RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 01/07/2026 | aceito: 20/07/2026 | publicação: 16/08/2026

Inteligência artificial aplicada à detecção de ameaças e resposta a incidentes cibernéticos

Artificial intelligence applied to threat detection and cyber incident response

Gabriel Lima

Resumo

Este estudo tem como objetivo avaliar a eficácia e a viabilidade da implementação de técnicas de inteligência artificial e aprendizado de máquina na detecção de ameaças e na resposta a incidentes cibernéticos, visando otimizar a segurança operacional e proteger infraestruturas críticas contra ataques virtuais. A metodologia adotada compreende a análise de sistemas avançados de monitoramento de rede, a análise comportamental do tráfego e algoritmos preditivos para a identificação de anomalias e vulnerabilidades. Os resultados demonstram que a automação impulsionada por inteligência artificial reduz significativamente o tempo médio de detecção e resposta a incidentes, embora persistam desafios como a ocorrência de falsos positivos, a necessidade de treinamento contínuo dos modelos e os elevados custos de implementação. Conclui-se que a adoção sustentável dessas tecnologias requer investimentos em capacitação técnica, governança de dados e esforços contínuos em pesquisa e desenvolvimento.

Palavras-chave: Inteligência Artificial. Cibersegurança. Detecção de ameaças. Resposta a incidentes. Aprendizado de Máquina.

Abstract

This study aims to evaluate the effectiveness and feasibility of implementing artificial intelligence and machine learning techniques for threat detection and cyber incident response, aiming to optimize operational security and protect critical infrastructures against cyberattacks. The adopted methodology includes the analysis of advanced network monitoring systems, behavioral traffic analysis, and predictive algorithms in identifying anomalies and vulnerabilities. The results show that AI-driven automation significantly reduces the mean time to detect and respond to incidents, although challenges such as false positives, the need for continuous model training, and high implementation costs persist. The findings suggest that sustainable adoption of these technologies requires investment in technical training, data governance, and ongoing research and development.

Keywords: Artificial Intelligence. Cybersecurity. Threat Detection. Incident Response. Machine Learning.

Resumen

Este estudio tiene como objetivo evaluar la eficacia y la viabilidad de la implementación de técnicas de inteligencia artificial y aprendizaje automático en la detección de amenazas y la respuesta a incidentes cibernéticos, con el fin de optimizar la seguridad operativa y proteger las infraestructuras críticas contra ataques virtuales. La metodología adoptada comprende el análisis de sistemas avanzados de monitoreo de red, análisis de comportamiento del tráfico y algoritmos predictivos en la identificación de anomalías y vulnerabilidades. Los resultados demuestran que la automatización impulsada por la inteligencia artificial reduce significativamente el tiempo medio de detección y respuesta a incidentes, aunque persisten desafíos como la ocurrencia de falsos positivos, la necesidad de entrenamiento continuo de los modelos y los altos costos de implementación. Se concluye que la adopción sostenible de estas tecnologías requiere inversiones en capacitación técnica, gobernanza de datos y esfuerzos continuos en investigación y desarrollo.

Palabras clave: Inteligencia Artificial. Ciberseguridad. Detección de Amenazas. Respuesta a incidentes. Aprendizaje Automático.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 01/07/2026 | aceito: 20/07/2026 | publicação: 16/08/2026

1. Introdução

Este estudo se propõe a analisar a aplicação de métodos avançados de inteligência artificial (IA) e aprendizado de máquina (*machine learning*) na detecção de ameaças e na resposta a incidentes cibernéticos, com o objetivo de otimizar a segurança operacional, mitigar riscos de ataques virtuais e promover uma gestão mais eficiente da proteção de dados e infraestruturas tecnológicas.

A gestão de segurança proposta neste estudo baseia-se na integração de algoritmos de análise comportamental e sensores de monitoramento de rede que atuam de forma contínua. Em caso de anomalias ou tentativas de intrusão, esses sistemas inteligentes sinalizam em tempo real à central de operações de segurança (SOC), permitindo a rápida identificação, contenção e mitigação das ameaças.

Portanto, este estudo visa responder à seguinte questão: qual é a eficácia e a viabilidade da implementação de métodos avançados baseados em inteligência artificial para a detecção de ameaças e resposta a incidentes cibernéticos, visando aumentar a resiliência das organizações contra ataques virtuais?

Tem-se como objetivo geral avaliar a eficácia e a viabilidade da implementação de técnicas avançadas de inteligência artificial e aprendizado de máquina na automação do monitoramento de redes, na detecção precoce de ameaças e na otimização da resposta a incidentes de cibersegurança.

2 Referencial Teórico

2.1 Sistemas Inteligentes no Contexto da Cibersegurança

O conhecimento é fundamental para o desenvolvimento da sociedade, que evoluiu da economia agrícola para a industrial e está na era da informação, onde a informação se tornou o ativo mais valioso e estratégico das organizações. Esse cenário desempenha um papel central no avanço das forças produtivas, sendo que o sucesso e a resiliência corporativa dependem de como as entidades criam, gerenciam e protegem seus

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 01/07/2026 | aceito: 20/07/2026 | publicação: 16/08/2026

conhecimentos e dados contra ameaças digitais crescentes (Rezende, 2003).

As mudanças na sociedade moderna são numerosas, sendo a maioria impulsionada pelo avanço das tecnologias de informação, que trouxeram processamento de dados em tempo real, interconexão global e a quebra de barreiras geográficas. Contudo, essa hiperconectividade expandiu a superfície de ataque virtual, impondo às organizações a necessidade de atualização e vigilância constantes para garantir a integridade de seus ecossistemas digitais (Chaves Junior, 2021).

Nessa transformação contínua, a transição do trabalho puramente físico para o intelectual consagrou a informação como o motor da economia contemporânea. Nesse ambiente, a preservação da confidencialidade, disponibilidade e autenticidade dos dados tornou-se requisito essencial tanto para a estabilidade econômica das empresas quanto para a sustentabilidade operacional do mercado. A tecnologia da informação e da comunicação, ao derrubar fronteiras entre países, viabilizou novos modelos de negócios, mas também expôs sistemas a ciberameaças transnacionais altamente sofisticadas (Rezende, 2003).

Na era do conhecimento, a capacidade de adaptação e a infraestrutura de segurança cibernética de uma empresa definem sua sobrevivência no mercado. À medida que a sofisticação dos ataques virtuais acelera a obsolescência das defesas tradicionais baseadas em regras rígidas, surge a necessidade de mecanismos capazes de analisar grandes volumes de dados de rede de forma autônoma. Nesse cenário, os avanços em hardware e software viabilizaram a aplicação de Sistemas Inteligentes (SI), que utilizam técnicas computacionais avançadas para manipular conhecimento especializado e identificar comportamentos maliciosos.

Conforme destaca Rezende (2003), o comportamento e os atributos de um Sistema Inteligente diferem substancialmente dos sistemas de computação convencionais. Enquanto ferramentas tradicionais atuam de forma reativa e estática, os Sistemas Inteligentes aplicados à cibersegurança são capazes de analisar padrões complexos, correlacionar eventos de rede e inferir novos riscos. Essa capacidade de manipular representações do mundo real de forma dinâmica permite identificar anomalias e mitigar incidentes cibernéticos com superioridade técnica e menor intervenção humana (Rezende, 2003).

2.2 Inteligência Artificial e Machine Learning em Cibersegurança

O termo "aprendizagem de máquina" (*machine learning*) surgiu no final do século XX e pode

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 01/07/2026 | aceito: 20/07/2026 | publicação: 16/08/2026

ser definido como a capacidade de um sistema melhorar seu desempenho em uma tarefa por meio da experiência e da identificação de padrões em grandes volumes de dados (Magalhães, 2015). No campo da segurança da informação, essa tecnologia emprega ferramentas como redes neurais artificiais e máquinas de vetores de suporte (SVM), que se mostram altamente eficazes no tratamento e na análise de dados complexos e ruidosos, uma característica marcante dos pacotes de dados e logs de tráfego de rede (Ventura, 2012).

Além disso, o uso do processamento de linguagem natural (NLP) permite que os sistemas analisem textos não estruturados, como relatórios de ameaças (*threat intelligence*), logs de auditoria e e-mails suspeitos, identificando padrões de ataque e vetores de engenharia social, o que contribui para aumentar a precisão na detecção de vulnerabilidades (Syam; Sharma, 2018). Dessa forma, a aprendizagem de máquina estabelece-se como uma ferramenta indispensável para otimizar operações de segurança em ambientes digitais dinâmicos e sujeitos a constantes mutações de ameaças (Magalhães, 2015).

Ferreira (2024) explica que um modelo de aprendizagem de máquina adquire e utiliza conhecimento quando é capaz de empregar informações históricas para inferir novos resultados e identificar comportamentos inéditos. No contexto cibernético, isso significa utilizar o histórico de tráfego e requisições passadas para reconhecer novos vetores de ataque antes imprevisíveis. Assim, a aprendizagem de máquina refere-se ao campo no qual são desenvolvidos e analisados algoritmos, técnicas e ferramentas que viabilizam essa capacidade adaptativa de proteção.

Metodologicamente, a aprendizagem de máquina aplicada à cibersegurança categoriza-se em diferentes abordagens:

- **Aprendizagem não supervisionada:** agrupa dados de rede sem rotulação prévia para identificar anomalias, comportamentos fora do padrão e novas variantes de ataques (*zero-day*);
- **Aprendizagem supervisionada:** utiliza dados previamente classificados (como tráfego benigno versus código malicioso) como exemplos de treinamento para que o modelo possa categorizar novas ameaças com alta precisão;
- **Aprendizagem semissupervisionada:** combina dados rotulados e não rotulados para otimizar o treinamento do sistema, reduzindo o custo operacional de etiquetagem de dados sem comprometer a capacidade preditiva (Syam; Sharma, 2018).

No que tange à contenção de riscos, a aprendizagem de máquina cumpre um papel decisivo ao permitir a identificação precoce de anomalias em infraestruturas computacionais complexas, como redes corporativas e servidores críticos, minimizando o tempo de exposição a

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 01/07/2026 | aceito: 20/07/2026 | publicação: 16/08/2026

explorações e reduzindo potenciais prejuízos financeiros e operacionais (Arbex, 2009). Por sua vez, a inteligência artificial (IA) surgiu na década de 1950 com o objetivo de desenvolver sistemas capazes de realizar tarefas que exigiam capacidade cognitiva humana ou que não possuíam uma solução algorítmica viável por meio da programação convencional (Skalfist, Mikelsten, Teigens, 2020). Pesquisadores da área utilizam teorias sobre processamento de informação como base para desenvolver sistemas capazes de emular raciocínios analíticos no monitoramento de dados (Aguiar, 2025).

Essas abordagens podem ser codificadas em programas que permitem às máquinas aprender, raciocinar e tomar decisões defensivas autônomas (Ventura, 2012). A IA tem evoluído continuamente, influenciando vertentes como a automação de resposta a incidentes, a inteligência contra ameaças e o aprendizado de máquina, tornando-se pilar estratégico da segurança cibernética moderna (Magalhães, 2015).

Aguiar (2025) ressalta que a IA pode ser aplicada para otimizar o monitoramento e a proteção contínua de ecossistemas de TI, permitindo a análise em tempo real de eventos de segurança. Com a capacidade de prever intrusões e executar bloqueios automáticos de acessos não autorizados, a inteligência artificial eleva substancialmente a resiliência das defesas digitais.

Ao atuar diretamente na detecção de falhas e invasões, a IA analisa anomalias em dados operacionais e identifica desvios de comportamento nos usuários ou sistemas, reduzindo drasticamente o tempo de inatividade causado por ataques como *ransomware* ou indisponibilidade de serviço em setores críticos (Borruso, 2019).

Borruso (2019) destaca que a aplicação da IA na gestão da segurança cibernética oferece benefícios expressivos, como a economia de tempo na triagem de alertas, a diminuição da fadiga dos analistas e a redução de erros humanos. Ao automatizar processos complexos de contenção de incidentes, o sistema otimiza a atuação das centrais de operações de segurança (SOC). No entanto, é fundamental reconhecer que a IA também apresenta desafios, incluindo o risco de falsos positivos, vieses nos modelos e o surgimento de táticas adversárias direcionadas a enganar os próprios. Tais desafios devem ser gerenciados de forma contínua para garantir que a automação traga confiabilidade operacional sem introduzir novas vulnerabilidades (Córdova, 2025). Assim, a integração de algoritmos inteligentes na defesa cibernética transforma radicalmente a governança da informação, desde que acompanhada de supervisão humana especializada e aprimoramento constante.

2 Metodologia

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 01/07/2026 | aceito: 20/07/2026 | publicação: 16/08/2026

Este estudo adotou uma abordagem metodológica qualitativa e exploratória, fundamentada em uma revisão integrativa da literatura para analisar a aplicação de técnicas avançadas de inteligência artificial e aprendizado de máquina na detecção de ameaças e resposta a incidentes cibernéticos.

A busca por referenciais teóricos e empíricos foi realizada nas bases de dados acadêmicas de alto impacto *IEEE Xplore*, *Scopus*, *Web of Science* e *Google Acadêmico*. Utilizaram-se descritores combinados nos idiomas português e inglês, tais como: "inteligência artificial em cibersegurança" (*artificial intelligence in cybersecurity*), "detecção de ameaças" (*threat detection*), "resposta a incidentes cibernéticos" (*cyber incident response*), "aprendizado de máquina em intrusões" (*machine learning intrusion detection*) e "automação em SOC" (*security operations center automation*). Adicionalmente, foram examinados artigos relevantes identificados por meio da técnica de amostragem em bola de neve (*snowballing*), analisando-se as referências dos trabalhos selecionados.

Os critérios de inclusão definidos contemplaram:

- Artigos científicos completos e capítulos de livros publicados em periódicos indexados;
- Estudos que abordassem diretamente a eficácia, os desafios operacionais e a viabilidade da implementação de algoritmos de inteligência artificial e *machine learning* na segurança da informação;
- Trabalhos focados na detecção de anomalias de rede, mitigação de ameaças conhecidas e desconhecidas (*zero-day*) e automação de resposta a incidentes cibernéticos.

Foram excluídos estudos com foco puramente teórico sem aplicabilidade prática à segurança computacional ou que tratassem de automação industrial sem interface com a cibersegurança.

Após a seleção do corpus bibliográfico, realizou-se uma análise categorial para mapear as principais tecnologias, algoritmos e arquiteturas computacionais aplicados. Para alcançar os objetivos específicos propostos, adotaram-se os seguintes procedimentos analíticos:

- **Mapeamento de Tecnologias de IA:** Identificação e categorização das principais arquiteturas de inteligência artificial e aprendizado de máquina (supervisionado, não supervisionado e processamento de linguagem natural) aplicadas ao monitoramento de tráfego de rede e análise de logs em tempo real;
- **Avaliação da Eficácia na Detecção de Ameaças:** Investigação do desempenho dessas ferramentas na identificação precoce de intrusões, análise comportamental de anomalias, prevenção de ataques complexos (como *ransomware* e violações de dados) e redução do tempo médio de detecção (MTTD);
- **Análise da Resposta e Integração Operacional:** Avaliação da viabilidade de integração

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 01/07/2026 | aceito: 20/07/2026 | publicação: 16/08/2026

dessas soluções a ecossistemas de automação de segurança, como ferramentas de *Security Orchestration, Automation and Response* (SOAR) e Centros de Operações de Segurança (SOC), visando otimizar a mitigação de incidentes e reduzir o tempo médio de resposta (MTTR).

3 Resultados e Discussão

Os estudos analisados sobre a aplicação de inteligência artificial (IA) e aprendizado de máquina (*machine learning*) na cibersegurança evidenciam avanços significativos na identificação de ameaças, na mitigação de riscos e na otimização operacional das centrais de segurança da informação (*Security Operations Centers* — SOC). A literatura correlacionada demonstra que a transição de métodos reativos tradicionais para ecossistemas preditivos baseados em IA altera fundamentalmente a dinâmica de defesa cibernética.

Estudos voltados ao monitoramento contínuo de tráfego de rede revelam que a implementação de algoritmos de aprendizado não supervisionado permite a criação de perfis comportamentais dinâmicos para dispositivos e usuários. Essa abordagem provou-se altamente eficaz na detecção de anomalias sutis e intrusões do tipo *zero-day* (ameaças sem assinatura conhecida), ultrapassando as limitações dos sistemas de detecção baseados estritamente em regras. Os resultados indicam que a análise preditiva em tempo real reduz drasticamente o tempo médio de detecção (*Mean Time to Detect* — MTTD), identificando exfiltrações de dados e movimentações laterais maliciosas nos estágios iniciais do ataque.

No âmbito da automação da resposta a incidentes cibernéticos, as pesquisas destacam o impacto da integração entre modelos de inteligência artificial e plataformas de orquestração e resposta de segurança (*Security Orchestration, Automation and Response* — SOAR). A aplicação de algoritmos inteligentes na triagem primária de alertas permite a execução autônoma de fluxos de contenção — como o isolamento imediato de máquinas comprometidas, o bloqueio automático de endereços IP suspeitos e a revogação preventiva de credenciais de acesso. Evidencia-se que a automação de respostas simples diminui significativamente o tempo médio de resposta (*Mean Time to Respond* — MTTR), além de aliviar a saturação dos analistas de segurança e reduzir a fadiga causada por excesso de alertas.

Adicionalmente, os achados da literatura abordam a viabilidade operacional e os desafios econômicos inerentes à adoção dessas tecnologias inteligentes:

- Eficácia Preditiva: O uso de processamento de linguagem natural (NLP) combinado a modelos preditivos para análise de inteligência de ameaças (*threat intelligence*) possibilita a

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

antecipação de vetores de ataques complexos, como campanhas de *phishing* sofisticadas e infecções por *ransomware*;

- Redução de Custos de Impacto: Embora o investimento inicial em infraestrutura computacional, licenciamento de software e capacitação especializada seja elevado, a análise de viabilidade econômica demonstra um retorno positivo à medida que previne indisponibilidades sistêmicas e evita perdas financeiras astronômicas decorrentes de vazamentos de dados e multas regulatórias;
- Desafios Operacionais: A literatura aponta limitações persistentes que exigem governança rigorosa, com destaque para a taxa de falsos positivos, o risco de envenenamento de dados de treinamento (*data poisoning*) e as táticas de evasão empregadas por cibercriminosos contra os próprios modelos de inteligência artificial.

A síntese dos resultados consolida que a integração de métodos avançados de IA e aprendizado de máquina na resposta a incidentes cibernéticos não apenas amplia a resiliência e a confiabilidade dos ecossistemas de TI, mas também se apresenta como uma estratégia sustentável e economicamente viável para a proteção de ativos digitais críticos a longo prazo.

Considerações Finais

O objetivo geral deste estudo foi avaliar a eficácia e a viabilidade da implementação de técnicas de inteligência artificial (IA) e aprendizado de máquina na detecção de ameaças e na resposta a incidentes cibernéticos, com foco em otimizar a segurança operacional, mitigar riscos de ataques virtuais e promover uma gestão eficiente de proteção de dados. Para atingir essa meta, os objetivos específicos orientaram a análise da literatura e sustentaram as conclusões apresentadas.

A investigação das tecnologias disponíveis para o monitoramento em tempo real demonstrou que a aplicação de IA e *machine learning* é amplamente reconhecida pelo seu impacto positivo na detecção precoce de intrusões e na automação de defesas de rede. No entanto, o estudo também apontou que a eficácia dessas ferramentas depende diretamente da qualidade dos dados de treinamento e da governança sobre os modelos computacionais, sendo crucial uma gestão precisa de *logs* e eventos para otimizar o aprendizado dos algoritmos e evitar vieses operacionais.

Na avaliação da detecção precoce de ameaças e prevenção de incidentes complexos (como *ransomware* e violações de dados), evidenciou-se que a análise comportamental preditiva supera as limitações das abordagens tradicionais baseadas apenas em assinaturas estáticas.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 01/07/2026 | aceito: 20/07/2026 | publicação: 16/08/2026

Todavia, observou-se que a ocorrência de falsos positivos e a sofisticação de técnicas de evasão empregadas por cibercriminosos ainda representam desafios técnicos que exigem a manutenção da supervisão humana especializada junto aos centros de operações de segurança (SOC).

No que tange à viabilidade econômica e operacional, o estudo avaliou o balanço entre investimentos e benefícios da automação em cibersegurança. Embora a aquisição, integração e manutenção de ferramentas inteligentes apresentem custos iniciais elevados, a análise demonstra que esse investimento é amplamente compensado pela redução do tempo médio de resposta (MTTR) e pela prevenção de prejuízos financeiros devastadores decorrentes de vazamentos de dados, paralisações sistêmicas e sanções regulatórias.

Assim, este estudo reafirma a importância crucial da inteligência artificial no fortalecimento da cibersegurança moderna. Contudo, ressalta a necessidade de superar desafios como a redução de falsos positivos, a mitigação de riscos de envenenamento de dados e a necessidade de capacitação técnica contínua. Para maximizar os benefícios observados, é essencial manter esforços constantes em pesquisa e desenvolvimento, garantindo que as soluções de inteligência artificial evoluam no mesmo ritmo das ciberameaças.

Referências

AGUIAR, David. Use of artificial intelligence for proactive detection of cyber threats in corporate environments. Aurum, p. 57-67, 2025.

CHAVES JUNIOR, Wankes Solony de Carvalho. Engenharia de Materiais no âmbito da Indústria
4.0. RCMOS-Revista Científica Multidisciplinar O Saber, v. 1, n. 6, p. 1–9, 2021.

CÓRDOVA, Paulo Roberto. Inteligência artificial: entre o fascínio e o medo. Contexto, 2025.

FERREIRA, Poliana N. Aprendizado de máquina. Senac São Paulo, 2024.

MAGALHÃES, Renato Vasconcelos. Inteligência artificial e direito: uma breve introdução histórica. Revista Direito e Liberdade, ESMARN, Mossoró, v. 1, n. 1, p. 355–370, jul./dez. 2015. ISSN Impresso 1809-3280 | ISSN Eletrônico 2177-1758.

REZENDE et al. Sistemas inteligentes: fundamentos e aplicações. Barueri, SP: Manole. 2003.

SYAM, Niladri; SHARMA, Arun. Waiting for a sales renaissance in the fourth industrial revolution: Machine learning and artificial intelligence in sales research and practice. Industrial Marketing Management, v. 69, p. 135-146, 2018.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 01/07/2026 | aceito: 20/07/2026 | publicação: 16/08/2026

SKALFIST, P., MIKELSTEN, D., TEIGENS, V. Inteligência Artificial: a quarta revolução industrial. Cambridge Stanford Books. 2020.

VENTURA, R.V. et al. Uso de redes neurais artificiais na predição de valores genéticos para peso aos 205 dias em bovinos da raça Tabapuã. Arq. Bras. Med. Vet. Zootec., v.64, n.2, p.411–418, 2012.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.