



Graduação  Pós-Graduação  
 Artigo completo  Relato de prática  Resumo expandido

## MATURIDADE DIGITAL E CIBERSEGURANÇA COMO CONDICIONANTES DA ADOÇÃO DA INTELIGÊNCIA ARTIFICIAL NA INDÚSTRIA 4.0: implicações para o agronegócio

**Ervilario Alves da Cunha Júnior**  
**Universidade Federal de Mato Grosso do Sul**  
**ervilario.junior@ufms.br**

### RESUMO

A Indústria 4.0 tem promovido transformações profundas nos sistemas produtivos por meio da integração de tecnologias digitais avançadas, entre as quais se destaca a Inteligência Artificial. Apesar de seu potencial estratégico, observa-se que a adoção da Inteligência Artificial no ambiente industrial e agroindustrial ocorre de forma heterogênea, sendo influenciada por fatores organizacionais e tecnológicos. Diante desse contexto, este estudo tem como objetivo analisar como a maturidade digital e a gestão da cibersegurança condicionam a adoção da Inteligência Artificial na Indústria 4.0. Para tanto, adotou-se uma pesquisa de natureza básica, com abordagem qualitativa e caráter descritivo, desenvolvida por meio de uma revisão bibliográfica narrativa. A análise da literatura evidenciou que organizações com maior nível de maturidade digital apresentam maior capacidade de integrar a Inteligência Artificial de forma efetiva, sustentada por processos digitalizados, governança de dados e cultura organizacional orientada à inovação. Em contrapartida, limitações estruturais e fragilidades em cibersegurança comprometem a escalabilidade, a confiabilidade e a sustentabilidade das soluções adotadas. Conclui-se que a Inteligência Artificial assume papel estratégico na Indústria 4.0, porém sua implementação bem-sucedida depende de uma abordagem integrada, que alinhe maturidade digital, infraestrutura tecnológica, conectividade e gestão de riscos cibernéticos, de modo a promover eficiência, segurança e resiliência nos sistemas produtivos.

**Palavras-chave:** Agronegócio digital; Inteligência Artificial; Maturidade digital; Cibersegurança agroindustrial; Transformação digital.

## 1 INTRODUÇÃO

A Quarta Revolução Industrial, amplamente conhecida como Indústria 4.0, tem promovido transformações profundas nos sistemas produtivos ao integrar tecnologias digitais avançadas aos processos industriais tradicionais. Esse novo paradigma caracteriza-se pela convergência entre sistemas físicos e digitais, viabilizada por tecnologias como Internet das Coisas (IoT), sistemas ciberfísicos, computação em nuvem, Big Data e Inteligência Artificial (IA), possibilitando níveis inéditos de automação, conectividade e tomada de decisão orientada por dados (KAGERMANN et al., 2013; SCHWAB, 2016; WINDMANN et al., 2024).

Nesse contexto, a Inteligência Artificial emerge como uma das tecnologias centrais da Indústria 4.0, ao permitir o processamento de grandes volumes de dados agroindustriais, a identificação de padrões complexos e o suporte a decisões em tempo real. Aplicações como manutenção preditiva, otimização de processos produtivos, controle de qualidade inteligente e planejamento avançado da produção ilustram o potencial da IA para elevar a eficiência operacional, reduzir custos e aumentar a resiliência organizacional (LEE; DAVARI; SINGH, 2021; GABSI, 2024). Apesar desse potencial amplamente reconhecido, a adoção da Inteligência Artificial no ambiente industrial ainda ocorre de forma heterogênea, especialmente em economias emergentes, onde limitações estruturais e organizacionais persistem.

No contexto do agronegócio, especialmente nas cadeias agroindustriais e nos sistemas produtivos rurais altamente mecanizados e digitalizados, a Indústria 4.0 tem impulsionado a incorporação de tecnologias como sensores inteligentes, sistemas ciberfísicos e soluções baseadas em Inteligência Artificial. A crescente digitalização do campo, observada em agroindústrias, cooperativas, usinas e propriedades rurais tecnificadas, amplia ganhos de eficiência e produtividade, ao mesmo tempo em que impõe novos desafios relacionados à maturidade digital e à cibersegurança dos sistemas produtivos.

A literatura recente evidencia que a adoção bem-sucedida da Inteligência Artificial não depende exclusivamente da disponibilidade da tecnologia, mas está fortemente condicionada ao nível de maturidade digital das organizações. A maturidade digital refere-se ao grau de preparo organizacional para integrar tecnologias digitais aos seus processos, estratégias e modelos de gestão, envolvendo aspectos como infraestrutura tecnológica, governança de dados, competências organizacionais e cultura orientada à inovação (WESTERMAN; BONNET; MCAFEE, 2014; KANE et al., 2017). Logo, organizações com maior maturidade digital tendem a apresentar maior capacidade de absorção de inovações tecnológicas, reduzindo barreiras

relacionadas à complexidade, compatibilidade e integração de soluções baseadas em IA (SENNA et al., 2023; NICK et al., 2024).

Paralelamente, a intensificação da conectividade, elemento estruturante da Indústria 4.0, amplia de forma significativa a superfície de exposição a riscos cibernéticos. A interconexão entre máquinas, sensores, sistemas industriais (OT) e tecnologias da informação (IT) torna os ambientes produtivos mais vulneráveis a ataques cibernéticos capazes de comprometer não apenas dados, mas também a continuidade operacional, a segurança física e a confiabilidade dos processos industriais (BÉCUE; PRAÇA; GAMA, 2021; AZAMBUJA et al., 2023).

Nesse cenário, a cibersegurança industrial passa a assumir um papel estratégico na transformação digital, deixando de ser tratada apenas como um requisito técnico para se consolidar como um fator crítico de governança e sustentabilidade organizacional. A ausência de políticas robustas de segurança, aliada a baixos níveis de maturidade digital, pode comprometer a adoção e a escalabilidade de soluções baseadas em Inteligência Artificial, gerando riscos operacionais e reduzindo os benefícios esperados da automação inteligente (TEIXEIRA et al., 2024; OFUSORI et al., 2024).

Dessa forma, observa-se que a adoção da Inteligência Artificial na Indústria 4.0 resulta da interação entre múltiplos fatores organizacionais e tecnológicos, com destaque para a maturidade digital e a gestão da cibersegurança em ambientes altamente conectados. Compreender como esses elementos condicionam a incorporação efetiva da IA torna-se fundamental para orientar estratégias de inovação e transformação digital no contexto industrial contemporâneo.

Diante desse cenário, este artigo é orientado pela seguinte pergunta norteadora: *Como a maturidade digital e a gestão da cibersegurança influenciam a adoção da Inteligência Artificial no contexto da Indústria 4.0?*

Este trabalho tem como objetivo geral analisar como a maturidade digital e a gestão da cibersegurança influenciam a adoção da Inteligência Artificial no contexto da Indústria 4.0, com ênfase em organizações agroindustriais e nos sistemas produtivos do agronegócio, considerando seus impactos na eficiência operacional, na sustentabilidade e na resiliência dos sistemas produtivos. Para atingir o objetivo geral, pretende-se dividi-lo em específicos, sendo:

a) Discutir o papel da maturidade digital como fator estruturante para a adoção da Inteligência Artificial em ambientes agroindustriais;

b) Analisar a conectividade e a cibersegurança agroindustrial como fatores críticos para a sustentabilidade das soluções baseadas em Inteligência Artificial na Indústria 4.0;



c) Sintetizar, a partir da literatura, os principais desafios organizacionais associados à adoção da Inteligência Artificial em contextos agroindustriais digitalmente conectados.

## 2 REVISÃO DA LITERATURA

Esta seção consolida o referencial teórico necessário para responder à pergunta norteadora supracitada. Sendo dividida em: a) transformação digital e Indústria 4.0 no agronegócio e na agroindústria; b) Inteligência Artificial e Agricultura 4.0 como vetores de eficiência e decisão no agronegócio; c) maturidade digital como condição organizacional para adoção e escalabilidade da IA no agronegócio; e d) conectividade e cibersegurança como requisitos de continuidade, confiança e resiliência em ambientes do agronegócio digital.

### 2.1 TRANSFORMAÇÃO DIGITAL, INDÚSTRIA 4.0 E AGRONEGÓCIO: DO CAMPO À CADEIA AGROINDUSTRIAL

A Indústria 4.0, entendida como a integração entre sistemas físicos e digitais com automação, conectividade e decisões orientadas por dados, tem sido apropriada pelo agronegócio em duas frentes complementares: a) na produção rural (Agricultura 4.0/Agro 4.0) e b) nas cadeias agroindustriais (processamento, logística, rastreabilidade e qualidade). Schwab (2016) descreve a Quarta Revolução Industrial como um movimento de convergência tecnológica com impactos sobre operações e modelos de negócio, o que no agronegócio se traduz em redes de sensores, plataformas digitais e sistemas inteligentes capazes de reorganizar rotinas de produção e gestão em escala.

No âmbito das cadeias agroalimentares, Hassoun et al. (2023) argumentam que a digitalização no setor agroalimentar avançou com o emprego de tecnologias como inteligência artificial, big data, IoT, blockchain, robótica e sensores, destacando que tais ferramentas têm alto potencial para mitigar riscos e elevar a capacidade de resposta do setor diante de disrupções. Essa leitura reforça que o agronegócio não digitaliza “por moda”, mas por pressões concretas de eficiência, sustentabilidade e resiliência, o que exige capacidades gerenciais e organizacionais que sustentem a transformação.

Especificamente sobre Indústria 4.0 aplicada ao setor agroalimentar, Bigliardi et al. (2023) exploram aplicações de tecnologias 4.0 em cadeias agroalimentares e indicam que o setor já convive com tecnologias em diferentes estágios de maturação, do que se depreende que



a adoção é desigual e depende de condições e prioridades setoriais. No mesmo sentido, Kayikci et al. (2020) discutem que, em cadeias de alimentos, a demanda por rastreabilidade, transparência e confiança na era 4.0 impulsiona soluções digitais, mas a implementação esbarra em desafios relacionados a pessoas e tecnologia, o que reconecta o debate ao papel de maturidade organizacional no agronegócio.

Assim, para o propósito deste artigo, a transformação digital no agronegócio é entendida como um processo sociotécnico: tecnologias 4.0 criam possibilidades, mas os resultados dependem de preparo organizacional (maturidade digital) e de proteção dos ambientes conectados (cibersegurança), dimensões que condicionam a adoção sustentável de Inteligência Artificial do campo à agroindústria.

## 2.2 INTELIGÊNCIA ARTIFICIAL E AGRICULTURA 4.0 NO AGRONEGÓCIO: APLICAÇÕES, VALOR E LIMITAÇÕES DE ADOÇÃO

A Inteligência Artificial vem sendo posicionada como tecnologia central para o agronegócio digital, pois permite tratar grandes volumes de dados de sensores, imagens e sistemas de gestão, convertendo dados em decisões e automações. Lee, Davari e Singh (2021) discutem a IA industrial e o uso de analytics preditivo para elevar eficiência e confiabilidade em ambientes produtivos, o que, por analogia operacional, sustenta o uso de IA em operações agroindustriais onde manutenção, inspeção e estabilidade de processos são críticos.

No setor agroalimentar, Hassoun et al. (2023) destacam aplicações de tecnologias digitais (incluindo IA) em diversos usos ligados a cadeias de alimentos, com ênfase em monitoramento e tomada de decisão apoiada por dados. Essa abordagem é altamente pertinente ao agronegócio porque conecta IA a problemas típicos do setor: variabilidade de produção, restrições de recursos, risco sanitário e necessidade de rastreabilidade.

No contexto brasileiro, a IA e machine learning transformam processos de gestão na Agricultura 4.0 quando integrados a tecnologias correlatas (sensoriamento, conectividade e plataformas digitais). Silva (2025) discute IA e ML na otimização da gestão da Agricultura 4.0, explicitando que tais ferramentas, quando combinadas a infraestrutura digital, apoiam decisões e eficiência, o que se alinha diretamente ao objetivo do artigo de compreender condicionantes de adoção no agronegócio.

Ainda assim, a adoção de Agricultura 4.0 mostra que o potencial não se converte automaticamente em adoção ampla. Fragomeli, Annunziata e Punzo (2024) identificam que



barreiras como restrições econômicas e falta de infraestrutura digital são relevantes para adoção de tecnologias 4.0 no contexto agrícola, o que reforça que a adoção de IA no agronegócio depende de condições organizacionais e estruturais (maturidade digital) e não apenas de oferta tecnológica. Portanto, a Inteligência Artificial no agronegócio é tratada neste artigo como tecnologia de alto valor potencial, mas cuja adoção efetiva é condicionada por maturidade digital e por cibersegurança, pois a IA é dependente de dados íntegros, conectividade e continuidade operacional ao longo do tempo.

### 2.3 MATURIDADE DIGITAL NO AGRONEGÓCIO: PRONTIDÃO ORGANIZACIONAL PARA ADOÇÃO E ESCALABILIDADE DA IA

A maturidade digital, aplicada ao agronegócio, pode ser compreendida como a capacidade organizacional de integrar tecnologias digitais aos processos, à governança de dados, às competências e à estratégia, de modo a sustentar inovação e desempenho. No plano agrícola, Büyük et al. (2021) propõem um modelo de avaliação de maturidade digital para *smart agriculture*, vinculando competências digitais e requisitos de Indústria 4.0 à construção de *roadmaps*, o que explicita que o setor agrícola demanda instrumentos próprios para medir prontidão e orientar decisões.

Lima (2023) propõe e valida um modelo de aceitação para tecnologias digitais na agricultura aplicado a sistemas de informação de gestão agrícola (FMIS), evidenciando que fatores como esforço percebido, pressões externas e custo percebido afetam a intenção de uso. Essa evidência é central para o agronegócio, pois indica que prontidão e adoção dependem de dimensões organizacionais e de percepção de valor/custo, o que converge com a ideia de maturidade digital como pré-condição para adoção consistente de tecnologias avançadas (incluindo IA).

Além disso, evidências setoriais recentes em cadeias agroindustriais mostram que maturidade e prontidão podem ser operacionalizadas em modelos específicos. Sobre isso, Beducci, Acerbi e De Carolis (2026) descrevem um modelo de maturidade digital adaptado à cadeia de laticínios (setor agroindustrial), mostrando que a avaliação de maturidade pode orientar ações e investimentos conforme dimensões de monitoramento, execução, organização e infraestrutura tecnológica. Isso reforça que “maturidade digital” no agronegócio não é abstrata: ela pode ser medida e utilizada para priorização gerencial.

No mesmo horizonte, discussões sobre adoção de Agricultura 4.0 apontam que barreiras

de infraestrutura e capacidades interferem diretamente na transição digital. Ao tratar drivers e barreiras de adoção no setor agrícola, Fragomeli, Annunziata e Punzo (2024) reforçam que falta de infraestrutura (como conectividade) e restrições econômicas dificultam adoção, o que, no vocabulário deste artigo, significa que baixa maturidade digital reduz a probabilidade de adoção sustentável de IA no agronegócio.

Assim, a maturidade digital é posicionada aqui como condicionante estruturante para a adoção de Inteligência Artificial no agronegócio: sem integração de dados, governança e competências, a IA tende a permanecer pontual, pouco confiável e difícil de escalar, o que se conecta diretamente aos objetivos específicos do estudo (discutir maturidade digital como fator estruturante e sintetizar desafios organizacionais).

#### 2.4 CONECTIVIDADE E CIBERSEGURANÇA NO AGRONEGÓCIO DIGITAL: CONTINUIDADE, INTEGRIDADE E CONFIANÇA PARA IA

A conectividade é elemento central da Agricultura 4.0 e do agronegócio digital, pois viabiliza coleta e transmissão contínua de dados de sensores e dispositivos conectados, integrando operações e sistemas de decisão. Contudo, ao ampliar conectividade, ampliam-se também riscos cibernéticos, o que torna cibersegurança um requisito de continuidade, integridade e confiança. Demestichas, Peppes e Alexakis (2020) analisam ameaças em IoT agrícola e *smart farming*, destacando que a digitalização traz benefícios, mas também expõe o setor a ameaças e vulnerabilidades que podem afetar dados e operações.

Yang et al. (2021) discutem tecnologias e aplicações de *smart agriculture* e explicitam desafios de segurança e privacidade, organizando contramedidas como autenticação e controle de acesso, criptografia, preservação de privacidade e detecção de intrusões. Essa contribuição é decisiva para o agronegócio porque conecta diretamente a viabilidade de sistemas inteligentes (incluindo IA) ao conjunto de controles que preservam integridade e disponibilidade de dados — elementos sem os quais modelos de IA podem se tornar frágeis e pouco confiáveis.

No mesmo campo, Ali et al. (2024) discutem segurança e privacidade em IoT aplicado a *smart farming* e reforçam que o aumento de dispositivos conectados amplia a necessidade de salvaguardas contra ameaças, o que intensifica a relevância de gestão de cibersegurança em ambientes rurais e agroindustriais. Complementarmente, Adewusi, Chiekezie e Eyo-Udo (2022) abordam desafios de segurança em fazendas conectadas por IoT e propõem medidas como autenticação robusta, atualização regular e segmentação, reforçando que segurança é

componente organizacional e técnico ao mesmo tempo.

No plano das cadeias agroalimentares, Kayikci et al. (2020) discutem que a necessidade de transparência e rastreabilidade na cadeia de alimentos demanda soluções digitais robustas, mas a implementação encontra impedimentos que incluem desafios tecnológicos e humanos, o que reforça que cibersegurança deve ser tratada como parte da governança do agronegócio e não como adição posterior.

Dessa forma, a literatura sustenta o argumento central do artigo: no agronegócio, a adoção de Inteligência Artificial no contexto da Indústria 4.0 é condicionada (i) pela maturidade digital, que estabelece base de dados, integração e competências, e (ii) pela cibersegurança, que assegura continuidade operacional e confiança em ambientes conectados. Esse encadeamento fundamenta a discussão e os resultados do trabalho ao integrar maturidade digital, conectividade e cibersegurança como dimensões interdependentes da adoção sustentável de IA no agronegócio.

### 3 PROCEDIMENTOS METODOLÓGICOS

O presente estudo foi desenvolvido a partir de um delineamento metodológico compatível com investigações de natureza teórica, cujo objetivo central consiste em analisar, à luz da literatura, como a maturidade digital e a gestão da cibersegurança influenciam a adoção da Inteligência Artificial no contexto da Indústria 4.0. Para tanto, adotaram-se procedimentos metodológicos fundamentados em referenciais clássicos da pesquisa científica e da pesquisa qualitativa, assegurando rigor conceitual e coerência entre problema, objetivos e método.

#### 3.1 NATUREZA E ABORDAGEM DA PESQUISA

Quanto à natureza, esta pesquisa caracteriza-se como pesquisa básica, uma vez que tem como finalidade ampliar o entendimento conceitual acerca de fenômenos organizacionais e tecnológicos, sem a intenção imediata de aplicação prática ou de intervenção direta em contextos específicos. Segundo Gil (2019), a pesquisa básica busca produzir conhecimentos voltados à ampliação do saber científico, contribuindo para o avanço teórico de determinada área do conhecimento.

No que se refere à abordagem, o estudo adota uma abordagem qualitativa, pois privilegia a compreensão de significados, interpretações e relações conceituais presentes na literatura. De

acordo com Minayo, Deslandes e Gomes (2016) a pesquisa qualitativa é adequada para o estudo de fenômenos complexos, nos quais as dimensões simbólicas, organizacionais e contextuais são essenciais para a compreensão do objeto investigado.

Essa abordagem mostra-se particularmente pertinente ao tema em análise, uma vez que a adoção da Inteligência Artificial, a maturidade digital e a cibersegurança industrial envolvem múltiplas dimensões organizacionais, tecnológicas e estratégicas, que não podem ser adequadamente apreendidas por meio de mensurações quantitativas isoladas.

### 3.2 TIPO DE PESQUISA

Do ponto de vista de seus objetivos, a pesquisa enquadra-se como descritiva, pois busca descrever e analisar como a literatura científica tem tratado os fatores que condicionam a adoção da Inteligência Artificial na Indústria 4.0. Conforme Gil (2019), a pesquisa descritiva tem como propósito principal a descrição das características de determinado fenômeno ou o estabelecimento de relações entre conceitos, sem a pretensão de explicar causalidades.

No que diz respeito aos procedimentos técnicos, trata-se de uma pesquisa bibliográfica, desenvolvida a partir de material já publicado, como livros, artigos científicos, dissertações, teses e documentos acadêmicos relevantes. Lakatos e Marconi (2022) destacam que a pesquisa bibliográfica permite ao pesquisador estabelecer contato direto com a produção intelectual existente sobre o tema investigado, possibilitando a análise crítica e a organização do conhecimento acumulado.

### 3.3 ESTRATÉGIA METODOLÓGICA: REVISÃO BIBLIOGRÁFICA NARRATIVA

Como estratégia metodológica, adotou-se a revisão bibliográfica de caráter narrativo. Esse tipo de revisão caracteriza-se por uma abordagem ampla e interpretativa da literatura, sendo especialmente indicado para mapear o estado do conhecimento em campos de estudo complexos ou em consolidação. Diferentemente das revisões sistemáticas, a revisão narrativa não segue protocolos rígidos de busca e seleção, permitindo maior flexibilidade analítica ao pesquisador (CAVALCANTE; OLIVEIRA, 2020).

Autores que discutem especificamente os métodos de revisão da literatura ressaltam que a revisão narrativa cumpre um papel relevante na síntese teórica, na identificação de tendências e lacunas e na construção crítica de campos científicos emergentes (FERNANDES; VIEIRA;

CASTELHANO, 2021). Dessa forma, essa estratégia mostrou-se adequada para discutir as inter-relações entre maturidade digital, cibersegurança e adoção da Inteligência Artificial em ambientes agroindustriais.

### 3.4 PROCEDIMENTOS DE BUSCA E SELEÇÃO DAS FONTES

A busca das fontes bibliográficas foi realizada de maneira não sistematizada, priorizando a relevância teórica e a aderência das obras ao problema de pesquisa. As fontes foram identificadas principalmente por meio do Google Acadêmico, além de portais de periódicos científicos e repositórios institucionais, contemplando publicações nacionais e internacionais.

Foram considerados livros clássicos de metodologia científica, artigos publicados em periódicos acadêmicos, bem como trabalhos acadêmicos, como trabalhos de conclusão de curso, dissertações e teses, desde que apresentassem rigor metodológico e pertinência temática. O recorte temporal priorizou publicações entre 2015 e 2026, de modo a assegurar a atualidade das discussões, sem desconsiderar obras clássicas fundamentais para a compreensão da pesquisa qualitativa e bibliográfica (GIL, 2019; LAKATOS; MARCONI, 2022).

### 3.5 PROCEDIMENTOS DE ANÁLISE DO MATERIAL

A análise do material selecionado foi conduzida de forma qualitativa e interpretativa, seguindo etapas de leitura exploratória, leitura analítica e síntese interpretativa. Inicialmente, realizou-se uma leitura exploratória com o objetivo de identificar os principais conceitos, categorias e abordagens teóricas relacionadas à transformação digital, maturidade organizacional, adoção tecnológica e cibersegurança industrial.

Em seguida, procedeu-se à leitura analítica, buscando compreender convergências, divergências e complementaridades entre os autores. Por fim, os achados foram organizados de maneira temática, permitindo a construção de uma síntese teórica coerente com os objetivos do estudo. Esse procedimento está em consonância com as orientações de Lakatos e Marconi (2022), que destacam a análise e a interpretação como etapas centrais da pesquisa bibliográfica.

### 3.6 LIMITAÇÕES METODOLÓGICAS

Como limitação metodológica, destaca-se o fato de o estudo basear-se exclusivamente em fontes secundárias, não contemplando coleta de dados empíricos primários. Além disso, a revisão narrativa envolve maior grau de subjetividade na seleção e interpretação das fontes, característica inerente a esse tipo de delineamento metodológico.

Ainda assim, conforme ressaltam Minayo, Deslandes e Gomes (2016), a explicitação dos procedimentos adotados contribui para a transparência e a credibilidade do estudo, mitigando possíveis vieses interpretativos. Dessa forma, o delineamento metodológico adotado mostra-se adequado aos objetivos propostos, permitindo uma análise aprofundada e articulada da literatura sobre a adoção da Inteligência Artificial na Indústria 4.0.

## 4 DISCUSSÃO E ANÁLISE DOS DADOS

A presente seção discute os achados do estudo à luz da literatura científica recente, buscando compreender como a maturidade digital e a gestão da cibersegurança condicionam a adoção da Inteligência Artificial no contexto da Indústria 4.0. Inicialmente, realiza-se uma síntese interpretativa dos principais resultados e sua convergência com pesquisas empíricas e conceituais atuais.

Em seguida, analisa-se o papel da maturidade digital como base organizacional para a adoção de soluções inteligentes, bem como os impactos da conectividade e da cibersegurança na sustentabilidade dessas iniciativas. Por fim, a discussão integra esses elementos de forma sistêmica, evidenciando como capacidades organizacionais, tecnológicas e de governança interagem e influenciam a implementação bem-sucedida da Inteligência Artificial em ambientes agroindustriais altamente conectados.

### 4.1 SÍNTESE INTERPRETATIVA DOS ACHADOS E CONVERGÊNCIA COM A LITERATURA RECENTE

Os achados deste estudo sustentam que a adoção de Inteligência Artificial (IA) na Indústria 4.0 tende a ocorrer de forma desigual e condicionada por fatores organizacionais e estruturais, com destaque para maturidade digital e gestão da cibersegurança em ambientes conectados. Tal evidência converge com estudos empíricos que descrevem a implantação da Indústria 4.0 como um processo graduado e sistêmico, no qual tecnologias mais visíveis (front-end) podem avançar mais rapidamente que bases críticas, como dados e analytics, limitando a

escalabilidade de soluções inteligentes (FRANK; DALENOGARE; AYALA, 2019).

A Tabela 1 sintetiza os principais achados discutidos ao longo desta seção, evidenciando os condicionantes organizacionais e tecnológicos que influenciam a adoção da Inteligência Artificial na Indústria 4.0, com destaque para suas implicações no agronegócio.

**Tabela 1 – Síntese dos principais achados sobre a adoção de Inteligência Artificial na Indústria 4.0**

Condicionante analisado	Caracterização no estudo	Efeito sobre a adoção de IA	Implicações para o agronegócio
Maturidade digital	Grau de preparo organizacional em processos, dados, cultura e estratégia	Viabiliza integração e escalabilidade da IA	Permite adoção consistente em agroindústrias e cooperativas
Integração de dados e sistemas	Interoperabilidade entre sistemas produtivos e informacionais	Condiciona confiabilidade e desempenho dos modelos	Favorece rastreabilidade e decisão baseada em dados
Conectividade	Interconexão contínua entre ativos físicos e digitais	Potencializa automação e análise em tempo real	Amplia eficiência operacional em sistemas agroindustriais
Cibersegurança industrial	Gestão de riscos cibernéticos em ambientes conectados	Sustenta continuidade e confiança na IA	Reduz riscos operacionais e falhas críticas no agro
Dimensão organizacional	Cultura, competências e gestão da mudança	Influencia aceitação e uso efetivo da IA	Determina capacidade de absorção tecnológica

Fonte: Elaborado pelo autor (2026).

Nessa perspectiva, a maturidade digital não se manifesta apenas como “digitalização” ou “automação” em sentido estrito, mas como capacidade organizacional de integrar processos, dados e tecnologias para sustentar decisões e rotinas. Ao estudar padrões de implementação em empresas manufatureiras, Frank, Dalenogare e Ayala (2019) observaram que a adoção se relaciona a uma incorporação sistêmica de tecnologias de *front-end*, enquanto a implementação de tecnologias-base (incluindo big data e *analytics*) é desafiadora e menos difundida, o que ajuda a explicar por que muitas iniciativas de IA permanecem pontuais e difíceis de escalar (FRANK; DALENOGARE; AYALA, 2019).

Além disso, os resultados se alinham a análises que mostram que barreiras organizacionais, especialmente resistência interna, podem se impor mesmo quando há interesse em ganhos de controle e desempenho. Em estudo qualitativo com executivos, Horváth e Szabó (2019) identificaram que o desejo gerencial por maior controle e medição em tempo real é força motriz para Indústria 4.0, mas a resistência em níveis de colaboradores e média gerência pode

dificultar significativamente a introdução de novas tecnologias; os autores também apontam diferenças entre multinacionais e PMEs quanto a forças e barreiras (HORVÁTH; SZABÓ, 2019).

#### 4.2 MATURIDADE DIGITAL COMO CONDICIONANTE PARA ADOÇÃO DE IA: CAPACIDADES, INTEGRAÇÃO E PRÁTICAS ORGANIZACIONAIS

A análise evidencia que a maturidade digital atua como condicionante da adoção de IA ao influenciar diretamente integração de sistemas, disponibilidade de dados e capacidade de operar em ecossistemas conectados. Essa leitura encontra suporte em estudos que discutem determinantes para o sucesso da transformação digital no contexto da Indústria 4.0, incluindo prontidão tecnológica e competências organizacionais. Ao propor diretrizes estratégicas para o sucesso de transformação digital em PMEs de manufatura, Ghobakhloo (2021) identificou determinantes essenciais e destacou que fatores como prontidão em tecnologia operacional e maturidades associadas ao ambiente digital condicionam o sucesso do processo, sugerindo que a transformação sob Indústria 4.0 é “complexa e intensiva em recursos” (GHOBAKHLOO, 2021).

Os achados também dialogam com evidências de que a adoção de tecnologias avançadas se beneficia quando práticas organizacionais estruturantes já estão presentes. Em pesquisa com fabricantes brasileiros, Tortorella e Fettermann (2018) observaram associação positiva entre práticas de produção enxuta (*lean*) e implementação de tecnologias da Indústria 4.0, indicando que a implementação concomitante tende a produzir melhorias de desempenho superiores, o que sugere que rotinas e disciplina operacional podem facilitar a absorção de tecnologias digitais (TORTORELLA; FETTERMANN, 2018).

Essa evidência é relevante para IA porque soluções baseadas em dados dependem de processos estáveis, governança operacional e capacidade de padronizar e integrar informações. Em termos práticos, a maturidade digital pode ser entendida como a capacidade de sustentar: a) coleta e qualidade de dados; b) integração entre tecnologias-base e aplicações; c) alinhamento entre gestão e operação; e d) adaptação organizacional (mudança cultural e competências). Nessa linha, Horváth e Szabó (2019) reforçam que tecnologias de Indústria 4.0 podem transformar funções gerenciais, mas barreiras de resistência organizacional podem interromper esse avanço, especialmente em empresas com menos recursos e menor estrutura de gestão da mudança (HORVÁTH; SZABÓ, 2019).

Complementarmente, estudos que modelam barreiras de adoção destacam que obstáculos não atuam isoladamente, mas se estruturam em relações de dependência e encadeamento. Kamble, Gunasekaran e Sharma (2018) analisam barreiras à adoção da Indústria 4.0 usando modelagem estrutural interpretativa e análise de dependência/dirigência, indicando que compreender relações entre barreiras é crucial para orientar ações gerenciais e políticas de mitigação (KAMBLE; GUNASEKARAN; SHARMA, 2018). Esse aspecto é particularmente sensível no contexto agroindustrial brasileiro, marcado por heterogeneidade estrutural e assimetrias de acesso tecnológico. A Tabela 2 apresenta os diferentes níveis de maturidade digital e seus efeitos esperados sobre a adoção da Inteligência Artificial, conforme discutido na literatura analisada.

**Tabela 2 – Níveis de maturidade digital e efeitos sobre a adoção de Inteligência Artificial**

Nível de maturidade digital	Características organizacionais	Padrão de adoção de IA
Baixa	Sistemas fragmentados, baixa governança de dados e resistência cultural	Uso pontual, experimental e pouco escalável
Intermediária	Integração parcial, iniciativas isoladas de inovação	Adoção gradual, com benefícios limitados
Alta	Processos integrados, cultura orientada a dados e estratégia digital clara	Adoção ampla, sustentável e alinhada aos objetivos organizacionais

Fonte: Elaborado pelo autor (2026).

À luz da revisão da literatura apresentada, constata-se que a adoção da Inteligência Artificial no contexto da Indústria 4.0 é condicionada por um conjunto articulado de fatores organizacionais e tecnológicos, entre os quais se destacam a maturidade digital, a conectividade e a cibersegurança industrial. A análise dos estudos evidencia que diferentes níveis de maturidade digital resultam em padrões distintos de incorporação da IA, conforme sintetizado na Tabela 2, reforçando que a simples disponibilidade tecnológica não é suficiente para garantir adoções consistentes e sustentáveis.

Ademais, a intensificação da conectividade amplia simultaneamente o potencial de uso da IA e a exposição a riscos cibernéticos, tornando a gestão da cibersegurança elemento central para a continuidade e a confiabilidade dos sistemas produtivos. Esse arcabouço teórico

fundamenta a análise desenvolvida nas seções seguintes, nas quais se discutem os achados do estudo e suas implicações para a adoção sustentável da Inteligência Artificial em ambientes agroindustriais.

#### 4.3 CONECTIVIDADE E CIBERSEGURANÇA: SUSTENTABILIDADE DA ADOÇÃO DE IA EM AMBIENTES AGROINDUSTRIAIS CONECTADOS

A discussão dos achados mostra que a conectividade, embora habilitadora da Indústria 4.0, amplia a superfície de exposição a riscos cibernéticos, tornando a cibersegurança condicionante da adoção sustentável de IA. Esse ponto é consistente com estudos que descrevem a transição de arquiteturas agroindustriais historicamente isoladas para estruturas mais conectadas devido à incorporação de IoT/IIoT e integração com ambientes corporativos.

Boyes et al. (2018) destacam que sistemas de automação e controle industrial (IACS), antes isolados, vêm passando por mudanças arquiteturais com maior conectividade, e propõem um framework para caracterizar dispositivos IIoT visando apoiar análises de arquiteturas, ameaças e vulnerabilidades (BOYES et al., 2018). A Tabela 3 sistematiza a relação entre conectividade, riscos cibernéticos e seus efeitos sobre a adoção da Inteligência Artificial, conforme evidenciado na discussão teórica.

**Tabela 3 – Relação entre conectividade, cibersegurança e adoção de Inteligência Artificial**

Aspecto	Benefício associado à IA	Risco cibernético potencial	Impacto na adoção
Conectividade intensiva	Monitoramento e decisões em tempo real	Ampliação da superfície de ataque	Exige maior maturidade em segurança
Integração OT/IT	Automação e inteligência operacional	Propagação de falhas e ataques	Condiciona sustentabilidade da IA
Uso intensivo de dados	Melhoria da acurácia dos modelos	Vazamento e perda de integridade	Afeta confiança nos sistemas
Ambientes ciberfísicos	Autonomia e eficiência produtiva	Interrupções operacionais	Pode comprometer continuidade

Fonte: Elaborado pelo autor (2026).

Sob a ótica de sistemas ciberfísicos (CPS), base operacional da Indústria 4.0, a literatura também aponta que a heterogeneidade de componentes (ciber, físico e ciberfísico) e a



diversidade de sistemas ampliam desafios de segurança e dificultam abordagens generalistas. Humayed et al. (2017) sistematizam a literatura de segurança em CPS sob um framework que considera ameaças, vulnerabilidades, ataques e controles, além de distinguir componentes e tipos de sistemas (incluindo sistemas agroindustriais), reforçando que a complexidade estrutural e a variedade de integrações elevam o desafio de proteção (HUMAYED et al., 2017).

Em termos de adoção de IA, essa discussão é central porque a IA depende de dados confiáveis e de disponibilidade operacional. Se conectividade aumenta a produção de dados e viabiliza decisões em tempo real, ela também aumenta o risco de comprometimento da integridade e disponibilidade dos ativos digitais que alimentam modelos de IA. Assim, fragilidades em cibersegurança podem limitar tanto a confiança nos sistemas automatizados quanto a continuidade operacional. Isso se aproxima do argumento de que maturidade digital e maturidade cibernética precisam evoluir conjuntamente.

Essa interdependência aparece de forma explícita em estudos sobre determinantes de implementação de tecnologias digitais na manufatura inteligente. Ghobakhloo (2020) identificou fatores determinantes para implementação de tecnologias de informação e digitais na manufatura inteligente e apontou que “maturidade em tecnologia operacional” e “maturidade em cibersegurança” figuram como determinantes dependentes, fortemente influenciados por outros determinantes do processo de digitalização, o que sugere que segurança e operações digitais são resultados de uma cadeia de capacidades e decisões organizacionais (GHOBAKHLOO, 2020).

Além disso, a literatura de gestão de segurança da informação aponta crescimento de vulnerabilidades devido à multiplicação de pontos de entrada em redes e reforça a necessidade de abordagens holísticas e gerenciais para segurança. Em revisão sistemática sobre ISO/IEC 27001, Culot et al. (2021) destacam que tecnologias emergentes e novas práticas aumentam a vulnerabilidade e defendem a necessidade de abordagens holísticas para enfrentar desafios crescentes de segurança da informação, o que se conecta diretamente ao requisito de governança e gestão de riscos em iniciativas de IA agroindustriais (CULOT et al., 2021).

#### 4.4 DISCUSSÃO INTEGRADORA: COMO MATURIDADE DIGITAL E CIBERSEGURANÇA CONDICIONAM A ADOÇÃO DE IA

Os achados deste estudo possuem implicações diretas para o agronegócio, sobretudo em agroindústrias, cooperativas, usinas sucroalcooleiras e propriedades rurais tecnificadas, nas

quais a adoção da Inteligência Artificial depende de níveis adequados de maturidade digital e de práticas consistentes de cibersegurança. A integração de tecnologias digitais no campo amplia a capacidade de monitoramento, automação e tomada de decisão baseada em dados, mas também expõe os sistemas produtivos agroindustriais a riscos cibernéticos que podem comprometer operações críticas. Nesse sentido, a adoção da Inteligência Artificial no agronegócio exige abordagens integradas que alinhem inovação tecnológica, governança digital e gestão de riscos. A Tabela 4 apresenta um modelo integrador dos condicionantes da adoção da Inteligência Artificial, evidenciando a interdependência entre maturidade digital, conectividade e cibersegurança.

**Tabela 4 – Modelo integrador dos condicionantes da adoção sustentável de Inteligência Artificial**

Dimensão	Elementos centrais	Papel na adoção de IA	Resultado esperado
Maturidade digital	Processos, dados, cultura e estratégia	Base organizacional para integração	Escalabilidade e eficiência
Conectividade	IIoT, integração de sistemas e dados em tempo real	Potencializa automação e análise	Ganhos operacionais
Cibersegurança	Gestão de riscos e proteção de ativos digitais	Sustenta confiabilidade e continuidade	Resiliência dos sistemas
Integração sistêmica	Alinhamento entre dimensões	Viabiliza adoção sustentável	Valor organizacional contínuo

Fonte: Elaborado pelo autor (2026).

Ao integrar as evidências, a discussão sugere que a adoção de IA em Indústria 4.0 é condicionada por um conjunto de capacidades organizacionais que se desenvolvem de forma incremental e interdependente. Em primeiro plano, a maturidade digital atua como base de integração de processos e dados; em seguida, a conectividade amplia o potencial de IA, mas torna indispensável a incorporação de práticas e maturidade de cibersegurança para assegurar sustentabilidade.

A literatura de implementação oferece suporte para esse encadeamento: a adoção pode avançar em tecnologias visíveis, mas fica limitada quando tecnologias-base (dados e *analytics*) são difíceis de consolidar (FRANK; DALENOGARE; AYALA, 2019). Além disso, mesmo quando há motivação gerencial por controle e mensuração em tempo real, resistências organizacionais podem impedir o avanço (HORVÁTH; SZABÓ, 2019). Ao mesmo tempo,

práticas organizacionais estruturantes (ex.: disciplina operacional e melhoria contínua associadas a *lean*) se relacionam positivamente com implementação de Indústria 4.0 e ganhos de desempenho, sugerindo que capacidades internas favorecem absorção tecnológica (TORTORELLA; FETTERMANN, 2018).

Em paralelo, a conectividade crescente muda arquiteturas agroindustriais e demanda enquadramentos robustos para análise de ameaças e vulnerabilidades, especialmente em ambientes IIoT/IACS (BOYES et al., 2018). A complexidade e heterogeneidade de CPS elevam o desafio de segurança e indicam que a gestão de controles precisa considerar múltiplas dimensões do sistema (HUMAYED et al., 2017). Por fim, evidências apontam a maturidade de cibersegurança como componente que emerge como dependente do conjunto de determinantes da transformação, isto é, segurança madura depende de decisões e capacidades organizacionais que vêm “antes” na cadeia de digitalização (GHOBAKHLOO, 2020).

Dessa forma, a resposta à pergunta norteadora deste artigo aponta que maturidade digital condiciona a adoção de IA ao fornecer integração, dados e capacidade de implementação; enquanto a gestão da cibersegurança condiciona a sustentabilidade da adoção ao assegurar integridade, disponibilidade e confiança em ambientes agroindustriais conectados. Em termos gerenciais, isso implica que estratégias eficazes de adoção de IA devem combinar iniciativas técnicas com governança de dados, gestão da mudança organizacional e programas consistentes de segurança, evitando a implantação isolada de IA em infraestrutura ainda fragmentada.

## 5 CONCLUSÕES

Este estudo teve como propósito analisar, à luz da literatura científica, como a maturidade digital e a gestão da cibersegurança influenciam a adoção da Inteligência Artificial no contexto da Indústria 4.0. Partindo de uma abordagem qualitativa e de uma revisão bibliográfica narrativa, buscou-se compreender a adoção da Inteligência Artificial não como um fenômeno puramente tecnológico, mas como um processo organizacional complexo, condicionado por capacidades estruturais, estratégicas e de governança em ambientes agroindustriais cada vez mais conectados.

Os resultados e a discussão desenvolvidos ao longo do trabalho permitem afirmar que a adoção da Inteligência Artificial na Indústria 4.0 ocorre de forma heterogênea e progressiva, sendo fortemente condicionada pelo nível de maturidade digital das organizações. Observou-se que empresas com maior maturidade digital tendem a apresentar melhores condições para

incorporar soluções baseadas em Inteligência Artificial de maneira integrada, sustentável e alinhada aos seus objetivos estratégicos. Nessas organizações, a presença de processos digitalizados, sistemas integrados, cultura orientada a dados e capacidade de adaptação organizacional favorece a transformação da Inteligência Artificial em valor operacional e estratégico.

Em contrapartida, organizações com menor maturidade digital enfrentam obstáculos significativos, tais como fragmentação de sistemas, ausência de dados estruturados, limitações de infraestrutura tecnológica e resistência cultural à mudança. Esses fatores comprometem não apenas a adoção da Inteligência Artificial, mas também a percepção de seus benefícios, resultando, muitas vezes, em iniciativas pontuais, pouco escaláveis e de impacto limitado. Dessa forma, o estudo reforça a compreensão de que a Inteligência Artificial não se configura como uma solução isolada, mas como parte de um ecossistema digital mais amplo, cuja efetividade depende de bases organizacionais previamente consolidadas.

Outro achado central diz respeito ao papel ambivalente da conectividade no contexto da Indústria 4.0. A conectividade contínua mostrou-se elemento essencial para viabilizar a coleta, o processamento e a análise de dados em tempo real, ampliando significativamente o potencial da Inteligência Artificial aplicada aos processos agroindustriais. Entretanto, essa mesma conectividade amplia a superfície de exposição a riscos cibernéticos, tornando a cibersegurança agroindustrial um fator crítico para a sustentabilidade da adoção tecnológica. O estudo evidencia que a ausência de políticas, práticas e estruturas adequadas de cibersegurança compromete a confiabilidade, a integridade e a disponibilidade dos sistemas produtivos, limitando os ganhos esperados da automação inteligente.

Nesse sentido, a gestão da cibersegurança emerge não apenas como um requisito técnico, mas como um componente estratégico da transformação digital. Observou-se que organizações capazes de integrar a cibersegurança às suas estratégias de digitalização apresentam maior propensão à adoção consistente de soluções baseadas em Inteligência Artificial. Essa integração contribui para a mitigação de riscos operacionais, para o fortalecimento da confiança nos sistemas automatizados e para o aumento da resiliência organizacional em ambientes agroindustriais altamente conectados e dinâmicos.

A análise integrada dos achados permite compreender que maturidade digital, capacidade tecnológica, conectividade e cibersegurança não atuam de forma isolada, mas de maneira interdependente. A maturidade digital estabelece as bases organizacionais necessárias; a capacidade tecnológica viabiliza a implementação prática das soluções; a conectividade

potencializa o uso da Inteligência Artificial; e a cibersegurança assegura a continuidade, a confiabilidade e a sustentabilidade das operações. Fragilidades em qualquer um desses elementos tendem a comprometer o sucesso da adoção da Inteligência Artificial, evidenciando a necessidade de abordagens sistêmicas e integradas.

Do ponto de vista teórico, este estudo contribui ao reforçar uma compreensão ampliada da adoção da Inteligência Artificial na Indústria 4.0, deslocando o foco de análises estritamente tecnológicas para uma perspectiva organizacional e estratégica. Ao articular os conceitos de maturidade digital e cibersegurança como condicionantes centrais da adoção, o trabalho contribui para o avanço do debate acadêmico sobre transformação digital, evidenciando que o sucesso da Inteligência Artificial depende menos da disponibilidade isolada de tecnologias e mais da capacidade organizacional de integrá-las, governá-las e sustentá-las ao longo do tempo.

Sob a ótica gerencial, os resultados oferecem subsídios relevantes para gestores agroindustriais e formuladores de estratégias. O estudo indica que iniciativas de adoção da Inteligência Artificial devem ser precedidas, ou ao menos, acompanhadas por investimentos em maturidade digital, governança de dados, capacitação de pessoas e fortalecimento das práticas de cibersegurança. Estratégias focadas exclusivamente na aquisição de soluções tecnológicas tendem a gerar resultados limitados se não estiverem alinhadas a um projeto mais amplo de transformação organizacional e gestão de riscos. Assim, a Inteligência Artificial deve ser compreendida como parte de um processo contínuo de transformação, e não como uma iniciativa pontual de automação.

No que se refere às limitações, destaca-se que este estudo se baseia exclusivamente em fontes secundárias, não contemplando dados empíricos primários oriundos de organizações agroindustriais específicas. Além disso, a revisão bibliográfica narrativa, embora adequada aos objetivos propostos, envolve maior grau de interpretação por parte do pesquisador, o que exige cautela na generalização dos achados. Ainda assim, a explicitação dos procedimentos metodológicos e a comparação sistemática com a literatura contribuem para a transparência e a consistência analítica do trabalho.

Como sugestões para pesquisas futuras, recomenda-se o desenvolvimento de estudos empíricos que investiguem a adoção da Inteligência Artificial em diferentes segmentos agroindustriais, considerando níveis distintos de maturidade digital e graus variados de exposição a riscos cibernéticos. Estudos de caso, pesquisas survey e abordagens mistas podem aprofundar a compreensão dos mecanismos organizacionais que facilitam ou dificultam a adoção sustentável da Inteligência Artificial. Sugere-se, ainda, o aprofundamento de



investigações que explorem a integração entre Inteligência Artificial e cibersegurança agroindustrial, especialmente no que se refere à construção de modelos de governança capazes de equilibrar inovação, eficiência e segurança em ambientes produtivos complexos.

Em síntese, conclui-se que a Inteligência Artificial desempenha papel estratégico na Indústria 4.0, mas sua adoção bem-sucedida depende de uma abordagem integrada que alinhe tecnologia, maturidade organizacional e gestão de riscos. Ao evidenciar a interdependência entre maturidade digital e cibersegurança, este estudo contribui para uma compreensão mais realista e crítica da transformação digital no ambiente agroindustrial, oferecendo fundamentos teóricos e práticos para o avanço de estratégias de inovação tecnológica sustentáveis e resilientes.

## REFERÊNCIAS

- ADEWUSI, Adebunmi O.; CHIEKEZIE, Njideka R.; EYO-UDO, Nsisong L. Securing smart agriculture: cybersecurity challenges and solutions in IoT-driven farms. *World Journal of Advanced Research and Reviews*, v. 15, n. 3, p. 480–489, 2022. DOI: <https://doi.org/10.30574/wjarr.2022.15.3.0887>.
- ALI, Iram Asghar et al. Security and privacy in IoT-based smart farming: a review. *Multimedia Tools and Applications*, v. 84, p. 15971–16031, 2025. DOI: <https://doi.org/10.1007/s11042-024-19653-3>.
- AZAMBUJA, Antonio J. G. et al. Artificial intelligence-based cyber security in the context of Industry 4.0: a survey. *Electronics*, Basel, v. 12, n. 8, p. 1–32, 2023. DOI: <https://doi.org/10.3390/electronics12081920>.
- BÉCUE, Adrien; PRAÇA, Isabel; GAMA, João. Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities. *Artificial Intelligence Review*, Dordrecht, v. 54, p. 3849–3886, 2021. DOI: <https://doi.org/10.1007/s10462-020-09942-2>.
- BEDUCCI, Elena; ACERBI, Federica; DE CAROLIS, Anna. Assessing Industry 4.0 readiness and maturity in the dairy sector: a case study. *Operations Management Research*, 2026. DOI: <https://doi.org/10.1007/s12063-026-00583-2>.
- BIGLIARDI, Barbara et al. Industry 4.0 in the agrifood supply chain: a review. *Procedia Computer Science*, v. 217, p. 1755–1764, 2023. DOI: <https://doi.org/10.1016/j.procs.2022.12.375>.
- BOYES, Hugh; HALLAQ, Bilal; CUNNINGHAM, Joe; WATSON, Tim. The industrial internet of things (IIoT): an analysis framework. *Computers in Industry*, Amsterdam, v. 101, p. 1–12, 2018. DOI: <https://doi.org/10.1016/j.compind.2018.04.015>.
- BÜYÜK, Aysu Melis et al. Digital maturity assessment model for smart agriculture. In: DURAKBASA, Numan M.; GENYILMAZ, Mehmet G. (org.). *Digital Conversion on the*

Way to Industry 4.0. Cham: Springer, 2021. p. 289–301. DOI: [https://doi.org/10.1007/978-3-030-62784-3\\_24](https://doi.org/10.1007/978-3-030-62784-3_24).

CAVALCANTE, Lívia T. C.; OLIVEIRA, Adélia A. S. Métodos de revisão bibliográfica nos estudos científicos. *Psicologia em Revista*, Belo Horizonte, v. 26, n. 1, p. 82–100, 2020. DOI: <https://doi.org/10.5752/P.1678-9563.2020v26n1p82-100>.

CULOT, Giovanna; NASSIMBENI, Guido; PODRECCA, Matteo; SARTOR, Marco. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, Bingley, v. 33, n. 7, p. 76–105, 2021. DOI: <https://doi.org/10.1108/TQM-09-2020-0202>.

DEMESTICHAS, Konstantinos; PEPPE, Nikolaos; ALEXAKIS, Theodoros. Survey on security threats in agricultural IoT and smart farming. *Sensors*, v. 20, n. 22, 2020. DOI: <https://doi.org/10.3390/s20226458>.

FERNANDES, Jaciara M. B.; VIEIRA, Lidiane T.; CASTELHANO, Marcos V. C. Revisão narrativa enquanto metodologia científica significativa: reflexões técnicas-formativas. *Revista Eletrônica de Comunicação*, 2021. Disponível em: <https://www.editoraverde.org/portal/revistas/index.php/rec/article/download/223/340/1029>. Acesso em: 14 mar. 2026.

FRAGOMELI, Roberto; ANNUNZIATA, Azzurra; PUNZO, Gennaro. Promoting the transition towards Agriculture 4.0: a systematic literature review on drivers and barriers. *Sustainability*, v. 16, n. 6, 2024. DOI: <https://doi.org/10.3390/su16062425>.

FRANK, Alejandro Germán; DALENOGARE, Lucas Santos; AYALA, Néstor Fabián. Industry 4.0 technologies: implementation patterns in manufacturing companies. *International Journal of Production Economics*, Amsterdam, v. 210, p. 15–26, 2019. DOI: <https://doi.org/10.1016/j.ijpe.2019.01.004>.

GABSI, Abd E. H. Integrating artificial intelligence in Industry 4.0: insights, challenges, and future prospects – a literature review. *Annals of Operations Research*, Cham, 2024. DOI: <https://doi.org/10.1007/s10479-024-06012-6>.

GHOBAKHLOO, Morteza. Determinants of information and digital technology implementation for smart manufacturing. *International Journal of Production Research*, London, v. 58, n. 8, p. 2384–2405, 2020. DOI: <https://doi.org/10.1080/00207543.2019.1630775>.

\_\_\_\_\_. Digital transformation success under Industry 4.0: a strategic guideline for manufacturing SMEs. *Journal of Manufacturing Technology Management*, Bradford, v. 32, n. 8, p. 1533–1556, 2021. DOI: <https://doi.org/10.1108/JMTM-11-2020-0455>.

GIL, Antonio C. *Como elaborar projetos de pesquisa*. 6. ed. São Paulo: Atlas, 2017.

\_\_\_\_\_. *Métodos e técnicas de pesquisa social*. 7. ed. São Paulo: Atlas, 2019.

HASSON, Abdo A. et al. Digital transformation in the agri-food industry: recent applications



and the role of the COVID-19 pandemic. *Frontiers in Sustainable Food Systems*, v. 7, 2023. DOI: <https://doi.org/10.3389/fsufs.2023.1217813>.

HORVÁTH, Dóra; SZABÓ, Roland Zs. Driving forces and barriers of Industry 4.0: do multinational and small and medium-sized companies have equal opportunities? *Technological Forecasting and Social Change*, Amsterdam, v. 146, p. 119–132, 2019. DOI: <https://doi.org/10.1016/j.techfore.2019.05.021>.

HUMAYED, Abdulmalik et al. Cyber-Physical Systems Security—A Survey. *IEEE Internet of Things Journal*, New York, v. 4, n. 6, p. 1802–1831, 2017. DOI: <https://doi.org/10.1109/JIOT.2017.2703172>.

KAGERMANN, Henning; WAHLSTER, Wolfgang; HELBIG, Johannes. *Recommendations for implementing the strategic initiative INDUSTRIE 4.0*. Munich: acatech, 2013.

KAMBLE, Sachin S.; GUNASEKARAN, Angappa; SHARMA, Rohit. Analysis of the driving and dependence power of barriers to adopt Industry 4.0 in Indian manufacturing industry. *Computers in Industry*, Amsterdam, v. 101, p. 107–119, 2018. DOI: <https://doi.org/10.1016/j.compind.2018.06.004>.

KANE, Gerald C. et al. Achieving digital maturity. *MIT Sloan Management Review*, Cambridge, v. 59, n. 1, p. 1–20, 2017.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Fundamentos de metodologia científica*. 8. ed. São Paulo: Atlas, 2022.

LEE, Jay; DAVARI, Hossein; SINGH, Jaskaran. Industrial AI and predictive analytics for smart manufacturing. *Journal of Manufacturing Systems*, Amsterdam, v. 60, p. 20–30, 2021. DOI: <https://doi.org/10.1016/j.jmsy.2021.03.005>.

LIMA, Anderson R. *Modelo de aceitação para tecnologias digitais na agricultura: aplicação a sistemas de informação de gestão agrícola*. 2023. Tese (Doutorado em Engenharia de Produção) – Universidade Federal de São Carlos, São Carlos, 2023.

MINAYO, Maria C. S.; DESLANDES, Suely F.; GOMES, Romeu. *Pesquisa social: teoria, método e criatividade*. Petrópolis, RJ: Vozes, 2016.

MINAYO, Maria C. S.; COSTA, António P. *Técnicas que fazem uso da palavra, do olhar e da empatia: pesquisa qualitativa em ação*. Aveiro: Ludomedia, 2019.

NICK, Gábor et al. Artificial intelligence enriched Industry 4.0 readiness in manufacturing. *Production & Manufacturing Research*, London, v. 12, n. 1, 2024. DOI: <https://doi.org/10.1080/21693277.2024.2357683>.

OFUSORI, Lizzy; BOKABA, Tebogo; MHLONGO, Siyabonga. Artificial intelligence in cybersecurity: a comprehensive review and future direction. *Applied Artificial Intelligence*, London, v. 38, n. 1, p. 1–46, 2024. DOI: <https://doi.org/10.1080/08839514.2024.2439609>.

SCHWAB, Klaus. *The Fourth Industrial Revolution*. Geneva: World Economic Forum, 2016.

SENN, Pedro P. et al. Development of a digital maturity model for Industry 4.0. *Computers & Industrial Engineering*, Oxford, v. 185, 2023. DOI: <https://doi.org/10.1016/j.cie.2023.109645>.

SILVA, Erik M. D. *Inteligência artificial e machine learning na otimização da gestão da Agricultura 4.0: uma revisão sistemática da literatura*. 2025. **Trabalho de Conclusão de Curso – Universidade Federal de Mato Grosso do Sul**, Campo Grande, 2025.

TEIXEIRA, Henrique et al. Cybersecurity in Industry 4.0 and Internet of Things. In: *Digital Sustainability: Inclusion and Transformation*. Cham: Springer, 2024. p. 69–83. DOI: [https://doi.org/10.1007/978-3-031-57650-8\\_6](https://doi.org/10.1007/978-3-031-57650-8_6).

TORTORELLA, Guilherme Luz; FETTERMANN, Diego. Implementation of Industry 4.0 and lean production in Brazilian manufacturing companies. *International Journal of Production Research*, London, v. 56, n. 8, p. 2975–2987, 2018. DOI: <https://doi.org/10.1080/00207543.2017.1391420>.

WESTERMAN, George; BONNET, Didier; McAFEE, Andrew. *Leading digital: turning technology into business transformation*. Boston: Harvard Business Press, 2014.

WINDMANN, Alexander et al. Artificial intelligence in Industry 4.0: a review of integration challenges for industrial systems. *arXiv*, 2024. Disponível em: <https://arxiv.org/abs/2405.18580>. Acesso em: 14 mar. 2026.

YANG, Xing et al. A survey on smart agriculture: development modes, technologies, and security and privacy challenges. *IEEE/CAA Journal of Automatica Sinica*, v. 8, n. 2, p. 273–302, 2021. DOI: <https://doi.org/10.1109/JAS.2020.1003536>.