**ENGENHARIA DE COMPUTAÇÃO**

Leonardo Munhoz Libardi

**IA de análise de dados para reconhecer ataques cibernéticos**

Piracicaba

2024

Leonardo Munhoz Libardi

**IA de análise de dados para reconhecer ataques cibernéticos do tipo *Phishing***

Trabalho de Conclusão de Curso apresentado à Escola de Engenharia de Piracicaba como parte dos requisitos para obtenção do título de Bacharel em **Engenharia de Computação**.

Orientador: Prof. Clerivaldo José Roccia

Piracicaba

2024

Leonardo Munhoz Libardi

**IA de análise de dados para reconhecer ataques cibernéticos do tipo *Phishing***

Trabalho de Conclusão de Curso apresentado à Escola de Engenharia de Piracicaba como parte dos requisitos para obtenção do título de Bacharel em Engenharia de Computação.

Piracicaba, 05 de novembro de 2024

**Banca Examinadora:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nome e sobrenome do Professor Orientador – (Presidente)

Titulação

Instituição onde trabalha

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nome e sobrenome – (Membro)

Titulação

Instituição onde trabalha

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nome e sobrenome – (Membro)

Titulação

Instituição onde trabalha

*Dedico este trabalho aos meus pais Sra. Ana Paula Munhoz Libardi e Sr. Juliano Zangelmi Libardi, ao meu irmão Sr. Rafael Munhoz Libardi, à minha namorada Srta. Ana Flávia Ortiz de Paula, aos meus tios Sr. Mauricio Munhoz e Sr. Alexandre Zangelmi Libardi, a minha tia Sra. Viviane Munhoz Andrade, as minhas avós Sra. Ivete Ferrer Munhoz e Sra. Neide Zangelmi Libardi e aos meus falecidos avôs Sr. Orlando Munhoz e Sr. Antônio Jair Libardi.*

AGRADECIMENTOS

Meus agradecimentos a todos os que contribuíram, direta ou indiretamente, para a realização deste trabalho, em especial:

Aos professores do curso pela ..................

A meu orientador Prof. Clerivaldo José Roccia, pela paciência,

Aos meus familiares pela paciência que tiveram comigo durante esses cinco anos, por sempre me apoiarem, por me fornecerem forças e continuar lado a lado comigo nessa difícil jornada que realizamos.

RESUMO

Este estudo investiga o emprego da Inteligência Artificial (IA) na análise de dados com o propósito de identificar situações de ataques *Phishing*. O objetivo principal é desenvolver um sistema de IA capaz de detectar padrões suspeitos e responder de forma eficaz a possíveis ataques virtuais. Para alcançar esse objetivo, foi adotada uma abordagem que combina revisão da literatura especializada com a implementação prática de algoritmos de IA em um ambiente de teste simulado.

A pesquisa revela que a integração da IA na análise de dados é uma estratégia promissora para fortalecer a segurança cibernética. Os resultados obtidos demonstram a eficácia do sistema desenvolvido na detecção precoce de ameaças cibernéticas, permitindo uma resposta rápida e assertiva para mitigar potenciais danos. A análise detalhada das métricas de desempenho do sistema revela uma taxa significativa de detecção de ameaças, com uma baixa taxa de falsos positivos, o que confirma a viabilidade e eficácia da abordagem proposta.

Como conclusão, destaca-se a importância da IA como uma ferramenta poderosa na proteção contra ameaças cibernéticas. Este estudo evidencia a capacidade da IA de analisar grandes volumes de dados em tempo real e identificar comportamentos anômalos, possibilitando uma resposta proativa diante de possíveis ataques. Além disso, ressalta-se a necessidade contínua de pesquisa e desenvolvimento de técnicas avançadas de IA para enfrentar os desafios em constante evolução no cenário da segurança cibernética.

Em síntese, este estudo contribui significativamente para o avanço do conhecimento na área de segurança cibernética, oferecendo uma solução prática e aplicável para fortalecer a proteção digital contra ameaças virtuais, mais especificamente o *Phishing*. Ao integrar a IA na análise de dados, torna-se possível não apenas identificar e neutralizar estes ataques, mas também antecipar e prevenir futuras ameaças, garantindo assim um ambiente online mais seguro e confiável para indivíduos e organizações.

**Palavras-chave:** Inteligência Artificial, Análise de Dados, Segurança Cibernética, Ameaças Cibernéticas, Detecção de Padrões, *Phishing*.

**LISTA DE ILUSTRAÇÕES**

[**Desenho 1 -** Livro de abertura 15](#_Toc43242143)

[**Gráfico1** - As curvas produzidas pelo VarioCam Plus 16](#_Toc43242144)

[**Fotografia 1 -** Concretagem finalizada 16](#_Toc43242146)

[**Quadro 1 -** Rolamentos 17](#_Toc43242147)

[**Fluxograma 1 -** Processo do Quality Gate 17](#_Toc43242148)

**LISTA DE TABELAS**

[**Tabela 1 -** Faixa etária 18](#_Toc43242340)

**LISTA DE ABREVIATURAS E SIGLAS**

**ABCCMM:** Associação Brasileira de Criadores de Cavalos Manga Larga Marchador

**FUMEP:** Fundação Municipal de Ensino de Piracicaba

**EEP:** Escola de Engenharia de Piracicaba

**SUMÁRIO**

[**1 INTRODUÇÃO** 12](#_Toc43243811)

[**2 REFERENCIAL CIENTÍFICO E TECNOLÓGICO** 13](#_Toc43243812)

2.1. **Segurança Cibernética: Conceitos e Desafios**

2.2 ....

[**3 MATERIAIS E MÉTODOS** 26](#_Toc43243833)

[**4 DESENVOLVIMENTO** 27](#_Toc43243834)

4.1 ....

4.2 .....

[**5 CONSIDERAÇÕES FINAIS** 28](#_Toc43243835)

5.1

5.2

5.3

[**REFERÊNCIAS** 29](#_Toc43243836)

[**APÊNDICE A – Título do apêndice** 30](#_Toc43243837)

[**ANEXO A – Título do anexo** 32](#_Toc43243838)

# INTRODUÇÃO

Na era digital em que vivemos, a segurança cibernética emergiu como um dos principais desafios enfrentados pelas organizações e indivíduos. Com o aumento exponencial de dados gerados e transações realizadas online, a necessidade de proteger sistemas e redes contra-ataques cibernéticos torna-se cada vez mais importante. Nesse contexto, a Inteligência Artificial (IA) surge como uma ferramenta promissora para a detecção e prevenção de ameaças virtuais.

A presente pesquisa se insere no campo da segurança cibernética, mais especificamente na área de análise de dados para o reconhecimento de ataques cibernéticos. Com base em uma revisão da literatura atualizada, constata-se que os ataques cibernéticos têm se tornado cada vez mais sofisticados e frequentes, representando uma ameaça significativa para organizações de todos os setores e para os usuários individuais da internet.

Os ataques cibernéticos apresentam diversas formas e podem resultar em consequências devastadoras, como roubo de dados sensíveis, interrupção de serviços essenciais e danos financeiros. Diante desse cenário, torna-se essencial desenvolver técnicas avançadas de detecção e prevenção de ataques cibernéticos, capazes de identificar padrões suspeitos e agir proativamente para mitigar potenciais danos.

O objetivo principal deste trabalho é desenvolver e implementar um sistema de IA para análise de dados, visando reconhecer e responder a ataques cibernéticos de maneira eficaz. Ao final desta pesquisa, espera-se fornecer uma contribuição significativa para a área de segurança cibernética, apresentando uma solução viável e eficiente para proteger sistemas e redes contra ameaças virtuais.

Ao abordar esses aspectos, este estudo busca não apenas apresentar um panorama atualizado do problema dos ataques cibernéticos, mas também propor uma abordagem inovadora e eficaz para lidar com essa questão premente. A partir dessa introdução, o presente trabalho se desenvolverá, explorando em detalhes os fundamentos teóricos, metodológicos e práticos relacionados ao tema proposto.

# REFERENCIAL CIENTÍFICO E TECNOLÓGICO

A crescente digitalização dos processos e a expansão das redes de informação têm exposto sistemas e dados a uma variedade de ameaças cibernéticas cada vez mais sofisticadas. Nesse contexto, a necessidade de desenvolver e implementar métodos eficazes para a detecção e mitigação de ataques cibernéticos tornou-se primordial. A Inteligência Artificial (IA) e a análise de dados têm emergido como ferramentas poderosas na defesa contra possíveis ameaças, oferecendo novas possibilidades para a segurança cibernética.

* 1. **Segurança Cibernética: Conceitos e Desafios**

A segurança cibernética refere-se às práticas e tecnologias utilizadas para proteger sistemas, redes e dados de ataques digitais. Segundo Stallings (2011), a segurança cibernética envolve a proteção de informações e sistemas de informações contra acessos não autorizados, ataques, destruição ou modificação. Com o aumento da complexidade e frequência dos ataques, as abordagens tradicionais de segurança, baseadas em assinaturas e regras fixas, mostraram-se insuficientes (SYMANTEC, 2019). Um dos métodos de ataque mais comuns é o phishing, uma forma de ataque em que os cibercriminosos enganam as vítimas para que revelem informações sensíveis, como senhas ou detalhes bancários, disfarçando-se como entidades confiáveis (JAKOBSSON; MYERS, 2006). O phishing representa um desafio contínuo na segurança cibernética, especialmente com a evolução de técnicas de ataque que utilizam engenharia social e personalização para aumentar a taxa de sucesso (KASPERSKY LAB, 2018).

* 1. **Análise de Dados na Segurança Cibernética**

A análise de dados envolve a inspeção, limpeza e modelagem de dados com o objetivo de descobrir informações úteis e apoiar a tomada de decisões. Na segurança cibernética, a análise de dados é utilizada para identificar padrões e anomalias que possam indicar atividades maliciosas. De acordo com Chandola, Banerjee e Kumar (CHANDOLA, V.; BANERJEE, A.; KUMAR, V., 2009), a detecção de anomalias é um campo essencial na segurança cibernética, pois permite identificar comportamentos incomuns que podem ser sinais de ataques. No caso de phishing, a análise de dados pode ajudar a identificar e bloquear mensagens fraudulentas, com base em padrões comportamentais ou características típicas das comunicações de phishing, como domínios suspeitos, solicitações de informações sensíveis e erros gramaticais.

* 1. **Inteligência Artificial e Aprendizado de Máquina**

A IA, especialmente o aprendizado de máquina (ML), tem revolucionado a forma como a análise de dados é conduzida na segurança cibernética. O aprendizado de máquina envolve a criação de algoritmos que podem aprender a partir de dados e fazer previsões ou tomar decisões sem serem explicitamente programados para isso (GOODFELLOW; BENGIO; COURVILLE, 2016). Técnicas de ML, como redes neurais, florestas aleatórias e máquinas de vetores de suporte, têm sido aplicadas com sucesso na detecção de anomalias e ameaças (SOMMER; PAXSON, 2010). No combate ao phishing, algoritmos de ML são frequentemente usados para identificar e bloquear tentativas de phishing, treinando modelos com grandes conjuntos de dados de exemplos de phishing e emails legítimos, permitindo assim uma detecção mais eficaz e automatizada.

# ****Aplicação da IA na Detecção de Ataques Cibernéticos****

A aplicação da IA na detecção de ataques cibernéticos inclui o uso de algoritmos de aprendizado supervisionado e não supervisionado para identificar atividades maliciosas. Buczak e Guven (2016) destacam que o aprendizado supervisionado pode ser usado para treinar modelos com base em dados rotulados de ataques conhecidos, enquanto o aprendizado não supervisionado é eficaz na detecção de anomalias em dados sem rótulos. Além disso, técnicas de deep learning têm mostrado grande potencial na análise de grandes volumes de dados em tempo real (KASPERSKY LAB, 2018). Especificamente no caso de phishing, a IA pode ser utilizada para analisar grandes quantidades de comunicações digitais em busca de padrões que indiquem fraudes, oferecendo defesas em tempo real contra tentativas de engano.

* 1. **Desafios e Futuras Direções**

Apesar dos avanços, a implementação de IA na segurança cibernética enfrenta desafios significativos. Estes incluem a necessidade de grandes volumes de dados rotulados para treinar modelos supervisionados, a dificuldade em interpretar os resultados dos modelos de IA e a evolução contínua das técnicas de ataque (SOMMER; PAXSON, 2010). No combate ao phishing, os desafios envolvem a constante sofisticação das táticas de ataque, como o uso de spear phishing, onde os atacantes personalizam suas mensagens para indivíduos específicos, tornando mais difícil sua detecção por sistemas automatizados. A pesquisa contínua é necessária para desenvolver algoritmos mais robustos e interpretáveis e para criar sistemas capazes de se adaptar a novas ameaças.

1. **MATERIAS E MÉTODOS**

Os materiais e ferramentas utilizadas nesta pesquisa foram:

Plataforma de Dados: Kaggle, utilizado para a obtenção dos conjuntos de dados.

Linguagem de Programação: Python, versão 3.12.4

Ambiente de Desenvolvimento: Visual Studio Code (VS Code).

Bibliotecas e Pacotes Python:

*Pandas*: Para a manipulação e análise de dados.

*Numpy*: Para operações com arrays e matrizes.

*Warnings*: Para gerenciamento de alertas no programa.

*Seaborn*: Para visualização de dados.

*Matplotlib*: Para visualização de dados, utilizado em conjunto com o seaborn.

Scikit-Learn:

Métodos utilizados:

*RandomForestClassifier*: Para a construção e avaliação de modelos de classificação.

*LogisticRegression*: Para a construção e avaliação de modelos de regressão.

train\_test\_split: Para a divisão dos dados em conjuntos de treinamento e teste.

Os resultados dos modelos foram analisados e comparados utilizando métricas de desempenho como acurácia, precisão, recall e F1-score. A análise foi realizada com o auxílio da biblioteca scikit-learn, utilizando as funções classification\_report e confusion\_matrix.

# DESENVOLVIMENTO

* 1. **Introdução ao *Phishing* e a Aplicação de Machine Learning:**

A rápida expansão do uso de tecnologias digitais trouxe consigo uma crescente exposição a ciberataques. Entre as formas mais comuns desses ataques está o *phishing*, no qual hackers se disfarçam de entidades confiáveis para enganar usuários e obter informações sensíveis, como senhas, números de cartão de crédito ou detalhes de contas bancárias (JAKOBSSON; MYERS, 2006). Esses ataques têm evoluído em sofisticação, utilizando técnicas avançadas de engenharia social e personalização de mensagens, tornando-se cada vez mais difíceis de detectar. Relatórios recentes apontam que o *phishing* é uma das principais ameaças à segurança cibernética, com atacantes explorando vulnerabilidades em e-mails, redes sociais e até mesmo em aplicativos de mensagens (KASPERSKY LAB, 2018).

Em um cenário onde grande parte das interações e transações ocorre em ambientes digitais, as consequências de ataques de *phishing* podem ser devastadoras tanto para indivíduos quanto para organizações, resultando em perdas financeiras, violação de dados e danos à reputação. Para enfrentar essa ameaça crescente, é fundamental desenvolver métodos mais eficazes de detecção. As abordagens tradicionais, como listas negras e regras estáticas, têm se mostrado insuficientes para lidar com a agilidade dos ataques, especialmente em um ambiente de ameaças em constante evolução (SYMANTEC, 2019).

Nesse contexto, o uso de Machine Learning (ML) tem se mostrado promissor como uma solução inovadora para detectar ataques de *phishing*. Algoritmos de aprendizado supervisionado e não supervisionado permitem a análise automática de grandes volumes de dados, identificando padrões de comportamento suspeitos com maior precisão e rapidez (GOODFELLOW; BENGIO; COURVILLE, 2016). Técnicas de ML oferecem uma vantagem significativa, pois conseguem aprender com dados históricos e ajustar-se a novas variantes de ataques, o que reduz a necessidade de intervenção manual e melhora a capacidade de resposta a novas ameaças.

Este trabalho explora a aplicação de diferentes algoritmos de ML, como Regressão Logística, *Random Forest* e *Naive Bayes*, na detecção de tentativas de *phishing* em ambientes digitais. Além de investigar a eficácia desses métodos, o estudo busca discutir as limitações, o desempenho em cenários reais e o as potenciais aplicações futuras desses modelos no campo da segurança cibernética.

* 1. **Modelos de Classificação:**
     1. **Regressão Logística:**

A Regressão Logística é uma técnica de análise de dados que usa matemática para encontrar as relações entre dois fatores de dados (AMAZON WEB SERVICES, 2023). No contexto da detecção de phishing, a regressão logística pode ser utilizada para prever se uma transação ou e-mail é legítimo ou malicioso com base em características observadas.

Este algoritmo é amplamente utilizado devido à sua simplicidade e eficiência em problemas de classificação binária. A equação da regressão logística transforma uma combinação linear das características em uma probabilidade, que é então comparada a um limiar (geralmente 0,5) para classificar o evento.

* + 1. **Random Forest:**

O Random Forest é um algoritmo de aprendizado supervisionado baseado em um conjunto de árvores de decisão (BREIMAN, 2001). Ele constrói múltiplas árvores de decisão em diferentes subconjuntos dos dados de treino e, posteriormente, combina suas previsões para melhorar a precisão e reduzir o overfitting. No caso de detecção de phishing, o Random Forest oferece uma vantagem em relação à regressão logística ao lidar com relações mais complexas entre as variáveis, além de ser robusto a dados ruidosos.

Um dos principais pontos fortes do Random Forest é sua capacidade de operar em grandes conjuntos de dados com muitas características, além de fornecer medidas de importância para cada variável, o que pode ajudar na interpretação do modelo.

* + 1. ***Naive Bayes*:**

O *Naive Bayes* é um classificador probabilístico baseado no Teorema de *Bayes*, que assume independência entre as características (ZHANG, 2004). Embora essa suposição nem sempre seja verdadeira em problemas do mundo real, o Naive Bayes tem se mostrado eficaz em uma ampla gama de problemas de classificação, especialmente em filtragem de e-mails e detecção de *phishing*.

Esse modelo calcula a probabilidade de uma amostra pertencer a uma determinada classe com base na probabilidade condicional das características e escolhe a classe com a maior probabilidade. Apesar de ser um modelo simples, o *Naive Bayes* tem o benefício de ser muito rápido e escalável para grandes volumes de dados.

* 1. **Metodologia:**
     1. **Conjunto de Dados:**

O conjunto de dados utilizado para o treinamento e teste do modelo foi dividido em subconjuntos de treinamento e teste usando a função train\_test\_split. Este procedimento garante que o modelo seja treinado em uma parte dos dados e avaliado em uma parte independente, garantindo uma avaliação imparcial da performance.

* + 1. **Treinamento do Modelo:**

Para o treinamento, utilizou-se a função LogisticRegression da biblioteca Scikit-learn. O treinamento foi realizado em dados rotulados, e a precisão do modelo foi avaliada no conjunto de teste. A função fit() foi usada para ajustar o modelo, e a função score() para calcular a precisão.

* + 1. **Avaliação de Desempenho:**

O modelo de Regressão Logística foi avaliado com base na métrica de acurácia, que indica a porcentagem de previsões corretas realizadas pelo modelo no conjunto de teste. A acurácia final obtida foi de aproximadamente 95%, o que sugere que o modelo é eficaz na classificação de eventos como maliciosos ou legítimos.

* 1. **Resultados:**

O modelo treinado apresentou uma acurácia de 95%, o que indica um alto nível de precisão na detecção de atividades maliciosas. No entanto, outros fatores, como a sensibilidade (capacidade de detectar ataques) e a especificidade (capacidade de evitar falsos positivos), devem ser analisados para avaliar melhor a performance do modelo em diferentes cenários.

# CONSIDERAÇÕES FINAIS

**5.1 Discussão sobre os Resultados**

**5.2 Dificuldades Encontradas**

**5.3 Trabalhos Futuros**

**REFERÊNCIAS**

Referência nada mais é que a descrição de documento citado no trabalho. Estas se fazem necessárias para possibilitar que demais leitores possam ter acesso aos materiais utilizados para elaboração do trabalho, permitindo assim, a replicação ou comprovação científica.

As referências possuem regras próprias de apresentação, portanto, devem ser representadas com espaçamento simples, alinhadas à margem esquerda (não justificadas) e separadas entre si por um espaço simples.

Devem seguir descritas em ordem alfabética crescente.

A norma que regulamenta a elaboração de referências passou por atualização em novembro de 2018, e as principais alterações foram:

Quando no livro ou revista a palavra Editora constar antes do nome desta, pela norma anterior essa informação era suprimida, aparecendo apenas o nome da editora. Com a revisão da norma, hoje deve-se indicar a palavra Editora antes do nome quando assim estiver descrito no documento consultado, porém, ainda deve-se suprimir as palavras que designam a natureza jurídica ou comercial, como por exemplo S.A. ou LTDA.

Outra alteração foi a supressão dos símbolos < > nas referências de documentos eletrônicos onde se deve indicar o endereço web. Assim, com a nova diretriz, o aluno autor deve apenas indicar a url utilizada precedida da expressão Disponível em:

Pela nova norma, agora quando se elabora uma referência de artigo extraído de anais de evento, o termo **Anais** [...] em destaque agora deve ter os três pontos entre colchetes.

Por fim, além de exemplos de referências de redes sociais, a versão de 2018 da NBR 6023 previu a utilização de livros digitais. Com isso, após a referência do livro utilizado em uma plataforma ou aplicativo de leitura, se deve acrescentar a expressão *E-book* após o ano.

Para diminuir as dúvidas em relação a elaboração de referências, os autores deste manual resolveram apresentar a seguir alguns exemplos como forma de elucidar as explicações vislumbradas com o texto deste subcapítulo.

Veja alguns exemplos utilizando o padrão obrigatório ABNT

