



INSTITUTO FEDERAL
Rondônia



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Rondônia

CAMPUS PORTO VELHO ZONA NORTE
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

JOÃO PEDRO REGINATO
JÉFERSON OLIVEIRA
SOUSA

AUTOMAÇÃO DE REDES NA INDÚSTRIA 4.0: DESAFIOS
TECNOLÓGICOS, ECONÔMICOS E DE SEGURANÇA NA
IMPLEMENTAÇÃO

PORTO VELHO/RO

2025



JOÃO PEDRO REGINATO
JÉFERSON OLIVEIRA SOUSA

**AUTOMAÇÃO DE REDES NA INDÚSTRIA 4.0: DESAFIOS
TECNOLÓGICOS, ECONÔMICOS E DE SEGURANÇA NA
IMPLEMENTAÇÃO**

Artigo apresentado ao Curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia – IFRO Campus Porto Velho Zona Norte como requisito avaliativo para obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Silmar Antonio Buchner de
Oliveira Coorientador: Douglas Moro Piffer

PORTO VELHO/RO

2025



INSTITUTO FEDERAL
Rondônia



MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Rondônia

JOÃO PEDRO REGINATO
JÉFERSON OLIVEIRA SOUSA

AUTOMAÇÃO DE REDES NA INDÚSTRIA 4.0:
DESAFIOS TECNOLÓGICOS, ECONÔMICOS E DE SEGURANÇA NA
IMPLEMENTAÇÃO

Artigo entregue como Trabalho de Conclusão de Curso ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), *Campus Zona Norte*, como requisito parcial para obtenção do grau de tecnólogo, junto ao Curso Tecnologia em Redes de Computadores, sob a orientação do professor Silmar Antonio Buchner de Oliveira.

Aprovado em: 09/04/2025 pela banca examinadora.



Documento assinado digitalmente
SILMAR ANTONIO BUCHNER DE OLIVEIRA
Data: 25/06/2026 15:44:24-0300
Verifique em <https://validar.iti.gov.br>

Orientador



Documento assinado digitalmente
JHORDANO MALACARNE BRAVIM
Data: 25/06/2026 20:44:16-0300
Verifique em <https://validar.iti.gov.br>

Coordenador do curso

Ficha catalográfica elaborada pelo Sistema Gerador de Ficha Catalográfica do IFRO.

Reginato, João Pedro.

Automação de redes na indústria 4.0: desafios tecnológicos, econômicos e de segurança na implementação / João Pedro Reginato, Jéferson Oliveira Sousa. - Porto Velho, 2025.
24 f. : il.

Orientador(a): Prof. Me. Silmar Antonio Buchner de Oliveira.
Coorientador(a): Prof. Me. Douglas Moro Piffer.

Trabalho de Conclusão de Curso (Superior de Tecnologia em Redes de Computadores) – Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Porto Velho, 2025.

1. Automação de redes. 2. Indústria 4.0. 3. Interoperabilidade. 4. Segurança cibernética. I. Sousa, Jéferson Oliveira. II. Oliveira, Silmar Antonio Buchner de (orient.). III. Piffer, Douglas Moro (coorient.). IV. Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO. V. Título.

Bibliotecário(a) Responsável: Marlene Fouz da Silva, CRB-11/946

AUTOMAÇÃO DE REDES NA INDÚSTRIA 4.0: DESAFIOS TECNOLÓGICOS, ECONÔMICOS E DE SEGURANÇA NA IMPLEMENTAÇÃO

NETWORK AUTOMATION IN INDUSTRY 4.0: TECHNOLOGICAL, ECONOMIC AND SECURITY CHALLENGES IN IMPLEMENTATION

DOI: 10.55908/RGCV19N1-006

Originals received:

12/13/2024 Acceptance for
publication: 01/10/2025

Jéferson Oliveira Sousa

Tecnólogo em Redes de Computadores

Instituição: Instituto Federal de Rondônia (IFRO) - Campus Porto Velho Zona Norte

Endereço: Porto Velho, Rondônia, Brasil

E-mail: jeferson.sousa@estudante.ifro.edu.br

João Pedro Reginato

Tecnólogo em Redes de Computadores

Instituição: Instituto Federal de Rondônia (IFRO) - Campus Porto Velho Zona Norte

Endereço: Porto Velho, Rondônia, Brasil

E-mail: reginato610@gmail.com

Silmar Antonio Buchner de Oliveira

Mestre em Ensino Tecnológico pelo Instituto Federal do Amazonas (IFAM)

Instituição: Instituto Federal de Rondônia (IFRO) - Campus Porto Velho Zona

Norte Endereço: Porto Velho, Rondônia, Brasil

E-mail: silmar.oliveira@ifro.edu.br

Douglas Moro Piffer

Mestre em Administração pelo Universidade Federal de Rondônia (UNIR)

Instituição: Instituto Federal de Rondônia (IFRO) - campus Porto Velho Zona

Norte Endereço: Porto Velho, Rondônia, Brasil

E-mail: douglas.piffer@ifro.edu.br

RESUMO: A automação de redes é um dos pilares centrais da Indústria 4.0, sendo responsável por integrar de maneira inteligente e eficiente dispositivos, sistemas e processos. Este estudo examina os desafios técnicos, estruturais e de segurança cibernética relacionados à implementação dessa tecnologia em ambientes industriais. A partir de uma revisão bibliográfica

qualitativa, foram identificadas barreiras associadas à interoperabilidade entre sistemas heterogêneos, à infraestrutura tecnológica necessária para sustentar redes automatizadas e aos crescentes riscos de ciberataques. Verificou-se que a ausência de padrões universais e a dependência de tecnologias legadas dificultam a integração de sistemas e restringem o potencial inovador. Além disso, a implementação de redes robustas, como as que utilizam 5G e computação em nuvem, é essencial para atender à crescente demanda por conectividade em tempo real, mas apresenta desafios econômicos e logísticos. No que tange à segurança cibernética, estratégias como a adoção de arquiteturas com o conceito de "zero trust" e o uso de inteligência artificial para detecção de ameaças têm se mostrado eficazes na mitigação de riscos. Conclui-se que, para superar os desafios da automação de redes na Indústria 4.0, é necessário adotar uma abordagem integrada que combine avanços tecnológicos, capacitação profissional e políticas de governança robustas. Este estudo oferece contribuições teóricas e práticas para indústrias que desejam se adaptar às exigências da transformação digital, promovendo uma automação eficiente, segura e sustentável.

PALAVRAS-CHAVE: Automação de Redes. Indústria 4.0. Interoperabilidade. Segurança Cibernética.

ABSTRACT: Network automation is one of the central pillars of Industry 4.0, responsible for intelligently and efficiently integrating devices, systems, and processes. This study examines the technical, structural, and cybersecurity challenges related to the implementation of this technology in industrial environments. Based on a qualitative literature review, barriers were identified regarding interoperability between heterogeneous systems, the technological infrastructure required to support automated networks, and the increasing risks of cyberattacks. It was found that the lack of universal standards and the reliance on legacy technologies hinder system integration and limit innovative potential. Furthermore, the implementation of robust networks, such as those using 5G and cloud computing, is essential to meet the growing demand for real-time connectivity but presents economic and logistical challenges. In terms of cybersecurity, strategies like adopting "zero trust" architectures and using artificial intelligence for threat detection have proven effective in mitigating risks. It is concluded that to overcome the challenges of network automation in Industry 4.0, an integrated approach is needed, combining technological advances, professional training, and robust governance policies. This study provides both theoretical and practical contributions for industries seeking to adapt to the demands of digital transformation, promoting efficient, secure, and sustainable automation.

KEYWORDS: Network Automation. Industry 4.0. Interoperability. Cybersecurity.

1. INTRODUÇÃO

A evolução para a Indústria 4.0, marcada pela convergência de tecnologias físicas, digitais e biológicas, tem transformado significativamente a forma como as empresas desenvolvem, produzem e administram seus processos industriais. Nesse contexto, a automação de redes desempenha um papel central, conectando máquinas, sistemas e pessoas em tempo real, o que resulta em maior eficiência e flexibilidade operacional. Contudo, esse progresso enfrenta desafios como a integração de tecnologias diversas, a necessidade de uma infraestrutura sólida e a garantia de segurança cibernética em um ambiente amplamente conectado (Saito *et al.*, 2024). Além disso, o avanço acelerado de tecnologias como a Internet das Coisas (IoT) e a inteligência artificial (IA) exige a adoção de novos paradigmas de automação, superando sistemas tradicionais isolados e exigindo soluções inovadoras e adaptáveis para responder às demandas da indústria contemporânea (Andrade *et al.*, 2024).

Uma das características fundamentais da automação de redes na Indústria 4.0 é sua capacidade de viabilizar uma produção inteligente, com dispositivos conectados que coletam e analisam dados em tempo real, fornecendo informações valiosas para decisões estratégicas. Entretanto, a interoperabilidade entre sistemas de diferentes fabricantes, que frequentemente utilizam protocolos incompatíveis, representa um desafio significativo. Essa barreira demanda o desenvolvimento de padrões universais e modelos de integração que harmonizem a comunicação entre dispositivos sem prejudicar o desempenho e a segurança dos sistemas (Monteiro *et al.*, 2025). Além disso, a implementação em larga escala de redes automatizadas exige uma infraestrutura de comunicação robusta, como redes 5G e tecnologias baseadas em fibra óptica, capazes de atender à alta demanda por conectividade estável e de baixa latência (Sacomano *et al.*, 2018).

Por outro lado, o aumento da conectividade também amplifica os riscos relacionados à segurança cibernética, uma vez que cada dispositivo conectado pode se tornar um ponto de vulnerabilidade. Assim, a proteção de dados sensíveis e a privacidade tornam-se aspectos cruciais no desenvolvimento de redes automáticas para a Indústria 4.0. Pesquisas recentes destacam que a ausência de estratégias de segurança robustas pode comprometer operações

críticas, além de expor as organizações a perdas financeiras e danos reputacionais irreparáveis (Branquinho e Branquinho, 2021). Nesse cenário, o uso de soluções como criptografia avançada, autenticação multifator e monitoramento contínuo surge como essencial para mitigar os riscos cibernéticos.

Embora a automação de redes na Indústria 4.0 prometa avanços significativos em produtividade e inovação, sua implementação enfrenta barreiras técnicas e operacionais que dificultam a integração plena desses sistemas. Assim, quais estratégias podem ser adotadas para superar os desafios relacionados à interoperabilidade, à infraestrutura e à segurança cibernética, promovendo uma automação de redes eficiente e segura?

Este estudo tem como objetivo geral analisar os desafios enfrentados pela automação de redes na Indústria 4.0 e propor estratégias para mitigá-los, visando otimizar a integração tecnológica nas organizações industriais. Os objetivos específicos incluem: identificar os principais obstáculos técnicos da automação de redes na Indústria 4.0, avaliar os impactos da falta de interoperabilidade e infraestrutura nos sistemas automatizados e apresentar soluções práticas e inovadoras para melhorar a segurança cibernética em redes industriais automatizadas. A relevância deste estudo está na crescente necessidade de adaptação das indústrias às exigências tecnológicas da Indústria 4.0. A automação de redes, ao conectar dispositivos, processos e pessoas, é um elemento estratégico para a transformação digital das organizações. Contudo, os desafios enfrentados nesse campo podem comprometer a adoção integral dessas tecnologias, resultando em perda de competitividade em um mercado global altamente dinâmico (Martins Junior e Silva, 2024). Dessa forma, compreender essas barreiras e propor soluções viáveis é fundamental para assegurar o sucesso da transformação digital nas indústrias. Além disso, o avanço de tecnologias como IoT e IA tem gerado novas oportunidades, mas também ampliado os riscos relacionados à segurança e à confiabilidade das redes automatizadas. Em um cenário no qual os dados são o principal ativo das organizações, proteger essas informações contra ameaças externas e falhas internas é uma prioridade estratégica. Este estudo contribui para o desenvolvimento de um arcabouço teórico e prático que auxilie as indústrias a enfrentar esses desafios, promovendo uma automação de redes segura, eficiente e sustentável.

2. METODOLOGIA

Esta pesquisa segue uma abordagem qualitativa de revisão bibliográfica, caracterizada pela análise detalhada de fontes teóricas e empíricas relevantes ao tema. Essa metodologia possibilita uma compreensão ampla dos desafios relacionados à automação de redes na Indústria 4.0, integrando diferentes perspectivas e saberes disponíveis na literatura científica. A seleção das fontes baseou-se em critérios como relevância, atualidade e confiabilidade, priorizando publicações dos últimos dez anos em periódicos indexados e eventos de destaque. Além disso, foram incluídos livros, relatórios técnicos e normas internacionais, proporcionando uma visão abrangente e detalhada sobre o assunto. A busca foi realizada em bases de dados como Scopus, Web of Science e Google Scholar, utilizando palavras-chave relacionadas à automação de redes, Indústria 4.0, interoperabilidade, infraestrutura tecnológica e segurança cibernética.

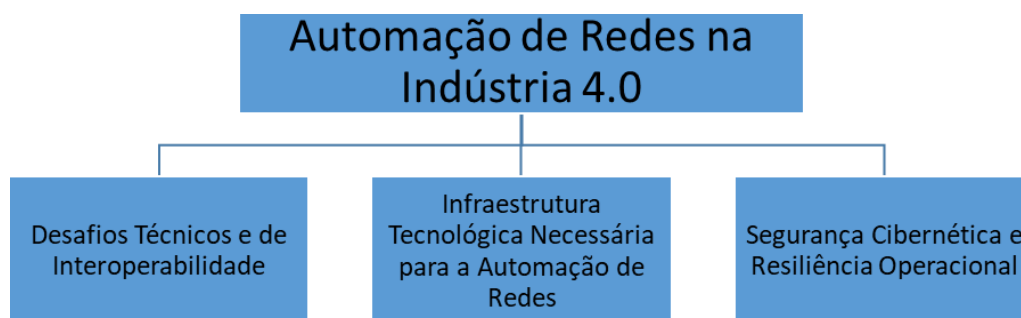
O processo de análise envolveu a organização e categorização sistemática dos materiais selecionados, garantindo rigor metodológico. Primeiramente, foram avaliados os títulos e resumos para verificar sua pertinência em relação aos objetivos do estudo. Posteriormente, os textos completos das fontes escolhidas foram analisados criticamente, com o objetivo de identificar conceitos essenciais, tendências e lacunas na literatura. A triangulação das fontes contribuiu para validar os resultados, ao integrar dados de diferentes autores e contextos, resultando em uma análise robusta e confiável.

A abordagem qualitativa adotada nesta revisão não apenas descreveu os desafios da automação de redes na Indústria 4.0, mas também interpretou e contextualizou os achados à luz de teorias e práticas contemporâneas. Isso possibilitou a exploração das interconexões entre diversos aspectos do tema, como as implicações tecnológicas, econômicas e sociais da automação. Além disso, considerando o contexto das indústrias emergentes, foram examinadas as particularidades e os desafios enfrentados em regiões em desenvolvimento, incluindo o Brasil. Essa perspectiva favoreceu a formulação de recomendações fundamentadas e mais aplicáveis, capazes de subsidiar estudos futuros e orientar estratégias práticas no campo da automação industrial.

3. DESENVOLVIMENTO

A automação de redes na Indústria 4.0 configura-se como um tema de alta complexidade, abrangendo diversos aspectos técnicos, operacionais e estratégicos. Este capítulo explora os principais elementos associados aos desafios e às possíveis soluções nessa área, oferecendo uma análise detalhada de suas particularidades. Para organizar a discussão, o conteúdo foi estruturado em três seções: a seção 3.1 aborda os desafios técnicos e questões de interoperabilidade; a seção 3.2 examina a infraestrutura tecnológica indispensável para a automação de redes; e a seção 3.3 foca nas questões de segurança cibernética e resiliência operacional. O objetivo é apresentar uma visão integrada e aprofundada, que conecta fundamentos teóricos às práticas industriais.

Figura 1: Organograma dos achados da pesquisa



Fonte: Elaborado pelos autores.

3.1 DESAFIOS TÉCNICOS E DE INTEROPERABILIDADE

A automação de redes na Indústria 4.0 enfrenta desafios consideráveis, principalmente no que diz respeito à interoperabilidade entre os sistemas. Em um cenário no qual dispositivos, máquinas e plataformas digitais de fabricantes distintos precisam operar em conjunto, a ausência de padrões globais se torna uma barreira significativa. A falta de protocolos comuns de comunicação dificulta não apenas a integração, mas também compromete a eficiência operacional, gerando custos adicionais e prolongando o tempo necessário para a implementação das soluções tecnológicas (Saito *et al.*, 2024).

A diversidade dos sistemas exigiu a adoção de arquiteturas adaptáveis, que viabilizem a integração de tecnologias mais antigas com as soluções contemporâneas. Muitas empresas ainda operam com sistemas de controle e automação desenvolvidos há várias décadas, o que impõe dificuldades técnicas para conectá-los às plataformas digitais atuais. Um exemplo disso é a integração de sistemas SCADA com redes inteligentes, que evidencia os obstáculos enfrentados pelas organizações para alinhar tecnologias antigas e novas (De Araújo *et al.*, 2024).

Outro ponto relevante é o custo envolvido na padronização tecnológica no nível industrial. Para resolver os problemas de interoperabilidade, as empresas precisam investir em soluções middleware, que funcionam como intermediárias entre diferentes sistemas. No entanto, essa abordagem pode ser financeiramente inviável para pequenas e médias empresas (PMEs), aumentando ainda mais a desigualdade tecnológica entre organizações de diferentes tamanhos (Auletta *et al.*, 2023).

A formação técnica das equipes também representa uma barreira significativa para a automação de redes. Profissionais precisam estar atualizados com as tecnologias emergentes, como protocolos de IoT, aprendizado de máquina e computação em nuvem. A escassez de mão de obra qualificada dificulta a implementação de soluções inovadoras e impacta diretamente a eficiência dos sistemas automatizados (Kusma e Chiroli, 2021).

Além disso, a interoperabilidade em sistemas globais enfrenta desafios relacionados a aspectos linguísticos, culturais e regulatórios. Empresas multinacionais lidam frequentemente com normas técnicas divergentes em diferentes países, o que torna o desenvolvimento de soluções escaláveis ainda mais complexo. Esse cenário reforça a necessidade de uma colaboração internacional para a criação de padrões globais que promovam a integração universal dos sistemas (Colcher, 2019).

A interoperabilidade nos sistemas de automação de redes da Indústria 4.0 é um desafio significativo devido à coexistência de tecnologias legadas e emergentes. Máquinas e equipamentos instalados há muito tempo utilizam protocolos proprietários que muitas vezes não são compatíveis com as tecnologias atuais. Esse desalinhamento técnico prejudica a integração e limita a coleta e análise de dados em tempo real, essencial para processos

industriais modernos (Ponte, 2022). Além disso, a falta de padronização global de protocolos de comunicação industrial dificulta a escalabilidade das soluções tecnológicas em ambientes industriais multinacionais.

Outro fator limitante é a alta dependência de tecnologias intermediárias, como middleware e gateways, que funcionam como tradutores entre sistemas diferentes. Embora sejam eficazes no curto prazo, essas soluções aumentam a complexidade, elevam os custos operacionais e podem gerar pontos únicos de falha. Isso ressalta a necessidade de desenvolver padrões internacionais, como OPC UA e MQTT, que garantam interoperabilidade nativa entre dispositivos de fabricantes diversos (Versoni, 2020).

A falta de colaboração entre fabricantes e desenvolvedores de tecnologias também agrava o problema da interoperabilidade. Muitos fornecedores optam por soluções proprietárias visando vantagem competitiva, o que dificulta a integração com sistemas de outros fornecedores. Esse cenário cria um ambiente fragmentado, no qual os usuários finais enfrentam dificuldades na implementação de soluções integradas. A formação de alianças industriais, como o Industrial Internet Consortium (IIC), é um passo importante para promover a criação de padrões abertos e facilitar a colaboração (Milanil e Loureiro, 2013).

Além dos desafios técnicos, a interoperabilidade também envolve questões organizacionais e culturais. Muitas empresas enfrentam resistência interna à mudança, especialmente em setores mais tradicionais. Essa barreira cultural exige esforços significativos de gestão de mudança e treinamento das equipes para adotar e operar novas tecnologias (Santos *et al.*, 2024). Caso contrário, mesmo soluções tecnicamente robustas podem não alcançar seu potencial.

A falta de suporte técnico adequado também representa um obstáculo considerável. À medida que os sistemas se tornam mais complexos, aumenta a demanda por profissionais especializados que compreendam os detalhes da interoperabilidade tecnológica. No entanto, muitas indústrias têm dificuldades em encontrar ou formar esses especialistas, o que compromete a eficiência dos processos de automação (Vargas, 2024).

O elevado custo inicial das soluções interoperáveis é outro impeditivo para a adoção por pequenas e médias empresas, que geralmente operam com orçamentos restritos. Incentivos.

governamentais e subsídios podem desempenhar um papel fundamental na superação dessa barreira financeira, possibilitando o acesso das PMEs às tecnologias avançadas de automação (Santos *et al.*, 2019).

3.2 INFRAESTRUTURA TECNOLÓGICA PARA AUTOMAÇÃO

A automação de redes requer uma infraestrutura robusta e confiável, capaz de gerenciar grandes volumes de dados e diversas conexões simultâneas. Nesse cenário, as redes 5G têm se consolidado como uma solução indispensável devido à sua elevada capacidade de transmissão, baixa latência e potencial para conectar dispositivos em larga escala. Entretanto, sua implementação encontra barreiras financeiras e logísticas, especialmente em áreas onde a infraestrutura de telecomunicações ainda é deficiente (Souza *et al.*, 2019).

O uso de tecnologias baseadas em fibra óptica é outro fator essencial, pois garante alta velocidade e confiabilidade na transmissão de informações. Essa infraestrutura é especialmente necessária para conectar dispositivos industriais que exigem comunicação em tempo real, como sistemas de robótica autônoma e monitoramento contínuo. Contudo, os custos elevados de instalação e manutenção representam desafios significativos, particularmente para empresas localizadas em áreas rurais ou remotas (Sacomano *et al.*, 2018).

A computação em nuvem exerce um papel crucial na automação de redes ao possibilitar o armazenamento, processamento e integração de grandes volumes de dados provenientes de dispositivos conectados. No entanto, para o pleno funcionamento dessa tecnologia, é indispensável contar com data centers robustos, redes de alta velocidade e políticas claras que garantam a proteção de dados e a privacidade (Paz e Loos, 2020).

Como alternativa complementar, as soluções de edge computing vêm ganhando destaque, ao transferir o processamento de dados para dispositivos próximos à sua origem. Essa abordagem melhora a eficiência e reduz a dependência de redes centralizadas. Apesar disso, desafios como os custos elevados de implementação e a necessidade de criar algoritmos otimizados para dispositivos com capacidades limitadas ainda precisam ser superados (De Araújo *et al.*, 2024).

Tecnologias emergentes, como gêmeos digitais e redes definidas por software (SDN), também se destacam como tendências para aprimorar a infraestrutura de redes. Essas soluções permitem simular, monitorar e gerenciar processos industriais em tempo real. Porém, sua aplicação em larga escala depende de investimentos expressivos em pesquisa e desenvolvimento, além de tecnologias de suporte adequadas (Monteiro *et al.*, 2025).

A base tecnológica da automação de redes da Indústria 4.0 é vital para garantir a conectividade, velocidade e confiabilidade exigidas por operações industriais avançadas. As redes 5G, que oferecem alta capacidade de transmissão e baixa latência, são um componente-chave dessa infraestrutura. Contudo, a implementação dessa tecnologia requer investimentos significativos, especialmente em áreas periféricas e rurais, onde a cobertura de telecomunicações ainda é insuficiente (Baldan *et al.*, 2024).

A dependência de sistemas de fibra óptica, embora ofereça alta estabilidade e capacidade de transmissão, apresenta desafios logísticos e financeiros. O custo elevado limita sua aplicação em várias regiões, o que tem levado à proposição de soluções híbridas, combinando redes 5G com tecnologias sem fio de menor custo para expandir a conectividade em áreas menos favorecidas (Jussiani, 2019).

A computação em nuvem continua sendo uma peça central na infraestrutura tecnológica, viabilizando o gerenciamento e a análise de grandes volumes de dados gerados por dispositivos conectados. Entretanto, questões relacionadas à privacidade e à segurança de dados permanecem uma preocupação. Para enfrentá-las, torna-se essencial implementar políticas de governança e compliance adequadas, principalmente em setores que lidam com informações sensíveis, como saúde e defesa (Ideyama e Becker, 2024).

De forma complementar, o edge computing desponta como uma alternativa promissora, ao realizar o processamento de dados localmente, próximo à fonte de geração. Essa tecnologia reduz atrasos e melhora a eficiência operacional, mas enfrenta desafios técnicos, como o desenvolvimento de algoritmos otimizados para dispositivos com capacidades limitadas de processamento (Romeiro, 2022).

A incorporação de tecnologias emergentes, como gêmeos digitais, possibilita a simulação e o monitoramento em tempo real de processos industriais. Essas soluções dependem

de redes de alta capacidade e ferramentas avançadas de modelagem. Contudo, sua implementação exige investimentos substanciais em infraestrutura e capacitação de equipes (Da Silva *et al.*, 2024).

O planejamento da infraestrutura de automação deve priorizar características como modularidade e escalabilidade, permitindo que as indústrias se adaptem rapidamente às inovações tecnológicas e às novas demandas do mercado. Nesse contexto, destaca-se a relevância de um planejamento estratégico sólido para o desenvolvimento da infraestrutura tecnológica (Santos *et al.*, 2024).

3.3 SEGURANÇA CIBERNÉTICA E RESILIÊNCIA OPERACIONAL

A segurança cibernética representa um dos maiores desafios na automação de redes na Indústria 4.0, devido ao aumento acelerado do número de dispositivos conectados e ao grande volume de dados sensíveis em circulação. Cada dispositivo pode se tornar um ponto de vulnerabilidade, e ataques cibernéticos têm o potencial de interromper gravemente as operações industriais, resultando em prejuízos financeiros e danos à imagem da empresa (Branquinho e Branquinho, 2021).

A fim de reduzir esses riscos, soluções de segurança que envolvem criptografia avançada e autenticação multifatorial têm sido amplamente adotadas. No entanto, é fundamental atualizar essas tecnologias constantemente para lidar com as ameaças emergentes. Além disso, a implementação de estratégias proativas de detecção de intrusões, como a utilização de inteligência artificial para identificar padrões atípicos, é uma prática recomendada para aumentar a resiliência das redes (Demolo Luque *et al.*, 2024).

A conscientização dos colaboradores também desempenha um papel vital na segurança dos sistemas automatizados. Pesquisas indicam que a maior parte dos incidentes cibernéticos ocorre devido a erros humanos, como o uso de senhas frágeis ou a abertura de e-mails fraudulentos. Programas de treinamento regulares, portanto, são essenciais para fortalecer a segurança organizacional (Kusma e Chiroli, 2021). Outro aspecto importante é a criação de políticas claras de governança e conformidade, que estabeleçam responsabilidades e

procedimentos em casos de ataques. Essas políticas devem ser acompanhadas de auditorias periódicas e simulações de incidentes para avaliar a capacidade de resposta das organizações (Auletta *et al.*, 2023).

Além disso, a adoção de arquiteturas de segurança com base no conceito de "zero trust" tem se destacado. Essa abordagem parte do princípio de que todos os dispositivos e usuários podem ser ameaças em potencial, exigindo autenticação contínua e monitoramento rigoroso de todas as atividades (De Arruda *et al.*, 2023). Isso diminui significativamente os riscos associados ao acesso não autorizado e ao movimento lateral dentro da rede. A segurança cibernética na automação das redes da Indústria 4.0 é um dos maiores desafios devido ao crescimento exponencial de dispositivos conectados e à complexidade crescente dos sistemas. A ampliação da superfície de ataque torna as redes industriais alvos frequentes de ciberataques, os quais podem causar interrupções operacionais e perdas financeiras significativas (Xavier, 2024). Estratégias de proteção, como firewalls avançados e sistemas de detecção de intrusões, são indispensáveis, mas não são suficientes diante da sofisticação das ameaças modernas.

Uma abordagem proativa utilizando inteligência artificial (IA) tem ganhado destaque na detecção e prevenção de ataques cibernéticos. Sistemas de IA podem monitorar o tráfego de rede continuamente, identificar padrões anômalos e reagir a incidentes em tempo real. Contudo, a eficácia dessas soluções depende da qualidade dos dados e de modelos de aprendizado robustos, os quais exigem investimentos consideráveis em pesquisa e desenvolvimento (Silva *et al.*, 2018).

A adoção de políticas de governança cibernética também é crucial para assegurar a conformidade com regulamentos internacionais e mitigar riscos organizacionais. Essas políticas devem incluir auditorias regulares, simulações de ataques e treinamentos para as equipes, promovendo uma cultura organizacional focada na segurança (Torres e Silva *et al.*, 2021).

Por outro lado, a resiliência operacional, entendida como a capacidade de uma organização de continuar suas operações durante e após um ataque cibernético, é um ponto crucial. A implementação de sistemas redundantes e estratégias de recuperação rápida é fundamental para minimizar os impactos de incidentes (Vargas, 2024).

A segurança cibernética na Indústria 4.0 exige a colaboração entre empresas, governos e instituições acadêmicas. Essa parceria é fundamental para compartilhar informações sobre novas ameaças e desenvolver soluções conjuntas que fortaleçam a resiliência de toda a cadeia produtiva (Pavão *et al.*, 2018).

A proteção das redes automatizadas requer a implementação de soluções integradas que cubram diversas camadas de segurança, desde a proteção física dos dispositivos até a segurança lógica dos sistemas de informação. A crescente complexidade das redes, que envolve dispositivos IoT, sensores industriais e sistemas em nuvem, expande consideravelmente a superfície de ataque. Para mitigar esses riscos, é essencial adotar firewalls avançados, sistemas de prevenção de intrusões (IPS) e segmentação de redes, criando barreiras adicionais contra a exploração de vulnerabilidades e reduzindo a propagação de ataques no ambiente industrial (Xavier, 2024).

O avanço das ameaças cibernéticas exige que as organizações adotem uma postura proativa na detecção e resposta a incidentes. Nesse contexto, soluções baseadas em inteligência artificial (IA) têm sido amplamente utilizadas, permitindo a detecção em tempo real de padrões atípicos no tráfego de rede. A IA possibilita que os sistemas de segurança aprendam continuamente com os dados gerados, ajustando suas respostas conforme o tipo de ameaça identificada. No entanto, a eficácia dessas soluções depende da qualidade dos dados processados e da robustez dos algoritmos, evidenciando a necessidade de investimentos substanciais em infraestrutura e capacitação (Baldan *et al.*, 2024).

A adoção de arquiteturas de segurança baseadas no conceito de "zero trust" tem se mostrado uma das abordagens mais eficazes para enfrentar os desafios de segurança cibernética na Indústria 4.0. Esta estratégia parte da premissa de que nenhuma entidade, seja interna ou externa, deve ser automaticamente confiável, exigindo autenticação contínua, criptografia de ponta a ponta e monitoramento rigoroso de todas as atividades. Contudo, essa transição representa um desafio técnico e cultural significativo, pois implica mudanças profundas na estruturação das redes organizacionais e no treinamento das equipes (Torres e Silva *et al.*, 2021).

A resiliência operacional é um pilar fundamental da segurança cibernética na Indústria 4.0. As empresas precisam estar preparadas para lidar com falhas ou ataques cibernéticos de maneira eficiente, garantindo a continuidade das operações essenciais. A adoção de sistemas redundantes, como servidores de backup e redes secundárias, é uma prática comum para mitigar os impactos de falhas. Além disso, a implementação de planos de recuperação de desastres (disaster recovery) e a realização de testes regulares de suas funcionalidades são essenciais para reduzir o tempo de inatividade e os prejuízos financeiros (Vargas, 2024).

A segurança cibernética também envolve aspectos humanos e organizacionais, como a conscientização e a capacitação dos colaboradores. Muitos ataques bem-sucedidos exploram falhas humanas, como o uso de senhas fracas ou a falta de cautela ao abrir e-mails de phishing. Para mitigar esse risco, as organizações devem investir em treinamentos contínuos, simulando cenários de ataques e promovendo boas práticas de segurança digital. Isso não apenas diminui a vulnerabilidade a ataques, mas também fortalece uma cultura organizacional mais resiliente e comprometida com a proteção dos ativos digitais (Torres e Silva *et al.*, 2021).

A colaboração entre organizações, governos e instituições acadêmicas é outro aspecto essencial para reforçar a segurança cibernética na Indústria 4.0. O compartilhamento de informações sobre ameaças emergentes e o desenvolvimento de padrões conjuntos são estratégias que possibilitam a abordagem coordenada dos riscos. Parcerias público-privadas, por exemplo, têm se mostrado eficazes na implementação de iniciativas de segurança em larga escala, como redes nacionais de monitoramento de ameaças e programas de certificação em cibersegurança (Pavão *et al.*, 2018).

A segurança cibernética na Indústria 4.0 deve ser encarada como um processo contínuo e dinâmico, acompanhando a evolução tecnológica e as mudanças no cenário das ameaças. As organizações precisam adotar uma abordagem de melhoria constante, avaliando suas vulnerabilidades regularmente, atualizando suas ferramentas e integrando novas tecnologias de proteção. Essa visão de longo prazo, aliada a uma governança eficaz e uma infraestrutura robusta, é fundamental para garantir a segurança e a resiliência operacional das redes automatizadas (Xavier, 2024).

4. CONSIDERAÇÕES FINAIS

A automação de redes na Indústria 4.0 representa um dos pilares centrais para a digitalização das indústrias, possibilitando maior eficiência, flexibilidade e inovação nos processos de produção. No entanto, a implementação bem-sucedida dessas tecnologias enfrenta obstáculos consideráveis, principalmente relacionados à interoperabilidade entre sistemas, à necessidade de uma infraestrutura sólida e à crescente complexidade da segurança cibernética. Para superar essas dificuldades, é necessário adotar uma abordagem estratégica que combine avanços tecnológicos com o desenvolvimento de padrões universais, a formação de profissionais e o fortalecimento das políticas de proteção de dados. A pesquisa abordou de maneira eficaz os desafios enfrentados pela automação de redes na Indústria 4.0, identificando os principais obstáculos técnicos, com ênfase na integração de sistemas heterogêneos e na modernização de infraestruturas legadas, que se mostram como barreiras significativas à automação eficiente. Além disso, foram avaliados os impactos da falta de interoperabilidade e infraestrutura, evidenciando como esses fatores comprometem a performance e escalabilidade das soluções industriais automatizadas. Por fim, foram apresentadas soluções práticas e inovadoras, como o uso de tecnologias emergentes, incluindo inteligência artificial e protocolos de "zero trust", para otimizar a conectividade e melhorar a segurança cibernética nas redes industriais. Dessa forma, a pesquisa atendeu aos objetivos propostos, oferecendo uma visão abrangente e estratégica sobre os desafios e as possíveis soluções para a automação de redes na Indústria 4.0.

Os desafios técnicos, como a integração de sistemas heterogêneos e a modernização de infraestruturas antigas, exigem soluções inovadoras que sejam viáveis economicamente e escaláveis, especialmente para empresas de menor porte. Simultaneamente, o avanço de tecnologias como redes 5G, computação em nuvem e edge computing apresenta novas possibilidades para otimizar a conectividade e o processamento de dados nos ambientes industriais. No entanto, esses avanços devem ser acompanhados por investimentos constantes em pesquisa e desenvolvimento, além de esforços colaborativos entre empresas, universidades e governos para a criação de um ecossistema digital integrado.

A segurança cibernética, por sua vez, continua sendo uma prioridade essencial na automação de redes, devido ao aumento de ataques cibernéticos avançados e à importância crítica das operações industriais interconectadas. A adoção de estratégias proativas, como o uso de inteligência artificial para detecção de ameaças e a implementação de políticas baseadas no conceito de "zero trust", é fundamental para garantir a resiliência operacional. Em síntese, a automação de redes na Indústria 4.0 não é apenas uma questão de tecnologia, mas também uma questão estratégica e multidimensional, exigindo esforços coordenados para transformar os desafios em oportunidades e alcançar os benefícios esperados dessa nova fase industrial.

Embora este estudo tenha abordado aspectos significativos da automação de redes na Indústria 4.0, é importante reconhecer algumas limitações que podem restringir a aplicabilidade e a abrangência das conclusões. Em primeiro lugar, a análise focou em perspectivas gerais, sem explorar de forma aprofundada casos específicos de implementação em diferentes setores industriais, o que poderia enriquecer a compreensão das variáveis contextuais que influenciam o sucesso dessas tecnologias. Além disso, a rápida evolução tecnológica e as mudanças constantes nos cenários regulatórios e de mercado apresentam desafios para a atualização contínua dos dados e das estratégias propostas. Portanto, novas pesquisas são sugeridas para investigar questões emergentes, como a viabilidade de soluções de automação para pequenas e médias empresas, o impacto econômico de longo prazo dessas inovações e o desenvolvimento de modelos preditivos para avaliar os riscos e benefícios da adoção de tecnologias disruptivas. Estudos interdisciplinares que integrem engenharia, gestão e políticas públicas também são essenciais para lidar com as complexidades multidimensionais da Indústria 4.0, ajudando a criar uma visão mais robusta e adaptada às realidades dinâmicas do setor industrial.

Referências

ANDRADE, S. C., RODRIGUEZ, C. M. T., MACHADO, N. T., & PINCHEIRA, J. G. C.

Barreiras à implementação da Indústria 4.0 no Polo Industrial de Manaus. **Revista de Gestão e Secretariado**, v. 15, n. 11, p. e4320-e4320, 2024. Disponível em: <https://ojs.revistagesec.org.br/secretariado/article/view/4320>. Acesso em 17/01/2025.

AULETTA, G. B. .; SANTOS, J. R. dos .; CAMUSSO, D. .; VICENTINI, R. M.

Governança de dados e a Indústria 4.0. **Revista Científica SENAI-SP - Educação, Tecnologia e Inovação**, [S. l.], v. 1, n. 2, p. 01–12, 2023. Disponível em: <https://periodicos.sp.senai.br/index.php/rcsenaisp/article/view/23>. Acesso em 17/01/2025.

BALDAN, A., GASPARINI, L. V. L., NAKAMURA, M. A., DOS SANTOS, P. R. G., &

DO NASCIMENTO, W. A. H. Conectividade Rural: Oferta de produtos e serviços inovadores para o agronegócio na região centro-oeste. **Revista de Administração de Roraima-RARR**, v. 15, n. 1, 2024. Disponível em: <https://revista.ufrr.br/adminrr/article/view/8167>. Acesso em 17/01/2025.

BARDIN, L. **Análise de conteúdo**. São Paulo: Edições 70, 2016. Disponível em: <https://acervo.enap.gov.br/cgi-bin/koha/opac-detail.pl?biblionumber=52319>. Acesso em 17/01/2025.

BRANQUINHO, Thiago; BRANQUINHO, Marcelo. **Segurança Cibernética Industrial**. Alta Books, 2021. Disponível em:

https://books.google.com.br/books/about/Seguran%C3%A7a_Cibern%C3%A9tica_Industrial.html?id=JrhrEAAAQBAJ&redir_esc=y. Acesso em 17/01/2025.

COLCHER, R. **A globalização e a transformação digital: Promessas e desafios de um novo mundo em construção**. 1ª Edição, Editora Scortecci, São Paulo/SP, 2019.

Disponível em:

<https://books.google.com.br/books?id=qKGkDwAAQBAJ&printsec=frontcover&hl=pt-BR#v=onepage&q&f=false>. Acesso em 17/01/2025.

CRESWELL, J. W.; CRESWELL, J. D. **Projeto de pesquisa: Métodos qualitativo, quantitativo e misto**. Penso Editora, 2021. Disponível em:

<https://books.google.com.br/books?id=URclEAAAQBAJ&printsec=frontcover&hl=pt-BR#v=onepage&q&f=false>. Acesso em 17/01/2025.

DA SILVA, N. R., AMICI, T. T., CAMUSSO, D., VICENTINI, R. M. Avanço na

simulação de sistemas virtuais: integração de gêmeos digitais, FMI e DPC. **Revista Brasileira de Mecatrônica**, v. 6, n. 2, p. 01-17, 2024. Disponível em:

<https://revistabrmecatronica.sp.senai.br/ojs/index.php/revistabrmecatronica/article/view/235>. Acesso em 17/01/2025.

DE ARAUJO, N. M. M.; MARINELLI FILHO, N.; GUIMARÃES, G. E.; CORREA, G.

N.; FERREIRA, M. R. Intelligent Capacity Supervision and Control System in

Industrial Processes: Integration of Scada, AI, and Machine Learning. **ARACÊ**, [S. l.], v. 6, n. 4, p. 16090–16112, 2024. DOI: 10.56238/arev6n4-295. Disponível em:

<https://periodicos.newsciencepubl.com/arace/article/view/2317>. Acesso em

17/01/2025.

DE ARRUDA, L. G. S., GIOZZA, W. F., NZE, G. D. A., NUNES, R. R.

Implementação da Arquitetura Zero Trust: uma Revisão Sistemática de Literatura.

Revista Ibérica de Sistemas e Tecnologias de Informação, n. E56, p. 261-275,

2023. Disponível em: [https://ppee.unb.br/wp-](https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf)

[content/uploads/2023/07/Comprovante de publicacao-3-1.pdf](https://ppee.unb.br/wp-content/uploads/2023/07/Comprovante_de_publicacao-3-1.pdf). Acesso em

17/01/2025.

DE MENEZES, Henrique Zeferino. Cooperação Científica e Tecnológica para o

Desenvolvimento e a Produção de Tecnologias Farmacêuticas: um caminho para a autonomia em saúde na América do Sul. **Revista Tempo do Mundo**, n. 31, p.

145-171, 2023. Disponível em:

DELOMO LUQUE, J. V.; TAMBASCO BRUNO, D. O.; CRISPIM, J. A.; SANTOS, . R.;

BERNARDES, V. P. A aplicabilidade da tecnologia 5G no contexto da Indústria 4.0:

impulsionando IoT, IA, computação em nuvem e segurança cibernética. **Revista Brasileira de Mecatrônica**, [S. l.], v. 6, n. 3, p. 53–78, 2024. DOI:

10.62899/revistabrmecatronica.v6i3.232. Disponível em:

<https://revistabrmecatronica.sp.senai.br/ojs/index.php/revistabrmecatronica/article/view/232>. Acesso em 17/01/2025.

DOS SANTOS, D. R. G.; VOLANTE, C. R. A importância da tecnologia sem fio na Indústria 4.0. **Revista Interface Tecnológica**, v. 15, n. 2, p. 245-254, 2018.

Disponível em:

<https://revista.fatectq.edu.br/interfacetecnologica/article/view/487/314>. Acesso em 17/01/2025.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

IDEYAMA, F.; BECKER, . J. L. Impactos da governança e elementos ESG na computação

em nuvem: Uma análise teórica e prática. **RGC - Revista de Governança Corporativa**, São Paulo (SP), v. 11, n. 00, p. e0146, 2024. DOI: 10.21434/IberoamericanJCG.v11i00.146.

Disponível em: <https://rgc.org.br/Journals/article/view/146>. Acesso em 17/01/2025.

JUSSIANI, W. A. **Desempenho e conectividade de redes híbridas em sistemas de transporte inteligente cooperativo**. Dissertação (Mestrado em Engenharia Elétrica e Informática Industrial) - Universidade Tecnológica Federal do Paraná, Curitiba/PR, 2019.

Disponível em: <https://repositorio.utfpr.edu.br/jspui/handle/1/4727>. Acesso em 17/01/2025.

KUSMA, V. V.; CHIROLI, D. M. G. A indústria 4.0: uma revisão sobre os impactos e as modificações na dinâmica de trabalho do modelo atual. **Revista**

princípios-divulgação científica e tecnológica do IFPB, n. 53, p. 131-140, 2021. Disponível em: <https://www.academia.edu/download/106949702/1527.pdf>. Acesso em 17/01/2025.

MARTINS JUNIOR, W.; SILVA, C. G. L. Segurança Cibernética e seus Paradigmas na Era Digital. **RCMOS - Revista Científica Multidisciplinar O Saber**, Brasil, v. 1, n. 1, p. 1–5, 2024. DOI: 10.51473/ed.al.v3i1.479. Disponível em:

<https://submissoesrevistacientificaosaber.com/index.php/rcmos/article/view/345>.

Acesso em 17/01/2025.

MILANIL, C. R. S.; LOUREIRO, J. C. S. Cooperação internacional e desenvolvimento: análise da atuação de agências internacionais em Duque de Caxias. **Cad. EBAPE.BR.** v. 11(2), 2013. Doi: <https://doi.org/10.1590/S1679-39512013000200004>. Disponível em: <https://www.scielo.br/j/cebape/a/DJb3rxsn4Bjk9F6M3zKgFpv/?lang=pt>. Acesso em 17/01/2025.

MONTEIRO, M. A.; GUIMARÃES, G. E.; MARINELLI FILHO, N.; SALAZAR, R. F. S.; CORREA, G. N. Projeto de uma Nova Linha de Produção de Indústria 4.0, com Ênfase na Mão de Obra Humana e Sistemas Robóticos, Baseado em Indicadores do Método de Simulação por Gêmeos Digitais. **ARACÊ**, [S. l.], v. 7, n. 1, p. 2–26, 2025. DOI: 10.56238/arev7n1-001. Disponível em: <https://periodicos.newsciencepubl.com/arace/article/view/2649>. Acesso em 17/01/2025.

PARENTE, A. P.; VALDMAN, A.; FOLLY, R. O. M.; SOUZA JR, M. B.; NASCIMENTO, I. C. S. Automação de Processos Industriais: do Pneumático à Indústria 4.0. **Revista Processos Químicos**, v. 12, n. 24, p. 101-108, 2 jul. 2018. DOI: <https://doi.org/10.19142/rpq.v12i24.468> Disponível em: https://ojs.rpqsenai.org.br/index.php/rpq_n1/article/view/468. Acesso em 17/01/2025.

PAVÃO, Caterina Groposo; ROCHA, Rafael Porte da; GABRIEL JUNIOR, Rene Faustino. Proposta de criação de uma rede de dados abertos da pesquisa brasileira. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, Campinas, SP, v. 16, n. 2, p. 329–343, 2018. DOI: 10.20396/rdbci.v16i2.8651180. Disponível em: <https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/8651180>. Acesso em 17/01/2025.

PAZ, A. C. M.; LOOS, M. J. A importância da computação em nuvem para a indústria 4.0. **Revista Gestão Industrial**, v. 16, n. 2, 2020. Disponível em: <https://revistas.utfpr.edu.br/revistagi/article/view/9317>. Acesso em 17/01/2025.

PONTE, F. W. G. **Supervisão de dados utilizando Node-Red, Node.js e ReactJS para adaptação de sistemas legados ao contexto da indústria 4.0**. Monografia (Departamento de Engenharia Elétrica) - Campus de Sobral, Universidade Federal do Ceará, Sobral/CE, 2022. Disponível em: <https://repositorio.ufc.br/handle/riufc/77900>. Acesso em 17/01/2025.

ROMEIRO, L. A. W. **Sistema de baixo custo para monitoramento e alerta remoto da temperatura de medicamentos termolábeis, com base em tecnologia Edge Computing, BLE e IoT**. 2022. x, 53 f., il. Dissertação (Mestrado Profissional em Engenharia Elétrica) — Universidade de Brasília, Brasília, 2022. Disponível em: <http://www.rlbea.unb.br/jspui/handle/10482/44061>. Acesso em 17/01/2025.

SACOMANO, J. B.; GONÇALVES, R. F.; SILVA, M. T.; BONILLA, S. H.; SÁTYRO, W. C. **Indústria 4.0**. Editora Blucher, 2018. Disponível em: <https://books.google.com.br/books?id=PNCuDwAAOBAJ&printsec=frontcover&hl=pt-BR#v=onepage&q&f=false>. Acesso em 17/01/2025.

SAITO, M. C. A., ANDREASSA, M. C., FERRER, J. A. G., & DOS SANTOS, J. R. Os

desafios do supply chain management diante das tecnologias habilitadoras da Indústria 4.0. **Revista Brasileira de Mecatrônica**, v. 6, n. 2, p. 57-82, 2024.

Disponível em:

<https://revistabrmecatronica.sp.senai.br/ojs/index.php/revistabrmecatronica/article/view/208>. Acesso em 17/01/2025.

SANTOS, I.G.; SANTANA, C. A. S.; OLIVEIRA, A.; ALCOFORADO, C. G. Impacto da implementação do BIM em uma empresa urbanizadora de condomínios horizontais em SE. In: ENCONTRO NACIONAL DE TECNOLOGIA DO AMBIENTE CONSTRUÍDO, 20., 2024. **Anais**. Porto Alegre: ANTAC, 2024. p. 1–10. DOI:

10.46421/entac.v20i1.6165. Disponível em:

<https://eventos.antac.org.br/index.php/entac/article/view/6165>. Acesso em 17/01/2025.

SANTOS, P. S.; ROCHA, M. T. S.; SOUZA, S. G. A. de. Financiamento da inovação no Brasil: uma abordagem sobre a influência dos incentivos fiscais na atividade inovativa industrial. **Economia e Desenvolvimento**, [S. l.], v. 31, p. e8, 2019. DOI:

10.5902/1414650933347. Disponível em: <https://periodicos.ufsm.br/eed/article/view/33347>. Acesso em 17/01/2025.

SILVA, A. L. E., DA SILVEIRA, T., MORAES, J. A. R., BRUM, T. M. M. Proposta de automação industrial em uma empresa fabricante de borrachas escolares. **Revista GEINTEC: Gestão. Inovação e Tecnologias**. p. 2237-0722, 2018. Disponível em:

https://oasisbr.ibict.br/vufind/Record/AESPI-1_9a70059687ada3f1ccf4d82a66309b75. Acesso em 17/01/2025.

SOUZA, C. F. TOLEDO, E. M. TEODORO DA SILVA, A. A. M. A Engenharia Civil no Planejamento e Desenvolvimento da Indústria 4.0. **RECIEC -Revista Científica de Engenharia Civil**. v. 02, n. 02, 2019. Disponível em:

<https://anais.unievangelica.edu.br/index.php/reciec/article/view/9388>. Acesso em 17/01/2025.

TORRES E SILVA, M. D.; CARVALHO, R. B.; DE CASTRO, J. M.; SOARES, M. V.

Governança da informação no contexto dos módulos contábeis dos sistemas Enterprise Resource Planning (ERP) para a indústria 4.0: proposta de framework. **AtoZ: novas práticas em informação e conhecimento**, [S. l.], v. 10, n. 3, p. 1–11, 2021. DOI:

10.5380/atoz.v10i3.81477. Disponível em: <https://revistas.ufpr.br/atoz/article/view/81477>. Acesso em 17/01/2025.

VARGAS, R. O. **Transformação digital na indústria de defesa: análise da adoção da inteligência artificial na performance e resiliência da cadeia de suprimentos**.

Dissertação (Departamento de Engenharia Industrial) - Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro/RJ, 2024. Disponível em:

<https://www.maxwell.vrac.puc-rio.br/66497/66497.PDF>. Acesso em 17/01/2025.

VERSIONI, J. A. **Segurança de Processos na Indústria 4.0**. Monografia (Departamento de Engenharia Química) - Universidade Federal de São Carlos, São Carlos/SP, 2020. Disponível em: <https://repositorio.ufscar.br/handle/ufscar/13754>.

Acesso em 17/01/2025.

XAVIER, F. Crimes cibernéticos e a falsa sensação de impunidade. **Revista Processus Multidisciplinar**, [S. l.], v. 5, n. 10, p. e101186, 2024. Disponível em: <https://periodicos.processus.com.br/index.php/multi/article/view/1186>. Acesso em 17/01/2025.