SEGURANÇA DA INFORMAÇÃO EM FUNÇÃO DE TECNOLOGIAS EMERGENTES NA AGRICULTURA DE PRECISÃO

EMERGING INFORMATION SECURITY TECHNOLOGIES FOR PRECISION AGRICULTURE

Ana Luiza Ferraz Silva
Faculdade de Tecnologia de Americana – Ministro Ralph Biasi
ana.silva2126@fatec.sp.gov.br

Daniel Santos Lima Silva
Faculdade de Tecnologia de Americana – Ministro Ralph Biasi
daniel.silva375@fatec.sp.gov.br

Jhony Kevin Mendonça
Faculdade de Tecnologia de Americana – Ministro Ralph Biasi
jhony.mendonca@fatec.sp.gov.br

João Emmanuel D'Alkmin Neves
Faculdade de Tecnologia de Americana – Ministro Ralph Biasi
joao.neves11@fatec.sp.gov.br

Resumo

O presente artigo destaca a relevância da Segurança da Informação na Agricultura de Precisão a qual emprega tecnologias como Internet das Coisas, para diminuição dos danos no meio ambiente e aumento da sua produtividade. Embora essas inovações promovam maior eficiência, a integração digital nas fazendas inteligentes cria vulnerabilidades significativas. O objetivo do estudo é analisar o cenário atual da segurança cibernética nas práticas de Agricultura de Precisão, destacando os riscos associados ao uso de sistemas Internet das Coisas na agricultura. A pesquisa baseia-se na análise de fontes bibliográficas sobre Segurança da Informação na agricultura, especificamente em relação ao uso de Internet das Coisas. Os resultados ressaltaram a importância de conscientizar a comunidade agrícola sobre riscos cibernéticos e incentivar boas práticas de segurança e investimentos em proteção, visando fortalecer a segurança cibernética das fazendas inteligentes e assegurar a estabilidade na produção alimentar. Esses esforços são cruciais para a segurança e sustentabilidade do setor a longo prazo.

Palavras-chave: Internet das Coisas; Agricultura Inteligente; Sustentabilidade

Abstract

This article highlights the relevance of Information Security in Precision Agriculture, which employs technologies such as the Internet of Things to reduce environmental damage and increase productivity. Although these innovations promote greater efficiency, digital integration in smart farms creates significant vulnerabilities. The study aims to analyze the current cybersecurity landscape in Precision Agriculture practices, emphasizing the risks associated with the use of Internet of Things systems in agriculture. The research is based on the analysis of bibliographic sources on Information Security in agriculture, specifically regarding the use of the Internet of Things. The results highlighted the importance of raising awareness among the agricultural community about cyber risks and encouraging good security practices and investments in protection, aiming to strengthen the cybersecurity of smart farms and ensure stability in food production. These efforts are crucial for the long-term security and sustainability of the sector.

Keywords*: Internet of Things; Smart Farming; Sustainability.*

1. Introdução

A projeção de que a população mundial alcançará cerca de 9 bilhões de pessoas até 2050 (Organização das Nações Unidas, 2015) evidencia a necessidade urgente de métodos inovadores na produção agrícola. Nesse contexto, Misra *et al*. (2020) destacam a importância da adoção de tecnologias que não apenas minimizem o desperdício de recursos, como água, fertilizantes e agroquímicos, mas também contribuam para a redução dos impactos ambientais, especialmente na camada de ozônio, promovendo uma agricultura mais sustentável.

Neste contexto, destaca-se a Agricultura de Precisão (AP), uma técnica de agricultura inteligente que propõe integrar Internet das Coisas (IoT), do inglês *Internet of Things*, para coletar e analisar dados sobre o solo, clima e plantio, com foco em ajustar e melhorar práticas agrícolas para potencializar o uso dos recursos conforme as necessidades específicas de cada parte do campo (Misra *et al.*, 2020).

Apesar dos benefícios proporcionados pela AP integrada a dispositivos de IoT, Moura e D'Alkmin Neves (2021) alertam que a crescente digitalização, em qualquer área, acarreta vulnerabilidades significativas para a Segurança da Informação (SI). Assim, os sistemas IoT implementados em fazendas inteligentes são suscetíveis a ciberataques, que podem resultar em danos de grande escala (Moraes *et al.*, 2022). Entre os potenciais impactos negativos, destaca-se a criação de ambientes de plantio e colheita inseguros e improdutivos. Além disso, ameaças

podem comprometer o controle e o monitoramento de sensores e veículos automatizados, como tratores e drones (Sontowski *et al.*, 2020).

Todavia, os esforços para implementar medidas de segurança nos sistemas de AP não são suficientemente rigorosos. A integração digital introduz diversos riscos à SI, que muitas vezes não são adequadamente mitigados devido ao investimento limitado das empresas em setores específicos (Vicentine *et al.*, 2022). Além disso, a falta de conhecimento entre os agricultores agrava essa problemática, tornando as fazendas inteligentes suscetíveis a ciberataques de concorrentes ou outras ameaças, o que representa uma preocupação significativa para o setor agrícola (Sontowski *et al.*, 2020).

Portanto, o objetivo deste artigo é realizar uma análise do cenário tecnológico atual no meio agrícola, ilustrando os riscos e danos relacionados à falta de SI nos sistemas de IoT, a fim de conscientizar sobre a importância de proteger as operações agrícolas contra ameaças cibernéticas e incentivar um aumento do investimento nesta área. Esse esforço é vital para manter a eficiência das fazendas inteligentes e mitigar os riscos cibernéticos que podem afetar a produção agrícola global.

2. Referencial Teórico

Esta seção propõe uma abordagem acadêmica da AP, delineando os tópicos a serem discutidos neste artigo com o intuito de facilitar a compreensão do leitor. É salientada a crescente importância da AP, um dos pilares das tecnologias contemporâneas, juntamente com o *Blockchain*, a IoT e a Inteligência Artificial. Essas tecnologias têm sido amplamente reconhecidas por promover a sustentabilidade e aprimorar as práticas de SI (Santos *et al.*, 2020; Neves *et al.*, 2023; Pedro *et al.*, 2024).

A adoção da AP tem impulsionado a inovação e o desenvolvimento de novas técnicas e práticas agrícolas, como o uso de drones para monitoramento de lavouras, a aplicação de técnicas de agricultura vertical em ambientes urbanos e a implantação de SI (Souza *et al.*, 2024). Essas inovações aumentam a eficiência e a rentabilidade da produção agrícola, como também contribuem para a criação de ambientes seguros e sustentabilidade do setor, garantindo a cibersegurança, a preservação dos recursos naturais e a segurança alimentar da população mundial.

2.1. Agricultura de Precisão

A AP pode ser conceituada como uma filosofia de gestão da produção agrícola que enfatiza a precisão e a integração da TI no campo. Essa abordagem é essencial na Era do Conhecimento Contemporâneo, onde a utilização de dados e tecnologias avançadas é fundamental para a eficácia e sustentabilidade de diversas áreas (Neves, 2018).

Na Era do Conhecimento, conforme descrito por Neves (2018), a valorização da informação e a inovação tecnológica são características predominantes. Nesse contexto, a informação assume um papel fundamental na AP. Através da coleta e análise de dados detalhados, que segundo Neves *et al.*, 2023 são métodos inerentes à Ciência de Dados, a AP pode tomar decisões que aprimoram a produtividade agrícola, maximizando a produção e reduzindo o desperdício de recursos. Por exemplo, uma parcela significativa do consumo de energia elétrica é atualmente atribuída ao desperdício decorrente dos hábitos comportamentais humanos (Neves, 2021).

A AP utiliza informações precisas para realizar decisões, a fim de gerir um campo produtivo de maneira específica, tendo em vista que cada parte do perímetro da área de produção possui propriedades distintas (Tschiedel; Ferreira, 2002).

Essencialmente, a AP trata da distribuição de quantidades corretas de insumos nos locais e momentos apropriados, conforme a necessidade do terreno, em áreas cada vez menores, dentro das limitações tecnológicas e recursos envolvidos. Trata-se também de um sistema de gerenciamento de produção integrado para regular a quantidade de materiais que entram na propriedade, de acordo com a cultura em pequenas áreas dentro dos campos de produção. No entanto, a AP não deve ser vista apenas como um método de tratamento do solo, mas sim como a capacidade de gerenciar, monitorar e acessar a atividade agrícola, levando em consideração a sustentabilidade, onde mudanças devem ocorrer sem causar prejuízos às reservas naturais para minimizar os danos ao meio ambiente (Tschiedel; Ferreira, 2002).

Além dos benefícios mencionados, o desenvolvimento de sistemas automáticos que integram *hardware* e *software* podem ser combinados com equipamentos de manejo agrícola como, por exemplo, semeadoras, colhedoras, sensores, entre outros (Mello; Caimi, 2008).

2.2. Inovações tecnológicas na Agricultura de Precisão

A AP utiliza a tecnologia, o que significa que os avanços nessa área a afetam diretamente. Nessa seção serão discorridos tipos de tecnologias que podem contribuir com o desenvolvimento da AP.

2.2.1. Internet das Coisas

A IoT é o termo utilizado para descrever a interação e acesso de controle total entre dispositivos físicos, em qualquer parte da Terra, através do uso da Internet e atribuições de funcionalidades específicas via *software* integrado (Gupta; Gupta, 2016; Moraes *et al.*, 2022).

A IoT oferece diversos benefícios principalmente na agricultura, onde sua implementação no meio é considerada essencial, pois há a necessidade de monitoramento e controle constante, uma vez que a IoT oferece estes recursos por meio remoto sem a interferência humana (Santos *et al.*, 2020; Yazdinejad *et al.*, 2021).

A utilização de IoT na AP influencia diretamente na criação de gado e estufas, por exemplo. Todas essas aplicações são monitoradas com a ajuda de sensores e dispositivos baseados em IoT através de redes de sensores sem fio as quais auxiliam os agricultores a recolherem, analisarem e processarem dados relevantes por meio de serviços em nuvem, quando empregados dispositivos IoT dessa maneira, cientistas da área agrícola conseguem tomar melhores decisões (Farooq *et al.*, 2020; Moraes *et al.*, 2022).

2.3. Desafios de Segurança Cibernética na Agricultura de Precisão

A AP, visa aumentar a eficiência e a produtividade agrícola por meio da integração de tecnologias. No entanto, esses avanços tecnológicos trazem vulnerabilidades cibernéticas. Um estudo conduzido por Window (2019) destaca que o aumento do uso de tecnologias na AP tem sido acompanhado pelo crescimento dos riscos de cibersegurança. Órgãos governamentais, como o FBI e o Departamento de Segurança Interna dos Estados Unidos, têm emitido alertas sobre os perigos associados a essa tendência. No entanto, na Europa a preocupação com a segurança cibernética na AP parece ser menor, conforme observado pela ausência de menção em relatórios relevantes da União Europeia (Window, 2019).

Conforme apontado por Racovita (2021), um relatório elaborado pelo Departamento de Segurança Interna dos Estados Unidos identificou ameaças importantes para a AP. Essas

ameaças incluem roubos de dados em sistemas de apoio à decisões, vazamento intencional de dados internos, venda de dados confidenciais, falsificação de dados e injeção de dados falsos, que representam ameaças à confidencialidade, integridade e disponibilidade dos sistemas.

Segundo estudos realizados por West (2018), o uso de sensores para monitoramento é uma prática aceita e as redes de sensores auxiliam os produtores permitindo o monitoramento e a automatização de operações em áreas remotas, assim como a obtenção de percepções mais precisas. Embora essas tecnologias ofereçam muitos benefícios, também representam alvos atraentes para ataques cibernéticos.

Os ataques cibernéticos podem assumir várias formas, desde a infiltração de *malware* (*softwares* maliciosos) por meio de terceiros, até o controle remoto de sistemas de irrigação e entrega de nutrientes. Essas ameaças são difíceis de detectar e podem passar despercebidas por longos períodos, representando um desafio significativo para a segurança da AP (West, 2018).

A maioria das redes IoT não possui nenhum mecanismo de segurança de rede e, portanto, são suscetíveis a ataques *Linux*, *Darlloz*[1] ou a ataque de negação de serviço (*DDoS*), com isso, muitas redes IoT enfrentam problemas de violação de dados importantes (Wu; Tsai, 2019). Um dos principais motivos para esse problema, segundo Wu e Tsai (2019) é a carência de mecanismos de autenticação.

O compartilhamento de dados de sensores é crucial em redes de sensores sem fio, porém, se o processo de compartilhamento for excessivamente complexo ou envolver muitas partes externas, o desempenho do sistema é comprometido, especialmente em um ambiente dinâmico (West, 2018; Souza *et al.*, 2024). Para garantir que entidades tenham acesso a informações sensíveis apenas para fins justificados, o controle do acesso é necessário (West, 2018).

Outro fator que impede a adoção da SI na AP é devido ao envelhecimento da população agrícola e seu nível relativamente baixo de conhecimento de tecnologias atuais, o que prejudica a disseminação de inovações. Ainda, segundo pesquisas, a falta de informação dificulta a ampliação da adoção de tecnologias que auxiliem os processos agrícolas, pois os agricultores precisam primeiro ter conhecimento de sua existência, entender seu funcionamento e acreditar que sua implementação pode melhorar a produtividade e desempenho (Angyalos; Botos; Szilágyi, 2021).

[1] Um tipo de software mal-intencionado que impacta aparelhos ligados à internet, como câmeras de vigilância e roteadores.

Porém, não apenas os agricultores mais velhos necessitam de apoio, mas também os mais jovens. Segundo Nikander, Manninen e Laajalahti (2020), mesmo os agricultores mais jovens e mais experientes em tecnologia também necessitam de auxílio. Em geral, um grande problema na SI na agricultura está nas pequenas e médias propriedades, devido ao fato de que funcionários das fazendas não são treinados como especialistas em tecnologia, muito menos especialistas em segurança cibernética.

De acordo com Souza *et al.* (2024), os ataques cibernéticos no setor agrícola inserem-se em um contexto mais amplo do que o das operações de informação, tornando urgente a implementação de medidas de segurança, dada a precarização da segurança digital no cenário . A rápida evolução tecnológica no ambiente agrícola, aliada à falta de barreiras de proteção, abre fronteiras para novas explorações e ataques que podem afetar não apenas a cadeia de produção, mas o setor agrícola em sua totalidade.

3. Metodologia

A metodologia do projeto consiste em uma pesquisa bibliográfica e exploratória. Os materiais utilizados para a revisão baseiam-se em artigos científicos e documentações que abordem assuntos relevantes ao tema principal: AP, IoT, ciberataques e avanço tecnológico no meio agrícola.

O desenvolvimento da pesquisa ocorreu através da leitura e análise de materiais relacionados a artigos, trabalhos científicos e livros, nas principais bases de material acadêmico como: Google Acadêmico, SciELO (internacional), IEEE *Xplore* e outras bases.

Grande parte dos resultados relacionados ao tema, são pouco referenciados e escassos em relação à importância do assunto. Além disso, diante das referências colhidas, foi possível observar que apenas 4 artigos que abordam o tema AP, discorrem sobre a SI, como ilustra a Tabela 1.

Tabela 1 – Artigos os quais abordam SI na AP

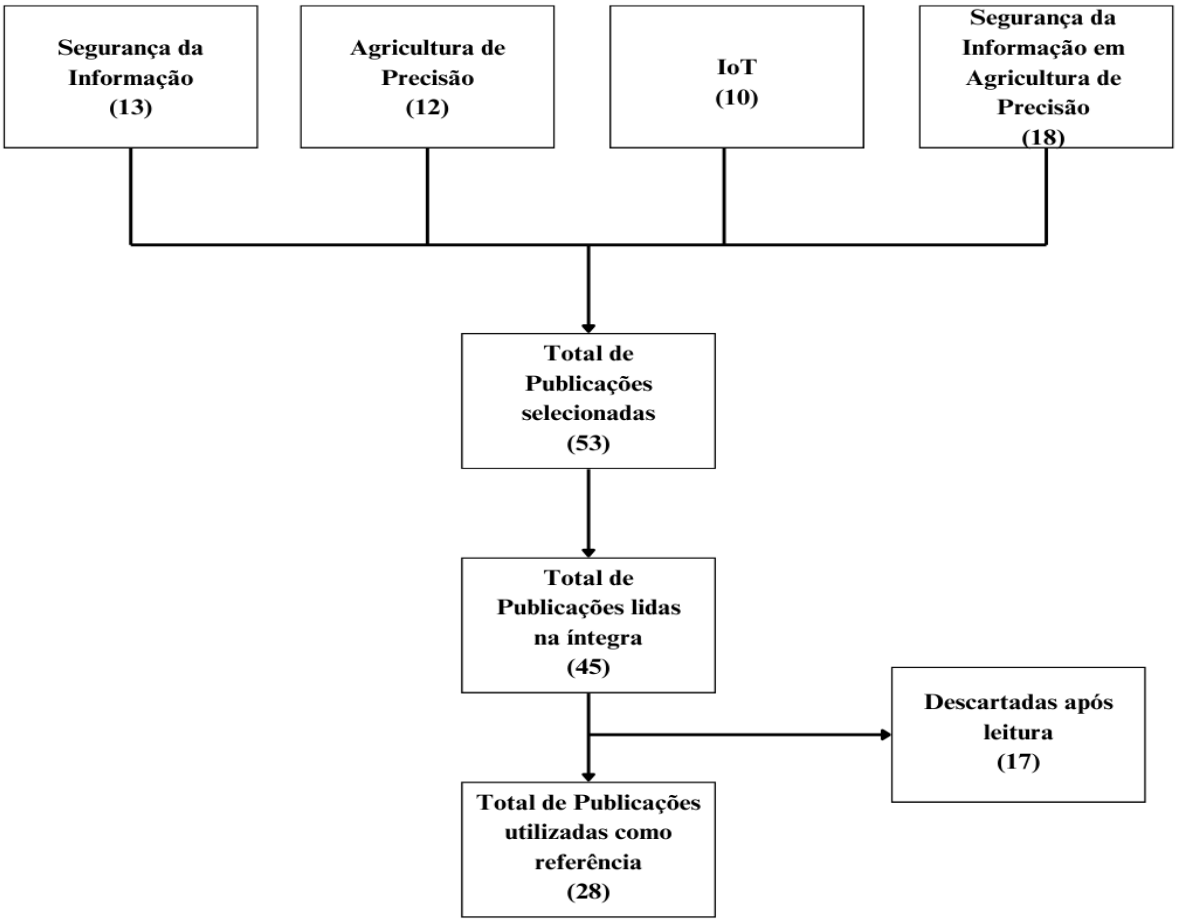
Nº	Título do Artigo	Autores	Ano	Resumo
1	Cybersecurity for the Internet of Things and Artificial Intelligence in the AgriTech Sector	Racovita Monica	2021	Este artigo aborda desafios e oportunidades na cibersegurança em IoT e Inteligência Artificial no setor Agritech.
2	Cyber Attacks on Smart Farming Infrastructure	Sina Sontowski, *et al.*	2020	Artigo que aborda uma discussão sobre ataques que exploram vulnerabilidades em redes de fazendas inteligentes.
3	A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats, and Countermeasures.	Abbas Yazdinejad, *et al.*	2021	Exame dos aspectos de segurança na Agricultura de Precisão, fazendas inteligentes e tipos de ataques.
4	Cibersegurança na Agricultura de Precisão: Exploração à Aplicação de Medidas Preventivas	Ana Laura Onofre de Souza, *et al.*	2024	Estudo que explora a cibersegurança na Agricultura de Precisão no Brasil, destacando lacunas no setor e a necessidade de medidas de Segurança.

Fonte: Elaborado pelos autores (2024)

Todos os referenciados foram submetidos a uma análise rigorosa quanto à origem dos arquivos utilizados, os quais foram publicados por congressos, universidades, revistas, entre outros, e possuíam boa reputação e renome em geral. Ademais, foi levada em consideração a relevância e a qualidade do material, bem como a quantidade de materiais relacionados que citavam as presentes referências utilizadas.

A Figura 1, demonstra o processo metodológico para a seleção das publicações utilizadas como referência na pesquisa. Foram identificadas publicações em quatro categorias principais: Segurança da Informação (13 artigos), Agricultura de Precisão (12 artigos), IoT (10 artigos) e Segurança da Informação em Agricultura de Precisão (18 artigos) e após isso foram escolhidos os artigos que preenchiam melhores os requisitos desejados pelos autores.

Figura 1 - Diagrama do processo de seleção dos materiais utilizados



Fonte: Elaborado pelos autores (2024)

4. Resultados e Discussões

Ao longo do desenvolvimento deste trabalho, foi possível identificar uma lacuna significativa na área de SI aplicada à AP. Embora haja um grande investimento em novas tecnologias e integrações com dispositivos digitais, conforme mencionado nas seções sobre IoT, a importância da SI na AP não tem recebido a devida atenção. Como apontado previamente, a SI desempenha um papel crucial nesse contexto, portanto, através da revisão bibliográfica, o objetivo é dar destaque para essa área.

O estudo conduzido por Naresh e Munaswamy. (2019), expõe uma análise dos sensores de IoT frequentemente empregados na AP, sendo que os autores desenvolveram uma tabela elucidativa desses dispositivos e suas funções, que desempenham papéis específicos e essenciais no monitoramento de variáveis ambientais, fornecendo dados críticos que auxiliam

na tomada de decisões e na melhoria da eficiência das operações na AP. A Tabela 2 os apresenta, acompanhados de uma breve descrição de seu funcionamento.

Tabela 2 - Principais sensores de IoT utilizados na AP

Sensor de umidade do solo	Sensor de nível de água	Sensor de umidade do ar	Sensor de temperatura
Detecta se o solo está úmido, enviando uma saída que deixa o circuito aberto quando o solo se encontra seco, e enviando saída que deixa o circuito fechado quando o solo estiver úmido.	Boias feitas de material leve e não elétrico, com marcadores visuais para mapear e medir níveis de água, podem ser conectadas a mecanismos para controlar o nível do líquido.	Resistor sensível à umidade que produz saída relativa à temperatura.	Sensor que processa informações incorporadas para calcular temperatura, informando uma saída elétrica em graus Celsius.

Fonte: Elaborado pelos autores com base em Naresh e Munaswamy (2019).

As questões de SI na AP ganharam ainda mais importância, à medida que o setor agrícola passa a depender cada vez mais de IoT, análise de dados e sistemas interconectados, tornando o ambiente suscetível a vulnerabilidades e ataques cibernéticos (Ongadi, 2024). Dessa forma, nota-se a suma importância de serem aplicados critérios de segurança, capazes de garantir a estabilidade agrícola.

De acordo com Yazdinejad *et al.* (2021), os principais parâmetros de segurança para AP podem ser descritos em alguns aspectos: privacidade e confidencialidade, em que a privacidade protege dados pessoais e assegura que os indivíduos possam controlar o compartilhamento de suas informações, enquanto a confidencialidade impede o acesso não autorizado a informações estratégicas e sensíveis, como dados sobre plantio e desempenho de culturas agrícolas; integridade, que se trata de assegurar que as informações não passem por alterações indevidas, por exemplo, no caso das informações sobre disposição de agroquímicos nas plantações, que se alteradas, podem causar danos irreversíveis à colheita ou alteração de dados de análise que geram diagnósticos sugeridos pelos *softwares* IoT; disponibilidade, responsável por assegurar que os serviços e informações estejam disponíveis para seu uso, como, na análise de informações usadas para auxílio em tomada de decisões, e confiança, que impossibilita uma pessoa de falsificar identidade, por exemplo, um atacante concorrente obter acesso de um indivíduo nos sistemas e infiltrar-se para capturar dados.

A importância da segurança cibernética na AP é evidenciada por incidentes que expõem as consequências de vulnerabilidades exploradas em ataques digitais. Por exemplo, a Dole, uma das maiores empresas de alimentos do mundo, foi vítima de um ataque de ransomware (software malicioso usado para extorquir vítimas por meio de criptografia dos dados) em fevereiro de 2023, o que causou uma paralisação temporária das operações de produção na América do Norte e comprometeu a distribuição de produtos para redes de supermercados, resultando em escassez em diversas localidades (Lyngaas, 2023). Além de interromper a cadeia de abastecimento, o incidente destacou o impacto direto de uma violação de segurança cibernética na disponibilidade e continuidade dos serviços essenciais para o setor.

Outro caso significativo é o ataque à JBS, a maior processadora de carne do mundo, em 2021. Nesse episódio, hackers exigiram um resgate milionário para restaurar o funcionamento dos sistemas, após a interrupção das operações nas indústrias produtoras de carne dos Estados Unidos, Canadá e Austrália. Esses exemplos não apenas demonstram a vulnerabilidade das cadeias de abastecimento alimentício a ataques cibernéticos, mas também evidenciam os custos e o efeito de tais ameaças sobre a segurança de setores essenciais (Forbes Agro, 2024).

Os dispositivos e sistemas empregados na AP muitas vezes foram projetados antes do surgimento de ameaças digitais complexas, o que contribui para o aumento das vulnerabilidades. Com frequência, tecnologias como sensores de irrigação e controle de temperatura não possuem as devidas proteções contra ataques, tornando-se alvos atrativos para cibercriminosos e aumentando o risco de comprometimento de dados críticos, indispensáveis para o manejo sustentável e eficiente das produções agrícolas (Forbes Agro, 2024).

Uma demonstração concreta da aplicação direta da proteção de dados pode ser observada nos sistemas inteligentes, como, de monitoramento climático. Conforme ressaltado por Angyalos, Botos e Szilágyi (2021), em seu estudo, os dados coletados pelos sistemas são aproveitados para mapear as condições meteorológicas e selecionar as culturas mais adequadas. Ao garantir a segurança adequada desses dados, é assegurado que as informações permaneçam íntegras e confidenciais, contribuindo para a tomada de decisões. Essa abordagem não apenas melhora a eficiência operacional, mas também contribui para a sustentabilidade e rentabilidade a longo prazo das operações agrícolas.

A adoção e conscientização em relação à SI na AP implicam em melhoria de segurança dos procedimentos, vantagem competitiva, diminuição de gastos como resgates de roubo de

dados, visto que, segundo Angyalos, Botos e Szilágyi (2021), no caso de um agricultor ter que decidir entre pagar determinada quantia a um atacante, ou uma interrupção e dano catastróficos na fazenda, o pagamento será o escolhido, e os atacantes têm consciência disso.

Além disso, a implementação eficaz de medidas de SI no setor agrícola desempenha um papel crucial na manutenção da estabilidade do fornecimento de alimentos. Como observado no trabalho de Bowcut (2024), um ataque cibernético direcionado a uma empresa de alimentos e agricultura pode causar interrupções na produção e distribuição de alimentos, potencialmente resultando em falta de alimento e alta de preços no mercado. Essa instabilidade afeta os produtores e a indústria, e tem consequências significativas para os consumidores e na cadeia de alimentos global. Portanto, o investimento em segurança também se torna essencial para preservar a estabilidade e segurança do abastecimento alimentar global.

Assegurar a resiliência dos sistemas de AP contra ameaças cibernéticas não só protege as informações, mas também fomenta a confiança entre os agricultores e as partes interessadas (stakeholders), facilitando a integração responsável e segura de tecnologias avançadas nas práticas agrícolas contemporâneas (Ongadi, 2024).

Em suma, a AP enfrenta desafios significativos em termos de SI, especialmente com a crescente dependência de tecnologias digitais e interconectadas. A implementação eficaz de medidas de segurança protege os dados sensíveis e as operações agrícolas, assim como também é crucial para garantir a qualidade e segurança dos produtos alimentares, preservar a estabilidade do fornecimento de alimentos e promover a confiança entre os stakeholders. De uma forma geral, os benefícios da implementação de SI na agricultura, superam significativamente os riscos, enquanto sua ausência causa múltiplos prejuízos, portanto, o investimento de SI na AP se faz necessário, uma vez que se torna essencial para enfrentar as ameaças emergentes e garantir a eficiência do setor agrícola moderno.

5. Considerações Finais

Após extensa revisão bibliográfica, constatou-se que o número de estudos relacionados à SI na AP não acompanha o ritmo dos avanços tecnológicos nesse setor. O aumento das ameaças no setor agrícola é evidente devido à rápida necessidade da adoção de tecnologias emergentes, como IoT, fomentadas pela indispensabilidade no aumento da eficiência, desempenho e da competitividade. Essas tecnologias, quando conectadas à Internet, ampliam o

cenário de vulnerabilidades, prejudicando potencialmente as plantações e comprometendo a integridade das informações essenciais para a produção agrícola.

Destaca-se a importância crucial da implementação de segurança nessas tecnologias, pois a falta de atenção a essa questão pode. Além disso, a SI é indispensável para mitigar a chance de ataques que afetem os processos agrícolas e proporcionem acesso a dados como, a quantidade adequada de nutrientes no solo e o uso correto de agrotóxicos, preservando tanto a produtividade quanto a saúde dos consumidores.

Observou-se que a maioria dos estudos revisados é recente, possuindo menos de dez anos, indicando a necessidade de mais pesquisas e aprofundamento na área. Dada a importância estratégica da agricultura na economia global, é primordial maior prudência e investimento na SI nesse setor. A conscientização e o treinamento são fundamentais para proteger toda a cadeia de produção agrícola contra ameaças cibernéticas.

Para futuras pesquisas e desenvolvimentos, sugere-se um foco maior na aplicação de IoT e tecnologias robustas para monitorar e assegurar dados na AP. Essas iniciativas são decisivas para mitigar os riscos e prejuízos associados à falta de segurança nas tecnologias agrícolas emergentes.

Referências

ANGYALOS, Z.; BOTOS, S.; SZILÁGYI, R. **The importance of cybersecurity in modern agriculture**. Journal of Agricultural Informatics (ISSN 2061-862X), v. 12, n. 2, p. 1-8, 2021. Disponível em: https://www.researchgate.net/publication/352412158_The_importance_of_cybersecurity_in_modern_agriculture. Acesso em: 9 maio 2024.

BOWCUT, S. **Shielding the supply: Cybersecurity in food and agriculture**. Cybersecurity Guide, 2024. Disponível em: https://cybersecurityguide.org/industries/food-and-agriculture/. Acesso em: 26 de maio de 2024.

FAROOQ, M. S.; RIAZ, S.; ABID, A.; UMER, T.; ZIKRIA, Y. B. **Role of IoT technology in agriculture: A systematic literature review.** Electronics, v. 9, n. 2, p.319, 2020. Disponível em: https://www.mdpi.com/2079-9292/9/2/319. Acesso em: 19 de abril 2024.

FORBES AGRO. **Ataques Cibernéticos são o "Novo Normal" do Setor Agroalimentar.** Forbes Brasil, São Paulo, 24 set. 2024. Disponível em: https://forbes.com.br/forbesagro/2024/09/ataques-ciberneticos-e-o-novo-normal-do-setor-agroalimentar/. Acesso em: 06 nov. 2024.

GUPTA, R.; GUPTA, R. **ABC of Internet of Things: Advancements, benefits, challenges, enablers and facilities of IoT.** In: 2016 Symposium on Colossal Data Analysis and Networking (CDAN). IEEE, 2016. p.1-5, 2016. Disponível em: https://ieeexplore.ieee.org/abstract/document/7570875. Acesso em: 19 de abril 2024.

LYNGAAS, Sean. **Cyberattack on food giant Dole temporarily shuts down North America production, company memo says**. CNN Business, Atlanta, 22 fev. 2023. Disponível em: https://edition.cnn.com/2023/02/22/business/dole-cyberattack/index.html. Acesso em: 06 nov. 2024.

MELLO, B. A. de; CAIMI, L. L. **Simulação na validação de sistemas computacionais para a agricultura de precisão.** Revista Brasileira de Engenharia Agrícola e Ambiental, v. 12, p. 666-675, 2008. Disponível em: https://doi.org/10.1590/S1415-43662008000600015. Acesso em: 19 de abril 2024.

MISRA, N. N.; DIXIT, Y.; AL-MALLAHI, A.; BHULLAR, M. S.; UPADHYAY, R.; MARTYNENKO, A. **IoT, big data, and artificial intelligence in agriculture and food industry.** IEEE Internet of Things Journal, v. 9, n. 9, p. 6305-6324, 2020. Disponível em: https://ieeexplore.ieee.org/document/9103523. Acesso em: 19 de abril 2024.

MORAES, J. M. de; QUIRINO, C.; ALMEIDA, R. M. de; NEVES, J. E. D. **Internet das Coisas (IoT)**: Casa inteligente, definições e aplicações. Revista Brasileira em Tecnologia da Informação, [S. l.], v. 4, n. 2, p. 31 - 37, 2022. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/52. Acesso em: 30 maio. 2024.

MOURA, T. M.; D'ALKMIN NEVES, J. E. **Análise de Segurança em Dispositivos Internet das Coisas**. Revista Interface Tecnológica, [S. l.], v. 18, n. 2, p. 15–27, 2021. Disponível em: https://doi.org/10.31510/infa.v18i2.1174. Acesso em: 26 maio 2024.

NARESH, M.; MUNASWAMY, P. **Smart agriculture system using IoT technology.** International journal of recent technology and engineering, v. 7, n. 5, p. 98-102, 2019. Disponível em: https://www.ijrte.org/portfolio-item/E1987017519/. Acesso em: 13 de maio 2024.

NEVES, J. E. D. **Estudo dos parâmetros do modelo de Mason para cerâmicas piezelétricas utilizando algoritmos genéticos**. Dissertação (Mestrado em Tecnologia) – Faculdade de Tecnologia, Universidade Estadual de Campinas. Limeira, p. 129. 2018. Disponível em: https://doi.org/10.47749/T/UNICAMP.2018.995710. Acesso em 26 de maio 2024.

NEVES, J. E. D. **Modelo Baseado em Agentes para Simulação de Consumo de Energia Elétrica em Função do Comportamento Humano**. Revista Eletrônica Anima Terra, v. 12, 2021. Disponível em: https://fatecmogidascruzes.com.br/pdf/animaTerra/edicao12/artigo7.pdf. Acesso em: 30 maio 2024.

NEVES, J. E. D.; PEDRO, P. S. M.; HERNANDEZ, M. F. G.; FABRI JUNIOR, L. A.

Simulation of the Implementation of Domestic Solar Systems Using Multi-agent Systems from Web Scraping. Smart Innovation, Systems and Technologies. 1ed.: Springer International Publishing, 2023, v. 1, p. 88-96. Disponível em: https://doi.org/10.1007/978-3-031-04435-9_8. Acesso em 26 de maio 2024.

NIKANDER, J.; MANNINEN, O.; LAAJALAHTI, M. **Requirements for cybersecurity in agricultural communication networks. Computers and electronics in agriculture**, v. 179, p. 105776, 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S0168169920314812. Acesso em: 13 de maio 2024.

ONGADI, P. A. **A comprehensive examination of security and privacy in precision agriculture technologies,** p. 345-346, 2024. Disponível em: https://doi.org/10.30574/gscarr.2024.18.1.0026. Acesso em: 13 de maio 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **World Population Prospects The 2015 Revision.** Volume I: Comprehensive Tables. ONU, 2015. Disponível em: https://population.un.org/wpp/publications/Files/WPP2015_Volume-I_Comprehensive-Tables.pdf. Acesso em: 13 de maio 2024.

PEDRO, A. M.; TURCI JUNIOR, M.; MONTEIRO, A. S.; ESPERANDIO, A. A. M.; BASTOS, C. V.; NEVES, J. E. D. **Blockchain como Fator de Transparência**. Revista Brasileira em Tecnologia da Informação, v. 5, p. 79-95, 2024. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/104. Acesso em 27 de maio 2024.

RACOVITA, M. **Industry briefing: cybersecurity for the Internet of Things and Artificial Intelligence in the AgriTech sector.** Industry Briefing PETRAS National Centre of Excellence for IoT Systems Cybersecurity: London, UK, p. 23, 2021. Disponível em: PETRAS_IndustryBriefing_Agritech.pdf (petras-iot.org). Acesso em: 19 de abril 2024.

SANTOS, B. S.; FONSECA, L. M. B.; SERNAGLIA, L.; NEVES, J. E. D. **Automação de casas e estabelecimentos comerciais através de microcontroladores**. REVISTA TECNOLÓGICA DA FATEC DE AMERICANA, v. 8, p. 70-80, 2020. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/6732. Acesso em: 28 maio 2024.

SONTOWSKI, S.; GUPTA, M.; CHUKKAPALLI, S. S. L.; ABDELSALAM, M.; MITTAL, S.; JOSHI, A.; SANDHU, R. **Cyber attacks on smart farming infrastructure.** In: 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC). IEEE, 2020. p. 135-143, 2020. Disponível em: https://www.researchgate.net/publication/346576000_Cyber_Attacks_on_Smart_Farming_Infrastructure. Acesso em: 19 de abril 2024.

SOUZA, A. L. O.; BASTOS, C. V.; SANTOS, P. M. S.; SOARES, N. M.; NEVES, J. E. D. **Cibersegurança na Agricultura de Precisão: Exploração à Aplicação de Medidas Preventivas**. Advances in Global Innovation & Technology, v. 2, p. 61-73, 2024. Disponível

em: https://doi.org/10.29327/2384439.2.2-5. Acesso em 28 de maio 2024.

TSCHIEDEL, M.; FERREIRA, M. F. **Introdução à agricultura de precisão: conceitos e vantagens.** Ciência Rural, v. 32, p. 159-163, 2002. Disponível em: https://doi.org/10.1590/S0103-84782002000100027. Acesso em: 19 de abril 2024.

VICENTINE, A. L.; SILVA, G. C. M.; NASCIMENTO, J. P. D. G.; NEVES, J. E. D. Software anti-cheat. Revista Brasileira em Tecnologia da Informação, v. 4, p. 1-10, 2022. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/54. Acesso em: 28 maio 2024.

WEST, J. **A Prediction Model Framework for Cyber-Attacks to Precision Agriculture Technologies.** Journal of Agricultural & Food Information, v. 19, n. 4, p. 307-330, 2018. Disponível em: https://doi.org/10.1080/10496505.2017.1417859. Acesso em: 13 de maio 2024.

WINDOW, M. **Security in precision agriculture: Vulnerabilities and risks of agricultural systems**, p. 7, 2019. Disponível em: https://www.diva-portal.org/smash/resultList.jsf?query=+Security+in+precision+agriculture%3A+Vulnerabilities+and+risks+of+agricultural+systems%2C&language=en&searchType=SIMPLE&noOfRows=50&sortOrder=author_sort_asc&sortOrder2=title_sort_asc&onlyFullText=false&sf=all&aq=%5B%5B%5D%5D&aqe=%5B%5D&aq2=%5B%5B%5D%5D&af=%5B%5D. Acesso em: 13 de maio 2024.

WU, H. T.; TSAI, C. W. **An Intelligent Agriculture Network Security System Based on Private Blockchains.** Journal of Communications and Networks, v. 21, n. 5, p. 503-508, 2019. Disponível em: https://doi.org/10.1109/JCN.2019.000043. Acesso em: 13 de maio 2024.

YAZDINEJAD, A.; ZOLFAGHARI, B.; AZMOODEH, A.; DEHGHANTANHA, A.; KARIMIPOUR, H.; FRASER, E.; GREEN, A. G.; RUSSELL, C.; DUNCAN, E. **A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures.** Applied Sciences, v. 11, n. 16, p.7518, 2021. Disponível em: https://doi.org/10.3390/app11167518. Acesso em: 19 de abril 2024.