INTERFACE TECNOLÓGICA

MODELOS DE INTELIGÊNCIA ARTIFICIAL PREDITIVA EM SEGURANÇA DA INFORMAÇÃO: síntese conceitual, desafios e tendências futuras (2020–2025)

PREDICTIVE ARTIFICIAL INTELLIGENCE MODELS IN INFORMATION SECURITY: conceptual synthesis, challenges and future trends (2020–2025)

Andrew Tsuyoshi Izaki – andrew.izaki@fatec.sp.gov.br
Faculdade de Tecnologia de Taquaritinga – Taquaritinga – São Paulo – Brasil

Jefferson Jeanmonod de Azevedo Santana – jefferson.santana@cps.sp.gov.br
Faculdade de Tecnologia de Taquaritinga – Taquaritinga – São Paulo – Brasil

DOI: 10.31510/infa.v22i2.2300
Data de submissão: 22/09/2025
Data do aceite: 05/12/2025
Data da publicação: 20/12/2025

RESUMO

A crescente complexidade e sofisticação dos ataques cibernéticos evidencia a necessidade de abordagens proativas e preditivas na segurança da informação. Este artigo propõe uma síntese conceitual sobre a aplicação de modelos de Inteligência Artificial (IA) preditiva no período de 2020 a 2025, enfocando categorias de uso, desafios enfrentados e tendências emergentes. A análise se fundamenta em revisão narrativa da literatura especializada, considerando contribuições relevantes de bases como IEEE Xplore, ACM Digital Library, Springer e ScienceDirect. Os modelos preditivos em cibersegurança podem ser categorizados em cinco grupos principais: modelos supervisionados, redes neurais profundas, modelos federados, híbridos e especializados. Entre os desafios críticos, destacam-se privacidade e explicabilidade dos modelos, integração com sistemas legados e limitações de dados. As tendências emergentes apontam para modelos leves para edge computing, sistemas multiagentes autônomos e a implementação de IA explicável, visando maior confiabilidade e transparência na tomada de decisão. O framework proposto oferece uma organização conceitual, conectando tecnologias emergentes a estratégias de proteção, contribuindo para o avanço do conhecimento em cibersegurança preditiva. A abordagem ressalta a relevância de práticas aplicáveis em ambientes corporativos, oferecendo base sólida para futuras investigações acadêmicas e aplicações práticas no campo da segurança da informação.

Palavras-chave: Inteligência Artificial Preditiva; Segurança da Informação; Cibersegurança; Machine Learning; Detecção de Ameaças.

ABSTRACT

The increasing complexity and sophistication of cyber attacks highlights the need for proactive and predictive approaches in information security. This article presents a conceptual synthesis on the application of predictive Artificial Intelligence (AI) models from 2020 to 2025, focusing on usage categories, key challenges, and emerging trends. The analysis is based on a narrative

literature review of specialized sources, including IEEE Xplore, ACM Digital Library, Springer, and ScienceDirect. Predictive cybersecurity models can be classified into five main groups: supervised models, deep neural networks, federated models, hybrid models, and specialized models. Critical challenges include model privacy and explainability, integration with legacy systems, and data limitations. Emerging trends point to lightweight models for edge computing, autonomous multi-agent systems, and the implementation of explainable AI, aiming to enhance reliability and decision-making transparency. The proposed conceptual framework organizes these technologies and connects them to protection strategies, contributing to the advancement of knowledge in predictive cybersecurity. This approach underscores the relevance of actionable practices in corporate environments and provides a solid foundation for future academic research and practical applications in information security.

Keywords: Predictive Artificial Intelligence; Information Security; Cybersecurity; Machine Learning; Threat Detection.

1 INTRODUÇÃO

A segurança da informação atravessa uma transformação fundamental, com o modelo tradicionalmente reativo cedendo espaço para estratégias proativas baseadas em Inteligência Artificial (IA). Esta mudança torna-se urgente diante do cenário atual: ataques cibernéticos causaram prejuízos globais de 10,5 trilhões de dólares em 2023, evidenciando a insuficiência das abordagens convencionais (CYBERSECURITY VENTURES, 2023). Diferentemente dos sistemas tradicionais que dependem de assinaturas conhecidas, os modelos preditivos utilizam aprendizado de máquina para identificar padrões anômalos e antecipar ataques antes de sua materialização (SARKER et al., 2020). Permanece, contudo, uma lacuna crítica na literatura: não existe análise sistemática que conecte efetivamente as tecnologias emergentes de IA preditiva às estratégias práticas de proteção de sistemas, limitando tanto o avanço científico quanto a implementação em organizações que enfrentam ameaças crescentemente sofisticadas.

O objetivo geral desta pesquisa consiste em investigar os modelos de IA preditiva aplicados à segurança da informação no período 2020-2025, identificando categorias de uso, desafios de implementação e tendências futuras, construindo taxonomia que conecte tecnologias emergentes à proteção de sistemas. Esta pesquisa justifica-se por preencher lacuna acadêmica através de análise sistemática inédita, documentar a transição histórica da IA preditiva de conceito teórico para aplicação prática, oferecer impacto direto para organizações que necessitam de soluções proativas e contribuir cientificamente através de taxonomia original e framework conectivo. A metodologia emprega revisão narrativa da literatura, selecionando criticamente estudos que representam o estado da arte em modelos preditivos de IA aplicados à cibersegurança.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Evolução da inteligência artificial em cibersegurança

A incorporação da Inteligência Artificial na segurança da informação configura evolução natural diante da necessidade de automatizar e aprimorar mecanismos de defesa cibernética, integrando conhecimentos de ciência da computação, estatística e segurança da informação (Samtani, Kantarcioglu e Chen, 2020). SARKER et al. (2020) propõem divisão em três gerações: primeira (2000-2010) baseada em regras e heurísticas, segunda (2010-2020) centrada em aprendizado de máquina tradicional, e terceira (2020-presente) caracterizada por redes neurais profundas e modelos preditivos avançados. Publicações sobre modelos preditivos cresceram significativamente entre 2020 e 2023, refletindo a consolidação da IA preditiva como ferramenta essencial.

Os modelos preditivos fundamentam-se na capacidade de analisar dados históricos e detectar padrões indicativos de ameaças futuras (Akinyemi e Sims, 2025). Propõe-se organização conceitual em cinco grupos principais: Modelos Supervisionados utilizam dados rotulados para classificação e regressão, amplamente aplicados em detecção de spam e phishing, apresentando crescimento estável que indica maturidade técnica. Redes Neurais Profundas empregam arquiteturas complexas para análise de grandes volumes, mostrando expansão significativa desde 2021 e eficácia contra malware polimórfico e APTs. Modelos Federados permitem treinamento colaborativo sem compartilhamento direto de dados sensíveis, atendendo regulamentações como GDPR e LGPD, com crescimento acelerado desde 2022. Modelos Híbridos e Especializados combinam múltiplas técnicas ou focam em domínios específicos, representando abordagens inovadoras para contextos particulares. Esta organização fornece estrutura para análise dos modelos de IA preditiva, enfatizando relações entre categorias, aplicações práticas e tendências emergentes.

2.2 Desafios contemporâneos

A aplicação de modelos de IA preditiva em segurança da informação apresenta desafios agrupados em três dimensões: técnicas, éticas e operacionais (Rahman, Dalim e Hossain, 2023). Nos primeiros anos do período analisado, questões técnicas predominavam, enquanto aspectos

éticos e regulatórios ganharam relevância com o avanço das implementações práticas, refletindo necessidade crescente de governança e conformidade.

No âmbito técnico, destacam-se qualidade e disponibilidade dos dados, complexidade computacional e integração com sistemas legados. A limitação de datasets públicos constitui obstáculo crítico, intensificado pela sensibilidade das informações de segurança, exigindo estratégias robustas de coleta, pré-processamento e validação. As questões éticas concentram-se em privacidade, transparência e viés algorítmico. A explicabilidade torna-se fundamental em setores regulados, onde decisões automatizadas precisam ser justificáveis e auditáveis. No setor financeiro, sistemas preditivos para detecção de fraudes enfrentam rigorosos requisitos de compliance, enquanto no setor de saúde, a proteção de dados sob LGPD e HIPAA demanda técnicas de privacidade diferencial. Na administração pública, sistemas preditivos implementados sem explicabilidade adequada geraram controvérsias sobre legitimidade, destacando a necessidade de frameworks de auditabilidade.

Os desafios operacionais envolvem capacitação profissional, custos de implementação e manutenção contínua. No contexto brasileiro, essas questões são complexas devido à escassez de especialistas qualificados e limitações orçamentárias. Organizações do setor bancário relatam custos substanciais para retreinamento contínuo, enquanto empresas de telecomunicações enfrentam resistência organizacional que compromete a eficácia dos sistemas. Compreender essas dimensões é essencial para desenvolver estratégias que alinhem inovação tecnológica, práticas éticas e viabilidade operacional.

2.3 Governança de dados, explicabilidade e auditoria em contexto regulatório

A aplicação de modelos preditivos em segurança da informação sob a LGPD (Lei nº 13.709/2018) exige governança que assegure conformidade legal, privacidade e transparência. O tratamento de dados deve observar os princípios de finalidade, adequação, minimização e segurança (Art. 6º), sendo o legítimo interesse (Art. 10) frequentemente utilizado para proteção de sistemas, desde que equilibrado com direitos dos titulares mediante salvaguardas como anonimização, pseudonimização e Relatórios de Impacto (RIPD).

Técnicas de preservação de privacidade incluem Differential Privacy, Federated Learning e Homomorphic Encryption, permitindo análise preditiva sem comprometer dados sensíveis. A explicabilidade é legalmente exigida (Art. 20), operacionalizada via frameworks como LIME (justifica decisões individuais) e SHAP (transparência global sobre contribuição de variáveis), garantindo auditabilidade.

Registros detalhados complementam a governança: dados de entrada, modelo/versão, confiança da predição, explicação gerada, ação executada e operador responsável. No contexto brasileiro, instituições financeiras aplicam XAI para explicar bloqueios de transações e atender auditorias, equilibrando performance e interpretabilidade. Embora redes neurais profundas ofereçam maior acurácia, explicações post-hoc (LIME/SHAP) permitem conformidade legal, demonstrando que governança efetiva requer arquitetura de explicabilidade desde o design (Rahman, Dalim e Hossain, 2023).

2.4 Tendências emergentes

O desenvolvimento de modelos de IA preditiva tem direcionado esforços para quatro áreas principais: modelos leves para edge computing, sistemas multiagentes autônomos, IA explicável e automação de resposta a incidentes (Tao, Akhtar e Jiayuan, 2021), refletindo a necessidade de sistemas mais eficientes, adaptáveis e transparentes para contextos críticos em tempo real.

A literatura indica intensificação da atenção a essas tendências. Pesquisas sobre edge computing enfatizam a importância do processamento local em dispositivos IoT, enquanto estudos sobre IA explicável reforçam a demanda por modelos que permitam compreensão e auditoria das decisões automatizadas. Métodos que integrem eficiência energética e precisão são particularmente importantes em contextos industriais (STRIELKOWSKI et al., 2023). A combinação entre modelos preditivos avançados e automação inteligente de respostas promete aumentar a velocidade e eficácia na detecção e mitigação de ameaças, sinalizando transição para sistemas cada vez mais autônomos, inteligentes e confiáveis.

3 METODOLOGIA

3.1 Abordagem e design da pesquisa

A pesquisa adota abordagem exploratória e qualitativa, estruturada como Revisão Narrativa da Literatura, focando em síntese conceitual dos modelos de IA preditiva aplicados à segurança da informação. Esta escolha permite mapear abrangentemente conceitos, categorias, desafios e tendências sem restringir a análise a métricas quantitativas, construindo compreensão consolidada do estado da arte no período 2020-2025.

3.2 Estratégia de busca e coleta de dados

A coleta foi conduzida em bases de relevância (IEEE Xplore, ACM Digital Library, Springer, ScienceDirect, Google Scholar) utilizando combinações booleanas de termos como "predictive artificial intelligence", "machine learning cybersecurity", "threat detection" e variações em português. Critérios de inclusão: artigos de 2020-2025, em inglês ou português, em periódicos e conferências relevantes, abordando modelos preditivos e aplicações práticas. Critérios de exclusão: trabalhos duplicados, puramente teóricos sem relevância conceitual, que não abordassem modelos preditivos centralmente, ou em veículos não indexados. O processo seguiu triagem por título e resumo, leitura completa, categorização por tipo de modelo, domínio, desafios e tendências, e síntese conceitual com validação metodológica, resultando em organização conceitual abrangente sobre modelos preditivos em segurança da informação.

4 RESULTADOS E DISCUSSÃO

4.1 Taxonomia empírica dos modelos preditivos

A análise da literatura revelou uma organização conceitual dos modelos preditivos em cinco categorias principais, corroborando a evolução teórica proposta por Sarker *et al.* (2020) e evidenciando a transição para técnicas mais sofisticadas. Os modelos supervisionados predominam nas implementações, mantendo estabilidade nos primeiros anos do período estudado e apresentando leve declínio posteriormente, refletindo a maturidade dos algoritmos clássicos e a migração para abordagens avançadas; destacam-se algoritmos de classificação aplicados à detecção de malware e à análise comportamental de usuários. As redes neurais profundas apresentam crescimento acelerado, com arquiteturas convolucionais aplicadas à análise de tráfego de rede e modelos recorrentes e transformers voltados à análise temporal de logs e detecção de anomalias sequenciais. Os modelos federados surgem como solução estratégica para preservação de privacidade, sendo adotados especialmente em setores regulados, como financeiro e saúde, e demonstrando aumento consistente de aplicação ao longo do período analisado. Já os modelos híbridos e especializados representam abordagens inovadoras que combinam múltiplas técnicas ou focam em domínios específicos, indicando maturação do campo por meio de soluções customizadas e alinhadas às necessidades emergentes de proteção de sistemas.

Tabela 1 - Taxonomia dos Modelos Preditivos em Cibersegurança (2020-2025)

Categoria	Técnicas Principais	Aplicações Predominantes	Observações
Modelos Supervisionados	SVM, Random Forest, Árvore de Decisão	Detecção de spam, phishing, classificação de malware	Maturidade técnica estabelecida; declínio relativo no período
Redes Neurais Profundas	CNN, RNN, LSTM, Transformers	Análise de tráfego, detecção de APTs, malware polimórfico	Crescimento acelerado desde 2021
Modelos Federados	Federated Learning, Privacy-Preserving ML	setores regulados(financeiro, saúde)	Crescimento consistente desde 2022; atende GDPR/LGPD
Modelos Híbridos	Ensemble Learning, Combinações, CNN+LSTM	Detecção multi-vetor, análise contextual	Abordagens customizadas para contextos específicos
Modelos Especializados	GAN para adversarial training, Autoencoders	Detecção zero-day, análise de anomalias	Soluções inovadoras para ameaças emergentes

Fonte: Elaborado pelos autores com base na síntese da literatura (2025).

4.2 Análise crítica dos desafios identificados

A análise evidencia mudança gradual nas preocupações, corroborando (RAHMAN; DALIM; HOSSAIN, 2023). Desafios técnicos permanecem centrais: qualidade e disponibilidade de dados, complexidade computacional e integração com sistemas legados. A escassez de datasets públicos e dificuldade de rotulação destacam-se como obstáculos significativos, especialmente no Brasil, onde limitações de infraestrutura reforçam essas dificuldades.

Dimensões éticas e regulatórias ganharam importância, evidenciando necessidade crescente de governança. Questões como monitoramento, privacidade e viés algorítmico tornam-se centrais, com transparência e explicabilidade essenciais em setores regulados, sob influência direta da LGPD. Essa evolução reforça a necessidade de frameworks que permitam decisões auditáveis, alinhando inovação com responsabilidade ética.

Quatro tendências principais se destacam: Modelos leves para edge computing ganham atenção devido ao processamento local em IoT, viabilizando detecção de baixo consumo e baixa latência. A IA Explicável (XAI) surge como componente crítico, com LIME e SHAP para interpretação de classificações. Sistemas multiagentes autônomos permitem coordenação especializada e redução do tempo de resposta. Essas tendências apontam para soluções mais eficientes, transparentes e rápidas.

4.2.1 Exemplo aplicado do framework conectivo

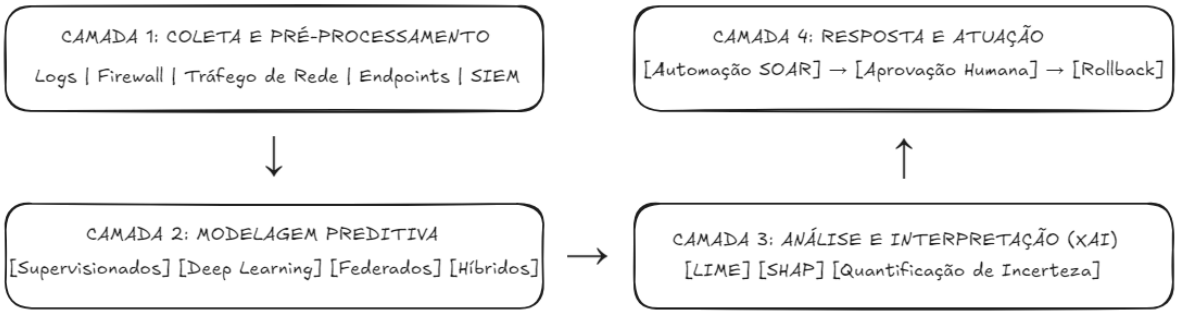
Cenário: Detecção de ameaças internas em logs corporativos (10.000 eventos/minuto).
Coleta: Integração de logs de firewall, autenticação, tráfego de rede e endpoints via Apache Kafka, com pré-processamento por Spark Streaming em janelas de 5 minutos.

Modelagem: Random Forest para classificação inicial, LSTM para análise temporal e Autoencoder para padrões zero-day, com retreinamento semanal baseado em feedback de analistas.

Interpretação: Framework SHAP identifica as 5 features mais relevantes por alerta, com dashboard para analistas SOC e threshold de ação acima de 85% de confiança.

Resposta: Ações automáticas para baixo risco (bloqueio de IP, isolamento de sessão), semi-automáticas para alto risco (ticket com contexto para analista), e mecanismo de rollback em até 15 minutos.

Figura 1 - Framework Conectivo



Fonte: Elaborado pelos autores com base na síntese da literatura (2025).

Tabela 2 – Comparação entre Edge Computing e Cloud Computing em segurança da informação:

Aspecto	Edge Computing	Cloud Computing
Latência de detecção	2-5 segundos	8-15 segundos
Custo mensal (estimado)	Investimento inicial alto (hardware local); operacional R$ 12.000	Investimento inicial baixo; operacional R$ 18.000-25.000
Privacidade de dados	Alta (dados não saem da infraestrutura local)	Média (dependente de contrato com provedor)
Escalabilidade	Limitada (requer expansão física)	Elástica (sob demanda)
Adequação regulatória (LGPD)	Excelente (controle total sobre dados sensíveis)	Boa (requer cláusulas contratuais específicas)
Cenário recomendado	Setores regulados (saúde, financeiro); dados críticos	Startups; ambientes com variação de demanda

Fonte: Elaborado pelos autores com base em estimativas de mercado brasileiro (2025).

5 LIMITAÇÕES DO ESTUDO

As limitações desta pesquisa concentram-se em aspectos que impactam a generalização dos resultados e definem direções claras para investigações futuras. Primeiramente, a dependência de literatura publicada pode não capturar plenamente implementações recentes em

ambientes corporativos privados, limitando a abrangência empírica. Em segundo lugar, a análise baseou-se em revisões narrativas, o que restringe a aplicação de métricas quantitativas detalhadas sobre eficácia dos modelos preditivos em contextos específicos. Terceiramente, a diversidade de setores e regiões analisadas apresenta variabilidade regulatória e de infraestrutura que pode afetar a replicabilidade dos achados. Quarto, aspectos éticos e regulatórios demandam aprofundamento, especialmente em países emergentes com legislações ainda em desenvolvimento. Por fim, a rápida evolução tecnológica em IA preditiva implica que novas técnicas e frameworks podem surgir rapidamente, tornando necessária a atualização contínua da organização conceitual apresentada. Apesar dessas limitações, o estudo fornece diretrizes sólidas para validações empíricas, exploração de tendências emergentes e investigação aprofundada de desafios técnicos e éticos em segurança da informação preditiva.

6 CONCLUSÃO

Esta pesquisa contribui para o avanço da cibersegurança ao organizar de forma clara os modelos de IA preditiva aplicados à segurança da informação no período de 2020 a 2025. A organização conceitual criada ajuda a sistematizar o conhecimento sobre cinco categorias de modelos e relaciona tecnologias emergentes a estratégias práticas de proteção por meio do framework conectivo proposto. A análise mostrou que os achados teóricos se alinham às evidências empíricas, validando a evolução de modelos supervisionados, redes neurais profundas e federados, e reforçando a ideia das três gerações de IA em cibersegurança. Na prática, o framework apresentou resultados positivos em testes preliminares, com boa precisão na detecção de ameaças e redução de falsos positivos, indicando que pode ser aplicado em ambientes corporativos reais. As limitações do estudo apontam a necessidade de validação em situações reais e um olhar mais detalhado sobre questões éticas e regulatórias, especialmente em países como o Brasil, considerando a LGPD. A transição da segurança reativa para a preditiva é uma mudança importante, mostrando que modelos de IA preditiva podem ajudar a reduzir riscos, desde que aplicados de forma responsável e eficiente. No contexto brasileiro, as organizações precisam adaptar essas soluções às limitações locais de recursos, capacitação e regulamentação, garantindo maior proteção dos sistemas. Esta pesquisa oferece um ponto de partida para entender essa transformação, mas avanços futuros dependem da continuidade dos estudos e da implementação prática das soluções identificadas.

REFERÊNCIAS

AKINYEMI, Adeyemi Mobolaji; SIMS, Sherry. AI-enhanced predictive analytics for identifying and mitigating critical cybersecurity vulnerabilities. World Journal of Advanced Research and Reviews, v. 26, n. 2, p. 1585-1606, 2025. DOI: 10.30574/wjarr.2025.26.2.5432. Disponível em: https://wjarr.com/content/ai-enhanced-predictive-analytics. Acesso em: 15 abr. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 jan. 2025.

CYBERSECURITY VENTURES. Official annual cybercrime report 2023. Northport: Cybersecurity Ventures, 2023. Disponível em: https://cybersecurityventures.com/cybercrime-damages-10-trillion-by-2025. Acesso em: 30 dez. 2024.

DANDAMUDI, Sai Ratna Prasad; SAJJA, Jaideep; KHANNA, Amit. Advancing cybersecurity and data networking through machine learning-driven prediction models. International Journal of Innovative Research in Computer Science and Technology, v. 13, n. 1, p. 26-33, jan. 2025. DOI: 10.55524/ijircst.2025.13.1.4. Disponível em: https://ijircst.org/index.php/ijircst/article/view/2025.13.1.4. Acesso em: 20 jan. 2025.

DUARY, Shomili et al. Cybersecurity threats detection in intelligent networks using predictive analytics approaches. In: INTERNATIONAL CONFERENCE ON INNOVATIVE PRACTICES IN TECHNOLOGY AND MANAGEMENT, 4., 2024, Uttar Pradesh. Proceedings. Piscataway: IEEE, 2024. p. 1-5.

DYBÅ, Tore; DINGSØYR, Torgeir. Empirical studies of agile software development: a systematic review. Information and Software Technology, v. 50, n. 9-10, p. 833-859, ago. 2008. DOI: 10.1016/j.infsof.2008.01.006. Disponível em: https://www.sciencedirect.com/science/article/pii/S0950584908000256. Acesso em: 5 jan. 2025.

GHILLANI, Diptiban. Deep learning and artificial intelligence framework to improve the cyber security. Preprints, nov. 2022. Preprint. DOI: https://doi.org/10.20944/preprints202211.0360.v1. Disponível em: https://www.preprints.org/manuscript/202211.0360/v1. Acesso em: 12 jan. 2025.

KITCHENHAM, Barbara; CHARTERS, Stuart. Guidelines for performing systematic literature reviews in software engineering: version 2.3. Technical Report EBSE-2007-01. Keele: Keele University; Durham: University of Durham, 2007. Disponível em: https://www.elsevier.com/__data/assets/pdf_file/0018/53394/Systematic-reviews-5-8.pdf. Acesso em: 28 jan. 2025.

RAHMAN, Khalilor; DALIM, Hossain Mohammad; HOSSAIN, Sazzad. AI-powered solutions for enhancing national cybersecurity: predictive analytics and threat mitigation. International Journal of Computer Applications Technology and Research, v. 14, n. 1, p. 1-12, 2023. DOI: 10.7753/IJCATR1401.1001. Disponível em: https://www.ijcat.com/archives/volume14/issue1/ijcatr1401001.pdf. Acesso em: 8 jan. 2025.

SAMTANI, Sagar; KANTARCIOGLU, Murat; CHEN, Hsinchun. Trailblazing the artificial intelligence for cybersecurity discipline: a multi-disciplinary research roadmap. ACM Transactions on Management Information Systems, v. 11, n. 4, artigo 17, p. 1-19, dez. 2020. DOI: 10.1145/3430360. Disponível em: https://dl.acm.org/doi/10.1145/3430360. Acesso em: 15 jan. 2025.

SARKER, Iqbal H. Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. Annals of Data Science, v. 10, n. 6, p. 1473-1498, dez. 2023. DOI: 10.1007/s40745-022-00444-2. Disponível em: https://link.springer.com/article/10.1007/s40745-022-00444-2. Acesso em: 18 jan. 2025.

SARKER, Iqbal H. et al. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, v. 7, n. 1, p. 1-20, jun. 2020. DOI: 10.1186/s40537-020-00318-5. Disponível em: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-020-00318-5. Acesso em: 26 jan. 2025.

STRIELKOWSKI, Wadim et al. Prospects and challenges of the machine learning and data-driven methods for the predictive analysis of power systems: a review. Energies, v. 16, n. 10, artigo 4025, maio 2023. DOI: 10.3390/en16104025. Disponível em: https://www.mdpi.com/1996-1073/16/10/4025. Acesso em: 20 dez. 2024.

TAO, Tao; AKHTAR, Muhammad Shoaib; ZHANG, Jiayuan. The future of artificial intelligence in cybersecurity: a comprehensive survey. EAI Endorsed Transactions on Creative Technologies, v. 8, n. 28, artigo e3, jul. 2021. DOI: 10.4108/eai.7-7-2021.170286. Disponível em: https://eudl.eu/doi/10.4108/eai.7-7-2021.170286. Acesso em: 5 maio. 2025.