INSTITUTO FEDERAL GOIANO
CAMPUS URUTAÍ
NÚCLEO DE INFORMÁTICA
CURSO DE SISTEMAS DE INFORMAÇÃO

FELIPE RIBEIRO DE REZENDE
CAUÊ GARCIA NASCIMENTO

RANSOMWARE: A PROBLEMÁTICA DO ATAQUE E O IMPACTO DO BALANCEAMENTO DE DADOS EM ALGORITMOS DE CLASSIFICAÇÃO DE ATAQUES.

Urutaí, 13 de agosto de 2025

INSTITUTO FEDERAL GOIANO
NÚCLEO DE INFORMÁTICA
SISTEMAS DE INFORMAÇÃO

FELIPE RIBEIRO DE REZENDE
CAUÊ GARCIA NASCIMENTO

RANSOMWARE: A PROBLEMÁTICA DO ATAQUE E O IMPACTO DO BALANCEAMENTO DE DADOS EM ALGORITMOS DE CLASSIFICAÇÃO DE ATAQUES.

Trabalho de Conclusão de Curso apresentado ao Núcleo de Informática, curso de Sistemas de Informação, do Instituto Federal Goiano, como parte das exigências para obtenção do título de Bacharel em Sistemas de Informação.

Orientador(a):
Prof. Dr. Gabriel da Silva Vieira
Urutaí, 13 de agosto de 2025

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema Integrado de Bibliotecas do IF Goiano - SIBi

Nascimento, Cauê Garcia
C371g Ransomware: A problemática do ataque e o impacto do balanceamento de dados em algoritmos de classificação de ataques. / Cauê Garcia Nascimento. Urutaí 2025.

33f. il.

Orientador: Prof. Dr. Gabriel da Silva Vieira.
Tcc (Bacharel) - Instituto Federal Goiano, curso de 0120201 - Bacharelado em Sistemas de Informação - Urutaí (Campus Urutaí).
1. Inteligência Artificial. 2. Ransomware. 3. Cibersegurança. 4. Malware Classification. 5. Machine Learning. I. Título.

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano, a disponibilizar gratuitamente o documento no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

Identificação da Produção Técnico-Científica

[ ] Tese	[ ] Artigo Científico
[ ] Dissertação	[ ] Capítulo de Livro
[ ] Monografia – Especialização	[ ] Livro
[X] TCC - Graduação	[ ] Trabalho Apresentado em Evento

[ ] Produto Técnico e Educacional - Tipo: _____

Nome Completo do Autor: Felipe Ribeiro de Rezende, Cauê Garcia Nascimento
Matrícula: 2021201202010016, 2021101202010060
Título do Trabalho:Ransomware: A problemática do ataque e o impacto do balanceamento de dados em algoritmos de classificação de ataques.

Restrições de Acesso ao Documento

Documento confidencial: [X] Não [ ] Sim, justifique: _____

Informe a data que poderá ser disponibilizado no RIIF Goiano: 13/08/2025
O documento está sujeito a registro de patente? [ ] Sim [X] Não
O documento pode vir a ser publicado como livro? [ ] Sim [X] Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O/A referido/a autor/a declara que:

1. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
2. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
3. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

gov.br Documento assinado digitalmente
FELIPE RIBEIRO DE REZENDE
Data: 13/08/2025 12:40:48-0300
Verifique em https://validar.iti.gov.br

gov.br Documento assinado digitalmente
CAUE GARCIA NASCIMENTO
Data: 13/08/2025 21:02:09-0300
Verifique em https://validar.iti.gov.br

Urutaí, 13/08/2025 .

_____
Assinatura do Autor e/ou Detentor dos Direitos Autorais

Ciente e de acordo:

gov.br Documento assinado digitalmente
GABRIEL DA SILVA VIEIRA
Data: 15/08/2025 20:40:55-0300
Verifique em https://validar.iti.gov.br

_____
Assinatura do(a) orientador(a)

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

Documentos 12/2025 - CCBSI-URT/GE-UR/DE-UR/CMPURT/IFGOIANO

CAUÊ GARCIA NASCIMENTO

FELIPE RIBEIRO DE REZENDE

RANSOMWARE: A PROBLEMÁTICA DO ATAQUE E O IMPACTO DO BALANCEAMENTO DE DADOS EM ALGORITMOS DE CLASSIFICAÇÃO DE ATAQUES

Monografia, defendida por Cauê Garcia Nascimentoe Felipe Ribeiro de Rezende, apresentada ao Instituto Federal de Educação, Ciência e Tecnologia Goiano, como parte das exigências para a obtenção do título de Bacharel em Sistemas de Informação, aprovados pela banca examinadora.

COMISSÃO EXAMINADORA

(Assinado Eletronicamente)

Prof. Dr. Gabriel da Silva Vieira

Orientador

(Assinado Eletronicamente)

Prof. Dr. Paulo Henrique Garcia Mansur

Avaliador

(Assinado Eletronicamente)

Profa. Dra. Vivian Cirino de Lima

Avaliador

Urutaí (GO), 25 de junho de 2025.

Documento assinado eletronicamente por:

- **Gabriel da Silva Vieira**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 15/08/2025 20:26:34.
- **Vivian Cirino de Lima**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 18/08/2025 07:44:02.
- **Paulo Henrique Garcia Mansur**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 18/08/2025 16:00:21.

Este documento foi emitido pelo SUAP em 25/06/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 720138
Código de Autenticação: 671b7aeb66

INSTITUTO FEDERAL GOIANO
Campus Urutaí
Rodovia Geraldo Silva Nascimento, Km 2.5, SN, Zona Rural, URUTAÍ / GO, CEP 75790-000
(64) 3465-1900

Dedicamos este trabalho aos nossos familiares e professores

AGRADECIMENTOS

Somos imensamente gratos a todas as pessoas que, de alguma forma, contribuíram para a realização e conclusão deste trabalho de conclusão de curso e que tornaram essa jornada possível.
Em primeiro lugar, expressamos nossa sincera gratidão ao nosso orientador, Gabriel da Silva Vieira, por toda a orientação, paciência e dedicação durante o desenvolvimento deste trabalho. Seu conhecimento técnico, apoio constante e generosidade em compartilhar seu tempo e expertise foram fundamentais para que pudéssemos concretizar este projeto com segurança e clareza.
Estendemos também nossos agradecimentos aos professores e demais membros do corpo docente do Núcleo de Informática, que, ao longo da graduação, contribuíram de forma significativa para a nossa formação acadêmica. As aulas, seminários, sugestões e discussões promovidas foram essenciais para o amadurecimento do pensamento crítico e para a consolidação dos conhecimentos que aplicamos neste trabalho.
Agradecemos, com carinho, aos nossos colegas de turma e amigos, que estiveram ao nosso lado ao longo desses anos. O apoio mútuo, os debates enriquecedores e os momentos compartilhados em grupo foram peças importantes para a construção da nossa trajetória acadêmica.
Não poderíamos deixar de agradecer também aos nossos familiares, pelo suporte incondicional em todos os momentos. Seu amor, compreensão e incentivo constante foram pilares que sustentaram nossa caminhada e nos motivaram a seguir em frente com determinação e perseverança.
A todos vocês que estiveram ao nosso lado durante essa jornada, deixamos aqui nosso mais profundo e sincero agradecimento. Este trabalho é resultado não apenas de nossos esforços, mas também do apoio de cada um que acreditou em nós ao longo de toda a nossa formação.

RESUMO

Esta pesquisa aborda a crescente preocupação com ataques de *ransomware*, impulsionada pelo aumento do uso da internet para comunicação e transferência de dados. Tais ataques comprometem operações críticas e a segurança de informações sensíveis. O estudo investigou o uso de algoritmos de *machine learning* na detecção de *ransomware*, com ênfase no balanceamento de dados para melhorar a confiabilidade dos modelos computacionais. Utilizando o método experimental, foram testados modelos com uma base de dados pública, avaliados por métricas quantitativas e qualitativas. Os resultados demonstraram que o balanceamento de dados aumenta significativamente a precisão da detecção, alcançando mais de 96% de assertividade. A pesquisa contribui para o aprimoramento de sistemas de segurança contra ciberataques, especialmente os baseados em *ransomware*.

Palavras-chave:

Inteligência Artificial; Machine Learning; Random Forest; Decision Tree; Malware Classification; Ransomware; Cibersegurança .

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ADASYN Adaptive Synthetic Sampling Approach. Pag.20

AGRM Adaptive Greedy Relevance Measure. Pag.18

ANN Artificial Neural Network. Pag.19

AUC Area Under the Curve. Pag.20

B-SMOTE Borderline-SMOTE. Pag.20

BoostARoota Boosted Automatic Root Cause Analysis. Pag.18

Chi Chi-Square. Pag.18

DL Deep Learning. Pag.19

DT Decision Tree. Pag.19

F1 F1-Score. Pag.20

FRUFS Feature Ranking Using Forward Selection. Pag.18

FSRM File Server Resource Manager. Pag.19

FSS File Screening Service. Pag.19

G-mean Geometric Mean. Pag.20

GANs Generative Adversarial Networks. Pag.20

HGB Hist Gradient Boosting. Pag.18

IA Inteligência Artificial. Pag.15

IoT *Internet of Things* (Internet das Coisas). Pag.13

k-NN k-Nearest Neighbors. Pag.18

LOFO Leave One Feature Out. Pag.18

MI Mutual Information. Pag.18

ML Machine Learning. Pag.18

MRMR Minimum Redundancy Maximum Relevance. Pag.18

NaN Not a Number. Pag.26

NB Naive Bayes. Pag.18

PLN Processamento de Linguagem Natural. Pag.35

RF Random Forest. Pag.18

RSMOTE Random SMOTE. Pag.20

SMB Server Message Block. Pag.23

SMOTE Synthetic Minority Over-sampling Technique. Pag.20

SVM Support Vector Machine. Pag.19

XGBoost Extreme Gradient Boosting. Pag.18

SUMÁRIO

CAPÍTULO 1

INTRODUÇÃO

Com o incidente da pandemia de COVID-19, oficialmente declarada em março de 2020 (Organização Pan-Americana de Saúde (OPAS), 2023), que levou ao início dos isolamentos, o volume de acessos à internet, regime de trabalho *home office* e uma maior demanda de ensino a distância passaram a contribuir significativamente para o crescimento de acessos e mais compartilhamento de informações.

Pôde-se notar ainda um grande aumento nos ataques cibernéticos a partir do crescente uso da internet. Os métodos de invasão são variados, porém todos os mecanismos estão diretamente relacionados ao comportamento dos usuários. Reshmi (2021) aponta como principais formas os anúncios maliciosos, sites comprometidos, *spam*, engenharia social e caminhos para *downloads*.

Os ataques de *ransomware* têm se mostrado uma ameaça significativa, causando transtornos, agravados por extorsão em diversos setores. Esses ataques têm o potencial de paralisar operações críticas, comprometer dados sensíveis e prejudicar a infraestrutura tecnológica de instituições governamentais e privadas. Portanto, é essencial desenvolver mecanismos e ferramentas que possam identificar, prevenir e conter os danos causados por esses ataques.

Embora as tecnologias de segurança estejam em constante evolução, os cibercriminosos também aprimoram suas táticas e exploram novas vulnerabilidades. Consequentemente, essa realidade exige a prática continua de monitoramento e aperfeiçoamento de ações que compreendam a estrutura dos ataques de *ransomware* e busquem formas de aumentar a segurança cibernética, em especial, nos setores que lidam constantemente com dados sensíveis.

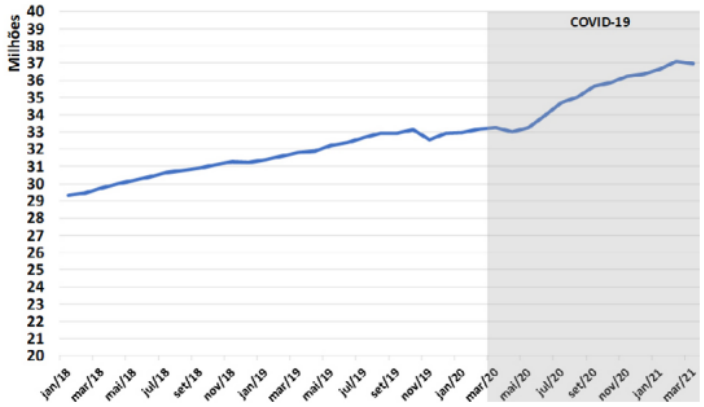
Contudo, acompanhar a evolução dos ataques cibernéticos é desafiador devido à rápida evolução das ferramentas de penetração em segurança. Dessa forma, esta monografia reforça

a necessidade de estimular as pesquisas para enfrentar os avanços apresentados pelos ataques de *ransomware*, buscando soluções eficazes por meio de estudos que atualizem e desenvolvam ferramentas que possam mitigar os impactos desses ataques. Neste trabalho, investigamos o comportamento de modelos computacionais em diferentes balanceamentos de dados para a classificação de ataques cibernéticos.

1.1 Contextualização

O acesso à internet no Brasil aumentou significativamente de março de 2020 para março de 2021, passando de 32 milhões para aproximadamente 37 milhões de acessos (Agência Nacional de Telecomunicações (ANATEL), 2021). Esse crescimento é ilustrado na Figura 1.1, que mostra o crescimento de acessos de banda larga fixa de 2018 a 2021. Além disso, em IoT (*Internet of Things* (Internet das Coisas)) esse aumento foi acompanhado por um incremento de aproximadamente 35% nos ataques cibernéticos no primeiro semestre de 2020, conforme reportado pela Microsoft (2020), que destacou a modernização dos métodos criminosos, especialmente o *ransomware*, conforme Figura 1.2.

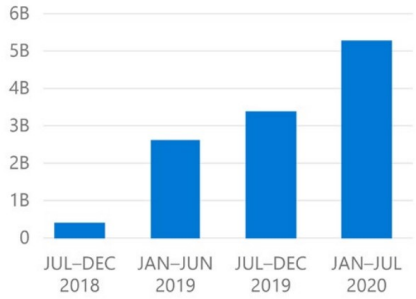
Figura 1.1: Crescimento de acessos de Banda Larga Fixa 2018-2021



Fonte: Relatório Analítico Do Impacto Da Pandemia De Covid-19 No Setor De Telecomunicações Do Brasil Jun/Jul 2021 - (Agência Nacional de Telecomunicações (ANATEL), 2021)

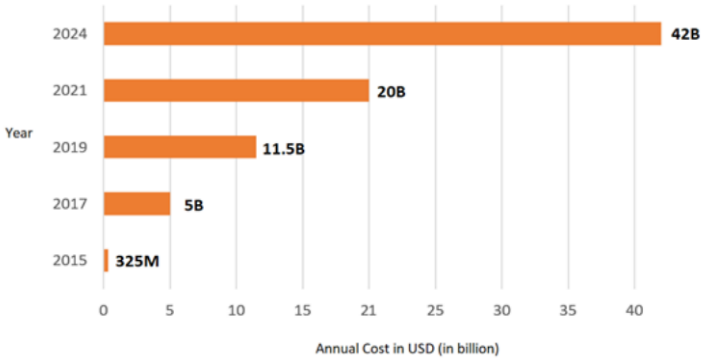
No segundo trimestre de 2021, o relatório do *software* de antivírus *Avast* demonstrou um aumento de 21% nos ataques de *ransomware* em relação ao primeiro semestre do mesmo ano (KLEINA, 2021). De acordo com Razaulla et al. (2023), os danos causados por esse tipo de ataque em 2015 foram de US$ 325 milhões, passando por uma crescente ao longo dos anos e atingindo um dano equivalente a US$ 42 bilhões em 2024, como pode ser percebido na Figura 1.3.

Figura 1.2: Ataques totais em honeypots



Fonte: Relatório de Defesa Digital da Microsoft (Microsoft, 2020).

Figura 1.3: Danos globais causados por ataques de *ransomware*



Fonte: (RAZAULLA et al., 2023).

Nesse cenário, o setor da educação também passou a sofrer ataques devido à expansão do ensino remoto após a pandemia. De acordo com a Associação Brasileira das Empresas de *Software* (ABES), as escolas lideraram a lista de alvos preferenciais em 2023, superando os ataques de *ransomware* no governo e na saúde (Associação Brasileira das Empresas de Software (ABES), 2024). Dentre os principais prejuízos estão os danos causados pelo roubo de dados confidenciais sobre alunos, finanças, operações e parcerias de pesquisa (SUAREZ et al., 2024).

O *ransomware* é um tipo de malware que se diferencia dos demais pelas etapas meticulosas de infecção e pela invasão dos mecanismos de defesa do sistema (RESHMI, 2021). Ao agir de forma silenciosa, sua presença passa despercebida até a fase final, quando o atacante assume o controle dos dados ou funções do dispositivo, destacando a necessidade de mecanismos inteligentes para sua detecção. Entre as principais variantes estão o *Crypto* e o *Locker* (RAZAULLA et al., 2023). O *Crypto* é caracterizado por criptografar os dados sem interferir no funcionamento do dispositivo, enquanto o *Locker* bloqueia o acesso e o uso do dispositivo com o intuito de extorsão.

A adaptabilidade do *ransomware* torna insuficientes as técnicas tradicionais de identificação baseadas em assinaturas fixas. Como resposta a essas limitações, o *machine learning* surge como uma alternativa eficaz no combate a essas ameaças. Um relatório recente da *Microsoft Intelligence* (2024) (Microsoft Threat Intelligence, 2024) destaca o papel da IA (Inteligência Artificial) e *machine learning* na detecção de ciberameaças. Recomenda a IA para o monitoramento de alterações no uso de recursos e tráfego de rede, além da identificação de comportamentos anômalos e tentativas de acesso suspeitas. A empresa relata que essas tecnologias permitiram interromper ciberataques oriundos de países como Rússia, Coreia do Norte, Irã e China, enfatizando a importância da IA na segurança digital atual.

Causando transtornos e extorsão em diversos setores, os ataques de *Ransomware* têm se mostrado uma ameaça significativa. Esses ataques têm o potencial de paralisar operações críticas, comprometer dados sensíveis e prejudicar a infraestrutura tecnológica de instituições governamentais e privadas. Portanto, é essencial desenvolver mecanismos e ferramentas que possam identificar, prevenir e conter os danos causados por esses ataques.

Embora as tecnologias de segurança estejam em constante evolução, os cibercriminosos também aprimoram suas táticas e exploram novas vulnerabilidades. Logo, é fundamental estimular e promover estudos atualizados que compreendam a estrutura dos ataques de *Ransomware* e busquem formas de aumentar a segurança cibernética.

O presente trabalho tem como objetivo explorar os estudos desenvolvidos nessa área e destacar os resultados mais relevantes em relação à aplicação do balanceamento dos dados em conjunto com algoritmos de classificação de *ransomware*. Além disso, será destacado o uso de *machine learning* para lidar com esses ataques. Ao analisar e compartilhar os conhecimentos obtidos, espera-se contribuir para o avanço da segurança cibernética, conscientizando sobre a importância de proteger as redes e dispositivos.

Dessa forma, este trabalho justifica-se pela necessidade de enfrentar os desafios impostos pelos ataques de *ransomware* na sociedade pós COVID-19, buscando soluções eficazes por meio de estudos e do desenvolvimento de ferramentas que possam mitigar os impactos desses ataques.

Diante do apresentado, este estudo foi organizado em 5 fases: Levantamento Bibliográfico, Triagem de Fontes, Execução do Trabalho, Implementação, Análise.

1. O projeto foi iniciado com uma pesquisa abrangente em motores de busca e bases bibliográficas, utilizando filtros de data no intervalo de 2019 a 2024. Isso permitiu abranger os estudos mais recentes, delimitar a busca para a área de Ciência da Computação e utilizar palavras-chave relevantes, como "*ransomware*", "detecção", "ciberataque"e "*machine learning*", além de outras identificadas como necessárias para atingir os objetivos do projeto.

2. Na segunda fase, foi realizada uma análise criteriosa das fontes coletadas durante o levantamento bibliográfico. Determinou-se a relevância e confiabilidade das fontes, considerando sua reputação, metodologia de pesquisa utilizada e contribuição para a compreensão dos ataques de *Ransomware* e do uso de *machine learning* na prevenção e no tratamento desses ataques. Foram coletados dados quantitativos sobre o volume de ataques, áreas-alvo e impactos sociais gerados durante o período de pesquisa, devido à possibilidade de discrepâncias nos dados encontrados em diferentes fontes.

3. Todo o material coletado foi verificado e a fundamentação teórica proposta para o projeto foi desenvolvida.

4. O conjunto de dados foi implementado na linguagem *python* utilizando os algoritmos *Decision Tree* e *Random Forest*, a fim de analisar a assertividade na detecção e prevenção dos ataques na prática.

5. Foram aplicados comparativos com base nas métricas definidas e os resultados foram analisados.

6. Os resultados da pesquisa foram reunidos e compõem este trabalho de conclusão de curso.

CAPÍTULO 2

TRABALHOS RELACIONADOS

Diversos estudos investigam o uso de modelos de ML (Machine Learning) para a detecção de *Ransomware*, explorando desde algoritmos clássicos, como RF (Random Forest) e k-NN (k-Nearest Neighbors) , até redes neurais profundas, capazes de lidar com grandes volumes de dados. As pesquisas indicam que a eficácia desses modelos está fortemente relacionada ao uso de técnicas de balanceamento de classes, como *Oversampling* e *Undersampling*, que corrigem a desproporção entre instâncias de *Ransomware* e *Goodware*. Quando combinadas, essas estratégias promovem uma detecção mais precisa e robusta, contribuindo significativamente para o fortalecimento da segurança cibernética.

O estudo de Rafique et al. (2023) comparou sete algoritmos de seleção de características (MRMR (Minimum Redundancy Maximum Relevance) , MI (Mutual Information) , Chi (Chi-Square) , LOFO (Leave One Feature Out) , FRUFS (Feature Ranking Using Forward Selection) , AGRM (Adaptive Greedy Relevance Measure) e BoostARoota (Boosted Automatic Root Cause Analysis)) em diferentes conjuntos de dados de Malware. Utilizando modelos como XGBoost (Extreme Gradient Boosting) , RF e HGB (Hist Gradient Boosting) , os autores observaram que nenhum algoritmo de seleção de características se destacou de forma consistente e o desempenho variou conforme os conjuntos de dados e os modelos. Em particular, o algoritmo BoostARoota teve um desempenho importante no conjunto de dados após otimizações específicas. O estudo conclui que ajustes de parâmetros e abordagens personalizadas são essenciais para otimizar a eficácia dos modelos de ML.

O trabalho de Shaambhavi et al. (2023) avaliou o desempenho de diferentes modelos de ML para a detecção de Malware, incluindo modelos baseados em árvores (como RF) quanto classificadores tradicionais como NB (Naive Bayes) e k-NN). A pesquisa revela que o modelo

RF alcançou a melhor acurácia (99,96%), destacando-se como a técnica mais eficaz entre os modelos testados. Contudo, o estudo recomenda a exploração de redes neurais profundas para enfrentar os desafios de detecção de Malware em grandes volumes de dados.

Em uma perspectiva voltada para o uso de algoritmos inteligentes na detecção de *Ransomware*, Bello et al. (2021) analisou o papel crescente de algoritmos de DL (Deep Learning) na análise de grandes volumes de dados e na resolução de problemas complexos. O estudo identifica a necessidade de uma exploração mais ampla de técnicas de *Big Data*, sugerindo que o DL e as análises de grandes volumes de dados podem representar um avanço significativo na detecção e prevenção de ataques de *Ransomware*.

Moore (2016) propõe o uso de *Honeypots* como iscas para detectar atividades de *Ransomware*, abordando uma metodologia que simula o comportamento de arquivos em pastas monitoradas. A pesquisa utilizou duas abordagens principais: o FSS (File Screening Service) do FSRM (File Server Resource Manager) e o *EventSentry* para monitoramento de logs de segurança do *Windows*. Os resultados indicaram que o uso de *Honeypots* pode ser uma camada adicional útil na detecção de *Ransomware*, embora as limitações sejam evidentes, especialmente em ambientes onde não há garantia de que o Malware interagirá com os recursos simulados.

Outra linha de pesquisa é apresentada por Evangelista e Lima (2023) que explora o uso de algoritmos de ML para classificar e identificar *Ransomwares* em um ambiente controlado. Nesse estudo, 102 amostras de arquivos executáveis foram coletadas e analisadas usando o *Cuckoo Sandbox*, e o conjunto de dados gerado foi classificado com seis algoritmos: DT (Decision Tree) , RF, k-NN, NB, SVM (Support Vector Machine) e ANN (Artificial Neural Network) . Os resultados mostraram que o RF e a ANN obtiveram as melhores taxas de acurácia, enquanto o k-NN e o NB apresentaram limitações em diferenciar com precisão as amostras benignas das maliciosas.

Uma questão particularmente importante no processo de tratamento de dados diz respeito aos conjuntos de dados desbalanceados. Nesse contexto, Ganganwar (2012) apresenta uma revisão abrangente sobre técnicas aplicadas à classificação desse tipo de dado, problema recorrente em domínios como detecção de fraudes e diagnóstico médico. O autor organiza as soluções em quatro abordagens principais: técnicas de reamostragem, como Oversampling e Undersampling; algoritmos modificados, que adaptam modelos como SVM, redes neurais e árvores de decisão; aprendizado sensível a custos, que aplica penalidades diferenciadas para erros de classificação; e abordagens híbridas, que integram diferentes estratégias com o objetivo

de melhorar o desempenho dos modelos.

Complementando Ganganwar (2012), Altalhan et al. (2025) aprofunda a discussão sobre os impactos práticos do desbalanceamento de dados e apresenta um panorama mais abrangente das estratégias de mitigação adotadas na literatura. O trabalho destaca métodos avançados de reamostragem, como SMOTE (Synthetic Minority Over-sampling Technique) , B-SMOTE (Borderline-SMOTE) , ADASYN (Adaptive Synthetic Sampling Approach) e RSMOTE (Random SMOTE) , além de explorar abordagens híbridas que buscam melhorar a eficiência dos modelos ao combinar diferentes técnicas. O estudo reforça a relevância do tema com exemplos práticos, como detecção de doenças raras e fraudes bancárias, e destaca métricas mais adequadas para avaliação, como F1 (F1-Score) , G-mean (Geometric Mean) e AUC (Area Under the Curve) . Além disso, discute limitações das abordagens existentes e aponta tendências futuras, como o uso de redes neurais profundas e modelos baseados em GANs (Generative Adversarial Networks) .

Esses trabalhos, ao lado das metodologias abordadas no presente estudo, reforçam a relevância da aplicação de ML e técnicas avançadas de detecção em ambientes que necessitam de alta precisão na classificação de ameaças. Ao incorporar diferentes abordagens, tanto baseadas em comportamento quanto em modelos de ML, é possível aprimorar a robustez dos sistemas de segurança contra *Ransomware*, destacando-se a importância de testar e adaptar métodos de detecção conforme as características dos dados e o ambiente de aplicação.

CAPÍTULO 3

MATERIAIS E MÉTODOS

3.1 Base de Dados

Herrera-Silva e Hernández-Álvarez (2023) desenvolveram um conjunto de dados dinâmico para a identificação de padrões comportamentais de diferentes variantes de *ransomware*, o qual foi utilizado neste trabalho. O conjunto de dados dinâmicos desenvolvido por eles baseou-se em três etapas principais: coleta de dados, extração de recursos e seleção de recursos.

Para a criação do conjunto de dados, foram realizados 2.000 experimentos que envolveram a execução de 20 amostras de *ransomware* e 20 de *goodware*, distribuídas em cinco plataformas distintas. Para a análise dinâmica das amostras, utilizou-se a ferramenta *Cuckoo Sandbox*, que permitiu a captura detalhada do comportamento dos artefatos durante a execução.

Foi desenvolvido pelos autores um aplicativo específico para processar os relatórios JSON gerados pelo *Cuckoo Sandbox*, permitindo a extração de 326 recursos dinâmicos essenciais para a análise comportamental dos artefatos. De acordo com os autores, esse aplicativo facilitou a visualização e o processamento dos dados contidos em diferentes categorias dos relatórios, como "Info" e "procmemory", e armazenou os dados extraídos em arquivos CSV para serem usados em algoritmos de *machine learning*. Os recursos extraídos abrangem uma ampla variedade de indicadores, incluindo chamadas de sistema, processos ativados, registros modificados, criação e manipulação de arquivos e diretórios, além de conexões de rede estabelecidas.

Para evitar redundâncias e concentrar-se nos atributos mais relevantes, foi realizada pelos autores uma seleção de recursos, resultando em um conjunto final de 50 características. Esses atributos foram escolhidos com base em sua capacidade de discriminar entre comportamentos maliciosos e legítimos de forma eficaz, contribuindo para a precisão dos algoritmos de detecção

de *ransomware*.

Os registros no conjunto de dados foram rotulados para facilitar o treinamento e a validação dos modelos de detecção. As amostras de *ransomware* foram divididas em duas categorias: encriptadores (*encryptors*) e bloqueadores (*lockers*). Por outro lado, o termo *goodware* representa *softwares* legítimos. Cada registro contém as 50 características dinâmicas selecionadas e viabiliza a identificação de comportamentos específicos de *ransomware* e sua diferenciação com *software* benigno.

3.2 Teoria em Sistemas de Informação

O uso da teoria dos sistemas de informação na segurança cibernética é baseado na ideia de que os incidentes de segurança cibernética são vistos como uma manifestação de falhas na utilização de TI (PUTRO et al., 2024). Essas falhas podem ocorrer devido a vulnerabilidades em pessoas, processos, tecnologia ou organização (MARCHEWKA, 2016). Neste trabalho, a teoria dos sistemas de informação é abordada sob a perspectiva sociotécnica que é considerada adequada para abordar questões de segurança cibernética porque envolve aspectos humanos, organizacionais e tecnológicos (MUJINGA et al., 2017). Neste sentido, damos ênfase aos aspectos tecnológicos e investigamos como modelos computacionais de *machine learning* podem ser assertivos e contribuir com a segurança de sistemas de informação.

Permitindo também, abrir um leque de possibilidades de capacitação, treino e inclusão de usuários treinados e capacitados para interagir com os sistemas de forma mais apropriada, diminuindo o risco de possibilidades de ataques.

3.3 Teoria do Caos e Segurança Cibernética

A Teoria do Caos aborda uma perspectiva da instabilidade geral acarretada em um sistema através de problemas ocasionados por pequenas partes, mas não só isso, segundo Dhillon e Ward (2002) ela pode colaborar com a análise, design e gerenciamento de sistemas de informação. O foco principal da Teoria é prever perturbações a curto prazo e atuar sobre elas para que não acarretem em problemas significativos a longo prazo, já que a incerteza a cerca de previsões a longo prazo é algo relevante e a incerteza permeia os sistemas quando o assunto é comportamento futuro.

Os relatórios de segurança ressaltados no trabalho como Microsoft 2020(Microsoft,

2020) e Microsoft 2024 (Microsoft Threat Intelligence, 2024) pontuaram a crescente nos ataques cibernéticos a corporações. De igual modo, canais de imprensa nacionais e internacionais como CNN, BBC, destacaram ataques que paralisaram organizações como o Ministério da Saúde no Brasil em dezembro de 2021 após sequestro de mais de 50TB de dados realizado pelo grupo Lapsu$ após invasão ao sistema do Ministério da Defesa, o que suspendeu o acesso a dados de saúde como o sistema do ConectSUS que continha os dados de vacinação da população que era crucial na época em decorrência à pandemia de COVID-19. Os mesmos criminosos atacaram o grupo Impressa de Portugal compartilhando mensagens de resgates e meios de pagamento para liberação dos dados. Além disso, como observado no ataque de *ransomware WannaCry* em 2017(CHEN; BRIDGES, 2017), a exploração de vulnerabilidade no protocolo SMB (Server Message Block) levou a uma propagação global, paralisando empresas e serviços essenciais. Desse modo, a Teoria do Caos sugere que, ao entender as interações entre componentes de um sistema, é possível prever comportamentos emergentes e aplicar estratégias de contenção proativa (DHILLON; WARD, 2002).

Ao aplicar seus princípios, é possível identificar como pequenas vulnerabilidades em sistemas interconectados podem gerar efeitos catastróficos, como nos exemplos mencionados. Essa perspectiva sublinha a importância de prever e mitigar riscos em seus estágios iniciais, visando minimizar os danos causados por invasões cibernéticas. Assim, esta pesquisa foca em aprimorar mecanismos para auxiliar na detecção antecipada de ataques cibernéticos, utilizando tecnologias e estratégias baseadas na análise de interações dos sistemas para assim antecipar e neutralizar ameaças, garantindo uma resposta ágil e eficaz para reduzir os impactos de forma significativa.

3.4 Métricas de Avaliação

Os modelos foram avaliados com as métricas de precisão (*Precision*), revocação (*Recall*), matriz confusão , F1-score e AUC-ROC, as duas últimas apontadas por Altalhan et al. (2025) como algumas das métricas mais adequadas e as demais por serem métricas comumente usadas na literatura.

Precisão:

A precisão calcula dentre todas as classificações positivas que o modelo realizou, isto é, quantas dessas classificações positivas estão corretas conforme apresentado na Eq. 3.1.

$$\text{Precisão} = \frac{VP}{VP+FP} \tag{3.1}$$

Recall:

O recall mede a capacidade do modelo de identificar todos os verdadeiros positivos da classe. Ele calcula a proporção de verdadeiros positivos com base em todos as instâncias que o modelo deveria ter classificado como positiva conforme apresentado na Eq.3.2.

$$\text{Recall} = \frac{VP}{VP+FN} \tag{3.2}$$

F1-Score:

O F1-score e a media harmônica entre a precisão e o recall, conforme apresentado na Eq. 3.3.

$$\text{F1-score} = 2 * \frac{Precision * Recall}{Precision + Recall} \tag{3.3}$$

AUC-ROC:

Em análises preditivas de classificadores, as Curvas AUC-ROC são fundamentais para medir a acurácia dos modelos. As curvas ROC mostram o comportamento dos modelos diante da variação nas taxas de verdadeiros e falsos positivos.

Matriz Confusão:

Matriz confusão é uma métrica bastante utilizada nos campos de *machine learning* e classificação de imagem. A matriz confusão é uma tabela que permite visualizar o desempenho do modelo de classificação em termos de verdadeiro positivo (VP), falsos positivo (FP), verdadeiro negativo (VN), e falso negativo (FN).

3.5 Organização da Pesquisa

O trabalho foi estruturado em quatro etapas: levantamento bibliográfico, triagem de fontes, seleção dos algoritmos e do conjunto de dados, e execução. O levantamento bibliográfico foi realizado por meio de uma pesquisa nos motores de busca *IEEE*, *ScienceDirect* e *ACM*, utilizando como conjunto de palavras-chave: *("malware"AND "machine learning models") OR ("dataset for ransomware detection") OR ("machine learning techniques for malware analysis") OR ("behavior-based malware detection") OR ("malware classification").*

Posteriormente, na triagem, foram identificadas as pesquisas mais coerentes com a abordagem esperada. Na seleção, foram analisados os mecanismos de trabalho mais atuais para a detecção e mitigação de ataques cibernéticos, com uma filtragem e escolha dos algoritmos a serem abordados neste trabalho. O conjunto de dados foi selecionado seguindo as mesmas abordagens bibliográficas, considerando critérios de volume de dados, classificação e resultados obtidos nas pesquisas.

3.6 Organização do Experimento

A execução dos algoritmos foi realizada na plataforma *Google Colab*, que oferece recursos computacionais escaláveis, permitindo o treinamento gratuito dos modelos de *machine learning* testados. O experimento foi conduzido entre 1 e 15 de outubro de 2024, abrangendo todas as etapas de análise e implementação.

O experimento desenvolvido neste trabalho baseou-se em um fluxo de pré-processamento, balanceamento de dados e construção de modelos de classificação utilizando os algoritmos *Random Forest* e *Decision Tree*. Dois modelos distintos foram implementados para avaliar o desempenho do modelo em condições balanceadas e desbalanceadas. Ambos os procedimentos seguiram etapas comuns de preparação de dados, mas diferiram no uso de técnicas de balanceamento.

3.7 Preparação dos Modelos

Dois modelos computacionais foram treinados com a base de dados selecionada. No primeiro modelo, o conjunto de dados foi utilizado em seu formato original, sem técnicas de balanceamento. Este método visou avaliar o impacto do desbalanceamento nas previsões do modelo e na acurácia final. Com o conjunto de dados desbalanceado, não foi necessário utilizar técnicas adicionais como a seleção aleatória de um subconjunto de dados. O *pipeline* de treinamento neste caso foi mais simples, contendo apenas os classificadores *Random Forest* e *Decision Tree*.

No segundo modelo, foi implementada uma técnica de balanceamento de dados, onde o número de amostras em cada classe foi ajustado para igualar a quantidade da classe minoritária. Utilizou-se o método de *undersampling*, que ajusta todas as classes para o número de registros da classe com menor frequência, mitigando o impacto do desbalanceamento no treinamento

do modelo. Este procedimento buscou reduzir o viés do modelo para as classes majoritárias, melhorando a representatividade das classes minoritárias nos resultados.

Após o balanceamento, os dados foram novamente embaralhados e salvos em um novo arquivo `CSV`. No *pipeline* de treinamento, foi adicionada uma função para balancear os dados, selecionando aleatoriamente um subconjunto. Em seguida, o conjunto de dados foi normalizado. Essa sequência de etapas ajudou a evitar a sobre-representação de qualquer classe e permitiu uma comparação mais justa entre as classes durante a avaliação do modelo.

3.8 Construção dos Modelos

A construção dos modelos contou com as seguintes etapas de processamento:

1. **Montagem do *Google Drive* e Carregamento de Dados:** Inicialmente, os arquivos de dados foram carregados diretamente do *Google Drive*, utilizando o *Google Colab* como ambiente de execução. O conjunto de dados utilizado continha registros de classes desbalanceadas e foi armazenado no formato `CSV`.

2. **Limpeza e Tratamento de Dados:** Em ambos os processos, foram removidas as linhas com valores NaN (Not a Number) para garantir consistência nos dados. Em seguida, os dados foram separados em variáveis independentes (características) e dependentes (rótulos).

3. **Codificação dos Rótulos:** Para facilitar o processamento do modelo, a coluna de rótulos foi convertida para valores numéricos por meio de uma função de conversão de dados categóricos para numéricos. Esse processo permitiu que o algoritmo de *machine learning* tratasse os rótulos como variáveis numéricas. O objeto construído com a conversão foi salvo no *Google Drive* para futura referência.

4. **Divisão dos Dados:** O conjunto de dados foi dividido em conjuntos de treino e teste, com 80% dos dados destinados ao treino e 20% para teste, utilizando uma "semente"para aleatoriamente misturar os dados. O valor 42 foi utilizado para a "semente", garantindo reprodutibilidade nos experimentos.

5. **Treinamento e Avaliação do Modelo:** Ambos os processos utilizaram os classificadores *Random Forest* e *Decision Tree* para modelar os dados. Após o treinamento, o modelo foi

avaliado utilizando a métrica de acurácia no conjunto de teste. O modelo treinado e os rótulos foram salvos no *Google Drive* para futuras análises.

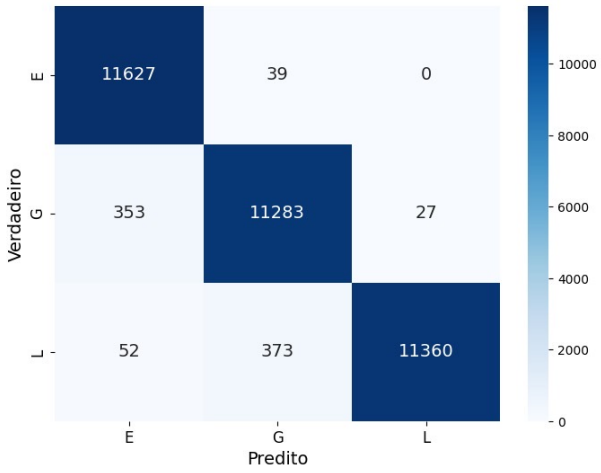
CAPÍTULO 4

RESULTADOS E DISCUSSÃO

A partir dos modelos treinados com os algoritmos *Random Forest* e *Decision Tree*, foram gerados resultados visuais em forma de gráficos que permitiram uma análise detalhada do desempenho de cada abordagem. Duas estratégias experimentais foram conduzidas: uma utilizando o conjunto de dados original, desbalanceado, e outra empregando o conjunto balanceado por meio da técnica de *undersampling*. Os resultados obtidos evidenciam a importância do balanceamento de classes para a detecção eficaz de *ransomware*.

No modelo balanceado, utilizando o algoritmo de *machine learning Random Forest*, as métricas obtidas indicaram um bom desempenho geral, com *Precision* de 96,70%, *Recall* de 96,64%, *F1-score* de 96,65% e *AUC-ROC* de 99,06%. A Figura 4.1 mostra a matriz confusão para este modelo, onde é possível observar uma distribuição mais harmoniosa dos acertos ao longo das três classes: *ransomware crypto* (E), *ransomware locker* (L) e *goodware* (G). A diagonal da matriz revela que o modelo balanceado foi capaz de identificar com maior precisão as três classes, sem um viés significativo para as classes majoritárias (isto é, classes com número maior de exemplares na base de dados original).

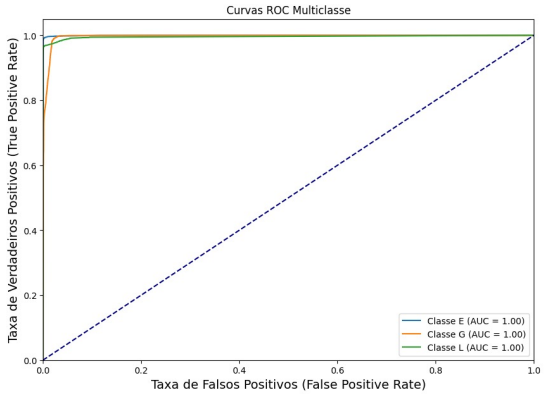
Figura 4.1: Matriz de Confusão do Modelo Balanceado - *Random Forest*



Fonte: Elaborado pelos autores.

Além disso, a Figura 4.2 apresenta a curva *ROC* para o modelo balanceado, demonstrando uma área sob a curva elevada, o que indica uma excelente capacidade de discriminação entre as classes.

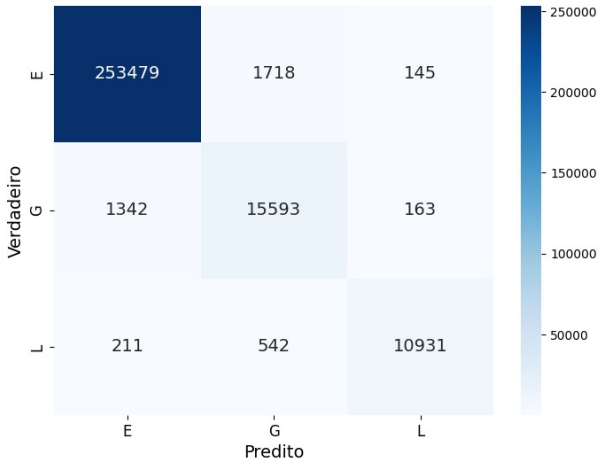
Figura 4.2: Curva ROC do Modelo Balanceado - *Random Forest*



Fonte: Elaborado pelos autores.

Em contrapartida, o modelo desbalanceado, também treinado com o *Random Forest*, apresentou métricas ligeiramente superiores: *Precision* de 98,58%, *Recall* de 98,55%, *F1-Score* de 98,56% e *AUC-ROC* de 99,35%. No entanto, ao analisar a Figura 4.3, que exibe a matriz confusão do modelo desbalanceado, observa-se que este modelo teve uma maior concentração de acertos nas classes majoritárias, resultando em uma menor precisão na classificação das classes minoritárias (como o *ransomware locker*). Essa distribuição menos equilibrada indica que, embora as métricas globais sejam mais elevadas, o modelo desbalanceado tende a falhar em identificar corretamente amostras de classes menos representadas.

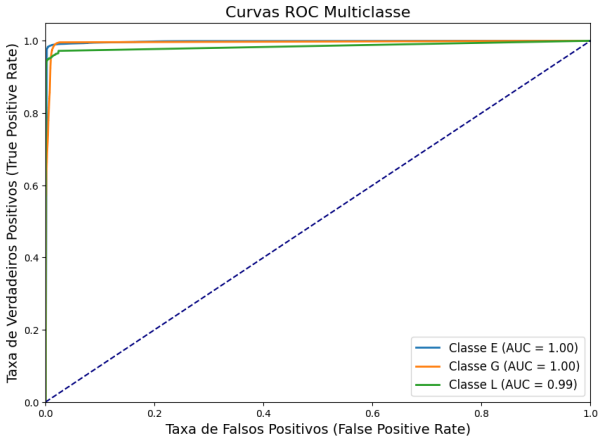
Figura 4.3: Matriz de Confusão do Modelo Desbalanceado - *Random Forest*



Fonte: Elaborado pelos autores.

A Figura 4.4 exibe a curva *ROC* do modelo desbalanceado, que mostra uma ligeira vantagem em relação ao modelo balanceado. Contudo, a análise da matriz confusão destaca o impacto negativo do desbalanceamento sobre a classificação de classes minoritárias.

Figura 4.4: Curva ROC do Modelo Desbalanceado - *Random Forest*



Fonte: Elaborado pelos autores.

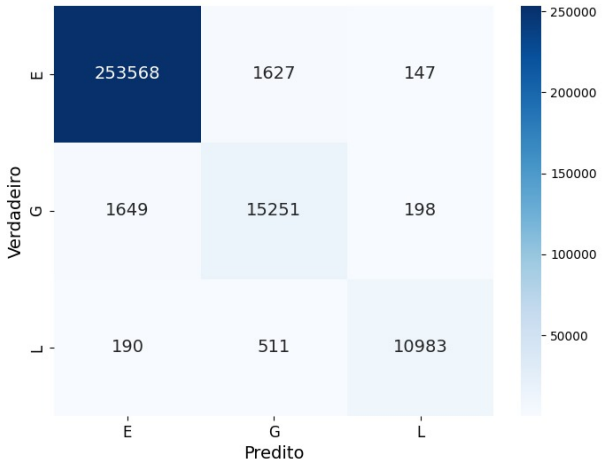
Apesar das métricas mais elevadas do modelo desbalanceado, é importante notar que o modelo balanceado apresentou uma matriz confusão mais harmoniosa, com uma melhor distribuição de acertos entre todas as classes. Essa diferença se reflete diretamente na capacidade de o modelo balanceado identificar de maneira mais uniforme os diferentes tipos de *ransomware* e *goodware*, sem favorecer as classes com mais amostras.

Em um segundo experimento, foi utilizado o algoritmo *Decision Tree* para comparar o desempenho do modelo em duas abordagens distintas: uma com o conjunto de dados balanceado

e outra com o conjunto de dados desbalanceado, de forma análoga ao experimento realizado com o *Random Forest*. Os resultados das métricas foram semelhantes aos observados anteriormente, confirmando a influência positiva do balanceamento de dados na distribuição dos acertos entre as classes.

Para o modelo treinado com o conjunto de dados desbalanceado, as métricas obtidas foram: *Precision* de 98,49%, *Recall* de 98,48%, *F1-Score* de 98,48% e *AUC-ROC* de 97,47%. A matriz confusão para este modelo, mostrada na Figura 4.5, revela uma maior concentração de acertos nas classes majoritárias:

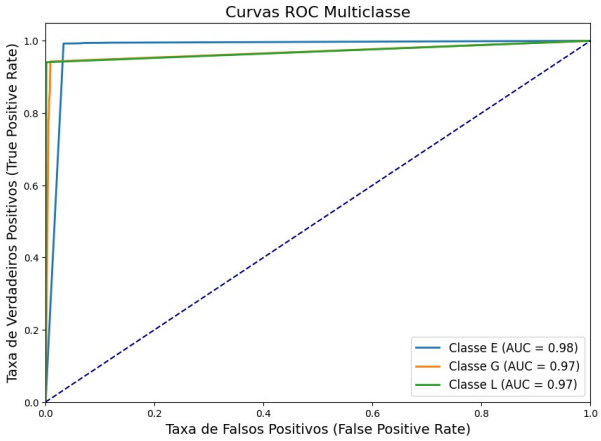
Figura 4.5: Matriz de Confusão do Modelo Desbalanceado - *Decision Tree*



Fonte: Elaborado pelos autores.

Conforme mostrado na Figura 4.6, a curva *ROC* do modelo desbalanceado utilizando o algoritmo *Decision Tree* revela uma área sob a curva (*AUC-ROC*) de 97,47%. No entanto, o desempenho do modelo é prejudicado pela dificuldade em classificar corretamente as classes minoritárias, evidenciando o impacto negativo do desbalanceamento dos dados.

Figura 4.6: Curva ROC do Modelo Desbalanceado - *Decision Tree*

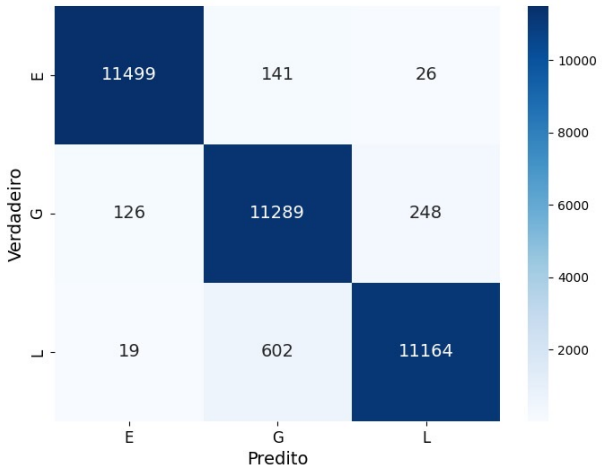


Fonte: Elaborado pelos autores.

A análise conjunta da curva *ROC* (Figura 4.6) e da matriz confusão (Figura 4.5) do modelo desbalanceado revela um desempenho ambíguo. Embora a área sob a curva (*AUC-ROC*) de 97,47% indique uma boa capacidade geral de discriminação entre as classes, a matriz confusão evidencia que os acertos estão concentrados nas classes majoritárias, resultando em um menor desempenho para as classes menos representadas, como a *ransomware locker*. Essa discrepância aponta para um viés significativo na classificação das classes minoritárias, refletindo a influência do desbalanceamento dos dados.

Por outro lado, o modelo treinado com o conjunto de dados balanceado apresentou as seguintes métricas: *Precision* de 96,73%, *Recall* de 96,69%, *F1-Score* de 96,70% e *AUC-ROC* de 97,60%. A matriz confusão para o modelo balanceado, apresentada na Figura 4.7, exibe uma distribuição de acertos mais equilibrada entre as três classes, incluindo *ransomware crypto* (E), *ransomware locker* (L) e *goodware* (G):

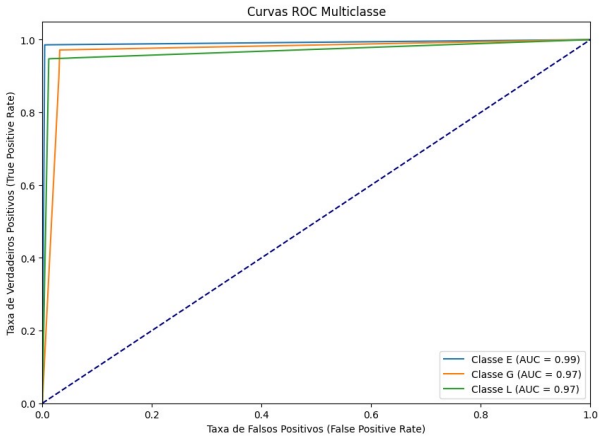
Figura 4.7: Matriz de Confusão do Modelo balanceado - *Decision Tree*



Fonte: Elaborado pelos autores.

A Figura 4.8 apresenta a curva *ROC* do modelo balanceado utilizando o algoritmo *Decision Tree*. Essa curva demonstra uma boa capacidade de discriminação entre as classes, evidenciada pela área sob a curva (*AUC-ROC*) de 97,60%, refletindo a eficácia do balanceamento dos dados em proporcionar um desempenho consistente na classificação das três classes.

Figura 4.8: Curva ROC do Modelo balanceado - *Decision Tree*



Fonte: Elaborado pelos autores.

Consequentemente, o modelo treinado com o conjunto de dados balanceado apresentou uma identificação mais uniforme entre as classes, conforme indicado pela matriz confusão (Figura 4.7). Essa uniformidade reflete uma redução no viés observado em modelos treinados com dados desbalanceados, resultando em uma distribuição mais equitativa dos acertos. Além disso, a curva *ROC* correspondente (Figura 4.8) reforça a consistência do desempenho do modelo, evidenciando que o balanceamento dos dados permitiu ao *Decision Tree* alcançar uma

classificação mais justa e representativa entre as classes.

Esses resultados comprovam que, mesmo ao empregar um algoritmo diferente, o balanceamento do conjunto de dados contribui para uma classificação mais equitativa, reduzindo o viés em relação às classes majoritárias e melhorando a capacidade do modelo de identificar amostras de classes menos representadas.

CONCLUSÃO

O desenvolvimento deste trabalho demonstra a importância do balanceamento de classes para a construção de modelos eficazes fazendo uso de *Random Forest* e *Decision Tree*, uma vez que a técnica de balanceamento de classes melhora a capacidade de identificação de diferentes tipos de *ransomware*. Essa análise evidencia a necessidade de pré-processamento dos dados em aplicações de detecção de ameaças cibernéticas, garantindo que todas as classes sejam representadas de forma adequada. A análise comparativa entre *datasets* balanceados e desbalanceados revela diferenças significativas no desempenho do modelo, especialmente na precisão da identificação das classes minoritárias.

Os resultados obtidos contribuem para pesquisas futuras em detecção de *ransomware*, oferecendo uma base sólida para o desenvolvimento de sistemas de segurança mais robustos e eficazes. Além disso, abrem caminho para trabalhos como a aplicação de algoritmos mais sofisticados baseados em IA, incluindo redes neurais profundas e modelos generativos, capazes de explorar representações mais complexas e detalhadas dos dados. Também pretende-se explorar a integração de técnicas de Processamento de Linguagem Natural (PLN) para a análise de metadados e padrões textuais associados a arquivos maliciosos, o que pode ampliar as capacidades de detecção e prevenção em sistemas heterogêneos.

4.1 Trabalhos Futuros

Diante dos resultados obtidos, para trabalhos futuros pretende-se:

- Estudar outros algorítimos de classificação.
- Analisar o desempenho do balanceamento em outros métodos de classificação.

- Investigar novos estudos relacionados à prevenção e mitigação de ataques.
- Realizar experimentos com outras bases de dados.

REFERÊNCIAS BIBLIOGRÁFICAS

Agência Nacional de Telecomunicações (ANATEL). Relatório analítico do impacto da pandemia de COVID-19 no setor de telecomunicações do Brasil (2ª edição). 2021. Acessado em: 27 out. 2024. Disponível em: <https://www.gov.br/anatel/pt-br/dados/relatorios-de-acompanhamento/2021#R202119>.

ALTALHAN, M.; ALGARNI, A.; ALOUANE, M. T.-H. Imbalanced Data Problem in Machine Learning: A Review. *IEEE Access*, v. 11, p. xxxx–xxxx, 2025.

Associação Brasileira das Empresas de Software (ABES). Ransomware: escolas lideram a lista de alvos preferenciais. 2024. Acessado em: 27 out. 2024. Disponível em: <https://abes.com.br/ransomware-escolas-lideram-a-lista-de-alvos-preferenciais/>.

BELLO, I.; CHIROMA, H.; ABDULLAHI, U. A.; GITAL, A. Y.; JAURO, F.; KHAN, A.; OKESOLA, J. O.; ABDULHAMID, S. M. Detecting Ransomware Attacks Via Intelligent Algorithms: Recent Development and Next Direction from Deep Learning and Big Data Perspectives. *Journal of Ambient Intelligence and Humanized Computing*, 2021. Disponível em: Springer. Acesso em: 13 nov. 2024.

CHEN, Q.; BRIDGES, R. Automated behavioral analysis of malware: A case study of WannaCry ransomware. *Proc. 16th IEEE Int. Conf. Mach. Learn. Appl.*, p. pp.454–460, 2017.

DHILLON, G.; WARD, J. Chaos Theory as a Framework for Studying Information Systems. *Information Resources Management Journal*, v. 15, 2002.

EVANGELISTA, D. W.; LIMA, H. de Cássia Sousa da C. *Aplicação de Aprendizado de Máquina na Classificação de Ransomwares*. [S.l.], 2023. Disponível em: UFOP. Acesso em: 13 nov. 2024.

GANGANWAR, V. An overview of classification algorithms for imbalanced datasets. *International Journal of Emerging Technology and Advanced Engineering*, v. 2, n. 4, p. 42–47, 2012.

HERRERA-SILVA, J. A.; HERNáNDEZ-ÁLVAREZ, M. Dynamic Feature Dataset for Ransomware Detection Using Machine Learning Algorithms. *Sensors*, v. 23, p. 1053, 2023.

KLEINA, N. Número de ataques contra empresas dispara em 2021. 2021. Acessado em: 27 out. 2024. Disponível em: <https://blog.avast.com/pt-br/numero-de-ataques-contra-empresas-dispara-em-2021>.

MARCHEWKA, J. T. *Information technology project management: Providing measurable organizational value*. [S.l.]: John Wiley & Sons, 2016.

Microsoft. Digital Defense Report. 2020. Acessado em: 27 out. 2024. Disponível em: <https://www.microsoft.com/pt-br/security/business/security-intelligence-report>.

Microsoft Threat Intelligence. Navigating cyberthreats and strengthening defenses in the era of AI. *Microsoft Cyber Signals*, 2024. Disponível em: <https://www.microsoft.com/security/blog/2024/02/01/navigating-cyberthreats-and-strengthening-defenses-in-the-era-of-ai>.

MOORE, C. Detecting Ransomware with Honeypot Techniques. *IEEE Computer Society*, 2016. Disponível em: IEEE. Acesso em: 13 nov. 2024.

MUJINGA, M.; ELOFF, M. M.; KROEZE, J. H. H. A socio-technical approach to information security. 2017.

Organização Pan-Americana de Saúde (OPAS). Folha informativa sobre COVID-19 / Histórico da pandemia de COVID-19. 2023. Acessado em: 27 out. 2024. Disponível em: <https://www.paho.org/pt/covid19>.

PUTRO, P. A. W.; HANDRI, E. Y.; SENSUSE, D. I. Information system approaches in cybersecurity. *Procedia Computer Science*, Elsevier, v. 234, p. 1372–1379, 2024.

RAFIQUE, M. F.; ALI, M.; QURESHI, A. S.; KHAN, A.; MIRZA, A. M. Enhancing Malware Classification: A Comparative Study of Feature Selection Models with Parameter Optimization. *Journal of Ambient Intelligence and Humanized Computing*, 2023. Disponível em: arXiv. Acesso em: 13 nov. 2024.

RAZAULLA, S.; FACHKHA, C.; MARKARIAN, C.; GAWANMEH, A.; MANSOOR, W.; FUNG, B. C. M.; ASSI, C. The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions. *IEEE Access*, v. 11, p. 40698–40723, 2023.

RESHMI, T. Information security breaches due to ransomware attacks - a systematic literature review. *International Journal of Information Management Data Insights*, v. 1, p. 100013, 2021.

SHAAMBHAVI, S.; MANOHAR, M. M.; VIJAYALAKSHMI, M. A Comparative Study of Machine Learning Models for Malware Detection. *Computer Vision and Robotics*, 2023. Disponível em: Springer. Acesso em: 13 nov. 2024.

SUAREZ, L.; ALSHUBRUMI, D.; O'CONNOR, T.; SUDHAKARAN, S. Unsafe at any Bandwidth: Towards Understanding Risk Factors for Ransomware in Higher Education. *Procedia Computer Science*, 2024.