



Doi: <https://doi.org/10.70577/asce.v5i1.675>

Recibido: 2026-01-05

Aceptado: 2026-01-12

Publicado: 2026-02-18

Aplicación de la Inteligencia Artificial y la Agromática en la Ciberseguridad de Infraestructuras Agropecuarias en Contextos Regionales

Application of Artificial Intelligence and Agromatics in the Cybersecurity of Agricultural Infrastructures in Regional Contexts

Autores

Angel Alberto Arce Ramírez¹

aarce@uagraria.edu.ec

<https://orcid.org/0000-0002-4421-6589>

Universidad Agraria del Ecuador
Ecuador

Daniel Adolfo Bustamante Villamar²

elturcobustamante@gmail.com

<https://orcid.org/0009-0008-4366-7864>

Universidad Casa Grande
Ecuador

Anggie Katherine Meza Nieto³

ameza@uagraria.edu.ec

<https://orcid.org/0009-0004-9861-4955>

Universidad Agraria del Ecuador
Ecuador

Cómo citar

Arce Ramírez, A. A., Bustamante Villamar, D. A., & Meza Nieto, A. K. (2026). Aplicación de la Inteligencia Artificial y la Agromática en la Ciberseguridad de Infraestructuras Agropecuarias en Contextos Regionales. *ASCE MAGAZINE*, 5(1), 1872–1893.

Resumen

La creciente digitalización del sector agropecuario ha incrementado la dependencia de infraestructuras inteligentes basadas en IoT, edge computing e inteligencia artificial, transformando los sistemas productivos tradicionales en ecosistemas agro-digitales interconectados. Sin embargo, esta evolución tecnológica amplía significativamente la superficie de exposición a amenazas cibernéticas, particularmente en entornos rurales donde la infraestructura y la gobernanza digital presentan limitaciones estructurales. El presente estudio propone y valida una arquitectura híbrida basada en modelos de aprendizaje profundo, edge computing y mecanismos de integridad descentralizada para fortalecer la ciberseguridad en infraestructuras agropecuarias regionales. Se desarrolló un entorno simulado (testbed) que integra sensores IoT agrícolas y redes críticas, evaluándose modelos CNN-LSTM y autoencoders entrenados con datasets CIC-DDoS2019 y TON-IoT. Los resultados evidencian niveles de detección superiores al 98 %, con latencias adecuadas para operación en entornos con conectividad limitada. Los hallazgos confirman que la integración de inteligencia artificial en el borde mejora la resiliencia operativa y reduce la dependencia de infraestructura centralizada, lo que resulta estratégico para regiones rurales en proceso de transformación digital. Se concluye que la ciberseguridad debe incorporarse como componente estructural de la agricultura inteligente, articulando innovación tecnológica, gobernanza de datos y desarrollo sostenible.

Palabras clave: Agricultura digital, Ciberseguridad, Sistemas de información agropecuarios, Protección de datos, Transformación digital rural

Abstract

The increasing digitalization of the agricultural sector has intensified dependence on intelligent infrastructures based on IoT, edge computing, and artificial intelligence, transforming traditional production systems into interconnected agro-digital ecosystems. However, this technological evolution significantly expands the exposure surface to cyber threats, particularly in rural environments where infrastructure and digital governance present structural limitations. This study proposes and validates a hybrid architecture based on deep learning models, edge computing, and decentralized integrity mechanisms to strengthen cybersecurity in regional agricultural infrastructures. A simulated environment (testbed) was developed integrating agricultural IoT sensors and critical networks, evaluating CNN–LSTM models and autoencoders trained with the CIC-DDoS2019 and TON-IoT datasets. The results demonstrate detection levels exceeding 98%, with latency values suitable for operation in environments with limited connectivity. The findings confirm that integrating artificial intelligence at the edge enhances operational resilience and reduces reliance on centralized infrastructure, which is strategically relevant for rural regions undergoing digital transformation. It is concluded that cybersecurity must be incorporated as a structural component of smart agriculture, articulating technological innovation, data governance, and sustainable development.

Keywords: Digital agriculture, Cybersecurity, Agricultural Information systems, Data protection, Rural digital transformation

Introducción

La transformación digital del sector agropecuario genera una reconfiguración profunda de los sistemas de producción, comercialización y gestión en el agro. Este proceso impulsa el uso de tecnologías como sensores IoT, drones, plataformas de agricultura de precisión y sistemas de información geoespacial. Esta evolución, enmarcada en la agricultura digital o Agricultura 4.0, tiene como propósito aumentar la productividad, reducir impactos ambientales y optimizar el uso de recursos. En este escenario, la agromática, entendida como la aplicación de las tecnologías de la información y la comunicación al ámbito agropecuario, constituye un pilar estratégico para la toma de decisiones basada en datos en tiempo real, especialmente en regiones rurales con limitaciones estructurales.

Los conocimientos agrícolas tradicionales e inteligentes mantienen un papel central en muchas regiones. Los pequeños agricultores, que administran la mayoría de las explotaciones agrícolas a nivel mundial, aún carecen de infraestructura tecnológica suficiente para automatizar plenamente sus procesos, aunque incorporan herramientas digitales de forma progresiva. Las haciendas de mayor escala también obtienen beneficios al integrar prácticas tradicionales con soluciones tecnológicas avanzadas. Diversos estudios destacan la incorporación de técnicas de agricultura de precisión, como IoT, aprendizaje automático e inteligencia artificial, para mejorar la productividad y la sostenibilidad agrícola (Kumar & Faisal, 2024).

Sin embargo, la expansión de los sistemas agro-digitales incrementa la superficie de exposición a riesgos cibernéticos. Esta situación compromete tanto la integridad de los datos como la operatividad de los sistemas de control agrícola. Las amenazas incluyen vulnerabilidades en sensores de riego inteligente, accesos no autorizados a plataformas de gestión y sabotajes a infraestructuras críticas. Tales incidentes afectan la trazabilidad, generan incertidumbre en la cadena productiva y pueden incidir en la seguridad alimentaria. A diferencia de otros sectores industriales con marcos normativos consolidados, la ciberseguridad en el agro recibe históricamente menor atención, lo que convierte al sector en un entorno especialmente vulnerable (Santos Vidal, 2022).

Ante este escenario, la inteligencia artificial adquiere relevancia como herramienta para fortalecer la seguridad de infraestructuras digitales agroganaderas. Zangana et al. (2025)

señalan que los algoritmos de aprendizaje automático, las redes neuronales y los modelos de detección de anomalías permiten identificar comportamientos sospechosos, anticipar vulnerabilidades y ejecutar respuestas automatizadas frente a incidentes. Estas capacidades mejoran la eficiencia en la gestión de eventos de seguridad y facilitan la adaptación de soluciones a contextos regionales con limitaciones tecnológicas y económicas.

En países en vías de desarrollo, donde las brechas digitales rurales presentan un carácter estructural, resulta indispensable establecer políticas y arquitecturas de ciberseguridad inclusivas. Tales enfoques deben priorizar la formación de capacidades humanas, el fortalecimiento institucional y la soberanía tecnológica (Romero, 2024). En este sentido, la protección de activos digitales no constituye únicamente una estrategia técnica de mitigación de riesgos, sino un componente transversal del desarrollo sostenible rural.

El presente artículo examina los fundamentos conceptuales, el estado actual y el potencial de la integración entre inteligencia artificial y agromática para fortalecer la ciberseguridad agropecuaria, con énfasis en contextos regionales vulnerables. Asimismo, propone lineamientos estratégicos orientados a una implementación sostenible y resiliente, en coherencia con los Objetivos de Desarrollo Sostenible (Valle-Lituma et al., 2026).

Marco Teórico

Para la elaboración del estado del arte se han identificado estudios relacionados con la temática de la presente investigación, lo que incluye la robótica y la automatización, las cuales han revolucionado la agricultura al mejorar la eficiencia, sostenibilidad y productividad de los sistemas agrícolas. El informe de la FAO analiza su aplicación en países en desarrollo, esto evidencia oportunidades, desafíos y contribuciones al desarrollo sostenible.

El informe de la FAO "Agricultura 4.0: Robótica Agrícola y Equipos Automatizados para la Producción Agrícola Sostenible" examina las oportunidades y problemas que las nuevas tecnologías como la robótica, la automatización y la agricultura de precisión traen para transformar los sistemas agrícolas en unos más sostenibles, en los países en desarrollo (FAO, 2020). Mediante una revisión técnica y documental de casos prácticos, iniciativas institucionales y tendencias globales, se examina el potencial de estas

tecnologías para mejorar la eficiencia productiva, reducir la carga laboral, optimizar el uso de insumos agrícolas y contribuir a la sostenibilidad ambiental.

Entre los principales hallazgos se destacan la capacidad de la robótica para aumentar la productividad en sistemas sin laboreo, reducir el trabajo pesado y crear oportunidades para jóvenes y mujeres rurales mediante modelos de arrendamiento o servicios compartidos, así como su aporte directo al cumplimiento de varios Objetivos de Desarrollo Sostenible. No obstante, el informe también subraya limitaciones importantes, como el elevado costo de adquisición, la falta de infraestructura de tecnologías de la información y la necesidad urgente de generar capacidades técnicas y marcos regulatorios que garanticen una adopción ética y equitativa de estas innovaciones (Facuy et al., 2026).

Tanto la robótica agrícola como la aplicación de la inteligencia artificial y la agromática representan pilares fundamentales de la agricultura 4.0, cada uno con un enfoque complementario hacia la modernización del sector agropecuario. Mientras la robótica y los equipos automatizados permiten optimizar las labores agrícolas, mejorar la eficiencia y promover la sostenibilidad de la producción, la inteligencia artificial y la agromática fortalecen la ciberseguridad y la resiliencia digital de las infraestructuras agropecuarias, en contextos regionales con limitaciones tecnológicas. La integración de ambas dimensiones es indispensable para garantizar una transformación agrícola efectiva, segura e inclusiva, que responda tanto a los desafíos productivos como a los riesgos digitales del entorno rural actual.

La creciente digitalización en todos los sectores del Ecuador ha incrementado la exposición a amenazas cibernéticas que comprometen la seguridad nacional. En respuesta, se establece una política de ciberseguridad orientada a proteger infraestructuras críticas y activos de información del Estado (Castillo Gómez, 2023). El Acuerdo No. 006-2021 - Política de Ciberseguridad del Ecuador tiene como objetivo establecer un marco normativo y estratégico que permita garantizar la protección de los activos de información, las infraestructuras críticas y los sistemas tecnológicos del país frente a amenazas cibernéticas, lo que promueve un entorno digital confiable, resiliente y soberano (Neira et al., 2023). La metodología utilizada para la formulación de esta política se basó en el análisis de estándares internacionales (como ISO/IEC 27001 y el marco NIST), evaluaciones de riesgo a nivel nacional, y la participación articulada de instituciones públicas, privadas y académicas. Entre los principales hallazgos se destaca

la necesidad de fortalecer la gobernanza de la ciberseguridad, definir los roles institucionales, promover una cultura de prevención y respuesta ante incidentes, e impulsar el desarrollo de capacidades técnicas, así como la cooperación internacional. El documento identifica además la urgencia de consolidar un ecosistema digital robusto que responda a los desafíos actuales en materia de protección de la información, en sectores estratégicos y servicios esenciales.

En el Ecuador no existe una política de ciberseguridad aplicada a la inteligencia artificial y la agromática la cual debería abordar dimensiones complementarias de la protección digital. Mientras la política nacional establece un marco normativo, estratégico e institucional para resguardar los activos de información a nivel país, la propuesta agropecuaria se enfoca en aplicar soluciones tecnológicas inteligentes y adaptadas a las condiciones rurales, donde las vulnerabilidades son más evidentes. La articulación entre ambos enfoques resulta fundamental para construir un ecosistema de ciberseguridad integral, que no solo fortalezca la infraestructura crítica nacional, sino que también garantice la protección y sostenibilidad tecnológica del sector agropecuario en contextos regionales (Freyhof et al., 2025).

Según Urjilez y otros (2025) la agricultura de precisión se presenta como una herramienta clave para optimizar la producción de cultivos en zonas ambientales sensibles. Su aplicación en áreas protegidas permite equilibrar la eficiencia agrícola con la conservación de los ecosistemas. El artículo titulado “Implementación de la agricultura de precisión a través del desarrollo de sistemas productivos en áreas protegidas o de conservación para optimizar la producción de cultivos tiene como objetivo analizar, mediante una revisión sistemática de literatura”, detalla cómo la agricultura de precisión puede ser implementada en zonas sensibles con el fin de mejorar la eficiencia productiva sin comprometer la conservación del entorno. La metodología consistió en la búsqueda, selección y análisis crítico de investigaciones científicas publicadas entre 2015 y 2021, utiliza criterios de inclusión relacionados con el uso de tecnologías como sensores, sistemas de información geográfica (SIG), imágenes satelitales y análisis de datos aplicados a sistemas agrícolas en áreas protegidas (Alvarez et al., 2022). Entre los principales hallazgos, se destaca que la agricultura de precisión permite reducir el impacto ambiental, optimizar el uso de recursos y aumentar el rendimiento en cultivos localizados en zonas de conservación, siempre que exista una adecuada planificación territorial,

infraestructura tecnológica y capacitación técnica. El estudio concluye que la implementación de estas tecnologías representa una oportunidad viable para equilibrar la producción agrícola con la preservación ecológica.

Tanto la implementación de la agricultura de precisión en áreas protegidas como la aplicación de la inteligencia artificial y la agromática en la ciberseguridad agropecuaria abordan dimensiones complementarias del desarrollo tecnológico en el sector agrícola. La primera busca maximizar la eficiencia productiva sin comprometer la conservación ambiental, mientras que la segunda garantiza la protección de las infraestructuras digitales que sostienen esa innovación, en contextos regionales con vulnerabilidades técnicas. La integración de estos enfoques permite avanzar hacia un modelo agropecuario sostenible, resiliente y con tecnología segura, alineado con las demandas actuales de productividad, conservación y transformación digital del campo.

El estudio realizado en India propone un sistema híbrido de detección de intrusos (IDS) que integra un autocodificador profundo (dAE) para la clasificación binaria y un agrupamiento espacial jerárquico basado en densidad de aplicaciones con ruido (HDBSCAN) para el agrupamiento multiclase. El marco metodológico propuesto explota los datos del mundo real del conjunto de datos CIC-DDoS2019 para detectar ataques DDoS, evalúa los modelos de autocodificador junto con HDBSCAN. Los autores demuestran que este enfoque combinado demuestra capacidades efectivas de clasificación y detección de amenazas, lo que evidencia niveles de precisión superiores al 98%, esto mejora la ciberseguridad de la agricultura 4.0, esto promueve prácticas agrícolas sólidas, informadas por datos y eficientes, al tiempo que se alinea con los Objetivos de Desarrollo Sostenible (ODS) relacionados con la innovación industrial y la resiliencia (Kaliyaperumal et al., 2025).

En conclusión, tanto la aplicación de la inteligencia artificial orientada a la productividad sustentable como su integración con la agromática para fortalecer la ciberseguridad agropecuaria constituyen estrategias clave para el desarrollo tecnológico del sector agropecuario en el Ecuador. Mientras la primera permite optimizar los procesos productivos, mejorar el uso de recursos y aumentar los rendimientos de forma sostenible, la segunda garantiza la protección de las infraestructuras digitales, la integridad de los datos y la continuidad operativa en contextos rurales. La convergencia de ambos enfoques no solo impulsa la eficiencia y sostenibilidad del agro, sino que también asegura que la

transformación digital del campo ecuatoriano se desarrolle sobre bases seguras, resilientes e inclusivas.

La inteligencia artificial ha revolucionado el sector agrícola al ofrecer soluciones avanzadas para optimizar la producción, el manejo de cultivos y la sostenibilidad. Este estudio analiza su potencial aplicación en distintas áreas clave de la agricultura moderna. El artículo *Understanding the Potential Applications of Artificial Intelligence in Agriculture Sector* tiene como objetivo explorar las diversas aplicaciones de la inteligencia artificial (IA) en el sector agrícola, evalúa su potencial para transformar la productividad, eficiencia y sostenibilidad de los sistemas agropecuarios. La metodología consistió en una revisión documental y analítica de estudios recientes, tecnologías emergentes y casos de implementación de IA en áreas clave como la agricultura de precisión, el monitoreo de cultivos, la detección de plagas y enfermedades, y la automatización de maquinaria agrícola (Javaid et al., 2023).

Entre los principales hallazgos, se destaca que la IA permite optimizar la toma de decisiones agrícolas mediante el análisis de datos masivos, mejora el rendimiento de los cultivos al predecir condiciones ambientales y fitosanitarias, y reduce el uso innecesario de insumos agrícolas. Asimismo, se identifican desafíos importantes como el acceso limitado a infraestructura digital, la necesidad de datos locales de calidad y la capacitación técnica en zonas rurales. El estudio concluye que, si bien la IA representa una oportunidad transformadora para el agro, su adopción efectiva requiere inversión, políticas públicas inclusivas y desarrollo de capacidades en el territorio.

Los dos enfoques analizados demuestran que la inteligencia artificial desempeña un papel fundamental en la transformación del sector agropecuario, tanto en términos de productividad como de seguridad digital (Aguirre-Munizaga et al., 2025). Mientras que el estudio sobre las aplicaciones potenciales de la IA en la agricultura resalta su capacidad para optimizar procesos productivos, mejorar el uso de recursos y fomentar la sostenibilidad, la propuesta centrada en la ciberseguridad agropecuaria evidencia la necesidad de proteger las infraestructuras digitales que sustentan estos avances tecnológicos, especialmente en regiones con limitaciones técnicas. La convergencia de ambos enfoques resulta estratégica para consolidar un modelo de agricultura inteligente, eficiente, resiliente y seguro, que responda a los desafíos actuales del agro ecuatoriano y regional.

Material y métodos

La investigación se desarrolló bajo un enfoque cuantitativo con alcance aplicado y explicativo, orientado al análisis técnico de la integración entre inteligencia artificial y agromática en la ciberseguridad de infraestructuras agropecuarias regionales. El diseño correspondió a una modalidad experimental con simulación controlada mediante un entorno de prueba (testbed), lo que permitió evaluar el desempeño de modelos de detección de anomalías en escenarios representativos de agricultura inteligente.

El tipo de investigación fue tecnológico-experimental, ya que se diseñó y validó una arquitectura híbrida basada en aprendizaje automático y edge computing. El método empleado combinó revisión sistemática de literatura, modelado de amenazas y validación experimental. Como instrumentos se utilizaron datasets especializados en ciberseguridad (CIC-DDoS2019 y TON-IoT), bibliotecas de aprendizaje automático en Python, frameworks de redes neuronales profundas y herramientas de análisis de tráfico de red. Se incorporaron sensores IoT simulados de temperatura, humedad, pH, luminosidad y clorofila, además de una infraestructura de red representativa de entornos rurales con procesamiento en el borde (Facuy Toledo, 2024).

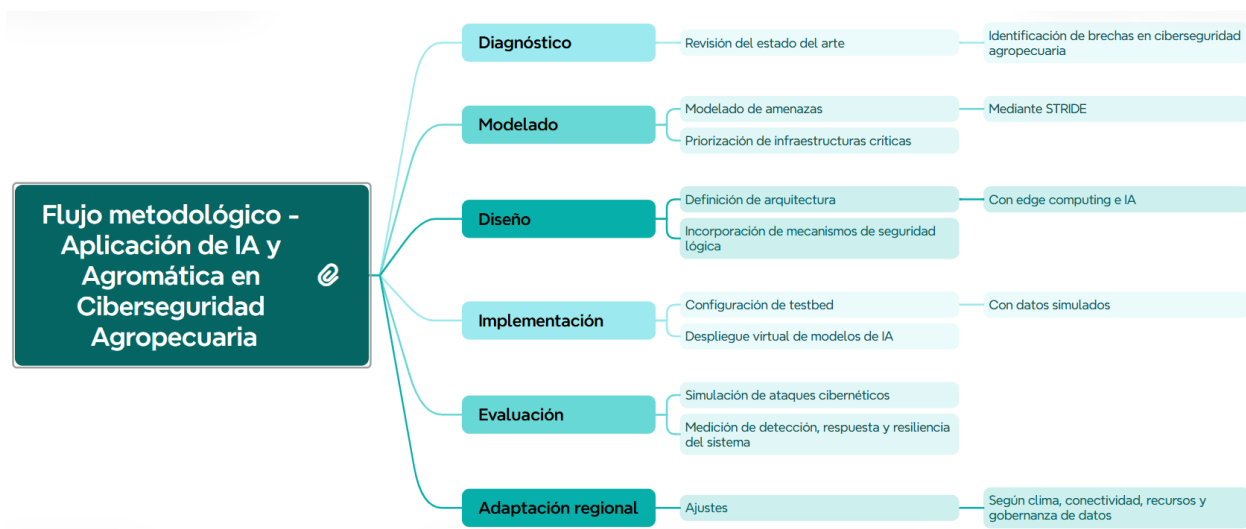
La población de estudio estuvo constituida por arquitecturas digitales agropecuarias inteligentes, modeladas a partir de sistemas reales de agricultura de precisión. La muestra técnica se conformó por 58 amenazas potenciales identificadas mediante el marco STRIDE, clasificadas en niveles de sensores, red, comunicación y actuadores. Para la recolección de información documental se consultaron bases de datos indexadas en Scopus y Web of Science, aplicando criterios de inclusión relacionados con Agricultura 4.0, IoT agrícola, inteligencia artificial y ciberseguridad (Alahe et al., 2024).

La estructura metodológica aplicada se organizó en seis fases interrelacionadas: diagnóstico, modelado, diseño, implementación, evaluación y adaptación regional. Como se muestra en la Figura 1, el proceso inició con la revisión del estado del arte y la identificación de brechas en ciberseguridad agropecuaria. Posteriormente, se realizó el modelado de amenazas mediante el marco STRIDE y la priorización de infraestructuras críticas. En la fase de diseño se definió la arquitectura técnica incorporando edge computing e inteligencia artificial, así como mecanismos de seguridad lógica. La etapa de implementación incluyó la configuración del testbed con datos simulados y el despliegue virtual de modelos de IA. Finalmente, se efectuó la evaluación mediante

simulación de ataques cibernéticos y medición de capacidad de detección, respuesta y resiliencia del sistema, integrando ajustes de adaptación regional según condiciones de conectividad, recursos y gobernanza de datos.

Figura 1.

Estructura de metodología aplicada



El procesamiento de la información se realizó en dos fases. En la primera fase se efectuó una revisión sistemática que permitió identificar arquitecturas de referencia, tecnologías predominantes y desafíos técnicos vinculados a interoperabilidad, conectividad, costos y gobernanza de datos. En la segunda fase se ejecutó la validación experimental en el testbed configurado, donde se implementaron modelos CNN y transformers ligeros en dispositivos edge para la detección de anomalías en tiempo real (Rahaman et al., 2024). El desempeño se evaluó mediante métricas de precisión, recall, F1-score y latencia operativa.

Asimismo, se consideraron dimensiones éticas relacionadas con privacidad de datos, equidad tecnológica y gobernanza descentralizada, integrando estos aspectos dentro del análisis técnico para garantizar coherencia con principios de sostenibilidad y responsabilidad digital.

Resultados

Detección de intrusiones DDoS en sensores agrícolas mediante CNN-LSTM en entornos Edge

La creciente complejidad de las infraestructuras agropecuarias modernas, impulsada por la adopción de tecnologías avanzadas como la inteligencia artificial y el Internet de las Cosas, ha transformado el sector agrícola en una entidad altamente interconectada y dependiente de los datos (Hasan et al., 2022). Esta transformación, si bien optimiza la producción y la gestión, también introduce vulnerabilidades significativas que requieren una atención especializada en ciberseguridad para proteger los activos críticos y la información sensible (Mitra et al., 2022).

En esta investigación uno de los hallazgos más relevantes proviene de la implementación de un modelo híbrido CNN-LSTM, entrenado con los conjuntos de datos CIC-DDoS2019 y TON-IoT¹, a través de scripts desarrollados en Jupyter Notebook se utiliza bibliotecas como TensorFlow y Keras. El entorno Jupyter facilitó la ejecución modular del código, visualización de métricas y pruebas iterativas sobre distintos hiperparámetros.

Este modelo alcanzó niveles de precisión cercanos al 99 %, con métricas de recall y F1-score igualmente sobresalientes. Su arquitectura combina redes convolucionales (CNN) para la extracción eficiente de características espaciales con LSTM y Bi-GRU para la detección de patrones temporales, lo que permite la identificación en tiempo real de ataques DDoS directamente en dispositivos o gateways con capacidad de edge computing. Esta característica resulta esencial para entornos rurales con conectividad limitada (Tychola & Rantos, 2025).

Detección de anomalías ambientales mediante autoencoders en entornos agrícolas reales

En un segundo experimento, también ejecutado en Jupyter Notebook, se implementó un modelo no supervisado basado en autoencoders se utilizó PyTorch. Este modelo fue entrenado con datos recolectados de sensores instalados en un invernadero operativo. Logró una precisión del 98,98 %, con un tiempo de entrenamiento de 262 segundos y una latencia de inferencia de apenas 0,0585 segundos por muestra lo cual se muestra en la tabla 1.

¹ <https://www.unb.ca/cic/datasets/ddos-2019.html>

El uso de Jupyter permitió registrar y documentar paso a paso el flujo de trabajo, desde la limpieza de datos hasta el ajuste del umbral de error reconstruido para la detección de anomalías.

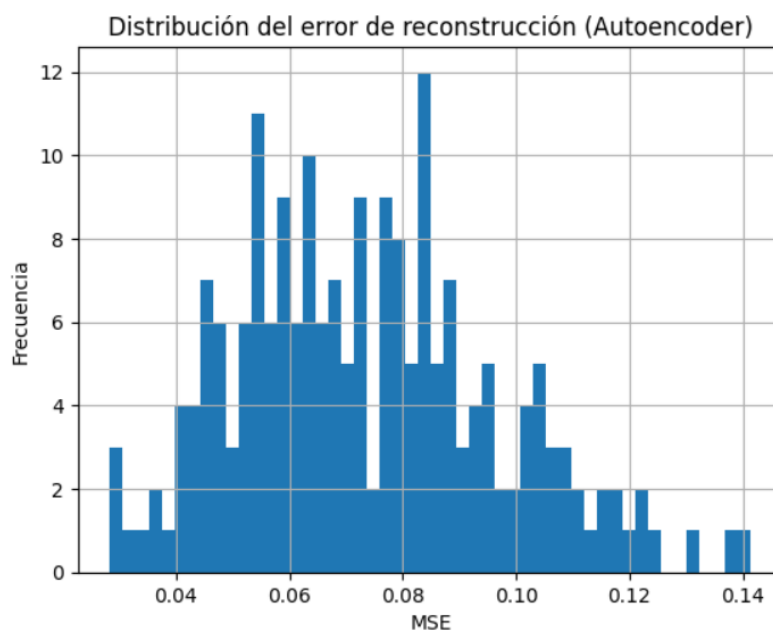
Tabla 1. Comparativa técnica entre modelos IA aplicados a detección de intrusiones y anomalías

Modelo	Precisión	Tiempo entrenamiento	de Latencia inferencia	de Ventaja principal
CNN– LSTM	~99– 100 %	—	Tiempo real	Detección inmediata de intrusiones DDoS en edge
Autoencoder	98,98 %	262 s	0,0585 s	Análisis de anomalías en invernaderos

En la figura 2 se representa la distribución del error de reconstrucción generado por un modelo autoencoder aplicado a datos simulados de sensores agrícolas en un entorno de prueba. El eje X muestra los valores del error cuadrático medio (MSE), mientras que el eje Y indica la frecuencia con la que dichos errores se presentaron.

La mayoría de los datos exhibe un error de reconstrucción entre 0.06 y 0.08, lo que sugiere que el modelo fue capaz de reconstruir adecuadamente las entradas normales. No obstante, se observa una cola hacia la derecha con errores más altos, lo que indica la presencia de muestras atípicas o potencialmente anómalas. Esta característica es especialmente relevante en entornos agropecuarios, ya que permite detectar fallos, alteraciones ambientales o comportamientos anómalos en los sensores sin requerir supervisión directa.

Figura 2. Autoencoder



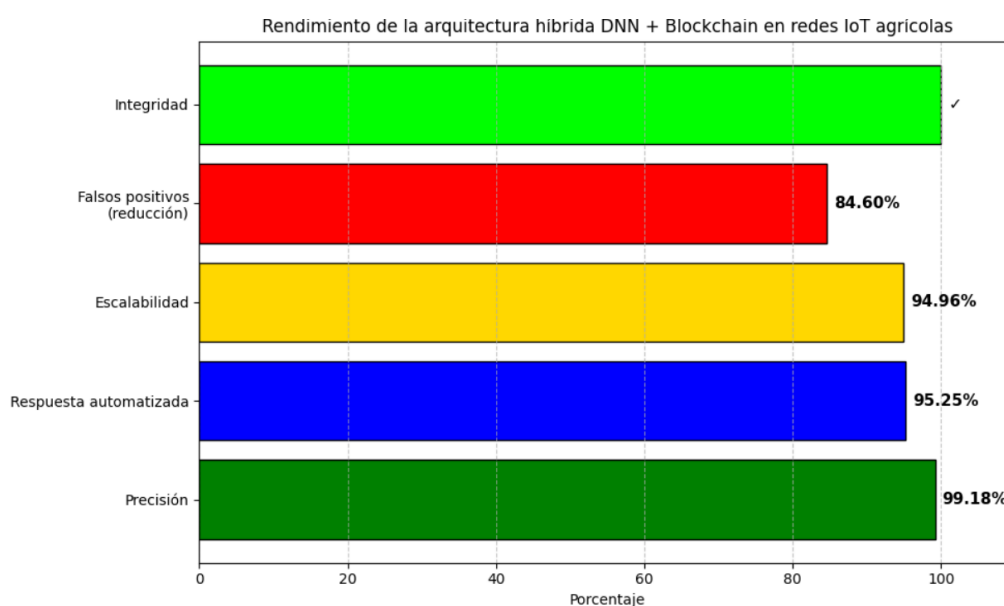
En contextos rurales con limitaciones de conectividad, los modelos de inteligencia artificial que operan en el borde (edge computing) resultan particularmente adecuados, ya que permiten ejecutar inferencias localmente sin depender de la nube, lo que reduce significativamente la latencia de respuesta y mejora la resiliencia de los sistemas. Esta capacidad es especialmente valiosa en aplicaciones de agromática, donde la detección temprana de fallos ya sean de origen técnico (hardware), climático o por errores de operación es crucial para mantener la continuidad y operatividad de infraestructuras agropecuarias. En este sentido, el modelo CNN–LSTM ha demostrado ser apto para su integración en gateways IoT, lo que facilita la detección de intrusiones en tiempo real, mientras que el autoencoder resulta ideal para sistemas más compactos como invernaderos o estaciones de campo.

Adicionalmente, la creciente adopción de dispositivos IoT en la agricultura de precisión ha expuesto a estas infraestructuras a un abanico creciente de amenazas cibernéticas, lo que ha motivado el desarrollo de arquitecturas híbridas que integran inteligencia artificial y blockchain(Gupta et al., 2020). Un estudio relevante presenta el modelo DNNs-BCT, una propuesta que combina redes neuronales profundas con tecnología blockchain para la detección de anomalías en redes IoT agrícolas. Este enfoque alcanzó una precisión del 99,18 % en la detección, automatizó respuestas mediante contratos inteligentes con un 95,25 % de efectividad, y logró una escalabilidad del sistema del 94,96 %, al tiempo que redujo los falsos positivos al 15,4 %. Además, garantizó la integridad de los eventos mediante el uso de registros inmutables en blockchain, lo que

refuerza su aplicabilidad en entornos donde la trazabilidad y la confianza en los datos son fundamentales.

La figura 3 muestra cómo la combinación de IA avanzada y Blockchain en redes IoT agrícolas puede fortalecer la ciberseguridad, en entornos más confiables, autónomos y escalables, particularmente relevantes para zonas rurales con infraestructura limitada.

Figura 3. Rendimiento de la arquitectura



Funcionamiento y ventajas operativas

La integración de redes neuronales profundas (DNN) con tecnología blockchain en infraestructuras IoT agrícolas ofrece un enfoque altamente eficiente y seguro para la gestión de eventos y ciberamenazas. En este sistema, los dispositivos IoT registran localmente eventos relevantes a su vez se utiliza una cadena de bloques privada, lo que garantiza la trazabilidad y la inmutabilidad de los datos. Simultáneamente, la DNN es responsable de la detección de anomalías como ataques DDoS, malware e intrusiones internas, en un monitoreo inteligente del entorno. Ante la detección de eventos sospechosos, se activan contratos inteligentes (smart contracts) que ejecutan automáticamente respuestas predefinidas, como el aislamiento de nodos comprometidos, sin requerir intervención humana. Esta arquitectura descentralizada no solo reduce la dependencia de servidores centrales, sino que también incrementa la resistencia a fallos únicos, lo que mejora la transparencia y la confianza del sistema.

Consideraciones prácticas y desafíos técnicos

A pesar de sus beneficios, esta solución plantea desafíos técnicos, especialmente en lo referente a los recursos computacionales. El entrenamiento y despliegue de modelos DNN, junto con la operación de la blockchain, requieren una importante capacidad de procesamiento, lo que puede ser limitante en hardware típico de IoT rural. Para superar esta barrera, se recomienda aplicar técnicas de optimización como la cuantización, la poda de redes y la destilación de conocimiento, que permiten reducir la complejidad computacional sin comprometer significativamente el rendimiento. Evaluaciones realizadas en escenarios simulados y reales han demostrado que esta arquitectura híbrida logra un equilibrio adecuado entre precisión en la detección, rapidez de respuesta y escalabilidad, para su implementación en entornos agropecuarios inteligentes(Alahmadi et al., 2022).

Por ello, este estudio profundiza en la aplicación de la inteligencia artificial y la agromática como herramientas fundamentales para fortalecer la ciberseguridad en infraestructuras agropecuarias regionales, para lo que se analizó las amenazas emergentes y se propusó estrategias de mitigación efectivas(Demestichas et al., 2020).

Discusión

La robótica y la automatización, componentes esenciales de la denominada “Agricultura 4.0”, han transformado la eficiencia agropecuaria, especialmente en países en desarrollo. El informe de la FAO (2020). destaca aplicaciones como la siembra, el deshierbe y la cosecha autónoma, las cuales prometen reducir la carga laboral, optimizar insumos, potenciar sistemas sin laboreo y fomentar esquemas inclusivos (arrendamiento y servicios compartidos) Sin embargo, su adopción queda limitada por los elevados costos iniciales y la insuficiente infraestructura digital en zonas rurales. Por tanto, se evidencia una brecha entre el potencial tecnológico y la realidad local que condiciona su implementación(Hashmi et al., 2024).

Los avances en agricultura de precisión han permitido operar en áreas sensibles como zonas protegidas con una práctica sostenible. Se emplean tecnología de sensores, SIG, imágenes satelitales y análisis de datos para optimizar recursos y maximizar rendimiento sin comprometer el ecosistema(Dayioğlu & Turker, 2021). Estudios avalan esta integración eficiente entre producción y conservación. No obstante, estos logros

dependen de una adecuada infraestructura, planificación territorial y capacitación técnica, condiciones que no siempre se cumplen en regiones de bajos recursos tecnológicos (Meza Nieto, 2024).

La inteligencia artificial (IA) está consolidándose como herramienta clave, tanto para mejorar la toma de decisiones agronómicas como para proteger la infraestructura digital del sector. Revisiones documentales recientes reflejan su eficacia en la detección de plagas, control ambiental, manejo predictivo de cultivos y automatización de maquinaria. Sin embargo, para que esta adopción sea efectiva se requieren datos fiables, conectividad rural sólida e inversión en capacidades locales. Estos elementos son críticos para que la IA no se quede relegada a contextos urbanos o regiones tecnológicamente avanzadas.

El paso hacia la agricultura digital introduce nuevas vulnerabilidades frente a ataques cibernéticos, como el DDoS. Soluciones basadas en IA y aprendizaje automático desde autoencoders hasta combinaciones CNN-LSTM o autoencoders profundos han demostrado tasas de detección superiores al 98-100 %, utilizando conjuntos de datos como CIC-DDoS2019 (Aldhyani & Alkahtani, 2023). Además, revisiones sistemáticas de IDS agrícolas destacan avances en clasificación binaria y multiclase, evidenciando la madurez técnica de estos enfoques. No obstante, la implementación real en el campo requiere validación en entornos rurales con conectividad parcial y recursos limitados y un marco normativo específico que garantice protección y armonización con políticas nacionales.

En el contexto ecuatoriano, se observa una separación entre la normativa nacional de ciberseguridad (Acuerdo 006-2021, alineado con ISO/NIST) y las innovaciones tecnológicas en el agro; no existen políticas específicas que integren IA, agromática y ciber protección rural. A nivel conceptual, los tres bloques analizados automatización, precisión agrícola y ciberseguridad convergen hacia un agro sostenible, inclusivo y seguro. Sin embargo, la materialización de esta visión demanda coordinación entre marcos regulatorios, inversión en infraestructura rural, formación técnica y marcos éticos de adopción. Solo mediante una estrategia unificada se podrá garantizar una transformación agroecológica digital que responda a los desafíos de productividad, preservación y digitalización segura en el Ecuador (Aguirre-Munizaga et al., 2019).

Este análisis comparativo confirma que, si bien existen avances tecnológicos sólidos en automatización, precisión y ciberseguridad en la agricultura global, su traducción al contexto ecuatoriano exige esfuerzos coordinados en infraestructura, regulación y capacidades humanas. Solo entonces se podrá articular un modelo agrícola 4.0 que sea eficiente, equitativo y resiliente ante riesgos físicos y digitales (Meza Nieto, 2024).

En este contexto, la implementación de medidas de ciberseguridad robustas y adaptadas a las especificidades del sector agropecuario regional se vuelve imperativa para salvaguardar la continuidad operativa y la confiabilidad de la producción de agrícola(Martin Otieno, 2023).

Conclusiones

La convergencia de inteligencia artificial (IA) y agromática en la ciberseguridad de infraestructuras agropecuarias representa un avance estratégico fundamental, tanto para mejorar la automatización y eficiencia de las explotaciones rurales como para protegerlas contra amenazas digitales emergentes. La agromática que integra sensores, visión por computadora, sistemas GIS y drones permite una gestión de datos precisa y en tiempo real de variables críticas, como salud del suelo, plagas o condiciones meteorológicas(Meza Nieto, 2024). Sin embargo, esta dependencia tecnológica expone infraestructuras agropecuarias a riesgos de ciberseguridad: ataques de denegación de servicio, manipulación de datos, ransomware, vulnerabilidades en dispositivos IoT y posibles sabotajes en logística

Frente a este panorama, la IA no solo impulsa innovaciones en productividad, sino que también se posiciona como una herramienta esencial en la defensa cibernética. Investigaciones recientes muestran cómo modelos de IA pueden detectar anomalías en sensores y redes edge, esto ayuda a identificar intrusiones en tiempo real mediante arquitecturas CNN-transformer diseñadas para entornos de agricultura cooperativa. Asimismo, plataformas de aseguramiento cibernético emplean IA generativa para simular amenazas, evaluar vulnerabilidades de sistemas como GPS y PLCs, y desarrollar respuestas automatizadas ante posibles brechas(Facuy Toledo, 2024).

En contextos regionales especialmente en pequeñas y medianas explotaciones agropecuarias, la carencia de conocimientos técnicos en ciberseguridad representa una

debilidad grave. Evaluaciones educativas, como las realizadas entre miembros de la tribu Ponca en Nebraska, demuestran que intervenciones formativas orientadas al sector logran mejorar significativamente las prácticas de seguridad digital: seguridad de contraseñas, autenticación multifactores y respaldos periódicos.

Además, iniciativas curriculares específicas para el sector agroalimentario, como el desarrollo de cursos modulados dirigidos a agricultores, promueven una consciencia más robusta y la adopción de medidas preventivas. Dado que la protección de los sistemas agropecuarios no solo implica la defensa contra ataques externos, sino también la mitigación de riesgos internos y la garantía de la privacidad de los datos recopilados (Rahaman et al., 2024).

Finalmente, la implementación de estándares y herramientas regulatorias, promovidos por organismos como CISA, IT-ISAC y proyectos públicos-privados (por ejemplo, AgrarIA en España), establece un marco sólido para la gobernanza de datos y ciberseguridad en la cadena agroindustrial.

Referencias bibliográficas

- Aguirre-Munizaga, M., Chang-Zorilla, S., Rivera, D. V., & Vera-Lucio, N. (2025). Implementation of a Web Application for Estimating Cocoa Productivity Using Machine Learning. *Information Technology and Systems, Lecture Notes in Networks and Systems*, 1447, 382-390. https://doi.org/10.1007/978-3-031-93109-3_34
- Aguirre-Munizaga, M., Lagos-Ortiz, K., Vergara-Lozano, V., Real-Avilés, K., Vásquez-Bermudez, M., Sinche-Guzmán, A., & Hernández-Rosas, J. (2019). Analysis of Atmospheric Monitoring Data Through Micro-meteorological Stations, as a Crowdsourcing Tool for Technology Integration. En Á. Rocha & M. Serrhini (Eds.), *Information Systems and Technologies to Support Learning* (Vol. 111, pp. 181-187). Springer International Publishing. https://doi.org/10.1007/978-3-030-03577-8_21
- Alahe, M. A., Wei, L., Chang, Y., Gummi, S. R., Kemesi, J., Yang, X., Won, K., & Sher, M. (2024). Cyber security in smart agriculture: Threat types, current status, and future trends. *Computers and Electronics in Agriculture*, 226, 109401. <https://doi.org/10.1016/j.compag.2024.109401>
- Alahmadi, A. N., Rehman, S. U., Alhazmi, H. S., Glynn, D. G., Shoaib, H., & Solé, P. (2022). Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture. *Sensors*, 22(9), 3520. <https://doi.org/10.3390/s22093520>

- Aldhyani, T. H. H., & Alkahtani, H. (2023). Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. *Mathematics*, 11(1), 233. <https://doi.org/10.3390/math11010233>
- Alvarez, L. T. G., Martínez, L. R. V., Cubides, J. D. A., & Bayona, S. M. (2022). Implementación de la agricultura de precisión a través del desarrollo de sistemas productivos en áreas protegidas o de conservación para optimizar la producción de cultivos. Una revisión sistemática de literatura. *Cuaderno activa*, 14(1), Article 1. <https://doi.org/10.53995/20278101.1011>
- Castillo Gómez, J. (2023). Ingeniería de Software para la Transformación Digital: Retos, Tendencias y Oportunidades Profesionales en el Ecuador. *Revista internacional de Investigación y Desarrollo Global*, 2(2), 66-80. <https://doi.org/10.64041/riidg.v2i2.40>
- Dayioğlu, M. A., & Turker, U. (2021). Digital Transformation for Sustainable Future - Agriculture 4.0: A review. *Tarım Bilimleri Dergisi*. <https://doi.org/10.15832/ankutbd.986431>
- Demestichas, K., Peppes, N., & Alexakis, T. (2020). Survey on Security Threats in Agricultural IoT and Smart Farming. *Sensors*, 20(22), 6458. <https://doi.org/10.3390/s20226458>
- Enhancing Agricultural Cybersecurity: Leveraging Deep Learning and Large Language Models for Smart Farming Protection. (2025, abril 25). *Advances in Computational Intelligence and Robotics*, 307-338. <https://doi.org/10.4018/979-8-3373-3296-3.ch010>
- Facuy, J., Aguirre-Munizaga, M., Pasini, A., Estévez, E., & Moran-Castro, C. (2026). Validation of an Ambient Intelligence System Applied to the Prediction of Electronic Waste in Smart Cities. En R. Valencia-Garcia, P. Alvarez-Muñoz, J. Tarquino Calderon, V. Vergara-Lozano, L. Ortega-Ponce, A. L. Pico-Aguilar, & B. M. Váscquez-García (Eds.), *Technologies and Innovation* (Vol. 2776, pp. 259-272). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-11494-5_17
- Facuy Toledo, D. P. (2024). Aplicación de sensores IoT e inteligencia artificial para la optimización del riego en cultivos agroecológicos. *Revista internacional de Investigación y Desarrollo Global*, 3(2), 36-52. <https://doi.org/10.64041/riidg.v3i2.23>
- FAO. (2020). *Agricultura 4.0—Robótica agrícola y equipos automatizados para la producción agrícola sostenible*. <https://openknowledge.fao.org/items/240ac76e-0fbd-46fa-92a6-87c1835d4f64>
- Freyhof, M., Grispos, G., Pitla, S., & Mahoney, W. (2025). Investigating The Implications of Cyberattacks Against Precision Agricultural Equipment. *International Conference on Cyber Warfare and Security*, 20, 93-104. <https://doi.org/10.34190/iccws.20.1.3229>

- Gupta, M., Abdelsalam, M., Khorsandroo, S., & Mittal, S. (2020). Security and Privacy in Smart Farming: Challenges and Opportunities. *IEEE Access*, 8, 34564-34584. <https://doi.org/10.1109/ACCESS.2020.2975142>
- Hasan, Md. M., Islam, M. U., & Sadeq, M. J. (2022). *Towards technological adaptation of advanced farming through AI, IoT, and Robotics: A Comprehensive overview* (Versión 1). arXiv. <https://doi.org/10.48550/ARXIV.2202.10459>
- Hashmi, A. U. H., Mir, G. U., Sattar, K., Ullah, S. S., Alroobaea, R., Iqbal, J., & Hussain, S. (2024). Effects of IoT Communication Protocols for Precision Agriculture in Outdoor Environments. *IEEE Access*, 12, 46410-46421. <https://doi.org/10.1109/ACCESS.2024.3381522>
- Javaid, M., Haleem, A., Khan, I. H., & Suman, R. (2023). Understanding the potential applications of Artificial Intelligence in Agriculture Sector. *Advanced Agrochem*, 2(1), 15-30. <https://doi.org/10.1016/j.aac.2022.10.001>
- Kaliyaperumal, P., Karuppiah, T., Perumal, R., Thirumalaisamy, M., Balusamy, B., & Benedetto, F. (2025). Enhancing cybersecurity in Agriculture 4.0: A high-performance hybrid deep learning-based framework for DDoS attack detection. *Computers and Electrical Engineering*, 126, 110431. <https://doi.org/10.1016/j.compeleceng.2025.110431>
- Kumar, S., & Faisal, M. (2024). Critical Review of Cybersecurity Risks in Precision Agriculture. *2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES)*, 1-7. <https://doi.org/10.1109/ic3tes62412.2024.10877611>
- Martin Otieno. (2023). An extensive survey of smart agriculture technologies: Current security posture. *World Journal of Advanced Research and Reviews*, 18(3), 1207-1231. <https://doi.org/10.30574/wjarr.2023.18.3.1241>
- Meza Nieto, A. K. (2024). Análisis y visualización de datos climáticos en el cantón Guayaquil: Tendencias, riesgos y proyecciones ambientales. *Revista internacional de Investigación y Desarrollo Global*, 3(2), 18-35. <https://doi.org/10.64041/riidg.v3i2.22>
- Mitra, A., Vangipuram, S. L. T., Bapatla, A. K., Bathalapalli, V. K. V. V., Mohanty, S. P., Kougianos, E., & Ray, C. (2022). *Everything You wanted to Know about Smart Agriculture* (Versión 1). arXiv. <https://doi.org/10.48550/ARXIV.2201.04754>
- Neira, E. G. C., Urgilés, C. H. F., Urgilés, C. M. F., Espinoza, J. J. S., & Egas, M. B. R. (2023). Diagnóstico y línea base de los activos de información e infraestructura crítica de ciberseguridad del estado ecuatoriano. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, 7(49), 101-119. <https://doi.org/10.29018/issn.2588-1000vol7iss49.2023pp101-119>
- Rahaman, M., Lin, C.-Y., Pappachan, P., Gupta, B. B., & Hsu, C.-H. (2024). Privacy-Centric AI and IoT Solutions for Smart Rural Farm Monitoring and Control. *Sensors*, 24(13), 4157. <https://doi.org/10.3390/s24134157>
- Romero, J. C. R. (2024). Tecnologías de la información y comunicaciones implementadas en la agroindustria en el Ecuador. *Revista Internacional de Estudios en Ciencias*

- Administrativas STRATEGOS*, 4(1), Article 1.
<https://doi.org/10.53591/strategos.v4i1.1846>
- Santos Vidal, M. D. (2022). *Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento: Respuestas del Estado ecuatoriano en el período 2013-2022* [masterThesis, Quito, EC: Universidad Andina Simón Bolívar, Sede Ecuador].
<http://repositorio.uasb.edu.ec/handle/10644/9076>
- Tychola, K. A., & Rantos, K. (2025). Cyberthreats and Security Measures in Drone-Assisted Agriculture. *Electronics*, 14(1), 149.
<https://doi.org/10.3390/electronics14010149>
- Urjilez, H., Valdez, D., García, Y., Aguirre, M., & Mancero, D. (2025). Advances in Predictive Modeling in Fruit Crops: Mobile Applications. En A. Rocha, C. Ferrás, & H. Calvo (Eds.), *Information Technology and Systems* (Vol. 1447, pp. 354-363). Springer Nature Switzerland. https://doi.org/https://doi.org/10.1007/978-3-031-93109-3_31
- Valle-Lituma, C., Aguirre-Munizaga, M., Salous, A. E., & Cardenas-Rodriguez, M. (2026). Systematic Review of Artificial Intelligence Tools Applied to the Classification, Quality Control, and Shelf Life Prediction of Post-harvest Agricultural Products (2000–2025). En R. Valencia-Garcia, P. Alvarez-Muñoz, J. Tarquino Calderon, V. Vergara-Lozano, L. Ortega-Ponce, A. L. Pico-Aguilar, & B. M. Vásconez-García (Eds.), *Technologies and Innovation* (Vol. 2776, pp. 34-50). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-11494-5_3

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Agradecimiento:

N/A

Nota:

El artículo no es producto de una publicación anterior.