Revista Científica Di Fatto, ISSN 2966-4527. Edição 4. Ano: 2025.
Submissão em: 22/03/2025
Aprovação em: 25/03/2025
Publicado em: 25/03/2025
Disponível em: https://revistadifatto.com.br/artigos/aplicacao-de-aplicacao-de-inteligencia-artificial-na-deteccao-de-ameacas-em-redes-de-computadores/

Aplicação de inteligência artificial na detecção de ameaças em redes de computadores

Wesley Barbosa Rodrigues
• Engenharia Elétrica – [Faculdade de Cariacica - UNIEST] • Especialização em Engenharia de Segurança do Trabalho – [Faculdade Cândido Mendes - FACAM] • Complementação Pedagógica em Matemática [Multivix - Campus Serra - ES] • Licenciatura em Física – [Instituto Federal do Espirito Santo - IFES - ES] • Ciências Econômicas – [Universidade Cruzeiro do Sul - UNISUL] • Cursando Mestrado em Tecnologias Emergentes em Educação [Must University - Flórida]

Resumo

O texto explora o uso emergente de Inteligência Artificial (IA) na segurança de redes de computadores, destacando como algoritmos de aprendizado de máquina podem identificar padrões anômalos e detectar ameaças em tempo real. A pesquisa bibliográfica exploratória de natureza qualitativa, investiga a eficácia da IA na detecção de intrusões, redução de falsos positivos e resposta a incidentes. O objetivo principal é analisar como a IA pode aprimorar a segurança em redes, monitorando dispositivos como switches, roteadores e servidores, e antecipando vulnerabilidades. A relevância do estudo reside na crescente frequência e complexidade dos ataques cibernéticos, que exigem soluções robustas e adaptativas. A integração da IA aos sistemas de segurança busca superar métodos tradicionais, fortalecendo a segurança preditiva com análises de dados históricos e tendências.
Palavras-Chave: Segurança da Informação, Detecção de A.meaças, Aprendizado de Máquina, Redes de Computadores, Inteligência Artificial

Abstract

The text explores the emerging use of Artificial Intelligence (AI) in computer network security, highlighting how machine learning algorithms can identify anomalous patterns and detect threats in real-time. The exploratory qualitative bibliographical research investigates the effectiveness of AI in intrusion detection, reduction of false positives, and incident response. The main objective is to analyze how AI can enhance network security by monitoring devices such as switches, routers, and servers, and anticipating vulnerabilities. The relevance of the study lies in the increasing frequency and complexity of cyber attacks, which demand robust and adaptive solutions. The integration of AI into security systems seeks to surpass traditional methods, strengthening

predictive security with historical data analysis and trends.
Keywords: *Information Security, Threat Detection, Machine Learning, Computer Networks, Artificial Intelligence.*

1. INTRODUÇÃO

Desde seu início, a internet passou por transformações drásticas, com um aumento significativo no número de dispositivos conectados e no volume diário de informações trafegadas. Como resultado, o mundo precisa de profissionais que entendam sobre a Arquitetura e evolução dos softwares para aplicar a segurança da informação e desta forma possam proteger seus equipamentos, ligados em redes, como: switches, roteadores, IoT, computadores, sala de servidores de ataques criminosos e terroristas.

De acordo com (DINO, 2024), os ataques cibernéticos continuam a ser uma ameaça crescente em 2025. A Kaspersky do Brasil apresentou um relatório que mostra que o Brasil enfrenta em média de 1.379 ataques cibernéticos por minuto (JOBIM, 2024). O custo médio de uma violação de dados no país é de aproximadamente R$ 6,75 milhões. (ITFORUM, 2024) Esses ataques afetam principalmente setores como Saúde e Serviços são os mais afetados, com custos médios de R$ 10,46 milhões e R$ 8,82 milhões por violação, respectivamente. Técnicas avançadas como ransomware e phishing são as mais comuns, contribuindo significativamente para esses custos. (ITFORUM, 2024)

A utilização de técnicas de inteligência artificial (IA) para aprimorar a segurança da arquitetura de redes e software é uma área emergente. Este artigo sugere uma pesquisa bibliográfica exploratória de natureza qualitativa, propõem avaliar os tipos de software utilizados para aplicar o algoritmo de aprendizado de máquina, a fim de, identificar padrões anômalos e detectar ameaças em tempo real, aumentando a eficácia dos sistemas de segurança na arquitetura de computadores e softwares.

A aplicação de Inteligência Artificial (IA) na detecção de ameaças em redes de computadores como dito anterior é um campo emergente onde se busca aprimorar a segurança cibernética por meio de técnicas avançadas de análise de dados e aprendizado de máquina.

Sendo assim, o objetivo é investigar como a IA pode ser utilizada para identificar e mitigar ameaças em redes de computadores, aumentando a eficiência e a precisão dos sistemas de segurança. A pesquisa foca no monitoramento do acesso físico a dispositivos, como switches, roteadores, data centers, racks de equipamentos e salas de servidores, que podem comprometer a rede. Além disso, busca verificar ambientes vulneráveis e aprimorar o monitoramento de locais onde esses dispositivos estão armazenados.

A análise de IA para detectar comportamentos anômalos é essencial para identificar padrões incomuns em dados. Avaliar sua eficácia na redução de erros e tempo de resposta é crucial. Desafios na análise em tempo real exigem soluções como algoritmos adaptativos e computação distribuída para melhorar a detecção.

Entretanto, o problema de nosso estudo está em como a IA pode ser integrada aos sistemas de segurança de redes para detectar e responder a ameaças de forma mais eficaz do que os métodos tradicionais?

Por se tratar de um tema que possui uma Justificativa importante para nosso estudo, principalmente com o aumento da complexidade e frequência dos ataques cibernéticos, há uma necessidade premente de soluções mais robustas e adaptativas. A IA oferece potencial para aprimorar a detecção de ameaças, permitindo respostas mais rápidas e precisas, além de reduzir a dependência de intervenções humanas.

A Inteligência Artificial também pode ser crucial na área da segurança preditiva. Com a capacidade de analisar dados históricos e tendências atuais, os sistemas de IA conseguem antecipar possíveis vulnerabilidades e vetores de ataque. Dessa forma, as organizações podem reforçar suas defesas de forma proativa.

2. DESENVOLVIMENTO

A Inteligência Artificial (IA) desempenha um papel dual na cibersegurança, atuando tanto como uma ferramenta de defesa quanto como um vetor de ataque. De acordo com os autores consultados, a evolução das tecnologias de IA tem potencializado a eficácia das medidas de segurança, permitindo a detecção e resposta a ameaças de forma mais rápida e precisa. Por exemplo, a análise de dados em tempo real e a automação de processos de segurança são citadas como inovações que melhoram a proteção contra ataques cibernéticos (CRUZ, CASEMIRO, et al., p. 12).

No competitivo mundo empresarial de hoje, a informação é um recurso valioso que requer proteção máxima. Garantir a segurança dessas informações é essencial para gerenciar negócios e garantir que informações vitais não sejam comprometidas. Proteger informações é fundamental para a sobrevivência de uma empresa. De acordo com (PEREIRA, 2024) a Inteligência Artificial (IA) emergiu como uma ferramenta poderosa no campo da segurança cibernética, revolucionando a forma como as organizações detectam, previnem e respondem às ameaças cibernéticas.

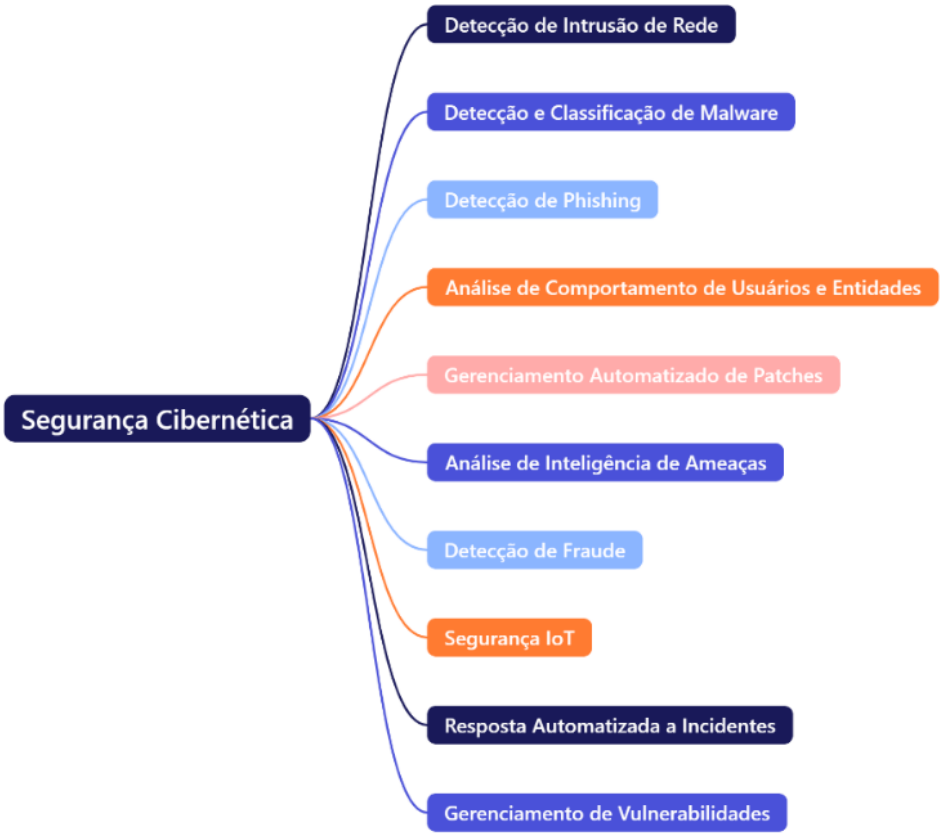
A segurança cibernética é uma prática de proteger informações e dados de fontes externas na Internet, abrangendo a proteção de redes, servidores, intranets e sistemas de computador. Com o aumento da sofisticação dos ataques cibernéticos, a Inteligência Artificial (IA) tornou-se uma

ferramenta essencial, analisando grandes volumes de dados, identificando padrões e respondendo a ameaças em tempo real. Ao aplicar algoritmos de aprendizado de máquina, a IA pode detectar anomalias no tráfego de rede e logs de sistema, melhorando significativamente a segurança cibernética ao identificar possíveis violações de segurança (PEREIRA, 2024)

A segurança da informação tem a ver com as informações que geralmente se concentram nos pilares da segurança da informação (CIA – confidencialidade, integridade e disponibilidade), e a cibersegurança trata de proteger coisas vulneráveis por meio das TIC (Tecnologias da Informação e Comunicação).
Contudo, a aplicação da inteligência artificial na cibersegurança apresenta obstáculos. Os malfeitores também estão empregando IA para elaborar ataques mais complexos, resultando em uma constante corrida tecnológica. Além disso, os sistemas de IA podem gerar alarmes falsos, potencialmente sobrecarregando as equipes de segurança com notificações. (PEREIRA, 2024)

A segurança cibernética tornou-se uma das principais preocupações no mundo digital atual, devido à crescente complexidade dos ataques, que variam de tentativas simples de phishing a malwares sofisticados que podem comprometer sistemas inteiros. Em resposta, a segurança cibernética tem evoluído com o uso de tecnologias avançadas, como a Inteligência Artificial, para prevenir e mitigar esses riscos, focando na detecção de intrusões e no gerenciamento de vulnerabilidades para proteger dados e infraestruturas críticas.

Figura 1 – 10 casos de uso de inteligência artificial na segurança cibernética.



Fonte: Próprio autor – 2025

Cada uma dessas áreas desempenha um papel crucial na defesa de redes e sistemas, sendo fundamentais para a implementação de uma estratégia robusta de segurança cibernética. A evolução da tecnologia, incluindo a inteligência de ameaças e a automação de processos de resposta a incidentes, permite que as organizações se adaptem mais rapidamente às novas ameaças.

Além disso, a segurança voltada para dispositivos da Internet das Coisas (IoT) e o gerenciamento de patches têm se mostrado vitais para evitar brechas de segurança que possam ser exploradas por cibercriminosos. Com isso, a segurança cibernética está cada vez mais centrada na integração de soluções inteligentes e rápidas para uma proteção efetiva e proativa.

2.1 IA e Segurança de Redes

A inteligência artificial (IA) tem se tornado uma ferramenta indispensável em diversos setores da economia, incluindo saúde, educação e segurança e tem se tornado uma ferramenta essencial na cibersegurança, proporcionando um aumento significativo na capacidade de detectar e responder a ameaças em redes de computadores.

De acordo com (ALMEIDA e NAS, 2024, p. 28), a implementação de tecnologias de IA permite que sistemas de segurança analisem grandes volumes de dados em tempo real, identificando padrões e comportamentos anômalos que poderiam passar despercebidos por métodos tradicionais. Essa capacidade de análise avançada não apenas acelera a resposta a incidentes, mas também melhora a prevenção de ataques cibernéticos, tornando as redes mais resilientes e seguras.

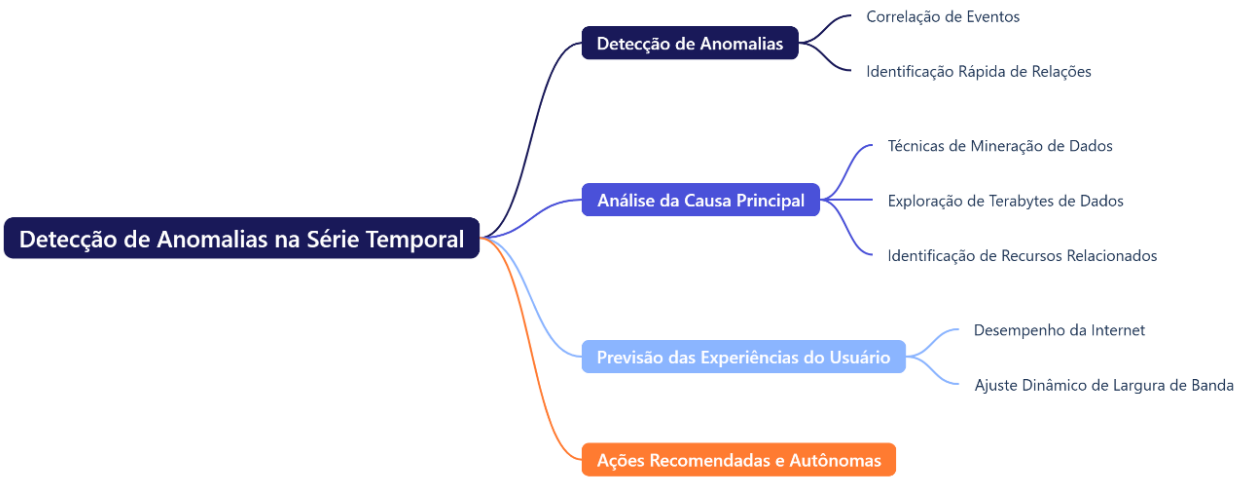
Mesmo assim, a segurança cibernética tornou-se um elemento indispensável no mundo digital contemporâneo, com o crescimento exponencial de ameaças e vulnerabilidades em ambientes conectados. Segundo uma notícia publicada pelo site (OLHAR DIGITAL, 2019), houve um incidente notável em que a rede da NASA foi hackeada devido a um dispositivo Raspberry Pi estar conectado. A segurança cibernética envolve práticas e tecnologias diversas destinadas a proteger redes, sistemas e dados contra ataques maliciosos, fraudes e outras ameaças.

Não é raro que os hackers explorem links para conexões não seguras, o que consequentemente enfraquece o sistema. No entanto, nesse incidente particular, eles conseguiram obter acesso a dados confidenciais, incluindo a Deep Space Network – a rede global de antenas que a NASA e outras agências espaciais utilizam para se comunicar (OLHAR DIGITAL, 2019).

Entre as áreas cruciais estão a detecção de intrusão em redes, a classificação de malwares, a análise de phishing e a inteligência de ameaças, que permitem identificar e mitigar riscos. Além disso, práticas como o gerenciamento automatizado de patches, a segurança IoT e a resposta automatizada a incidentes garantem maior resiliência frente às constantes inovações nas estratégias de ataque.

Assim, a segurança cibernética não só protege informações sensíveis, mas também assegura a continuidade de operações em um mundo cada vez mais dependente da tecnologia, como nos mostra a figura abaixo.

Figura 2. Detecção de Anomalias na série Temporal



Fonte: Próprio Autor – 2025.

De acordo com, (ALMEIDA e NAS, 2024) nos diz que é preciso verificar os desafios para a implementação das novas tecnologias no país na saúde, a IA é utilizada para antecipar necessidades médicas, diagnosticar doenças com maior precisão e otimizar o gerenciamento de recursos hospitalares, resultando em tratamentos mais eficazes e na melhoria da qualidade de vida dos pacientes.

Entretanto, a aplicação da IA na segurança é talvez uma das mais críticas, pois envolve a proteção de vidas, patrimônio e a manutenção da ordem pública. Sistemas de IA são empregados para monitorar atividades suspeitas, prever crimes e melhorar a resposta a emergências, mas também levantam questões éticas sobre privacidade e vigilância.

Assim, enquanto a IA promete avanços significativos em eficiência e eficácia, é fundamental que sua implementação seja acompanhada de diretrizes éticas rigorosas e uma governança responsável, garantindo que os benefícios sejam maximizados sem comprometer os direitos humanos e a justiça social.

Entretanto, a adoção da IA na cibersegurança também apresenta desafios significativos. A opacidade dos algoritmos de IA pode levar a decisões automatizadas que não são facilmente compreendidas, resultando em potenciais falhas de segurança ou discriminação em processos de autenticação (ALMEIDA e NAS, 2024, p. 17-24).

Portanto, é crucial que as organizações que implementam Inteligência Artificial em suas estratégias de cibersegurança adotem princípios de transparência e ética, garantindo que as tecnologias sejam utilizadas de maneira responsável e que os riscos associados sejam adequadamente gerenciados (BANO, 2023; ALMEIDA e NAS, 2024). Dessa forma, a IA pode não apenas fortalecer a

cibersegurança, mas também promover a confiança nas soluções tecnológicas utilizadas para proteger redes de computadores.

2.2 Algoritmos Relevantes

Os algoritmos são os pilares que sustentam a Inteligência Artificial (IA), desta forma (MTK, 2024) nos fala sofre a importância do acesso a software de IA gratuitos, para que os processos, regras e cálculos que permitem que máquinas executem tarefas de forma autônoma e inteligente possam ser usados para uma variedade de aplicações.
Alguns dos algoritmos mais relevantes em IA incluem Redes Neurais Artificiais, Máquinas de Vetores de Suporte, Algoritmos de Aprendizado de Reforço e Florestas Aleatórias (Random forest).

Quadro 1 – Principais Linguagens de programação aplicadas em IA

Categoria	Detalhes
Linguagens de Programação	Python, R, Java, C++, JavaScript
Principais Fabricantes de Hardware	NVIDIA, Intel, AMD, Google, Qualcomm
Plataformas e Frameworks	TensorFlow, PyTorch, Keras, Scikit-learn
Outros Itens Necessários	Computadores de alto desempenho, GPUs, infraestrutura de armazenamento, dados de treinamento de alta qualidade

Fonte: Próprio autor – 2025

Esses algoritmos são utilizados em diversas aplicações, desde a classificação e previsão de dados até o reconhecimento de padrões complexos em imagens e textos. O sucesso das soluções de IA depende diretamente da escolha e implementação dos algoritmos apropriados para cada problema específico.

A inteligência artificial (IA) tem se consolidado como uma área essencial no avanço da tecnologia, revolucionando a maneira como lidamos com grandes volumes de dados e tomamos decisões automatizadas.

De acordo com, (EDUKA.IA, 2023) A inteligência artificial é uma tecnologia versátil que pode ser utilizada em diferentes setores e áreas da sociedade. Um aspecto pouco conhecido por muitos é que essa ampla aplicabilidade é viabilizada pelos algoritmos que a compõem.

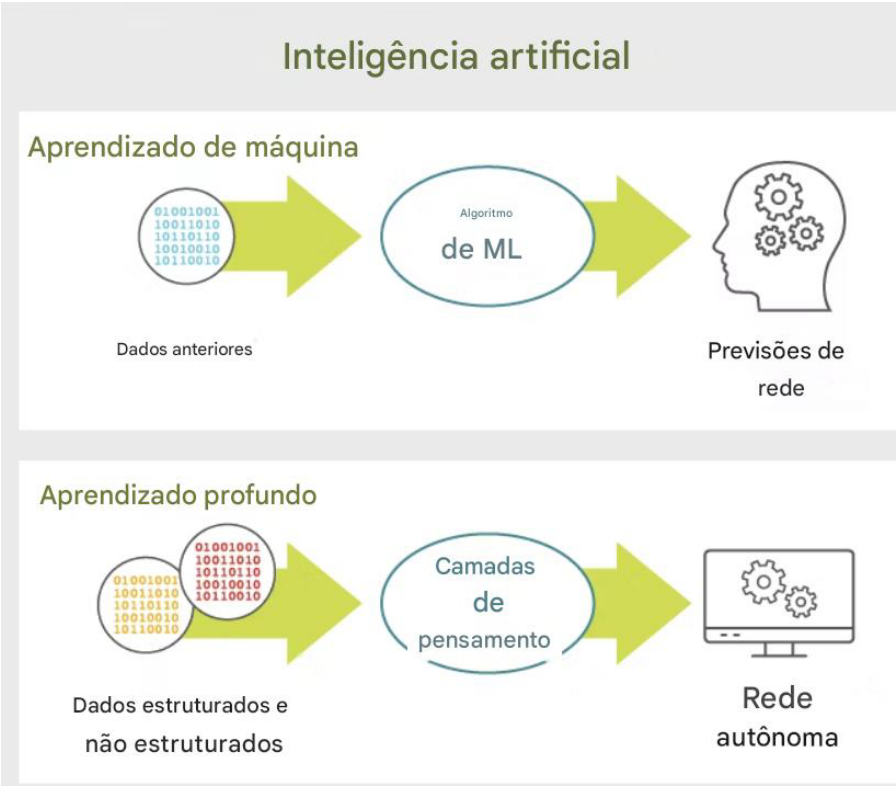
Entre os principais métodos utilizados, destacam-se o aprendizado de máquina (Machine Learning) e o aprendizado profundo (Deep Learning), que, embora relacionados, possuem abordagens distintas.

Os algoritmos representam a essência e o alicerce da inteligência artificial, sendo responsáveis por estabelecer as diretrizes, os critérios e os mecanismos que possibilitam às máquinas e dispositivos aprenderem, tomarem decisões e realizarem ações de maneira autônoma e adaptável. (EDUKA.IA, 2023)

Desta forma, O aprendizado não supervisionado pode ser comparado a um processo de aprendizado sem a orientação de um professor. Nesse caso, (JENNI, 2023) nos fala que os algoritmos analisam um conjunto de dados não rotulados, buscando identificar padrões e estruturas ocultas. Diferentemente do aprendizado supervisionado, esse método não possui uma métrica direta de precisão, já que não existe uma referência previamente conhecida para validação.

A imagem abaixo apresenta uma comparação entre aprendizado de máquina (ML) e aprendizado profundo, ambos componentes da inteligência artificial (IA).

Figura 2 – Aprendizado de Máquina x Aprendizado profundo



Fonte: Próprio Autor, 2025.

No aprendizado de máquina, os dados históricos são processados por algoritmos de ML para gerar abrangência, utilizando métodos estatísticos e matemáticos que permitem resolver problemas específicos. Esse tipo de aprendizado é altamente dependente de dados rotulados e busca de resultados otimizados a partir de padrões reconhecidos.

Por outro lado, o aprendizado profundo envolve uma maior complexidade, utilizando dados estruturados e não estruturados para redes alimentares neurais profundas, compostas por várias camadas de processamento (camadas de pensamento). Conforme (LALIBERTE, 2024), para que a Inteligência Artificial (IA) alcance êxito, é essencial o uso de aprendizado de máquina (AM). Este se caracteriza pela utilização de algoritmos que analisam dados, aprendem a partir deles e são capazes de realizar determinações ou predições sem a necessidade de instruções explícitas.

Isso resulta em sistemas mais independentes, como redes capazes de tomar decisões complexas de forma independente, sem a necessidade de intervenção humana direta. (LALIBERTE, 2024), nos fala que, Devido aos avanços nas capacidades de computação e armazenamento, o aprendizado de máquina (ML) evoluiu para modelos estruturados mais sofisticados, como o aprendizado profundo (DL). O DL utiliza redes neurais para processar uma quantidade ainda maior de informações e automatizar tarefas de maneira mais eficiente.

Isso resulta em sistemas mais autônomos, como redes capazes de tomar decisões complexas por conta própria. Podemos então, verificar o que nos diz, (LALIBERTE, 2024), na figura 2 que destaca a evolução da IA para lidar com dados diversificados e desempenhar tarefas com maior independência, processamento e a compreensão da linguagem natural (NLP/NLU), os modelos de linguagem de grande porte (LLM) e a IA generativa (GenAI).

Nesse contexto, o aprendizado não supervisionado, conforme aponta (JENNI, 2023), utiliza algoritmos para identificar padrões ou agrupamentos em dados não rotulados. Suas aplicações incluem segmentação de mercado, agrupando clientes com base em seus comportamentos de compra, e detecção de anomalias, destacando dados fora do padrão em um conjunto.

2.3 Desafios e Limitações

Criar um Fluxo de Trabalho para Inteligência Artificial (IA) começa com a coleta de dados, que deve ser relevante, de alta qualidade e representativa do problema a ser resolvido. Esses dados podem ser obtidos de várias fontes, como bancos de dados internos, APIs e sensores de IoT, sendo importante combinar diferentes fontes para garantir um conjunto robusto e diversificado.

Após a coleta, é necessário preparar os dados, de acordo com (JENNI, 2023) “à fundação de qualquer algoritmo de IA são os dados”, e desta forma é preciso fazer a limpeza para corrigir ou

remover valores ausentes, duplicados ou inconsistentes. Além disso, a normalização e transformação dos dados são realizadas para garantir que eles estejam prontos para alimentar os algoritmos de IA. A preparação adequada dos dados é essencial, pois dados mal preparados podem comprometer a eficácia do modelo.

De acordo com (EDUKA.IA, 2023), “A eficácia dos algoritmos na inteligência artificial depende fortemente dos dados de treinamento fornecidos, para exploração dos Dados, se faz necessário analisa-los exaustivamente para entender suas características e identificar padrões ou outliers. A análise exploratória de dados (EDA) ajuda a descobrir insights importantes que podem orientar as próximas etapas do projeto.

Para integrar ferramentas de visualização de dados e estatísticas descritivas são frequentemente usadas para resumir e entender os atributos principais dos dados. De acordo com, (MTK, 2024) o RapidMiner é conhecido por sua interface amigável e capacidade de automação para preparação e exploração de dados o que é crucial para fazer escolhas de ambiente integrado para treinamento do modelo.

Desta forma, com os dados preparados e explorados, o momento de desenvolver o modelo de IA. Isso envolve a seleção dos algoritmos adequados e o treinamento desses algoritmos com os dados disponíveis, conforme quadro abaixo.

Quadro 2 – Software para desenvolvimento de IA

Linguagem	Fabricante/Desenvolvedor	Características Principais
Pitão	Fundação de Software Python	Sintaxe simples, vasta coleção de bibliotecas como TensorFlow, Keras e PyTorch, ideal para prototipagem rápida. APRENDA R, PYTHON E CIÊNCIA DE DADOS ONLINE
R	Equipe principal R	Focada em análise estatística e visualização de dados, amplamente utilizada em aprendizado de máquina. APRENDA R, PYTHON E CIÊNCIA DE DADOS ONLINE
Java	Corporação Oracle	Robustez e portabilidade, utilizado em sistemas empresariais e aplicativos de grande escala. LMANCHA
C++	Norma ISO/IEC	Eficiência e capacidade de baixo nível, utilizadas em sistemas que requerem alto desempenho. LMANCHA
Júlia	Julia Computação	Alta performance em computação numérica, crescente popularidade em projetos de IA. APRENDA R, PYTHON E CIÊNCIA DE DADOS ONLINE
JavaScript	Comunicações Netscape	Utilizado principalmente no desenvolvimento web, com bibliotecas como TensorFlow.js para IA. GRIFO
Ceceio	John McCarthy	Uma das linguagens mais antigas para IA, conhecida por sua flexibilidade e capacidade de processamento simbólico. COMPRACO · COMPRA COORDENADA POR IA
Prólogo	Alain Colmerauer	Focado em lógica de programação, utilizado em sistemas de IA que envolvem cálculo lógico e resolução de problemas. ARXIV

Fonte: Próprio Autor – 2025.

Diversos modelos podem ser testados e comparados para escolher o que oferece o melhor desempenho. O desenvolvimento do modelo é um processo iterativo, onde os parâmetros são ajustados e a arquitetura do modelo é refinada para maximizar a acurácia e a eficiência.

3. METODOLOGIA

Dada a natureza conceitual e exploratória do trabalho, não foram utilizados dados primários ou amostras populacionais. A metodologia baseou-se em uma revisão detalhada da literatura existente e na análise de casos documentados referentes ao uso de IA em ataques cibernéticos e às estratégias de defesa empregadas em arquitetura de computadores.

A técnica central utilizada foi a revisão da literatura existente, com objetivo de identificar e resumir o conhecimento atual sobre a ligação entre inteligência artificial e cibersegurança. As fontes selecionadas incluíram artigos acadêmicos, artigos de revistas especializadas, sites, blogs e relatórios técnicos de organizações renomadas no campo e as publicações da Microsoft.

Os algoritmos de IA são fundamentais para a detecção proativa de ameaças em redes de computadores, permitindo a identificação de padrões suspeitos e anomalias em tempo real. Técnicas como aprendizado supervisionado, aprendizado não supervisionado e aprendizado por reforço são amplamente utilizadas para construir sistemas robustos de detecção e resposta a incidentes.

Quadro 3 – Aprendizado de máquina

Técnica	Descrição	Exemplos de Algoritmos
Aprendizado Supervisionado	Utiliza dados rotulados para treinar modelos que classificam ameaças e identificam comportamentos maliciosos.	Árvore de Decisão, Regressão Logística, SVM
Aprendizado Não Supervisionado	Identifica padrões e anomalias sem rótulos pré-definidos, essenciais para detectar novos tipos de ataques.	K-means, Clustering Hierárquico
Aprendizado por Reforço	Aprender políticas de resposta e mitigação de ameaças através de interações com o ambiente.	Q-learning, Deep Q-Network (DQN)

Fonte: Próprio Autor – 2025.

Essas técnicas são fundamentais para fortalecer a segurança cibernética, prevenindo ataques e minimizando riscos em um ambiente cada vez mais digital e ameaçador.

4. RESULTADOS E DISCUSSÕES

Os indicadores de sucesso para avaliar a eficácia da aplicação dos resultados do estudo sobre a utilização de Inteligência Artificial (IA) na detecção de ameaças em redes de computadores podem ser definidos em várias dimensões. Primeiramente, a redução de falsos positivos é um indicador crucial, pois a eficácia da IA deve ser medida pela sua capacidade de identificar ameaças reais sem gerar alarmes desnecessários, o que pode sobrecarregar as equipes de segurança (PEREIRA, 2024, p. 5).

Além disso, a velocidade de resposta a incidentes é um fator importante. A implementação de IA deve resultar em tempos de resposta mais rápidos a ameaças detectadas, permitindo que as organizações mitiguem riscos de forma mais eficiente (ALMEIDA e NAS, 2024, p. 28). A capacidade de identificar padrões anômalos em tempo real também é um indicador significativo, pois reflete a habilidade do sistema em aprender e se adaptar a novas ameaças, aumentando a segurança preditiva (EDUKA.IA, 2023).

Por fim, a satisfação das equipes de segurança com as ferramentas de IA implementadas pode ser um indicador qualitativo de sucesso. A aceitação e a confiança nas soluções tecnológicas são fundamentais para garantir que as equipes utilizem efetivamente as ferramentas disponíveis (BANO, 2023). Esses indicadores, quando monitorados, podem fornecer uma visão abrangente da eficácia da aplicação da IA na segurança cibernética.

5. CONSIDERAÇÕES FINAIS

A pesquisa busca fornecer insights sobre a viabilidade e eficácia da aplicação de IA na detecção de ameaças em redes de computadores, destacando benefícios, desafios e possíveis direções para trabalhos futuros. É fundamental para melhorar a segurança de ambientes onde dispositivos de rede estão armazenados. A integração de IA com sensores, câmeras e sistemas de acesso pode prevenir acessos indevidos e minimizar o impacto de ameaças físicas em redes de computadores.

6. REFERÊNCIA

ALMEIDA, V.; NAS, E. Desafios da IA responsável na pesquisa cientifica. Revista USP, 05 jun. 2024. 17-28. Acesso em: 12 jan. 2025.

BANO, M. E. A. “Investigating responsible AI for scientific research: an empirical study”. arXiv preprint arXiv:2312.09561, 2023.

CRUZ, J. V. D. S. et al. Inteligência artificial e cibersegurança: análise de ameaças emergentes e estratégias defensivas, Curitiba. 61-193.

DINO. Ataques cibernéticos podem ser atenuados, dizem peritos. Estado De Minas, 2024. Disponivel em: <https://www.em.com.br/mundo-corporativo/2024/12/7024037-ataques-ciberneticos-podem-ser-mitigados-dizem-peritos.html>. Acesso em: 10 jan. 2025.

EDUKA.IA. Algoritmos e Inteligência Artificial (IA). Entenda a relação. eduka.ai, 2023. Disponivel em: <https://eduka.ai/algoritmos-e-inteligencia-artificial-ia-entenda-a-relacao/>. Acesso em: 13 jan. 2025.

ITFORUM. Custo médio de violações de dados no Brasil é de R$ 6,75 milhões. itforum, 2024. Disponivel em: <https://itforum.com.br/noticias/custo-violacoes-de-dados-no-brasil-r-675-milhoes/>. Acesso em: 10 jan. 2025.

JENNI. Decodificando IA: Entendendo os Componentes Principais e Tipos de Algoritmos. Jenni, 2023. Disponivel em: <https://jenni.ai/pt/artificial-intelligence/algorithms>. Acesso em: 13 jan. 2025.

JOBIM, C. Brasil registra 1.379 ataques cibernéticos por minuto, revela relatório da Kaspersky. COINTELEGRAPH Brasil, 2024. Disponivel em: <https://br.cointelegraph.com/news/brazil-registers-1-379-cyber-attacks-per-minute-reveals-kaspersky-report>. Acesso em: 06 nov. 2024.

LALIBERTE, B. O que é inteligência artificial (IA) para redes? Juniper Networks, ? fev. 2024. Disponivel em: <https://www.juniper.net/br/pt/research-topics/what-is-ai-for-networking.html>.

Acesso em: 13 jan. 2025.

MTK. Explorando o Potencial da AI: Os 20 Melhores Softwares Inteligência Artificial Gratuito. Portal MKT Digital, 2024. Disponivel em: <https://portalmktdigital.com.br/softwares-inteligencia-artificial-gratuito/>. Acesso em: 13 jan. 2025.

OLHAR DIGITAL. REDAÇÃO. NASA foi hackeada porque havia um Raspberry Pi conectado à rede. Olhar Digital, 2019. Disponivel em: <https://olhardigital.com.br/2019/06/24/ciencia-e-espaco/nasa-foi-hackeada-porque-havia-um-raspberry-pi-conectado-a-rede/>. Acesso em: 14 jan. 2025.

PEREIRA, T. 10 Casos de Uso de Inteligência Artificial na Segurança Cibernética. Data Science. Data Science Academy, 2024. Disponivel em: <https://blog.dsacademy.com.br/10-casos-de-uso-de-inteligencia-artificial-na-seguranca-cibernetica/>. Acesso em: 09 jan. 2025.