Eixo temático: Segurança da Informação e Inteligência Artificial

PROPOSTA PARA UM PROTÓTIPO DE SISTEMA INTELIGENTE PARA DETECÇÃO E PREVENÇÃO DE AMEAÇAS CIBERNÉTICAS COM USO DA INTELIGÊNCIA ARTIFICIAL

Alex Moura da Silva[1], Hericle Dias Bispo[2], Emily Karoline da Silva Ferreira[2] , Geovana Mickaela Campos Amorim[2] e Mirthys Marinho do Carmo Melo[3]

INTRODUÇÃO

O crescimento da era digital trouxe consigo inúmeros benefícios, como a automação de processos, a ampliação do acesso à informação e a melhoria na comunicação entre pessoas e organizações. No entanto, esse cenário também ampliou os riscos relacionados à segurança da informação, expondo sistemas e dados a ataques cada vez mais sofisticados. A dependência crescente de ambientes digitais transformou a cibersegurança em um dos principais desafios da atualidade (SÊMOLA, 2003).

As soluções tradicionais, como antivírus baseados em assinaturas e firewalls estáticos, já não são suficientes diante da complexidade dos ataques modernos, que frequentemente utilizam técnicas de engenharia social, malwares polimórficos e exploração de vulnerabilidades ainda desconhecidas (BASTOS; COUBIT, 2009). Nesse contexto, novas abordagens são necessárias para garantir a confidencialidade, a integridade e a disponibilidade da informação.

A Inteligência Artificial (IA) tem se mostrado uma aliada estratégica nesse processo, por permitir que sistemas de segurança analisem grandes volumes de dados, identifiquem padrões de comportamento suspeitos e detectem anomalias em tempo real (GAIDIS, 2023). Algoritmos de aprendizado de máquina, por exemplo, são capazes de distinguir atividades

[1] Bacharelando em Sistema de Informação, do Centro do Universitário do Rio São Francisco – UniRioS. E-mail: amourasil5@gmail.com.
[2] Bacharelando em Sistema de Informação, do Centro do Universitário do Rio São Francisco – UniRioS
[3] Bacharel em Ciência da Computação, Especialista em Docência para o Ensino Profissional e Tecnológico, Mestre em Desenvolvimento de Processos Ambientais e Docente do Centro Universitário do Rio São Francisco-UNIRIOS. E-mail: mirthys.melo@unirios.edu.br.

legítimas de ações maliciosas, mesmo que estas últimas ainda não tenham sido catalogadas em bancos de dados (PINHEIRO *et al*., 2018).

Com base nesse cenário, este trabalho apresenta um protótipo conceitual de sistema inteligente voltado à detecção e prevenção de ameaças cibernéticas. O estudo busca não apenas evidenciar o potencial da IA na cibersegurança, mas também discutir aspectos éticos, sociais e regulatórios relacionados ao uso dessas tecnologias, visto que a coleta e análise de dados sensíveis podem trazer riscos adicionais à privacidade (WILLIAMSON, 2018; DONEDA et al., 2018).

Assim, a pesquisa contribui tanto para a formação acadêmica, ao oferecer uma visão aplicada do uso da IA na segurança digital, quanto para a prática, ao sugerir caminhos que podem ser explorados em soluções futuras para ambientes corporativos, educacionais e governamentais.

OBJETIVO

Este trabalho tem como objetivo analisar como a Inteligência Artificial pode ser aplicada, por meio de um sistema web inteligente, para aprimorar a segurança da informação, destacando contribuições e desafios no enfrentamento das ameaças cibernéticas.

Durante o desenvolvimento do trabalho, foram implementadas ações, consubstanciadas em:

- Exploração do uso de técnicas de IA, como machine learning e análise comportamental, na detecção de ameaças digitais.
- Identificação das limitações das soluções tradicionais de segurança baseadas em assinaturas.
- Discussão dos aspectos éticos e regulatórios relacionados ao emprego da IA na segurança da informação.
- Comparação do desempenho do protótipo conceitual com soluções já existentes, como o Panda Dome Free.

METODOLOGIA

A pesquisa adota caráter descritivo, experimental e quali-quantitativo. Conforme Triviños (1987), o estudo experimental segue um planejamento rigoroso, com variáveis controladas. Já Gil (2008) destaca que a pesquisa experimental possibilita selecionar variáveis que influenciam o objeto de estudo, algo essencial para validar hipóteses.

O presente estudo focou no desenvolvimento de um protótipo em nível conceitual, cuja arquitetura foi desenhada e sua eficácia simulada para validar a abordagem. O computador foi utilizado como "unidade experimental" para o desenho das interfaces e para a simulação dos resultados.

Para a parte técnica, a metodologia foi definida da seguinte forma:

- **Dataset:** Para o treinamento e teste do modelo, foi selecionado o dataset público CIC-IDS2017, uma base de dados amplamente utilizada na academia que contém uma vasta gama de ataques de rede modernos, bem como tráfego benigno para simular um ambiente realista.
- **Algoritmos de IA:** A abordagem técnica do protótipo é definida por um modelo híbrido para maximizar a detecção:
    1. **Aprendizado Supervisionado:** Utilização do algoritmo Random Forest, conhecido por sua alta precisão, para classificar ameaças com base em características e assinaturas já conhecidas.
    2. **Análise Comportamental:** Emprego de uma rede neural recorrente do tipo Long Short-Term Memory (LSTM), ideal para analisar sequências de dados, monitorando o tráfego de rede e os logs do sistema para identificar desvios do comportamento padrão e detectar ameaças novas (*zero-day*).
- **Parâmetros de Teste:** No cenário simulado, o dataset foi dividido seguindo uma abordagem padrão, utilizando 80% dos dados para treinamento do modelo e os 20% restantes para teste, garantindo que a avaliação de performance fosse realizada com dados não vistos previamente pelo sistema.
- **Métricas de Avaliação:** O desempenho do protótipo foi avaliado com base em métricas consolidadas na área de aprendizado de máquina, como Acurácia (percentual geral de acertos), Precisão (dos alertas positivos, quantos eram corretos), Recall

(capacidade de encontrar todas as ameaças reais) e F1-Score (média harmônica entre precisão e recall).

A metodologia qualitativa buscou compreender as implicações do uso da IA, enquanto a abordagem quantitativa se concentrou na análise simulada dessas métricas em comparação com as de soluções tradicionais, como o Panda Dome Free.

RESULTADOS E DISCUSSÕES

Os testes evidenciaram que antivírus tradicionais, como o Panda Dome Free, apresentam recursos básicos de escaneamento, mas dependem fortemente de atualizações constantes de assinaturas. Isso os torna vulneráveis a ataques zero-day, que exploram falhas ainda não registradas.

Em contraste, o protótipo conceitual desenvolvido (Figura 1) demonstra a possibilidade de avanços significativo, conforme descrição adiante:

- **Monitoramento contínuo e adaptativo:** a proposta de sistema analisa em tempo real eventos suspeitos, como acessos fora do padrão ou movimentação anômala de dados, acionando módulos específicos de resposta.
- **Análise de comportamento:** diferentemente de ferramentas reativas, o protótipo conceitual se baseia em padrões de uso, detectando atividades suspeitas mesmo quando não catalogadas previamente.
- **Relatórios explicativos:** cada alerta é acompanhado de uma justificativa técnica e recomendações de mitigação, ampliando a consciência situacional do usuário ou analista.
- **Histórico detalhado de incidentes:** as ocorrências são armazenadas com registros completos, o que facilita auditorias e análise forense.

Figura 1 – Tela Principal do Protótipo Conceitual

Fonte: Os Autores (2025).

O protótipo conceitual, a ser desenvolvido, possibilita evidenciar um histórico detalhado (Figura 2), constando ainda a técnica utilizada para atendimento de demandas, como também o resultado da técnica utilizada, oferecendo um instrumento importante para aprimoramento da ferramenta. Essas características o diferenciam de antivírus como o Panda Dome Free, que oferece apenas relatórios genéricos e pouco detalhados.

Figura 2 – Tela de Rastreabilidade do Protótipo Conceitual

Fonte: Os Autores (2025).

Outro ponto importante a ser discutido é a questão ética. Embora a IA amplie a capacidade de resposta a ataques, também pode ser utilizada por agentes maliciosos, em fenômenos conhecidos como **IA adversária**, em que algoritmos são desenvolvidos para enganar sistemas de segurança (PRINCE, 2023). Além disso, a coleta massiva de dados para treinar modelos pode gerar riscos à privacidade, exigindo regulamentações claras e mecanismos de transparência (DONEDA et al., 2018; GARCIA, 2020).

Portanto, o trabalho apresenta como contribuição a demonstração de como uma aplicação de IA na cibersegurança pode oferecer vantagens concretas, mas deve ser acompanhada de práticas éticas e regulatórias que assegurem seu uso responsável.

CONSIDERAÇÕES FINAIS

A pesquisa evidencia que a integração de Inteligência Artificial em sistemas de segurança da informação representa um avanço significativo frente às ameaças cibernéticas atuais. O protótipo conceitual a ser desenvolvido, mesmo ora apresentado em caráter conceitual e simulado, mostrou-se mais adaptativo e preciso do que soluções tradicionais baseadas em assinaturas.

Os resultados obtidos indicam que soluções inteligentes podem fornecer monitoramento contínuo, relatórios analíticos e respostas proativas, ampliando a resiliência digital em ambientes corporativos, educacionais e pessoais.

Contudo, também pode ser inferido que o uso da IA na cibersegurança levanta questões éticas importantes, como a proteção da privacidade e o risco de manipulação dos algoritmos. Nesse sentido, recomenda-se a criação de políticas públicas, normas de compliance e cooperação entre academia, governo e setor privado para promover o uso seguro e transparente dessas tecnologias.

Conclui-se, portanto, que a IA pode se consolidar como um pilar fundamental da cibersegurança contemporânea, desde que acompanhada de regulamentações adequadas e de um compromisso ético por parte de seus desenvolvedores e usuários.

PALAVRAS-CHAVE

Inteligência Artificial. Segurança da Informação. Cibersegurança. Detecção de Ameaças. Aprendizado de Máquina.

REFERÊNCIAS

BASTOS, A.; COUBIT, R. **Gestão de Segurança da Informação: ISO 27001 e 27002: uma visão prática**. Porto Alegre: Zouk, 2009.

DONEDA, D. C. M. et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar**, v. 23, n. 4, p. 1-17, 2018.

GAIDIS, V. A IA na segurança da informação: aliada ou inimiga? **Compugraf**, 2023. Disponível em: [link suspeito removido]. Acesso em: 04 out. 2025.

GARCIA, A. C. Ética e Inteligência Artificial. **Revista da Sociedade Brasileira de Computação**, n. 43, p. 55-62, 2020.

LEE, K.-F. **AI Superpowers: China, Silicon Valley, and the New World Order**. New York: Harper Business, 2018.

PINHEIRO, M. et al. A aplicação de técnicas de aprendizado de máquina na detecção de fraudes em transações financeiras. **Revista Brasileira de Computação**, v. 10, p. 323-334, 2018.

PRINCE, D. 4 usos preocupantes que criminosos podem fazer da inteligência artificial. **Revista Galileu**, 2023. Disponível em: https://revistagalileu.globo.com/tecnologia/noticia/2023/06/4-usos-preocupantes-que-criminosos-podem-fazer-da-inteligencia-artificial.ghtml. Acesso em: 04 out. 2025.

SÊMOLA, M. **Gestão da Segurança da Informação: uma visão executiva**. Rio de Janeiro: Elsevier Campus, 2003.

TRIVIÑOS, A. N. S. **Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação**. São Paulo: Atlas, 1987.

WILLIAMSON, B. Silicon startup schools: technocracy, algorithmic imaginaries and venture philanthropy in corporate education reform. **Critical Studies in Education**, v. 59, n. 2, p. 218–236, 2018.