técnica de Aprendizado de Máquina utilizada	ConvGRU	TCN + Self-Attention	SVM
Acurácia	98.8%	94,66%	91,062%
Taxa de falso positivo	4%	-	9%

Fonte: elaborado pela autora.

O trabalho de Korba e Karabadji (2019) se destaca pela abordagem aplicada no pré-processamento dos dados. Com base nas informações, foi utilizado três algoritmos de seleção de atributos resultando em uma lista de atributos mais relevantes para o processo de treinamento. O modelo atingiu uma acurácia de 91,062% e uma taxa de falso positivo de 9%.

O trabalho de Niu e Zhang (2021) se destaca pela capacidade das Redes Neurais Artificiais avaliarem os dados de forma isolada, selecionando um curto período, e temporal, analisando os dados semanais. Com isso, os autores conseguiram estabelecer um modelo mais assertivo, dado que existem diversos tipos de comportamentos

apresentados em situações de roubo de energia. Outro aspecto relevante do trabalho é o processo de pré-processamento dos dados, que emprega o algoritmo *K-means* para separar os dados em várias categorias, agrupando os registros com tipos de consumo similares. Esse trabalho conseguiu a maior acurácia entre os três estudos relacionados, atingindo 98.8%, com uma taxa de falso positivo de 4%. O trabalho mais recente, apresentado por Markovska *et al.* (2023), aplicou *Temporal Convolutional Nerworks* (TCN) e *Self-Attention* para detectar fraudes. Por meio de valores de consumo de 42.367 unidades consumidoras, o modelo proposto alcançou uma acurácia de 94,66%.

Diante desses resultados, pode-se afirmar que o uso de técnicas de aprendizado de máquina para a detecção de Perdas Não Técnicas é eficaz, aumentando a eficiência e agilidade dos processos, que hoje, são realizados manualmente. Sendo assim, o presente trabalho tem como objetivo auxiliar a CELESC, criando um protótipo para a detecção automática de Perdas Não Técnicas, utilizando técnicas de Aprendizado de Máquina. O protótipo tem como finalidade facilitar o trabalho dos técnicos, reduzir custos de trabalho e aumentar a eficiência da identificação de PNT em Blumenau. Além disso, este trabalho tem como objetivo a população blumenauense possibilitando a redução da tarifa de energia elétrica, bem como aumentar a segurança pública relacionada a distribuição de energia elétrica.

3.2 REQUISITOS PRINCIPAIS DO PROBLEMA A SER TRABALHADO

Os requisitos do protótipo são:

a) extrair as características de unidades consumidoras regulares e irregulares (Requisito Funcional - RF);
b) realizar o tratamento dos dados como normalização, limpeza e organização da base de dados da CELESC (RF);
c) realizar a detecção de possíveis consumidores irregulares utilizando modelos de aprendizado de máquina (RF);
d) exibir os resultados da detecção de PNT, atribuindo identificadores para cada unidade consumidora utilizada (RF);
e) utilizar a linguagem de programação Python para fazer a implementação do protótipo (Requisito Não Funcional - RNF);
f) utilizar base de dados cedida pela CELESC (RNF).

3.3 METODOLOGIA

O trabalho será desenvolvido observando as seguintes etapas:

a) levantamento bibliográfico: realizar pesquisa de trabalhos correlatos, técnicas de aprendizado de máquina, e detecção de anomalias em dados;
b) elicitação de requisitos: com base na pesquisa realizada, elencar os requisitos necessários para a implementação do protótipo;
c) requerimento da base de dados: submeter o requerimento da base de dados aos responsáveis da CELESC;
d) análise e refinamento da base de dados: a partir da base de dados coletada, utilizar técnicas de pré-processamento para refinamento da base de dados.
e) definição da técnica de aprendizado de máquina: avaliar a melhor técnica de aprendizado de máquina para gerar o modelo;
f) implementação do modelo: realizar a implementação do modelo de identificação de PNT baseado nos requisitos propostos;
g) testes: realizar os testes necessários e verificar a precisão do modelo, utilizando como métrica acurácia e taxa de falso positivo;
h) validação: validar o protótipo com os responsáveis da CELESC.

As etapas serão realizadas nos períodos relacionados no Quadro 2.

Quadro 2 - Cronograma

	2024									
	fev.		mar.		abri.		mai.		jun.	
etapas / quinzenas	1	2	1	2	1	2	1	2	1	2
levantamento bibliográfico										
elicitação dos requisitos										
requerimento da base de dados										
análise e refinamento da base de dados										
definição da técnica de aprendizado de máquina										
implementação do modelo										
testes										
validação										

Fonte: elaborado pela autora.

4 REVISÃO BIBLIOGRÁFICA

Nesta seção serão descritos brevemente os assuntos que fundamentarão o estudo a ser realizado, os quais: Aprendizado de Máquina e Detecção de Anomalias.

4.1 APRENDIZADO DE MÁQUINA

De acordo com Monterei (2022) o objetivo do Aprendizado de Máquina é a construção de modelos computacionais que descrevem sistemas complexos a partir da observação do comportamento do sistema. Segundo Norvig e Russell (2022) existem 3 tipos principais de aprendizado Não Supervisionado, Por Reforço e Supervisionado. No aprendizado não supervisionado, o agente aprende padrões na entrada, embora não seja fornecido nenhum feedback explícito. A tarefa mais comum de aprendizado não supervisionada é o agrupamento: a detecção de grupos de exemplos de entrada potencialmente úteis. No aprendizado por reforço o agente aprende a partir de uma série de reforços, isto é, recompensas ou punições. Por fim, no aprendizado supervisionado, o agente observa alguns exemplos de pares de entrada e saída, e aprende uma função que faz o mapeamento da entrada para a saída.

Dentre as técnicas de Aprendizado têm-se as Redes Neurais Artificiais (RNA). Uma RNA é um sistema projetado para modelar a maneira como o cérebro realiza e aprende a fazer uma tarefa específica. (FLECK *el al*., 2016). Segundo Ludemir (2021), a implementação mais simples de RNA é uma rede *Perceptron*. O algoritmo de aprendizado do *Perceptron* utiliza a correção de erros como base, isto é, a diferença entre a resposta desejada e a resposta da rede. Na fase de treinamento do *Perceptron* os exemplos rotulados são apresentados ao algoritmo. Os parâmetros da rede (pesos) são modificados a cada apresentação de um novo exemplo à rede. Depois do ajuste dos parâmetros, na fase de teste, o sistema é avaliado.

Para avaliar a eficácia de um algoritmo de Aprendizado de Máquina (AM), são empregadas diversas métricas, incluindo, acurácia, taxa de falso positivo, *recall*, *precision*, F1-Score, entre outras. A Acurácia é a quantidade de chamadas corretas (verdadeiro-positivo e verdadeiro-negativo) que foram feitas em proporção ao total conjunto de dados. A Taxa de Falso Positivo representa a probabilidade de identificar incorretamente um caso como positivo quando, na realidade, a condição não está presente. *Recall* é função que calcula probabilidade de o modelo detectar um caso verdadeiramente positivo. *Precision* é a função que calcula a probabilidade de que a previsão positiva seja realmente positiva. O F1-Score é a função sobre os valores de *recall* e *precision*, para dar uma indicação geral do desempenho do classificador (HANDELMAN *et al*., 2019).

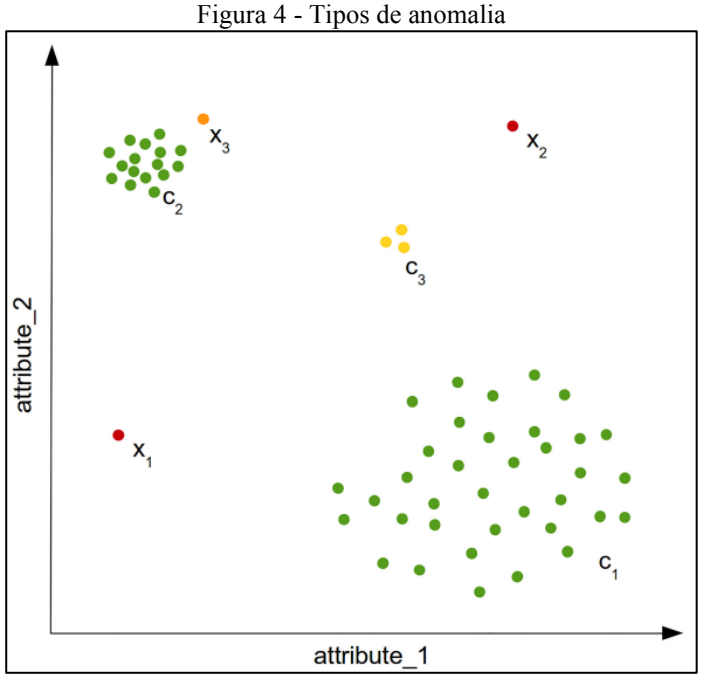
4.2 DETECÇÃO DE ANOMALIAS

De acordo com Goldstein e Uchida (2015) a detecção de anomalias é o processo de identificação de itens ou eventos inesperados em conjuntos de dados que diferem da norma. Em contraste com as tarefas de classificação padrão, a detecção de anomalias é frequentemente aplicada em dados não rotulados, levando em consideração apenas a estrutura interna do conjunto de dados. Este desafio é conhecido como detecção não supervisionada de anomalias.

Goldstein e Uchida (2015) também citam a existência de tipos de anomalias. A Figura 4 apresenta os agrupamentos de dados considerados normais, destacados em verde e atribuídos como “c1” e “c2”. Os dados em vermelho, atribuídos como “x1” e “x2” são chamados de anomalias globais, essas são facilmente detectadas devido à grande distância dos dados normais. Já o agrupamento em amarelo claro, atribuído de “c3” é chamado de *micro cluster*, e como esse agrupamento não fica tão longe dos dados normais os autores levantam a dúvida se esse caso deveria ser considerado anomalia ou não. Por fim, o ponto em amarelo escuro atribuído de “x3”, é chamado de anomalia local, isso devido a interpretação aberta. Se for observado os dados de forma global, o ponto “x3” aparenta ser um dado normal, dado a sua curta distância dos dados normais. Contudo, ao concentrar-se

exclusivamente no ponto "x3" e compará-lo com o agrupamento "c2", é possível classificar o ponto "x3" como uma anomalia.

Figura 4 - Tipos de anomalia



Fonte: Goldstein e Uchida (2015).

Goldstein e Uchida (2015) destacam que técnicas de detecção de anomalias podem ser usadas para a identificação de fraudes, mais especificamente em casos em que a identificação de características ou atributos que qualificam uma fraude é muito complexa, como por exemplo, em situação em que é utilizado uma base de dados desbalanceada. Exemplo disso é o trabalho de Albiero *et al.* (2019), que faz a detecção de anomalias por meio de uma comparação entre algoritmos de aprendizado supervisionado e não supervisionado, no contexto de detecção de Perdas Não Técnicas. Como aprendizado supervisionado os autores utilizaram a Regressão Logística, e como não supervisionado utilizaram o modelo *XGBoost*. Como nesse trabalho foi utilizado uma base que não tinha uma linha temporal muito distante, o modelo do *XGBoost* teve um resultado melhor, apresentando um F1-Score de 0.8. Já a Regressão Logística apresentou um F1-Score de 0.63. Com isso os autores concluem que o modelo de *XGBoost* apresentou melhores resultados comparado com a Regressão Logística, pois esse tipo de algoritmo é melhor para *datasets* desbalanceados, que foi o caso utilizado neste trabalho.

REFERÊNCIAS

ALBIERO, Beatriz et al. Employing Gradient Boosting and Anomaly Detection for Prediction of Frauds in Energy Consumption. **Anais do Encontro Nacional de Inteligência Artificial e Computacional (Eniac)**, Brasil, v. 1, n. 1, p. 1-10, out. 2019.

ANEEL (Brasil). Agência Nacional de Energia Elétrica. **Perdas de Energia**. 2023. Disponível em: https://www.gov.br/aneel/pt-br/assuntos/distribuicao/perdas-de-energia. Acesso em: 06 set. 2023.

BORGES, Fabricio Quadros. Crise de energia elétrica no Brasil - uma breve reflexão sobre a dinâmica de suas origens e resultados. **Recima21 - Revista Científica Multidisciplinar - Issn 2675-6218**, [S.L.], v. 2, n. 10, p. 1-11, 2 nov. 2021. Recima21 - Revista Cientifica Multidisciplinar. http://dx.doi.org/10.47820/recima21.v2i10.809.

CEMIG (Brasil). Companhia Energética de Minas Gerais. **Furto de Energia**. 2023. Disponível em: https://www.cemig.com.br/atendimento/furto-de-energia/. Acesso em: 19 set. 2023.

CORSINI, Luri. Energia elétrica aumentou mais do que o dobro da inflação nos últimos anos. **CNN Brasil**, Rio de Janeiro, 18 jan. de 2022. Disponível em: https://www.cnnbrasil.com.br/economia/energia-eletrica-aumentou-mais-do-que-o-dobro-da-inflacao-nos-ultimos-anos/. Acesso em: 27 set. 2023.

DESCHAMPS, Johnny. **Perdas não técnicas em Blumenau**. [Entrevista cedida a] Mônica Luíza Doege. Set. 2023.

FLECK, Leandro et al. Redes Neurais Artificiais: Princípios Básicos. **Revista Eletrônica Científica Inovação e Tecnologia**, v. 1, n. 13, p. 47-57, 2016.

GOLDSTEIN, Markus; UCHIDA, Seiichi. Unsupervised Anomaly Detection Benchmark. **Plus One**, Fukuoka, Japan, v. 1, n. 1, p. 1-31, 2015. Http://dx.doi.org/10.7910/DVN/OPQMVF.

HANDELMAN, Guy S. et al. Peering Into the Black Box of Artificial Intelligence: evaluation metrics of machine learning methods. **American Journal Of Roentgenology**, [S.L.], v. 212, n. 1, p. 38-43, jan. 2019. American Roentgen Ray Society. http://dx.doi.org/10.2214/ajr.18.20224.

KORBA, Abdelaziz Amara; KARABADJI, Nour El Islem. Smart Grid Energy Fraud Detection Using SVM. **2019 International Conference On Networking And Advanced Systems (Icnas)**, Annaba, v. 1, n. 1, p. 1-6, jun. 2019. IEEE. http://dx.doi.org/10.1109/icnas.2019.8807832.

LUDERMIR, Teresa Bernarda. Inteligência Artificial e Aprendizado de Máquina: estado atual e tendências. Estudos Avançados, Pernambuco, v. 35, n. 101, p. 85-94, abr. 2021. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0103-4014.2021.35101.007.

MARKOVSKA, Marija et al. Electricity Theft Detection Based on Temporal Convolutional Networks with Self-Attention. **2023 30Th International Conference On Systems, Signals And Image Processing (Iwssip)**, Skopje, v. 1, n. 1, p. 1-5, 27 jun. 2023. IEEE. http://dx.doi.org/10.1109/iwssip58668.2023.10180294.

MONTEREI, Rafaella Carine. Perspectivas do uso do aprendizado de máquina em bibliotecas: uma revisão sistemática de literatura. Universidade de Brasília, Brasília, v. 1, n. 1, p. 1-155, mar. 2022.

NIU, Zhewen; ZHANG, Gengwu. A Data-Driven Method for Electricity Theft Detection Combing ConvGRU and K-means Clustering. **2021 Ieee 5Th Conference On Energy Internet And Energy System Integration (Ei2)**, Taiyuan, v. 1, n. 1, p. 1-6, 22 out. 2021. IEEE. http://dx.doi.org/10.1109/ei252483.2021.9712851.

NORVIG, Peter; RUSSELL, Stuart. Capitulo 8. In: NORVIG, Peter; RUSSELL, Stuart. Inteligência Artificial: Uma Abordagem Moderna. Rio de Janeiro: Grupo Editorial Nacional S.A, 2022. p. 1-1324.

PIOTROWSKI, Leonardo Jonas et al. Análise das Perdas de Energia no Sistema Elétrico de Distribuição Brasileiro. **Proceedings Of The 13Th Seminar On Power Electronics And Control (Sepoc 2021)**, Santa Maria, v. 1, n. 1, p. 1-6, 18 maio 2021. Sepoc. http://dx.doi.org/10.53316/sepoc2021.012.