

Tecnologia e Riscos da Agricultura de Precisão: A Urgência da Cibersegurança no Campo

Technologies and Risks of Precision Agriculture: The Urgency of Cybersecurity in the Field

Tecnologías y Riesgos de la Agricultura de Precisión: La Urgencia de la Ciberseguridad en el Terreno

Recebido

Received

Recibido

12 mai. 2026

Aceito

Accepted

Aceptado

22 mai. 2026

Publicado

Published

Publicado

02 jun. 2026

<https://git.fateczl.edu.br>

e_ISSN

2965-3339

DOI

10.5281/zenodo.20332743

São Paulo

v. 4 | n. 3

v. 4 | i. 3

e43525

Abril-Junho

Abril-Junho

Abril-Junio

2026



Amanda Pereira de Freitas¹

amanda.freitas01@aluno.cps.sp.gov.br

Laryssa Meiryelle Martins¹

laryssa.martins@aluno.cps.sp.gov.br

Lucas de Paulo Perozzo¹

lucas.perozzo@aluno.cps.sp.gov.br

João Emmanuel D Alkmin Neves¹

joao.neves@cps.sp.gov.br

1 – Faculdade de Tecnologia de Americana “Ministro Ralph Biasi”.

Resumo:

O presente artigo tem como objetivo analisar as vulnerabilidades cibernéticas em dispositivos utilizados na agricultura de precisão (AP), identificando suas principais falhas de segurança e impactos no setor agrícola, com base em referências bibliográficas atualizadas. A pesquisa foi conduzida em caráter exploratório, por meio de revisão bibliográfica de estudos publicados nos últimos anos, selecionados com base em critérios de relevância, atualidade e confiabilidade das fontes. Os resultados apontam a ocorrência de vulnerabilidades associadas a ataques cibernéticos, capazes de comprometer a operação de sistemas agrícolas, a integridade dos dados e a tomada de decisão no campo. O estudo também aponta que a crescente adoção de tecnologias digitais no setor agrícola amplia a exposição a riscos cibernéticos, especialmente em ambientes com infraestrutura limitada e baixa maturidade em segurança da informação. Como contribuição, o artigo organiza os principais riscos associados à agricultura de precisão e reforça a necessidade de integração entre práticas de segurança da informação e a gestão tecnológica no setor. Conclui-se que a adoção de estratégias de segurança alinhadas às especificidades do ambiente agrícola é fundamental para garantir a proteção das informações e a continuidade das operações no campo.

Palavras-chave: Agricultura de Precisão; Ameaças Cibernéticas; Vulnerabilidades; Gestão de Riscos.

Abstract:

This article aims to analyze cyber vulnerabilities in devices used in precision agriculture (PA), identifying their main security flaws and impacts on the agricultural sector, based on updated bibliographic references. The research was conducted in an exploratory manner through a bibliographic review of studies published in recent years, selected according to criteria of relevance, timeliness, and reliability of sources. The results indicate the occurrence of vulnerabilities associated with cyberattacks that may compromise the operation of agricultural systems, data integrity, and decision-making Processes in the field. The study also highlights that the increasing adoption of digital technologies in agriculture expands exposure to cyber risks, especially in environments with limited infrastructure and low maturity in information security. As a contribution,

the article systematizes the main risks associated with precision agriculture and reinforces the need for integration between information security practices and technological management in the sector. It is concluded that the adoption of security strategies aligned with the specificities of the agricultural environment is essential to ensure information protection and operational continuity in the field.

Keywords: Precision Agriculture; Cyber Threats; Vulnerabilities; Risk Management.

Resumen:

Este artículo analiza las vulnerabilidades de ciberseguridad en dispositivos utilizados en la agricultura de precisión (AP), identificando sus principales fallos de seguridad e impactos en el sector agrícola, a partir de referencias bibliográficas actualizadas. La investigación se realizó de forma exploratoria, mediante una revisión bibliográfica de estudios publicados en los últimos años, seleccionados según criterios de relevancia, actualidad y fiabilidad de las fuentes. Los resultados indican la existencia de vulnerabilidades asociadas a ciberataques, capaces de comprometer el funcionamiento de los sistemas agrícolas, la integridad de los datos y la toma de decisiones en el campo. El estudio también señala que la creciente adopción de tecnologías digitales en el sector agrícola incrementa la exposición a riesgos de ciberseguridad, especialmente en entornos con infraestructura limitada y baja madurez en seguridad de la información. Como contribución, el artículo organiza los principales riesgos asociados a la agricultura de precisión y refuerza la necesidad de integrar las prácticas de seguridad de la información con la gestión tecnológica del sector. Concluye que la adopción de estrategias de seguridad alineadas con las especificidades del entorno agrícola es fundamental para garantizar la protección de la información y la continuidad de las operaciones en el campo.

Palabras clave: Agricultura de Precisión; Amenazas Cibernéticas; Vulnerabilidades; Gestión de Riesgos.

1. INTRODUÇÃO

Desde a década de 1950, a modernização da agricultura brasileira tem sido marcada pela mecanização e pela incorporação de tecnologias ao processo produtivo (Alves et al., 2005). Atualmente, o agronegócio representa um dos principais pilares da economia nacional, respondendo, em 2024, por 23,2% do Produto Interno Bruto (PIB) brasileiro (CNA Brasil, 2024). Diante do crescimento populacional global projetado para 2050, a produção agrícola torna-se estratégica para a economia e para a segurança alimentar mundial (Organização das Nações Unidas para Agricultura e Alimentação, 2009).

Nesse contexto, a Agricultura de Precisão (AP) consolida-se como uma abordagem voltada à otimização de recursos, ao aumento da produtividade e à sustentabilidade. Essa prática utiliza GPS, sensores, sistemas autônomos, veículos aéreos não tripulados e análise de dados para monitorar variáveis agrícolas e apoiar decisões no campo (Basso; Antle, 2020).

Entretanto, a digitalização do campo amplia a superfície de ataque cibernético. A dependência de Internet das Coisas (IoT), inteligência artificial e sistemas conectados expõe propriedades e empresas rurais a falhas que podem comprometer dados, equipamentos, cadeias produtivas e a continuidade operacional. Apesar do avanço das pesquisas sobre AP, ainda há lacunas quanto à integração entre segurança da informação e o ambiente rural brasileiro, especialmente em relação aos dispositivos IoT e à baixa maturidade em segurança digital.

Diante disso, formula-se o seguinte problema de pesquisa: quais são os principais riscos cibernéticos associados ao uso de tecnologias baseadas em IoT na Agricultura de Precisão no Brasil e quais estratégias podem ser adotadas para mitigá-los? Parte-se da hipótese de que a ausência de políticas estruturadas de segurança, somada à baixa capacitação técnica, contribui para o aumento dos riscos operacionais e econômicos (Bossoi et al., 2019).

O objetivo deste estudo é analisar e categorizar vulnerabilidades cibernéticas na Agricultura de Precisão e propor estratégias de mitigação alinhadas às boas práticas de segurança da informação, com foco no contexto brasileiro. A justificativa está na necessidade de garantir que a transformação digital do agronegócio ocorra de forma segura e sustentável, considerando ataques como DDoS, spoofing de GPS e ransomware (Zanella; Silva; Albini, 2020).

2. FUNDAMENTAÇÃO TEÓRICA

Distinta da agricultura convencional, que se baseia na aplicação uniforme de insumos em toda a área cultivada, a agricultura de precisão (AP) caracteriza-se como uma abordagem que visa o gerenciamento detalhado do sistema produtivo agrícola. Essa prática considera a variabilidade espacial e temporal das lavouras, permitindo a aplicação localizada de insumos, como fertilizantes, sementes, defensivos e água. Como resultado, promove ganhos econômicos e ambientais,

além de maior eficiência no uso de recursos (Artuzo et al., 2017; Bassoi et al., 2019; Molin et al., 2021).

O crescimento populacional mundial tem intensificado a demanda por alimentos, exigindo sistemas produtivos mais eficientes e sustentáveis. Nesse contexto, a adoção de tecnologias no campo torna-se essencial para o aumento da produtividade. A integração de dados em tempo real, aliada ao uso de equipamentos modernos e sistemas automatizados, contribui diretamente para a otimização da produção agrícola e redução de custos operacionais (Basso; Antle, 2020).

A evolução da agricultura está diretamente relacionada ao avanço tecnológico. A Agricultura 4.0 incorpora conceitos da Indústria 4.0, como automação, conectividade e análise de dados. Esse modelo permite a criação de sistemas inteligentes capazes de monitorar e responder às condições do ambiente em tempo real, promovendo maior eficiência e sustentabilidade (Dias et al., 2023).

2.1. Evolução da Agricultura de Precisão com a Introdução da Tecnologia

A agricultura de precisão resulta da integração entre práticas agrícolas tradicionais e tecnologias digitais. Segundo Gebbers e Adamchuk (2010), esse modelo funciona como um ciclo contínuo que envolve coleta de dados, análise, interpretação, tomada de decisão e aplicação no campo, seguido pela avaliação dos resultados.

A evolução da agricultura pode ser compreendida em diferentes fases. A Agricultura 1.0 foi marcada pelo trabalho manual e uso de tração animal, apresentando baixa produtividade. Posteriormente, a Agricultura 2.0 surgiu com a mecanização e o uso de insumos químicos, impulsionando a produção em larga escala (Queiroz et al., 2022).

Na década de 1990, a Agricultura 3.0 introduziu tecnologias digitais, como sensores, GPS e monitoramento remoto. Esse avanço possibilitou maior controle das variáveis agrícolas. Em seguida, a Agricultura 4.0 consolidou a integração entre automação, robótica e conectividade, permitindo o uso de dados em tempo real para tomada de decisão mais precisa (Dias et al., 2023).

Mais recentemente, a Agricultura 5.0 incorpora inteligência artificial, aprendizado de máquina e sistemas autônomos. Nesse modelo, decisões passam a ser orientadas por algoritmos, ampliando a eficiência produtiva e reduzindo desperdícios (Shepherd et al., 2018).

Apesar dos avanços, ainda existem desafios estruturais, como limitações de conectividade, falta de capacitação técnica e infraestrutura insuficiente no meio rural. Esses fatores dificultam a adoção plena das tecnologias digitais, evidenciando a necessidade de investimentos e políticas públicas (Bossoi et al., 2019).

2.2. O uso da IoT e os principais dispositivos aplicados na Agricultura de Precisão

A Internet das Coisas (IoT) representa um dos principais pilares da agricultura digital, permitindo a interconexão de dispositivos físicos, sensores e sistemas computacionais por meio da internet. De acordo com Mattern e Floerkemeier (2010), a IoT possibilita a comunicação entre objetos inteligentes capazes de coletar, processar e compartilhar dados de forma autônoma. Essa integração viabiliza a coleta, transmissão e análise de dados em tempo real, contribuindo diretamente para a tomada de decisão no ambiente agrícola.

A arquitetura da IoT pode ser compreendida em diferentes camadas funcionais. A camada de percepção é responsável pela coleta de dados por meio de sensores distribuídos no campo. A camada de rede realiza a transmissão dessas informações por meio de tecnologias de comunicação, como redes sem fio, satélites e internet móvel. Por fim, a camada de aplicação envolve o processamento dos dados, utilizando computação em nuvem e edge computing (computação de borda) permitindo análises em tempo real e maior eficiência operacional (Gupta, 2016).

Dentre os principais dispositivos utilizados na agricultura de precisão, destacam-se os sensores ambientais, responsáveis pelo monitoramento contínuo de parâmetros como umidade do solo, temperatura, pH e níveis de nutrientes. Além desses, veículos aéreos não tripulados (VANTs) são amplamente empregados, sendo equipados com sensores multiespectrais que permitem o imageamento e a análise detalhada das lavouras.

Também se destacam as estações meteorológicas automatizadas, que realizam a coleta e análise de dados climáticos em tempo real. No âmbito da mecanização, o maquinário agrícola autônomo, como tratores e implementos com sistemas de navegação por GPS e telemetria, tem ampliado a eficiência operacional no campo. Além disso, sistemas de irrigação inteligente utilizam dados provenientes de sensores para ajustar automaticamente a distribuição de água. Na pecuária, dispositivos vestíveis, como coleiras e chips com sensores biométricos, permitem o monitoramento da saúde e do comportamento animal.

A utilização desses dispositivos contribui para a redução do desperdício de recursos e para o aumento da produtividade. No entanto, a dependência de sistemas conectados também introduz desafios relacionados à segurança da informação, especialmente em ambientes com limitações de infraestrutura tecnológica (Zanella; Silva; Albini, 2020).

Além disso, a arquitetura distribuída da IoT amplia significativamente a superfície de ataque dos sistemas agrícolas. Dispositivos localizados na camada de percepção frequentemente operam em ambientes expostos, tornando-se vulneráveis a ataques físicos e digitais. Nas camadas de rede e aplicação, riscos como interceptação de dados, acesso não autorizado e falhas de comunicação podem comprometer o funcionamento dos sistemas.

Para análise dessas ameaças, destaca-se o modelo STRIDE, amplamente utilizado na identificação de riscos em sistemas computacionais. Esse modelo classifica as

ameaças em seis categorias: falsificação de identidade (spoofing), adulteração de dados (tampering), repúdio (repudiation), divulgação de informações (information disclosure), negação de serviço (denial of service) e elevação de privilégio (elevation of privilege). No contexto da agricultura de precisão, essas ameaças podem se manifestar na falsificação de dados de sensores, na interrupção de sistemas automatizados e no acesso indevido a informações estratégicas da produção.

Dessa forma, embora a IoT proporcione avanços significativos na agricultura de precisão, sua adoção exige a implementação de medidas de segurança adequadas. A proteção desses sistemas é essencial para garantir a confiabilidade das informações e a continuidade das operações no ambiente agrícola.

2.3. Ataques de cibersegurança na AP e a importância de investir em segurança digital

A aplicabilidade de blockchain na Agricultura de Precisão (AP) pode contribuir para a rastreabilidade e transparência nas transações entre produtores, fornecedores e clientes, além de auxiliar na autenticidade das informações sobre origem e qualidade dos produtos. Todavia, o uso dessas ferramentas e tecnologias, especialmente quando integradas a sistemas baseados em Internet das Coisas (IoT), traz um desafio crítico: a exposição significativa a ameaças cibernéticas. Embora promovam ganhos em eficiência, plataformas de gestão e sistemas conectados como sensores e dispositivos IoT tornam-se alvos vulneráveis a ataques sofisticados, conforme apontam Al Asif et al. (2022).

Nesse cenário, as ameaças podem atingir diferentes camadas do ecossistema tecnológico empregado na AP. Na camada de percepção, composta por sensores e atuadores em campo, há riscos relacionados à manipulação física e lógica dos dispositivos e à geração de leituras falsas. Na camada de rede, os ataques podem afetar a comunicação e o transporte de dados. Na camada edge (processamento intermediário próximo à fonte), acessos não autorizados e interceptações podem comprometer o tratamento dos dados. Já na camada de aplicação, onde as informações são utilizadas para decisões e rotinas operacionais, ataques podem comprometer usuários, sistemas e bases de dados.

Os principais ataques na AP incluem ransomware, phishing, negação de serviço (DDoS) e invasões a dispositivos IoT. O ransomware, conforme descrito por Braga et al. (2023), consiste em um artefato malicioso que restringe o acesso a um sistema, criptografando dados e bloqueando operações até que um resgate seja pago, mediante promessa de disponibilização de chaves de descryptografia. Já ataques de phishing utilizam mensagens fraudulentas para enganar usuários e obter senhas e dados confidenciais, elevando o risco de invasão (SNA Agronegócio, 2025). Ataques de DDoS, por sua vez, buscam impedir o acesso a serviços ao sobrecarregar recursos de rede e servidores, comprometendo a continuidade operacional. Adicionalmente, invasões e explorações de vulnerabilidades em dispositivos IoT podem permitir desde coleta indevida de dados até controle indevido de equipamentos e subsistemas, afetando diretamente a operação segura e a tomada de decisão no campo.

Esses incidentes afetam diretamente os princípios da segurança da informação, sintetizados na tríade CIA: confidencialidade, integridade e disponibilidade. A confidencialidade refere-se à proteção contra acessos não autorizados e vazamentos de informações sensíveis (por exemplo, dados de produção, logística e finanças). A integridade busca assegurar que os dados não sejam alterados indevidamente ao longo da coleta, transmissão e processamento (por exemplo, leituras de sensores adulteradas). A disponibilidade garante que sistemas e informações permaneçam acessíveis quando necessários, sendo fortemente impactada por ataques como DoS/DDoS e por falhas de conectividade (Nist, 2018).

Diante do exposto, é fundamental evidenciar a necessidade de estratégias de proteção. Investimentos em monitoramento de rede, auditorias de segurança e conscientização de colaboradores contribuem para aumentar a estabilidade e a resiliência das operações (Planeta Campo, 2024). Além disso, políticas de segurança da informação devem estabelecer normas, diretrizes e práticas adequadas ao contexto agrícola, considerando que propriedades rurais e empresas lidam diariamente com grandes volumes de dados sensíveis, como informações sobre safras, estoques, logística, contratos comerciais e dados financeiros (SNA Agronegócio, 2025).

Com a expansão das tecnologias no campo, a AP enfrenta dificuldades relacionadas à segurança digital. As ferramentas utilizadas também estão vulneráveis a ciberataques e aos problemas recorrentes de falta de conectividade. A seguir, apresentam-se os principais problemas de segurança na AP e suas consequências:

Interrupção de sistemas autônomos: modificação intencional dos recursos dos sistemas autônomos de drones, robôs e UAV (*unmanned aerial vehicles*), gerando operação inadequada, como paradas não programadas, colisões e destruição do campo.

Medição de dados irregulares: alteração dos dados obtidos pelo sistema, realizada incorretamente no implemento agrícola ou em nuvem, causando erro de leituras e estimativas de sementes, insumos, colheita e demais dados sobre o solo e atmosfera.

Ataques de DoS/DDoS: ataques que buscam impedir o acesso aos serviços dos dispositivos por meio de sobrecarga, causando, na maioria dos casos, parada total do sistema.

Controle de implementos forçado: acionamento indevido de sensores, pistões, dosadores e *sprayers*, provocando paradas e gastos irregulares de insumos.

Conectividade limitada no campo: ausência ou instabilidade de rede no ambiente rural, prejudicando sistemas que dependem de processamento em nuvem.

A tabela 1 apresenta os principais tipos de ataques praticados na AP.

Tabela 1 - Principais tipos de ataques

Percepção	Rede	Edge	Aplicação
Ativação randômica de sensores	DoS/DDoS	Acionamento de subsistemas	Phishing
Sequestro e interrupção de sistema autônomos	Interrupção de sinal	Man-in-the-Middle	Scripts maliciosos
Medidas incoerentes	Ataque de rotas	Acesso não autorizado	Não aplicação de boas práticas

Fonte: Elaborado pelos autores baseado em Zanella, Silva, Albini (2020)

Ao observar a Tabela 1, percebe-se que diferentes ameaças se concentram em pontos distintos do ecossistema: na percepção, ataques podem envolver ativação randômica de sensores, medições incoerentes e sequestro/interrupção de sistemas autônomos; na rede, destacam-se DoS/DDoS, interrupção de sinal e ataques de rotas; no edge, podem ocorrer acionamentos indevidos de subsistemas, Man-in-the-Middle e acessos não autorizados; e, na aplicação, aparecem phishing, scripts maliciosos e falhas decorrentes da não adoção de boas práticas. Isso reforça que a mitigação deve combinar controles técnicos (autenticação, criptografia, segmentação de rede, hardening, monitoramento) e medidas organizacionais (processos, políticas, treinamento e resposta a incidentes).

Para incentivar a adoção de tecnologias no campo, em 2022 foi sancionada a Lei 14.175/2022, que busca estimular agricultores a adotarem ferramentas e tecnologias para melhor aproveitamento do solo, uso de internet e satélites, incluindo máquinas agrícolas com sensores e softwares voltados à aplicação de sementes e defensivos e ao manejo racional do uso da terra. No entanto, para que haja maior contribuição com a sustentabilidade da produção agropecuária, é necessário que máquinas e equipamentos sejam adequados aos produtores e que haja capacitação para técnicos, produtores e prestadores de serviços adotarem as novas tecnologias disponíveis (Bossoi et al., 2019).

Nesse contexto, normas e frameworks fortalecem um plano estruturado de riscos e análise de vulnerabilidades. A ISO/IEC 27001 (Sistema de Gestão da Segurança da Informação) orienta a implementação de controles para tratar dados com confidencialidade, integridade e disponibilidade. De forma complementar, o framework do National Institute of Standards and Technology (NIST, 2018) contribui para uma postura proativa de segurança, apoiando avaliação contínua de riscos e adoção de controles de forma integrada. Além disso, a tecnologia blockchain pode atuar como mecanismo complementar de proteção, ao oferecer registros distribuídos e imutáveis, favorecendo rastreabilidade e integridade de informações em cadeias produtivas; entretanto, sua efetividade depende de boa governança, definição de acessos e integração com controles de segurança e processos operacionais.

Assim, compreender que a tecnologia é uma inovação constante e aplicar

segurança digital por meio da capacitação de usuários, investimento em ferramentas de proteção e execução de um plano de ação é crucial para reduzir ocorrências e minimizar vulnerabilidades nas estruturas de defesa da Agricultura de Precisão.

Salienta-se que não deve ter espaçamento entre o título da figura, tabela ou quadro e a figura, tabela ou quadro, seguindo o padrão das Figuras deste modelo, assim como não deve ter espaçamento entre a figura, tabela ou quadro e a fonte, quando houver. Deve-se deixar uma linha em branco antes do título da tabela e após a fonte. Conforme ocorre neste *template*, entre a Figura 2 e a Figura 3, só é permitido espaços em branco “órfãos” após uma figura e a página seguinte, se não houver como antecipar o que está disposto na página seguinte.

3. MÉTODO

A metodologia utilizada nesse artigo fundamenta-se em pesquisas bibliográficas e exploratórias de natureza integrativa. O conteúdo não fez uso de experimentações técnicas, sem o uso de aplicação prática e experimental, foi baseado em um conjunto de dados pesquisados e avaliados que trouxeram embasamento para toda a temática do artigo.

As publicações científicas, artigos acadêmicos, documentações técnicas e revistas especializadas foram selecionadas a partir do Google Acadêmico e sites com fontes confiáveis com combinações de palavras-chave como: Agricultura de Precisão, dispositivos de IoT agrícolas, vulnerabilidades e cibersegurança, que trouxeram relevância e amparo nas informações apresentadas. A fim de refinar a pesquisa foram usados operadores booleanos (AND, OR) e foram analisadas principalmente publicações entre 2019 e 2025, todavia foram consideradas publicações anteriores a esse período, trazendo embasamento para os conceitos clássicos e fundamentais do tema e a ascensão da agricultura digital.

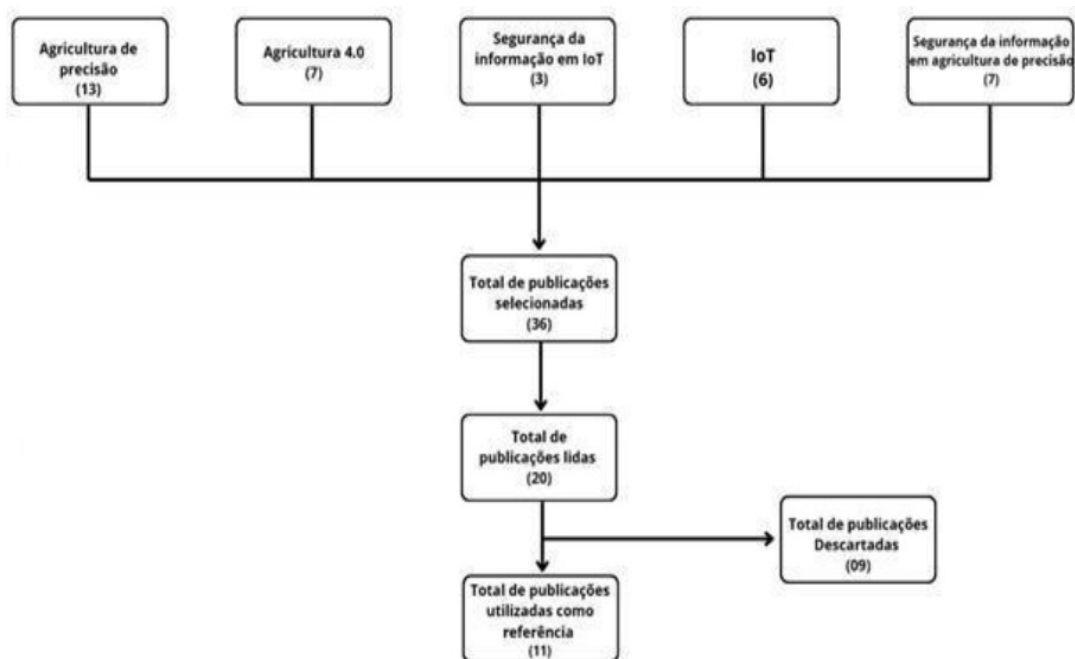
Houve o respaldo das normas de orientações e referências como ISO/IEC 27005 que trata da gestão de riscos de segurança da informação, e o NIST SP800-30 que traz orientações nos processos de análise e tratamento de riscos, conduzindo de forma qualitativa tais referências como: categorização e interpretação de riscos de segurança da informação, analíticos para identificação, construindo a discussão com instruções estabelecidas de gestão a avaliação de riscos.

As etapas foram organizadas conforme diagrama representado na Figura 1, definindo os descritivos de busca identificando 36 publicações. Em seguida foi realizada a triagem de publicações e títulos através da leitura exploratória, selecionando 20 estudos relevantes. Na sequência feita a leitura e parecer, levamos em consideração 11 estudos como base para fundamentação e discussão do artigo, desconsiderando então 9 publicações.

A figura 1 apresenta o processo de seleção das publicações utilizadas neste estudo, permitindo visualizar a filtragem das etapas realizadas, de identificação, filtragem e definição final dos trabalhos analisados, favorecendo a transparência e rastreabilidade do método adotado. O critério usado na triagem dos estudos,

foi baseado em inclusão e exclusão preliminarmente estabelecido. Foram incluídas publicações sobre temas diretos de Agricultura de Precisão, IoT, Agricultura 4.0 e segurança da informação, além de materiais disponíveis de fontes confiáveis. Trabalhos sem contribuição relevante ao tema, com abordagem limitada e sem alinhamento com a pesquisa foram excluídos, pois não tiveram relevância para a proposta do estudo.

Figura 1 – Diagrama do processo de seleção dos materiais utilizados.



Fonte: Elaborado pelos autores (2025).

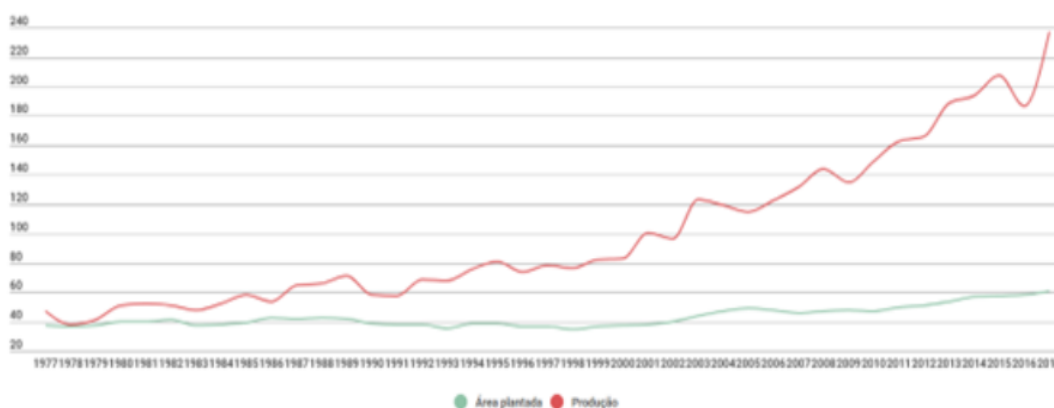
4. RESULTADOS E DISCUSSÃO

Conforme introduzido no início deste trabalho, a agricultura brasileira, vital para a economia e a segurança alimentar global, tem passado por um processo acelerado de modernização digital, materializado na expansão da Agricultura de Precisão (AP). Se, por um lado, esta pesquisa confirma que tal evolução foi impulsionada por incentivos legais e pela incorporação de tecnologias como IoT, drones e máquinas autônomas têm proporcionado ganhos inequívocos de produtividade, por outro, os resultados obtidos demonstram que a acelerada transformação digital no campo evidenciou um lado vulnerável e frequentemente negligenciado: a fragilidade cibernética inerente a esses novos paradigmas tecnológicos. A análise conduzida neste estudo revela que os riscos de segurança não são meramente teóricos, mas representam ameaças concretas e multifacetadas que podem comprometer a estabilidade operacional e a rentabilidade do setor. Esta pesquisa evidenciou que o setor de agricultura apresentou uma evolução significativa nas últimas décadas, usufruindo de incentivos nacionais como a Lei 14.475/2022, incorporando tecnologias como IoT, drones, sensores e máquinas autônomas, aumentando a produtividade de

sementes por hectare como demonstrado no Gráfico 1.

Contudo, a aceleração tecnológica também evidenciou graves vulnerabilidades. Dispositivos como sensores, smartphones e demais componentes de natureza frágil usados no campo os torna alvos suscetíveis. Essa fragilidade é particularmente crítica nos sensores integrados em Redes de Sensores Sem Fio (RSSF), utilizados na coleta de dados, frequentemente operam em locais não monitorados e desprovidos de segurança física. Essa condição os expõe a uma série de ameaças, que vão desde problemas ativos, como interferência intencional, até passivos, como o monitoramento indevido de informações (Hu; Sharma, 2017).

Gráfico 1 – Evolução da agricultura com a introdução das tecnologias.



Fonte: EMBRAPA (2018).

Não somente os sensores apresentam vulnerabilidades como toda a gama de novas tecnologias, os drones utilizados no monitoramento pode sofrer diversos ataques como dos mais básicos como ameaças baseadas no software exemplo: trojans, malwares, vírus, keyloggers, entre outros (Javaid et al., 2013).

Essa fragilidade inerente, somada à conectividade instável típica de zonas rurais, cria um ambiente propício a falhas e violações de segurança. A análise das fontes selecionadas revela que os principais riscos cibernéticos mapeados são:

- Ataques de Negação de Serviço (DDoS), que podem paralisar operações críticas;
- Violação de dados sensíveis da propriedade e da produção;
- Riscos de falha técnica e comportamento irregular de sistemas autônomos.

Os achados da revisão permitiram a organização das vulnerabilidades nas seguintes categorias, alinhadas aos critérios metodológicos estabelecidos:

Vulnerabilidade físicas e de infraestruturas: Natureza frágil de sensores sem fio e smartphones em locais não monitorados e desprovidos de barreiras físicas, além de conectividade instável e determinados locais.

Vulnerabilidade técnicas: Abrangem ameaças ativas e passivas, baseadas em software, como em drones, sensores, DDoS com o potencial e objetivo de paralisar operações e gerar leituras incorretas, além de poder causar acidentes

com a obstrução do sistema de navegação de sistema autônomos.

Vulnerabilidade Humana e socioeconômica: Foco principal na falta de conhecimento técnico e capacitação de uso de agricultores e operadores em geral, o que, pode causar problemas de segurança, problemas de conectividade e não adequação da infraestrutura existente, devido ao grande investimento inicial.

A falta de conhecimento técnico de muitos agricultores, custo elevados de entrada e a infraestrutura ineficiente ainda está sendo um obstáculo para esta tecnologia, entretanto podemos considerar nesse ponto que a educação dos agricultores em questões de treinamentos básicos a respeito de segurança dos equipamentos utilizados pode ser um ponto norteante a respeito da segurança da informação dentro da AP.

Estes desafios exigem abordagem integrada e urgente, contemplando três dimensões principais: inovação tecnológica (desenvolvimento de soluções acessíveis e resilientes), gestão de riscos (implementação de protocolos de segurança específicos para o agronegócio) e desenvolvimento profissional (programas de treinamento contínuo).

A revisão evidenciou que a modernização digital da agricultura brasileira introduziu vulnerabilidades que comprometem a segurança cibernética do setor. As vulnerabilidades técnicas (ataques DDoS e falhas em sistemas autônomos) ameaçam a continuidade operacional; as vulnerabilidades físicas e de infraestrutura (conectividade precária) ampliam a exposição a incidentes; e as vulnerabilidades humanas e socioeconômicas (falta de capacitação) dificultam a adoção de práticas de segurança. Conclui-se que a segurança na AP demanda abordagem integrada, contemplando soluções tecnológicas, adequações de infraestrutura em campo e capacitação de agricultores e operadores.

5. CONSIDERAÇÕES FINAIS

A AP representa uma das maiores revoluções tecnológicas no setor agropecuário, proporcionando ganhos em produtividade e eficiência no uso de recursos naturais. No entanto, a crescente dependência de tecnologias conectadas amplia os riscos cibernéticos, como em sensores, IoT, drones e sistemas autônomos.

O estudo demonstrou que apesar dos avanços tecnológicos, a segurança da informação ainda é negligenciada na adoção da Agricultura de Precisão no Brasil. As principais vulnerabilidades identificadas na revisão foram: conectividade limitada, falta de capacitação técnica, ausência de políticas públicas voltadas à segurança digital no campo e vulnerabilidades inerentes a sistemas integrados. Esses fatores tornam o setor exposto a ameaças como ataques DDoS, interceptação de dados, e mau funcionamento de dispositivos críticos.

Diante deste cenário, políticas integradas são necessárias. Elas devem combinar investimentos em infraestrutura digital, capacitação e boas práticas de segurança cibernética meio rural. A segurança da informação constitui um componente essencial da inovação no campo, não um elemento periférico.

Garantir a proteção dos sistemas e dados agrícolas deve ser tratado como questão estratégica, essencial para garantir a continuidade das operações e a sustentabilidade da agricultura conectada.

REFERÊNCIAS

AL ASIF, M. R.; HASAN, K. F.; ISLAM, M. Z.; KHONDOKER, R. **STRIDE-based cyber security threat modeling for IoT-enabled precision agriculture systems**. *arXiv*, 2022. Disponível em: <https://arxiv.org/abs/2201.09493>. Acesso em: 13 nov. 2025.

ALVES, E.; CONTINI, E.; HAINZELIN, E. **Transformações da agricultura brasileira e pesquisa agropecuária**. *Cadernos de Ciência & Tecnologia*, v. 22, n. 1, p. 37–51, 2005. Disponível em: <https://www.embrapa.br/busca-de-publicacoes/-/publicacao/1070076/transformacoes-da-agricultura-brasileira-e-pesquisa-agropecuaria>. Acesso em: 6 jun. 2025.

BASSO, B.; ANTLE, J. **Digital agriculture to design sustainable agricultural systems**. *Nature Sustainability*, v. 3, n. 4, p. 254–256, 2020. DOI: <https://doi.org/10.1038/s41893-020-0510-0>. Disponível em: <https://www.nature.com/articles/s41893-020-0510-0>. Acesso em: 7 jun. 2025.

BOSSOI, L. H.; INAMASU, R. Y.; BERNARDI, A. C. C.; VAZ, C. M. P.; SPERANZA, E. A.; CRUVINEL, P. E. **Agricultura de precisão e agricultura digital**. *TECCOGS: Revista Digital de Tecnologias Cognitivas*, n. 20, p. 17–36, 2019. Disponível em: <https://revistas.pucsp.br/index.php/teccogs/article/view/48542/32042>. Acesso em: 7 jun. 2025.

BRASIL. **Ministério da Agricultura e Pecuária. Conceitos relacionados à agricultura de precisão**. Brasília: MAPA, [s.d.]. Disponível em: <https://www.gov.br/agricultura/pt-br/assuntos/sustentabilidade/tecnologia-agropecuaria/agricultura-de-precisao-1/arquivos-de-agricultura-de-precisao/conceitos-relacionados-a-agricultura-de-precisao-1.pdf>. Acesso em: 7 jun. 2025.

CNA BRASIL. **Desempenho do quarto trimestre reverte a tendência de queda anual e PIB do agronegócio avança 1,81% em 2024**. Brasília: CNA, 2024. Disponível em: <https://www.cnabrazil.org.br/publicacoes/desempenho-do-quarto-trimestre-reverte-a-tendencia-de-queda-anual-e-pib-do-agronegocio-avanca-1-81-em-2024>. Acesso em: 14 nov. 2025.

DIAS, E. M. *et al.* (org.). **Agro 4.0: fundamentos, realidades e perspectivas para o Brasil**. Rio de Janeiro: Autografia, 2023. Disponível em: <https://cnabrazil.org.br/storage/arquivos/DCPV/files/Agro4.0-livro.pdf>. Acesso em: 6 jun. 2025.

FERRAZ SILVA, A. L.; SANTOS LIMA SILVA, D.; MENDONÇA, J. K.; NEVES, J. E. D. **Segurança da informação em função de tecnologias emergentes na agricultura de precisão**. *FatecSeg - Congresso de Segurança da Informação*, v. 1, 2024. Disponível em: <https://fatecseg.fatecourinhos.edu.br/index.php/fatecseg/article/view/215>. Acesso em: 6 out. 2025.

GEBBERS, R.; ADAMCHUK, V. I. **Precision agriculture and food security.** *Science*, v. 327, n. 5967, p. 828–831, 2010. DOI: <https://doi.org/10.1126/science.1183899>. Disponível em: <https://www.science.org/doi/10.1126/science.1183899>. Acesso em: 6 jun. 2025.

GOMES, J. A. **Agricultura de precisão: guia completo – da teoria à prática.** Agroadvance, 2024. Disponível em: <https://agroadvance.com.br/blog-guia-da-agricultura-de-precisao/>. Acesso em: 7 jun. 2025.

GUPTA, R.; GUPTA, R. **ABC of Internet of Things: advancements, benefits, challenges, enablers and facilities of IoT.** In: SYMPOSIUM ON COLOSSAL DATA ANALYSIS AND NETWORKING (CDAN), 2016, Indore. *Proceedings [...]*. [S.l.]: IEEE, 2016. p. 1–5. Disponível em: <https://ieeexplore.ieee.org/abstract/document/7570875>. Acesso em: 4 jun. 2025.

HU, F.; SHARMA, N. K. **Security considerations in wireless sensor networks.** *Ad Hoc Networks*, v. 3, n. 1, p. 69–89, jan. 2005. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1570870504000034>. Acesso em: 16 out. 2025.

JAVOID, A. Y.; SUN, W.; DEVABHAKTUNI, V. K.; ALAM, M. **Cyber security threat analysis and modeling of an unmanned aerial vehicle system.** In: INTERNATIONAL CONFERENCE ON COMPUTING, NETWORKING AND COMMUNICATIONS (ICNC), 2013, San Diego, CA. *Anais [...]*. San Diego, CA: IEEE, 2013. p. 214–218. Disponível em: <https://ieeexplore.ieee.org/abstract/document/6459914>. Acesso em: 16 out. 2025.

MACHADO, L. **Ataques cibernéticos no agro: quais impactos e como se proteger.** Sociedade Nacional da Agricultura, 2025. Disponível em: <https://www.sna.agr.br/ataques-ciberneticos-no-agro-quais-impactos-e-como-se-proteger/>. Acesso em: 12 out. 2025.

MATTERN, F.; FLOERKEMEIER, C. **From the Internet of Computers to the Internet of Things.** In: SACHS, K.; PETROV, I.; GUERRERO, P. (ed.). *From Active Data Management to Event-Based Systems and More*. Berlin: Springer, 2010. (Lecture Notes in Computer Science, v. 6462). p. 242–259. Disponível em: <http://hdl.handle.net/20.500.11850/159653>. Acesso em: 31 mar. 2026.

MELO, M.; COSTA, K. S. Q.; VAZ, C.; OLIVEIRA, C.; MELO, N.; MORAES, F. **Importância da agricultura de precisão para a eficiência da produção agrícola: uma revisão.** *Contribuciones a las Ciencias Sociales*, v. 17, e6760, 2024. DOI: <https://doi.org/10.55905/revconv.17n.5-102>. Disponível em: <https://www.eumed.net/rev/revconv/17/importancia-agricultura-precisao.html>. Acesso em: 4 out. 2025.

NANNINI, G. **Roubo de dados, máquinas invadidas: como o agro tem se tornado alvo de cibercriminosos.** Planeta Campo, 2024. Disponível em: <https://planetacampo.canalrural.com.br/agricultura/como-o-agro-tornou-se-alvo-de-cibercriminosos/>. Acesso em: 13 out. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Framework for improving critical infrastructure cybersecurity.** Version 1.1. Gaithersburg, MD: U.S. Department of Commerce, 2018. Disponível em:

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>. Acesso em: 18 out. 2025.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA AGRICULTURA E ALIMENTAÇÃO. **How to feed the world in 2050**. Roma: FAO, 2009. Disponível em: https://www.fao.org/fileadmin/templates/wsfs/docs/expert_paper/How_to_Feed_the_World_in_2050.pdf. Acesso em: 9 jun. 2025.

QUEIROZ, D. M.; VALENTE, D. S. M.; PINTO, F. A. C.; BORÉM, A. (ed.). **Agricultura digital**. São Paulo: Oficina de Textos, 2021. Disponível em: <https://books.google.com.br/books?id=9ehvEAAAQBAJ>. Acesso em: 7 jun. 2025.

SHEPHERD, M. *et al.* **Priorities for science to overcome hurdles thwarting the full promise of the ‘digital agriculture’ revolution**. *Journal of the Science of Food and Agriculture*, v. 100, n. 14, p. 5083–5092, 2020. DOI: <https://doi.org/10.1002/jsfa.9346>. Disponível em: <https://onlinelibrary.wiley.com/doi/10.1002/jsfa.9346>. Acesso em: 5 jun. 2025.

SILVA, D. A.; RIBEIRO, M. C. **A influência da agricultura de precisão na qualidade e segurança dos alimentos no mercado brasileiro**. *Direito em Foco*, n. 15, p. 733–750, 2023. Disponível em: <https://portal.unisepe.com.br/unifia/wp-content/uploads/sites/10001/2023/11/A-INFLU%C3%8ANCIA-DA-AGRICULTURA-DE-PRECIS%C3%83O-NA-QUALIDADE-E-SEGURAN%C3%87A-DOS-ALIMENTOS-NO-MERCADO-BRASILEIRO-p%C3%A1g-733-%C3%A0-750.pdf>. Acesso em: 4 jun. 2025.

UNISCED – UNIVERSIDADE ABERTA DO ISCED. **Transferência de tecnologia na agricultura 4.0**. Maputo: Universidade Aberta do ISCED, 2025. Disponível em: https://biblioteca.unisced.edu.mz/bitstream/123456789/3447/1/Transferencia_de_tecnologia_na_agricultura_40.pdf. Acesso em: 7 jun. 2025.

ZANELLA, A.; SILVA, L.; ALBINI, A. **Security challenges to smart agriculture: current state, key issues and future directions**. *Journal of Cybersecurity and Privacy*, v. 1, n. 1, 2020. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2590005620300333>. Acesso em: 6 jun. 2025

"Os conteúdos expressos no trabalho, bem como sua revisão ortográfica e das normas ABNT são de inteira responsabilidade do(s) autor(es)."

"Declara-se pelos autores que durante a preparação deste trabalho foi utilizado o serviço ChatGPT da OpenAI para esclarecimento, auxílio na formatação de trechos do texto e sugestões de redação. Após utilizar esta ferramenta/serviço, os autores editaram e revisaram o conteúdo conforme necessário e assumem total responsabilidade pelo conteúdo da publicação."

