ASCE MAGAZINE ISSN: 3073–1178

Revista ASCE Magazine, Periodicidad: Trimestral Octubre-Diciembre, Volumen: 4, Número: 4, Año: 2025 páginas 1608 - 1633

Doi: https://doi.org/10.70577/asce.v4i4.504

Recibido: 2025-10-13

Aceptado: 2025-10-29

Publicado: 2025-11-13

Ciberseguridad en los sistemas de información agropecuarios como desafío estratégico para la protección de datos en la agricultura digital

Cybersecurity in Agricultural Information Systems as a Strategic Challenge for Data Protection in Digital Agriculture.

Autor

Eddie Carrasco-Rivera[1]
Ingeniero en Sistemas Computacionales, Máster en Seguridad Informática Aplicada
https://orcid.org/0009-0008-9521-7769
ecarrasco@uagraria.edu.ec
Carrera Computación modalidad en línea, Facultad de Ciencias Agrarias,
Universidad Agraria del Ecuador
Guayaquil – Ecuador

Cómo citar

Carrasco Rivera, E. (2025). Ciberseguridad en los sistemas de información agropecuarios como desafío estratégico para la protección de datos en la agricultura digital. *ASCE MAGAZINE*, *4*(4), 1608–1633.

Resumen

La investigación aborda la ciberseguridad en los sistemas de información agropecuarios como un desafío estratégico en el contexto de la agricultura digital en Ecuador. Se identificaron debilidades críticas en la infraestructura tecnológica, falta de políticas específicas de seguridad y limitada capacitación del personal encargado de la gestión de datos, lo que incrementa la vulnerabilidad del sector frente a ciberataques, accesos no autorizados y pérdida de información sensible, afectando la sostenibilidad y trazabilidad productiva.

Objetivo: Analizar el estado de la ciberseguridad en los sistemas de información agropecuarios en Ecuador y proponer la incorporación de la ciberseguridad como un eje transversal en las políticas públicas y la innovación agrícola, mediante marcos normativos, formación especializada y tecnologías emergentes.

Metodología: Se utilizó un enfoque mixto que incluyó encuestas, revisión bibliométrica y análisis documental para evaluar la infraestructura tecnológica, las políticas de seguridad y la capacitación del personal en organizaciones del sector agropecuario.

Resultados: Más del 70% de las organizaciones carece de protocolos formales de seguridad, y la adopción de medidas como cifrado o autenticación multifactorial es prácticamente inexistente. Se concluye que es necesaria una gobernanza integral que articule a gobiernos, universidades y actores productivos para consolidar un ecosistema agropecuario digital seguro, resiliente y competitivo, incorporando inteligencia artificial para la detección de intrusiones y promoviendo la formación y regulación adecuadas.

Palabras clave: Agricultura digital, Ciberseguridad agropecuaria, Sistemas de información agropecuarios, Gestión de datos agropecuarios, Políticas públicas en seguridad digital, Gobernanza tecnológica rural, Inteligencia artificial en ciberseguridad

Abstract

The research addresses cybersecurity in agricultural information systems as a strategic challenge within the context of digital agriculture in Ecuador. Critical weaknesses were identified in technological infrastructure, the absence of specific security policies, and limited training of personnel responsible for data management. These shortcomings increase the sector's vulnerability to cyberattacks, unauthorized access, and loss of sensitive information, ultimately affecting productivity sustainability and traceability.

Objective: To analyze the state of cybersecurity in Ecuador's agricultural information systems and propose the integration of cybersecurity as a cross-cutting axis in public policies and agricultural innovation through regulatory frameworks, specialized training, and emerging technologies.

Methodology: A mixed-method approach was applied, combining surveys, bibliometric review, and documentary analysis to evaluate technological infrastructure, security policies, and staff training within agricultural organizations.

Results: More than 70% of the organizations lack formal security protocols, and the adoption of measures such as encryption or multifactor authentication is virtually nonexistent. The study concludes that a comprehensive governance model is required one that links governments, universities, and productive actors to build a secure, resilient, and competitive digital agricultural ecosystem that incorporates artificial intelligence for intrusion detection and promotes proper training and regulation.

Keywords: Digital agriculture, Agricultural cybersecurity, Agricultural information systems, Agricultural data management, Public policies on digital security, Rural technological governance, Artificial intelligence in cybersecurity

Introducción

La transformación digital del sector agropecuario impulsa el uso intensivo de tecnologías como sensores IoT, plataformas de gestión agrícola, sistemas de monitoreo meteorológico y bases de datos geoespaciales(Goldenits y Neubauer 2025). En consecuencia, estas innovaciones, que conforman la denominada agricultura digital, mejoran la eficiencia, sostenibilidad y productividad del sector. Sin embargo, esta digitalización trae consigo nuevos riesgos asociados a la exposición de información sensible, tales como datos productivos, genéticos, financieros y ambientales, lo que plantea un desafío estratégico en términos de ciberseguridad(Alahe et al. 2024a).

En este contexto la digitalización del sector agropecuario establece una nueva era productiva denominada agricultura digital, la cual se caracteriza por la incorporación de tecnologías avanzadas como sensores del Internet de las Cosas (IoT), sistemas de información geográfica (SIG), redes de estaciones meteorológicas, plataformas de gestión agrícola, inteligencia artificial y herramientas de análisis de datos masivos(Aguirre-Munizaga et al. 2019). Esta transformación optimiza los procesos de producción, mejorar la eficiencia en el uso de recursos, reducir impactos ambientales y facilitar una toma de decisiones basada en datos en tiempo real (Wiseman et al., 2019).

Por otra parte, la literatura reciente aborda la ciberseguridad no solo un tema técnico, sino como un elemento estratégico de gobernanza digital rural. La digitalización agrícola amplía enormemente la superficie de ataque, ya que muchos sensores carecen de protección, las redes presentan configuraciones deficientes y los sistemas de gestión no incorporan cifrado ni autenticación (Kristen et al. 2021). Sin embargo otros autores reconocen las posibilidades de la IA y el ML para crear IDS adaptativos que fortalecen la resiliencia del agro ante ciberataques (Ferrag et al. 2022). Esto refleja un debate no resuelto entre las soluciones tecnológicas automatizadas y los enfoques centrados en la construcción de capacidades humanas e institucionales para gestionar el riesgo digital.

Desde una perspectiva conceptualmente, la literatura distingue entre la “seguridad de la información” que protege la confidencialidad, integridad y disponibilidad de la información de la “ciberseguridad agropecuaria”, que es el conjunto de estrategias, políticas y prácticas que resguardan los ecosistemas digitales asociados con la producción, comercialización y trazabilidad de productos agrícolas (Neira et al. 2023). Esta última noción sitúa la seguridad informática en las sociotécnicas del agro, donde los datos productivos, genéticos y climáticos son nuevos activos estratégicos que determinan la competitividad y la soberanía alimentaria. A pesar de ello la mayoría de las políticas nacionales y marcos legales todavía no cuentan con directrices específicas

para la agricultura digital lo que genera vacíos legales y desigualdades en la protección de la información rural (Zamora Boza et al. 2021).

Asimismo, el despliegue acelerado de estas tecnologías en entornos agrícolas y rurales expone a los sistemas de información agropecuarios a nuevas amenazas vinculadas a la seguridad digital(Alahmadi et al. 2022). En la actualidad, la recopilación, transmisión y análisis de grandes volúmenes de datos agrícolas que incluyen información genética, financiera, climática, productiva y de propiedad intelectual los convierte en activos estratégicos vulnerables a diversos problemas como ciberataques, accesos no autorizados, sabotajes digitales, manipulación de datos y pérdida de información crítica (Sánchez y Zambrano Mendoza 2019). Estas amenazas comprometen la privacidad y seguridad de los actores involucrados, sino que también pueden afectar la continuidad de las cadenas de suministro alimentarias, la trazabilidad de productos y la soberanía alimentaria de los países.

En el ámbito latinoamericano, los avances en ciberseguridad agropecuaria son incipientes y fragmentados. Mientras que países como Brasil o México implementan estrategias nacionales de seguridad digital agrícola, Ecuador presenta rezagos estructurales por falta de inversión en infraestructura tecnológica y capacitación en seguridad informática para el sector agropecuario (De Salvo et al. 2025). Esta situación crea una desconexión entre la rápida digitalización de las cadenas productivas y la falta de capacidades técnicas e institucionales para proteger los datos que generan las plataformas agrícolas inteligentes. Dicha inconsistencia no solo pone en riesgo la sostenibilidad de los sistemas agroindustriales, sino que también socava la confianza de los agricultores y la integridad de los mercados rurales emergentes (Aguirre-Munizaga, Briones-Zambrano, y Jurado-Chagerben 2025).

Es así como la ciberseguridad se destaca en la presente investigación como un desafío estratégico para el desarrollo sostenible de la agricultura digital. Resulta importante que los gobiernos, universidades, centros de investigación y actores del sector diseñen e implementen políticas públicas que integren la protección digital de los sistemas agropecuarios como un eje transversal. Ello implica adoptar marcos normativos internacionales, establecer protocolos de autenticación y cifrado, fortalecer capacidades locales, promover el uso ético de los datos y fomentar una cultura de seguridad digital en el entorno agroindustrial(Castillo Gómez 2023).

Desde una perspectiva crítica, la ciberseguridad constituye un pilar transversal de la sostenibilidad agro-digital, y no una variable complementaria del desarrollo tecnológico. Si bien las soluciones de IA, blockchain o cloud pueden mejorar la trazabilidad y la eficiencia, su implementación sin marcos éticos, legales y organizativos puede agravar los riesgos existentes y crear nuevas formas

de dependencia tecnológica (Rodríguez Perea 2024a). En esa línea, la literatura plantea dar el salto hacia una "seguridad digital inclusiva" donde políticas públicas, universidades y centros de investigación trabajen en conjunto para fortalecer la gobernanza tecnológica rural y la cultura de protección de datos en los sistemas agropecuarios (Facuy Toledo 2024).

De la información planteada se destaca como objetivo general del estudio analizar el estado actual de la ciberseguridad en los sistemas de información agropecuarios en Ecuador y proponer lineamientos estratégicos para su incorporación como eje transversal en la política pública y la innovación agrícola. Entre los objetivos objetivos específicos se evalua el nivel de preparación tecnológica y las políticas de seguridad digital en organizaciones del sector agropecuario ecuatoriano. A su vez se Identifica brechas de conocimiento y vulnerabilidades en la gestión de datos agrícolas digitales.

Revisión de la literatura

A pesar de la creciente dependencia de herramientas digitales, gran parte del sector agropecuario carece de políticas integrales de ciberseguridad, infraestructura tecnológica segura y talento humano capacitado para gestionar riesgos digitales. Esta situación es aún más crítica en regiones rurales, donde persisten brechas en conectividad, gobernanza tecnológica y cultura de protección de datos (Thilakarathne et al. 2025). A ello se suma la ausencia de estándares técnicos específicos adaptados a las realidades del agro y la limitada conciencia de los productores sobre las implicaciones de la seguridad informática.

El estudio realizado por Sánchez y Zambrano (2019) analiza el nivel de alfabetización en ciberseguridad de los agricultores digitales en Ecuador, con el fin de identificar brechas de conocimiento y proponer estrategias para mejorar la protección de la información en entornos agrícolas digitalizados. La metodología usada por los autores se basa en un enfoque cuantitativo-descriptivo mediante la aplicación de encuestas a productores agropecuarios que utilizan tecnologías digitales, evaluando aspectos como conocimiento de riesgos, uso de contraseñas, prácticas de seguridad en línea y nivel de formación en ciberseguridad. Entre los principales hallazgos se evidencia un bajo nivel de conciencia y preparación frente a amenazas cibernéticas, destacándose la falta de capacitación formal, el uso de dispositivos sin protección adecuada y la exposición a riesgos derivados del desconocimiento de prácticas básicas de seguridad digital, lo que confirma la necesidad de programas de formación específicos para fortalecer la resiliencia digital del sector agropecuario.

La transformación digital del sector agropecuario en Ecuador avanza a mediana escala con la incorporación de tecnologías que mejoran la productividad y sostenibilidad, pero es importante evaluar que este progreso debe ir acompañado de estrategias sólidas de ciberseguridad(Ocampo Alvarado 2024). Mientras que la adopción tecnológica fortalece la eficiencia del sistema agrícola, la falta de protección de datos y conocimientos en seguridad digital expone a los productores a riesgos crecientes. Integrar ambos enfoques tecnológico y estratégico es fundamental para construir un agro moderno, seguro y capaz de enfrentar los desafíos productivos y digitales del siglo XXI(Flórez-Martínez 2024).

Según Alshammari et al.(2021) la digitalización de la agricultura ha incrementado los riesgos cibernéticos, requiriendo enfoques innovadores de protección, la investigación hace énfasis en la intersección entre la agricultura inteligente y la ciberseguridad, destacando que la inteligencia artificial (IA) puede fortalecer los mecanismos de defensa contra amenazas cibernéticas en entornos agrícolas digitalizados. La metodología se basa en una revisión comparativa de literatura científica reciente, identificando tipos de ciberataques, causas técnicas y no técnicas, y soluciones propuestas en el contexto de la agricultura inteligente. Entre los hallazgos principales se resalta que la mayoría de los ataques se relacionan con redes débiles, dispositivos mal configurados y falta de concienciación en ciberseguridad. Asimismo, se concluye que la integración de IA con sistemas agrícolas digitales permite una detección temprana de amenazas y una respuesta más eficaz ante posibles intrusiones.

Tanto el enfoque técnico usado en la investigación detallada con anterioridad como la visión estratégica sobre la ciberseguridad en sistemas de información agropecuarios reconocen que la agricultura digital enfrenta crecientes riesgos cibernéticos debido a su dependencia tecnológica. Sin embargo, mientras el primero propone soluciones basadas en inteligencia artificial para mitigar amenazas de forma automatizada, el segundo destaca la importancia de una gobernanza sólida, políticas públicas y formación especializada como pilares para una protección efectiva. La convergencia de ambos enfoques tecnológico y estratégico resulta indispensable para construir un ecosistema agropecuario digital seguro, resiliente y sostenible(Rodríguez Perea 2024b).

En Ecuador, fortalecer los sistemas de innovación requiere una articulación efectiva entre investigación, políticas públicas y actores del territorio. Siendo así que la innovación agrícola es un componente clave para mejorar la productividad, sostenibilidad y resiliencia del sector agropecuario(Rueda Barrios, González Bueno, y Luzardo Briceño 2022).

En este caso se cita la investigación realizada en Ecuador en 2023, donde se identifica actores, capacidades, limitaciones y oportunidades para fortalecer la articulación entre ciencia, tecnología

y producción agropecuaria(Castillo Gómez 2023). La metodología del artículo se basa en un enfoque cualitativo-descriptivo mediante revisión documental y análisis institucional, considerando políticas públicas, capacidades de investigación, redes de innovación y participación de los actores del sector productivo. Entre sus principales hallazgos se evidencia una débil articulación entre los centros de investigación, las universidades y los productores; escasa inversión en I+D agrícola; limitada transferencia tecnológica; y ausencia de políticas sostenidas que promuevan la innovación rural(Zamora Boza et al. 2021). El estudio concluye que es necesario consolidar un sistema nacional de innovación agropecuaria que articule esfuerzos públicos y privados con una visión territorial, participativa y orientada a la sostenibilidad del sector

Es así como se destaca que la ciberseguridad es un pilar fundamental para el desarrollo sostenible del sector agropecuario ecuatoriano. Mientras el fortalecimiento de los sistemas de innovación permite mejorar la productividad, la articulación institucional y la adopción tecnológica, la ciberseguridad garantiza que dicha digitalización se realice de manera segura, protegiendo los datos estratégicos del agro. La integración de ambas perspectivas es indispensable para consolidar un ecosistema agrícola moderno, resiliente y competitivo, capaz de enfrentar los retos productivos, tecnológicos y de seguridad del entorno actual(Aguirre-Munizaga et al. 2025).

En el estudio realizado por Ferrag et al. (2022) se identifica el papel de los sistemas de detección de intrusos (IDS) basados en aprendizaje automático como solución clave para enfrentar las amenazas cibernéticas en entornos de Agricultura 4.0, caracterizados por una alta conectividad e integración de tecnologías inteligentes. La metodología de la investigación se fundamenta en una revisión sistemática de literatura, que abarca investigaciones sobre IDS aplicados al sector agrícola, tipos de ataques comunes, técnicas de machine learning utilizadas (como redes neuronales, SVM, árboles de decisión) y los conjuntos de datos disponibles. Entre los principales hallazgos, el estudio revela una falta de datasets agrícolas específicos y actualizados para entrenar modelos eficaces, identifica que muchos IDS agrícolas aún dependen de datos simulados o genéricos, y destaca la necesidad urgente de soluciones adaptadas al contexto agrícola que sean ligeras, precisas y capaces de operar en tiempo real.

El enfoque técnico de los trabajos citados, así como la perspectiva estratégica sobre la ciberseguridad agropecuaria coinciden en la urgencia de proteger los sistemas digitales en el sector agrícola(Guerra Dávila et al. 2024). Mientras se propone soluciones basadas en machine learning para una detección eficiente de intrusiones, se destaca la necesidad de fortalecer la gobernanza, la normativa y la formación en seguridad digital. La convergencia de estos enfoques tecnológico y

estratégico resulta fundamental para garantizar una agricultura digital segura, sostenible y adaptada a los desafíos reales del entorno agropecuario(Aguirre-Munizaga et al. 2021).

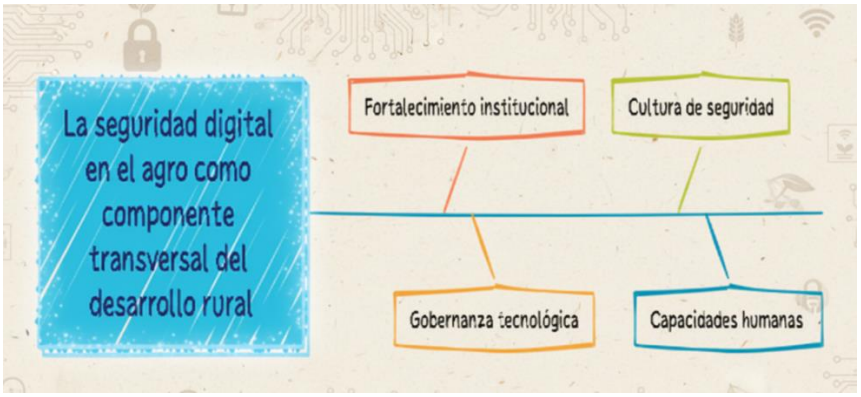
En la investigación realizada en el sector de la agroindustria se evidencia que se ha experimentado una tasa acelerada de ataques de ransomware tanto en sentido ascendente como descendente(Zambrano Burgos, Zambrano Mieles, y Mieles Cevallos 2025). El artículo analiza los ataques que se registraron durante más de una década y resume las principales tendencias (Kristen et al. 2021). La creciente conectividad y el despliegue de sofisticadas soluciones informáticas para la agricultura de precisión e inteligente hacen que este sector sea potencialmente muy vulnerable. Entre los principales hallazgos se identificó un conocimiento limitado sobre prácticas seguras en el entorno digital, bajo uso de herramientas de protección como autenticación en dos pasos, y una alta exposición a riesgos por desconocimiento, lo que evidencia la necesidad de integrar contenidos de ciberseguridad en los programas de formación universitaria (Mishra, Albarakati, y Sharma 2022).

Tanto el enfoque técnico de la ciberseguridad apoyada en Big Data, como el enfoque estratégico aplicado a los sistemas de información agropecuarios destacan la urgencia de fortalecer la protección digital en contextos distintos pero complementarios (Ahmed et al., 2023). Mientras el primero aporta herramientas avanzadas para anticipar y neutralizar amenazas mediante simulaciones controladas y análisis masivo de datos, el segundo enfatiza la necesidad de construir capacidades institucionales, normativas y humanas en sectores como el agro, donde la digitalización aún es incipiente. La integración de ambos enfoques es fundamental para garantizar una ciberseguridad integral, eficaz y adaptada a los distintos niveles de madurez tecnológica (Alahe et al. 2024b).

De los trabajos relacionados se concluye que la ciberseguridad en el agro se enfoca en ejes basados en el fortalecimiento a través de una cultura de seguridad que se complementen con el área de tecnologías y las capacidades humanas, como se muestra en la Figura 1.

Figura 1.

Ejes destacados de la seguridad digital en el agro



Nota. La seguridad digital en el agro impulsa el desarrollo rural mediante el fortalecimiento institucional, la gobernanza tecnológica, la cultura de seguridad y el desarrollo de capacidades humanas.

Fuente: Autor

Metodología

El presente artículo se desarrolló bajo un enfoque mixto, combinando técnicas cualitativas y cuantitativas con el propósito de identificar y analizar los desafíos estratégicos asociados a la ciberseguridad en los sistemas de información agropecuarios (SIA) en el marco de la agricultura digital(Kjønås y Wangen 2023). Se efectuó un diseño de investigación exploratorio descriptivo, que se consideró adecuado para abordar un tema emergente y escasamente documentado en el contexto agrícola, como es la protección y gestión segura de datos digitales vinculados a la producción agropecuaria(Mancero-Castillo et al. 2024).

Materiales

Para la recolección, procesamiento y análisis de la información se empleó una combinación de recursos tecnológicos, documentales y digitales que ayudaron a abordar de manera integral el objeto de estudio. En primer lugar, se analizaron Sistemas de Información Agropecuarios (SIA) implementados por entidades públicas y privadas, orientados a la gestión de datos agroproductivos, climáticos y fitosanitarios(Pinargote Bravo 2023).

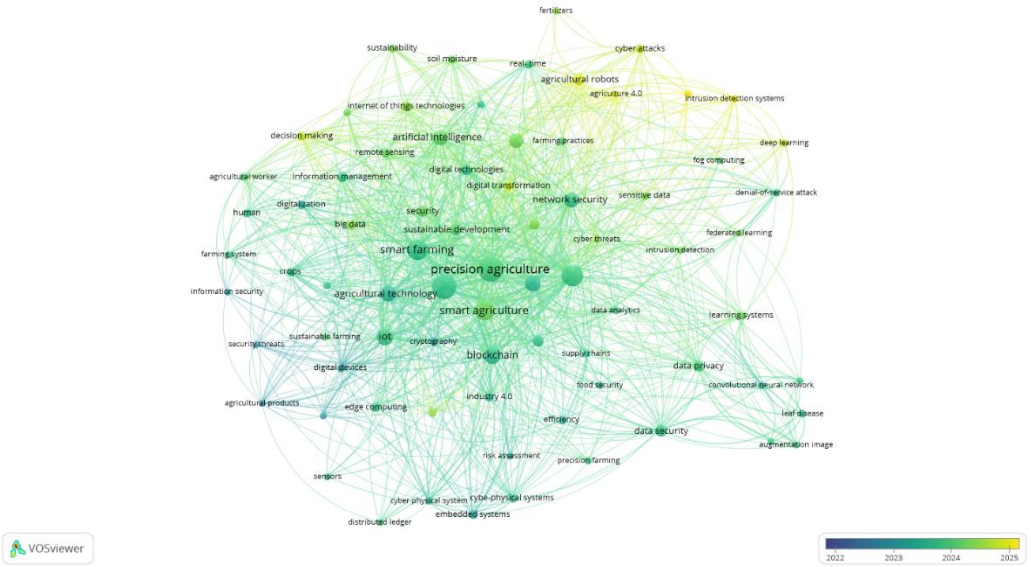
En cuanto a la recolección directa de información, se utilizaron instrumentos digitales diseñados mediante Google Forms, con el fin de aplicar encuestas estructuradas a profesionales del sector

agropecuario, responsables de tecnologías de la información y gestores de datos, garantizando la obtención de información precisa y sistemática.

Para el análisis bibliométrico y estadístico, se recurrió al uso de VOSviewer, con el que se construyeron y visualizaron redes bibliométricas a partir del archivo csv, que contiene registros de publicaciones científicas relacionadas con la ciberseguridad, los sistemas de información agropecuarios y la agricultura digital(Rodríguez-Correa et al. 2023). Este análisis permitió generar mapas de coocurrencia de términos, redes de colaboración entre autores y representaciones de la distribución temática por años de publicación.

Figura 2.

Mapa de coocurrencia de términos



Nota. El mapa muestra la red de coocurrencia de términos obtenida mediante el software VOSviewer, a partir del análisis bibliométrico de publicaciones indexadas relacionadas con ciberseguridad, sistemas de información agropecuarios y agricultura digital. El tamaño de los nodos representa la frecuencia del término; la distancia y el grosor de los enlaces indican la fuerza de asociación entre conceptos.

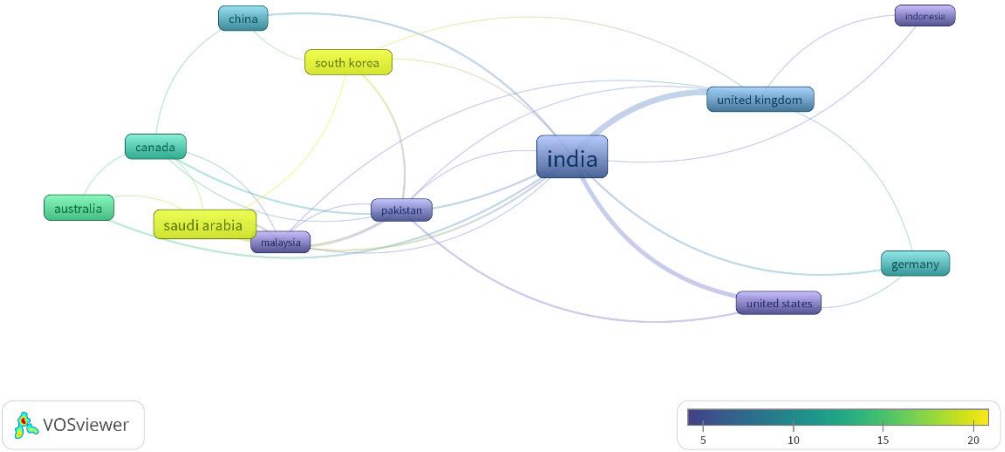
Fuente: Autor

La figura 2 muestra un mapa de coocurrencia de términos generado con VOSviewer a partir de publicaciones científicas relacionadas con ciberseguridad, sistemas de información agropecuarios y agricultura digital. En este gráfico, el tamaño de cada nodo representa la frecuencia de aparición del término en la literatura, mientras que la proximidad y la intensidad de los enlaces indican la fuerza de asociación entre conceptos. Se observa que “precision agriculture”, “smart agriculture”, “IoT” y “blockchain” son términos centrales que articulan la red, conectándose con áreas clave

como “data security”, “network security”, “artificial intelligence” y “cyber attacks”. El gradiente de color refleja la media de año de publicación, evidenciando un incremento reciente en tópicos como “agricultural robots”, “federated learning” y “intrusion detection systems”, lo que indica tendencias emergentes en la intersección entre agricultura de precisión y ciberseguridad.

Figura 3.

Mapa de colaboración internacional



Nota. La figura representa la red de coautoría entre países en publicaciones científicas relacionadas con ciberseguridad, sistemas de información agropecuarios y agricultura digital, elaborada con el software VOSviewer. El tamaño de los nodos refleja el número de documentos por país, mientras que el grosor de los enlaces indica la intensidad de la colaboración. India destaca como nodo central con fuertes vínculos con Estados Unidos, Reino Unido, Alemania y Arabia Saudita. El gradiente de color indica el promedio de citas por documento, mostrando mayor impacto en países con tonos más claros. Fuente: Elaboración propia con base en datos de Scopus (2025).

La figura 3 presenta un mapa de colaboración internacional, ponderado por el promedio de citas por documento (average citations per document). Cada nodo representa un país participante en publicaciones científicas sobre ciberseguridad, sistemas de información agropecuarios y agricultura digital, mientras que el tamaño del nodo está asociado a su producción y relevancia en función de las citas promedio (Padilla Díaz et al. 2024). Las líneas indican vínculos de coautoría entre países, y su grosor refleja la intensidad de la colaboración. En este análisis, India aparece como el nodo central, evidenciando una alta interconexión con países como Estados Unidos, Reino

Unido, Alemania, China y Australia, lo que indica un papel predominante en la generación y difusión de conocimiento en el área. El gradiente de color, que va del azul al amarillo, representa el promedio de citas por documento, destacando a naciones como Arabia Saudita, Malasia y China con valores más recientes y competitivos, lo que sugiere su creciente impacto en la temática.

Adicionalmente a estos análisis bibliométricos, se emplearon herramientas ofimáticas y software estadístico para el tratamiento de datos cuantitativos, aplicando análisis descriptivos y comparativos que facilitaron la interpretación de los resultados.

Para finalizar, se incluyó la revisión de fuentes documentales conformadas por marcos normativos nacionales e internacionales, estándares de ciberseguridad como la norma ISO/IEC 27001 y reportes de casos documentados sobre vulneraciones de seguridad en plataformas agrícolas digitales, lo que permitió contextualizar los hallazgos dentro de un marco regulatorio y técnico actualizado

Población y muestra

La población estuvo compuesta por profesionales del sector agropecuario, responsables de sistemas de información y expertos en seguridad informática vinculados a entidades públicas, universidades y empresas tecnológicas con actividad en el sector agroindustrial. Se aplicó un muestreo no probabilístico por conveniencia, seleccionando un total de 93 participantes que cumplían con los criterios de experiencia comprobada en gestión de datos agropecuarios y conocimientos en tecnologías digitales.

Resultados

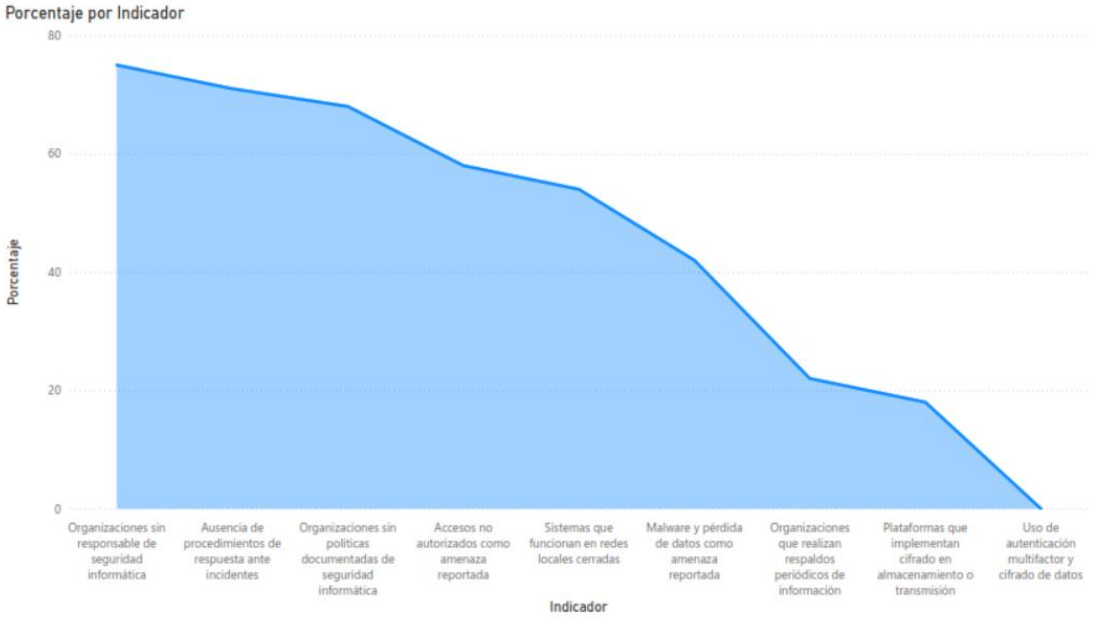
El análisis de los datos recopilados mediante encuestas estructuradas permitió identificar una situación crítica en torno a la gestión de la ciberseguridad en los sistemas de información agropecuarios (SIA)(Neira et al. 2023), caracterizada por una débil infraestructura tecnológica, escasa adopción de estándares de seguridad, y una cultura institucional poco orientada a la protección de los datos en el entorno digital agrícola (Urjilez et al. 2025).

Nivel de implementación de medidas de ciberseguridad

La Figura 4 muestra un gráfico de área que representa el nivel de implementación de medidas de ciberseguridad en organizaciones vinculadas al sector agropecuario. Cada punto del eje horizontal corresponde a un indicador clave extraído de las encuestas aplicadas a responsables de sistemas de información, mientras que el eje vertical refleja el porcentaje de incidencia reportado por los participantes.

Figura 4.

Nivel de implementación de medidas de ciberseguridad en organizaciones vinculadas al sector agropecuario



Nota. El gráfico muestra el porcentaje de implementación de medidas de ciberseguridad en organizaciones vinculadas al sector agropecuario, según los resultados de las encuestas aplicadas. Se observa una tendencia descendente que evidencia la falta de políticas, responsables y protocolos de seguridad, así como la escasa adopción de mecanismos de protección técnica.

Los resultados evidencian una tendencia descendente en la adopción de prácticas y controles relacionados con la seguridad informática, lo que confirma un bajo nivel de madurez digital en materia de protección de datos agropecuarios(Maraveas et al. 2024). En el extremo izquierdo del gráfico, se destacan indicadores críticos como:

- Ausencia de responsables de seguridad informática (75%)
- Falta de procedimientos de respuesta ante incidentes (71%)
- Carencia de políticas documentadas de seguridad (68%)

Estos datos reflejan deficiencias estructurales en la gobernanza tecnológica de las instituciones del sector, lo que incrementa significativamente su vulnerabilidad frente a ciberataques.

A medida que se avanza hacia la derecha del gráfico, se observan brechas adicionales en términos de infraestructura y medidas técnicas. Por ejemplo, un 58% de los encuestados reporta accesos no autorizados, mientras que solo el 18% cuenta con mecanismos de cifrado en el almacenamiento o

transmisión de datos, y apenas el 22% realiza respaldos periódicos de información. Finalmente, se identifica un dato especialmente preocupante: la nula implementación de autenticación multifactor y cifrado avanzado por parte de la mayoría de las organizaciones, lo que deja expuestos los sistemas incluso ante ataques de bajo nivel de sofisticación.

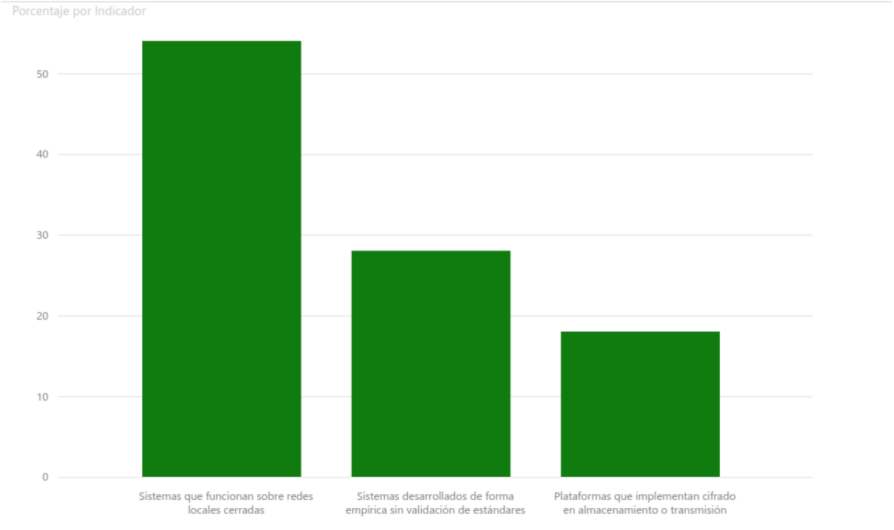
Este panorama refleja un nivel de madurez digital bajo en materia de seguridad, lo cual se agrava por la percepción errónea de que el sector agrícola no es un objetivo relevante para los ciber atacantes.

Infraestructura tecnológica y gestión de datos

La Figura 5 ilustra de forma comparativa las principales condiciones tecnológicas identificadas en los sistemas de información agropecuarios evaluados. A través de un gráfico de columnas, se visualiza el grado de implementación de prácticas clave relacionadas con la gestión segura de datos en entornos digitales agrícolas.

Figura 5.

Condiciones de infraestructura tecnológica en los SIA agropecuarios



Nota. La principal deficiencia en la infraestructura tecnológica de los SIA agropecuarios es el desarrollo empírico sin validación de estándares.

Fuente: Autor

El 54% de los sistemas analizados funcionan sobre redes locales cerradas, sin conexión a servicios en la nube. Si bien esta configuración limita la exposición directa a amenazas externas, también reduce considerablemente la escalabilidad, la automatización de respaldos y la posibilidad de aplicar medidas avanzadas de protección, como el monitoreo continuo o la inteligencia artificial.

Por otro lado, un 28% de los sistemas fueron desarrollados de manera empírica, sin validación de estándares de seguridad en el ciclo de vida del software. Esta condición representa una

vulnerabilidad estructural que expone a las plataformas a errores de diseño, puertas traseras no intencionadas y fallas en la protección de la información crítica, comprometiendo tanto la integridad de los datos como la continuidad operativa (Cedeño Zamora, Nauta Padilla, y Cabrera Toscano 2025).

Solo el 18% de las plataformas implementa cifrado en el almacenamiento o la transmisión de datos, lo cual representa un serio riesgo en términos de confidencialidad. La ausencia de cifrado básico hace que los datos productivos, climáticos o financieros puedan ser interceptados o manipulados fácilmente, especialmente en entornos con conectividad intermitente o escasa supervisión técnica(Arias Ariza y Vargas-Lombardo 2025).

Implicaciones para la seguridad agro-digital

Los resultados evidencian que la mayoría de los SIA agropecuarios carecen de una arquitectura tecnológica robusta, lo que limita su capacidad de resistir, detectar o responder a amenazas cibernéticas(Huo et al. 2024). El desarrollo empírico de sistemas, sin pruebas de penetración ni alineación con estándares internacionales como ISO/IEC 27001, convierte a estos entornos en objetivos vulnerables ante ciberataques, incluso de bajo nivel de sofisticación(Hastuti et al. 2025).

Estos hallazgos refuerzan la urgencia de establecer políticas públicas y marcos normativos adaptados al sector agropecuario, así como de invertir en formación técnica especializada para el diseño, desarrollo y mantenimiento de plataformas digitales seguras (Nurbojatmiko et al. 2025).

Resultados cualitativos: percepción, gestión institucional y conocimiento especializado

Las entrevistas a expertos en ciberseguridad y directores de TI revelaron que existe una brecha significativa entre el avance tecnológico de la agricultura digital y la protección de sus activos informáticos. La falta de capacitación, presupuestos reducidos para ciberseguridad, y una escasa articulación con marcos normativos vigentes dificultan la creación de entornos seguros(Alahe et al. 2024a).

En el plano institucional, el 75% de las organizaciones carece de una figura responsable de la seguridad de la información, y muchas delegan esa función en personal no especializado o de áreas administrativas, sin formación técnica en el manejo de riesgos cibernéticos. También se evidenció el desconocimiento generalizado de normativas como la ISO/IEC 27001 y otras buenas prácticas internacionales. Esta falta de alineación con estándares deja a las instituciones sin un marco de referencia claro para fortalecer sus capacidades defensivas.

Brechas normativas y ausencia de políticas públicas

Uno de los hallazgos más relevantes fue la ausencia de políticas públicas específicas para la protección de datos agropecuarios. Si bien existen normativas generales sobre protección de datos personales, estas no contemplan particularidades del entorno agrodigital, como:

- Datos productivos sensibles (por ejemplo, inventarios, rendimiento por hectárea o uso de fertilizantes),
- Información meteorológica procesada en tiempo real(Aguirre-Munizaga et al. 2019),
- Datos georreferenciados de parcelas productivas.

Esta ausencia de legislación específica genera zonas grises en cuanto a la responsabilidad legal en caso de pérdida de información, ciberataques o fallas de integridad en los sistemas.

Cultura de ciberseguridad y percepción del riesgo

Finalmente, los datos muestran que en el sector agropecuario existe una baja percepción del riesgo digital. Muchos actores aún consideran que sus sistemas “no son relevantes” para los atacantes y que “la seguridad no es una prioridad porque no manejan dinero directamente”, lo cual refleja una falta de conciencia del valor estratégico de los datos agrícolas(Alahmadi et al. 2022).

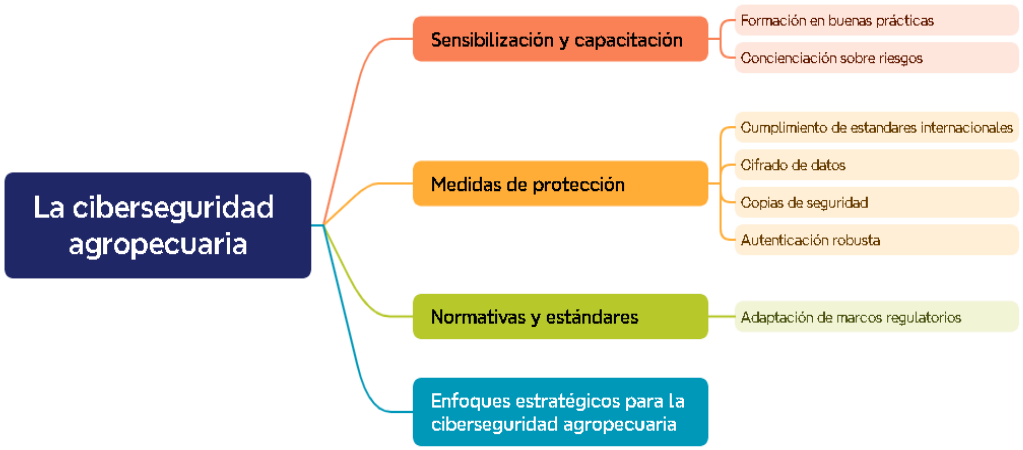
Esta percepción errónea limita la inversión en medidas preventivas, perpetúa una actitud reactiva y contribuye a la normalización de la inseguridad digital como parte de la operación cotidiana.

Enfoques estratégicos para fortalecer la ciberseguridad agropecuaria

A continuación, en la Figura 6 se presenta un mapa mental que resume los enfoques estratégicos derivados del estudio:

Figura 6.

Enfoque estratégico para fortalecer la ciberseguridad agropecuaria



Nota: La ciberseguridad agropecuaria requiere enfoques estratégicos que integren capacitación, protección tecnológica y marcos normativos adaptados al sector.

Fuente: Autor

Los resultados permiten concluir que la ciberseguridad en los sistemas de información agropecuarios es una dimensión crítica, actualmente desatendida, que representa una amenaza directa a la confiabilidad de la agricultura digital. La falta de normativas específicas, de recursos técnicos y de personal capacitado, sumada a una cultura organizacional limitada en cuanto a gestión de riesgos digitales, pone en evidencia la necesidad urgente de políticas integrales de ciberseguridad adaptadas al sector agropecuario.

Discusión

Los hallazgos del presente estudio confirman que los sistemas de información agropecuarios (SIA) en Ecuador enfrentan importantes desafíos en materia de ciberseguridad, los cuales coinciden con los problemas identificados por la literatura especializada. La limitada adopción de políticas de seguridad, la falta de procedimientos de respuesta ante incidentes y la baja implementación de tecnologías de protección reflejan un nivel de madurez digital incipiente, tal como señalan Sánchez y Zambrano (2019) al evidenciar la escasa alfabetización en seguridad informática entre productores agropecuarios ecuatorianos.

La exposición de los SIA a amenazas como accesos no autorizados, malware y pérdida de datos, observada en este estudio, se alinea con lo reportado por Alshammari et al. (2021), quienes

advierten que la digitalización de la agricultura incrementa la superficie de ataque debido a redes mal configuradas y dispositivos no seguros. En este sentido, si bien las tecnologías digitales han demostrado ser esenciales para mejorar la productividad, su adopción sin una estrategia de protección adecuada agrava los riesgos de vulneración de datos sensibles y compromete la trazabilidad de la producción.

El análisis también permitió identificar que más del 70% de las organizaciones carece de protocolos de seguridad y que solo una minoría aplica cifrado o respaldo automatizado, resultados que coinciden con los de Ferrag et al. (2022), quienes destacan la falta de soluciones específicas para el agro y la dependencia de datos simulados para entrenar sistemas de detección de intrusos. En este contexto, la incorporación de mecanismos como los Intrusion Detection Systems (IDS) basados en aprendizaje automático podría representar una línea de acción prioritaria para mejorar la vigilancia y respuesta frente a incidentes en tiempo real.

Además, el estudio revela una débil articulación entre marcos normativos, capacidades técnicas e institucionales, lo que refuerza la necesidad de un enfoque estratégico y sistémico. Zamora Boza et al. (2021). sostienen que esta falta de articulación entre la investigación, la política pública y el sector productivo ha limitado el desarrollo de una innovación agrícola sostenible. Esto concuerda con lo observado en los resultados, donde persisten vacíos normativos y una gestión institucional fragmentada de la ciberseguridad, especialmente en zonas rurales.

Desde un enfoque más técnico, Kristen et al. (2021)documentan cómo el aumento de los ataques de ransomware y otras amenazas avanzadas en el sector agroindustrial está vinculado a la escasa preparación técnica y a la subestimación del riesgo digital. Esta percepción errónea también fue evidenciada en el presente estudio, donde muchos actores del sector consideran que sus sistemas no son objetivos atractivos para los atacantes, lo cual frena la inversión en medidas preventivas y perpetúa una actitud reactiva.

Finalmente, los resultados cualitativos del estudio refuerzan la necesidad de fortalecer la cultura organizacional en torno a la seguridad digital, así como la formación técnica del personal que gestiona plataformas informáticas agropecuarias. Esto coincide con las recomendaciones de Wiseman et al. (2019), quienes señalan que la reticencia a compartir datos en la agricultura digital está influenciada por la falta de confianza y mecanismos robustos de protección.

Conclusiones

El presente estudio evidencia que la ciberseguridad en los sistemas de información agropecuarios representa un desafío estratégico crítico para el desarrollo sostenible de la agricultura digital en Ecuador (Facuy Toledo 2024). La investigación reveló que gran parte de las organizaciones agropecuarias opera con infraestructuras digitales mínimamente protegidas, sin políticas formales de seguridad, sin personal capacitado en gestión de riesgos cibernéticos y con una baja adopción de herramientas tecnológicas como cifrado, autenticación robusta o respaldos automatizados.

Asimismo, se constató que las amenazas más frecuentes, como accesos no autorizados, malware y ausencia de protocolos de respuesta ante incidentes, están directamente relacionadas con la falta de estándares técnicos, desconocimiento normativo y una cultura organizacional limitada en cuanto a la protección de datos estratégicos(Chávez García, Guacán Nepas, y Recalde Araujo 2025). Esta situación es especialmente preocupante en el contexto de la creciente digitalización del agro, donde la información productiva, genética, climática y georreferenciada constituye un activo esencial que debe ser resguardado.

La comparación con el estado del arte internacional demuestra que, si bien existen soluciones tecnológicas emergentes como los sistemas de detección de intrusos basados en inteligencia artificial, su adopción en el sector agropecuario ecuatoriano es aún incipiente. Del mismo modo, se evidencia una brecha entre el avance de la digitalización y la implementación de políticas públicas que regulen y promuevan la seguridad digital en el entorno rural.

En este marco, se concluye que la ciberseguridad debe ser abordada como un componente transversal en las políticas de innovación agrícola, integrando marcos normativos adaptados, fortalecimiento institucional, formación especializada y apropiación tecnológica segura. Solo mediante una visión articulada entre los sectores productivo, académico, gubernamental y tecnológico será posible consolidar un ecosistema agropecuario digital seguro, resiliente y competitivo, capaz de enfrentar los retos productivos, tecnológicos y de protección de datos del siglo XXI.

Aunque esta investigación proporciona una perspectiva completa de la ciberseguridad en los sistemas de información agropecuarios (SIA) en Ecuador, es importante reconocer algunas limitaciones metodológicas y analíticas que restringen la generalización de los resultados. Primero, el estudio se apoyó en un diseño exploratorio-descriptivo de encuesta y revisión bibliométrica, lo que limita la inferencia de relaciones de causalidad entre las variables estudiadas. La falta de estudios longitudinales o experimentales dificulta conocer cómo cambian en el tiempo las amenazas cibernéticas en el sector agropecuario y la efectividad de las medidas de mitigación

que sugieren las instituciones (Freyhof et al. 2025). Estas investigaciones, si bien son adecuadas para reconocer carencias, tienden a proporcionar una imagen estática más que una evaluación dinámica del riesgo digital rural.

Otra limitación importante tiene que ver con el tamaño y la representatividad de la muestra. Si bien se encuestaron 93 profesionales del sector, la mayoría de los encuestados trabajaban en instituciones públicas o universitarias, lo que puede sesgar la percepción del riesgo y la capacidad de respuesta ante incidentes. En el ámbito internacional, estudios comparativos como los de Alshammari et al. (2021) y Bissadu (2024) han encontrado que la cultura organizacional y la magnitud de la inversión en ciberseguridad difieren entre actores públicos, privados y cooperativas agrícolas, lo que limita la generalización de los resultados. Por lo cual, futuras investigaciones deberían usar un muestreo estratificado que incluya diferentes niveles de madurez tecnológica y tipos de explotaciones productivas, desde minifundios familiares hasta corporaciones agroindustriales, para mejorar la validez externa de los resultados.

En términos metodológicos, la investigación se apoyó en instrumentos bibliométricos como VOSviewer, con su fortaleza en la visualización de redes temáticas, pero con la limitación de depender de bases de datos indexadas. Esto puede crear un sesgo de cobertura, ya que mucha de la producción científica latinoamericana en ciberseguridad agrícola se queda en repositorios institucionales no indexados o en literatura gris (Douzet 2018b). Además, el abordaje bibliométrico no juzga la calidad metodológica de los estudios ni su impacto en la práctica, por lo cual es necesario suplementar estas herramientas con revisiones sistemáticas con criterios PRISMA y análisis cualitativos de contenido.

Desde el punto de vista conceptual, el análisis encontró que no existe acuerdo en la literatura sobre la definición de ciberseguridad agropecuaria. Mientras que algunos autores la tratan desde una perspectiva tecnológica, refiriéndose a la infraestructura digital y los mecanismos de seguridad (Palugula y Bevinakoppa 2024b), otros hablan de un problema sociotécnico relacionado con la gobernanza, la ética y la soberanía de los datos agrícolas (Barreto y Amaral 2018). Esta dispersión teórica impide la elaboración de un marco conceptual integral para orientar políticas y estrategias contextualizadas en el agro latinoamericano. Futuras investigaciones podrían crear modelos integradores que enlacen la seguridad tecnológica con la sostenibilidad y la equidad digital en la agricultura.

Además, la ausencia de datos empíricos sobre incidentes de seguridad en el sector agropecuario de Ecuador es una gran brecha. A diferencia de lugares como Asia o Europa, donde se registran métricas estandarizadas de ciberataques a infraestructuras agrícolas inteligentes (Hou et al. 2023),

en Ecuador no se cuenta con un sistema nacional de registro y seguimiento de ciberamenazas rurales. Por lo tanto, la medición del riesgo se apoya en opiniones y no en hechos. Se propone entonces la creación de observatorios sectoriales de ciberseguridad agropecuaria que aúnen bases de datos, protocolos de respuesta y canales de notificación de incidentes con los ministerios, las universidades y los productores.

Finalmente, una limitación transversal es que no se hace una evaluación económica de cuánto cuesta la vulnerabilidad informática y cuánto se gana invirtiendo en seguridad informática. Si bien la literatura internacional ya le da un valor económico a la ciberseguridad como un elemento de competitividad y sostenibilidad (Adli et al. 2023), aún no existen metodologías locales para calcular su impacto económico en el agro. Las futuras líneas de investigación deben incluir análisis costo-beneficio y modelos predictivos de IA para medir el ROI de la seguridad cibernética y su impacto en la productividad agrícola.

En resumen, este trabajo abre un nuevo campo de investigación que integra la ciberseguridad con la transformación digital del sector agropecuario(Rahmouni et al. 2022). Para superar las brechas encontradas se requiere un esfuerzo interdisciplinario para crear evidencia empírica, marcos regulatorios contextualizados y una cultura de protección de datos en el sector rural. Fortalecer la ciberseguridad agropecuaria como línea prioritaria de investigación no solo protegerá los activos cibernéticos del agro, sino que también contribuirá a la soberanía alimentaria y al desarrollo sostenible de los territorios rurales.

Referencias Bibliográficas

Adli, Hasyiya Karimah, Muhammad Akmal Remli, Khairul Nizar Syazwan Wan Salihin Wong, Nor Alina Ismail, Alfonso González-Briones, Juan Manuel Corchado, y Mohd Saberi Mohamad. 2023. «Recent Advancements and Challenges of AIoT Application in Smart Agriculture: A Review». *Sensors* 23(7):3752. doi:10.3390/s23073752.

Aguirre-Munizaga, Maritza, Mariana Briones-Zambrano, y Alberto Jurado-Chagerben. 2025. «Sistemas de Información Gerencial como una Herramienta Clave para la Toma de Decisiones Empresariales». *MQRInvestigar* 9(1):e138. doi:10.56048/MQR20225.9.1.2025.e138.

Aguirre-Munizaga, Maritza, Katty Lagos-Ortiz, Vanessa Vergara-Lozano, Karina Real-Avilés, Mitchell Vásquez-Bermudez, Andrea Sinche-Guzmán, y José Hernández-Rosas. 2019. «Analysis of Atmospheric Monitoring Data Through Micro-meteorological Stations, as a Crowdsourcing Tool for Technology Integration». *Information Systems and Technologies to Support Learning*, 181-87.

Aguirre-Munizaga, Maritza, Jorge Romero-Sánchez, Jefferson Quinde-Gonzabay, y Teresa Samaniego-Cobo. 2021. «Automation of Poultry Production Monitoring Through Web Services». Pp. 188-200 en *Technologies and Innovation*. Vol. 1460, *Communications in Computer and Information Science*, editado por R. Valencia-García, M. Bucaram-Leverone, J. Del Cioppo-Morstadt, N. Vera-Lucio, y E. Jácome-Murillo. Cham: Springer International Publishing.

Ahmed, Soumaya Marfoun-Dini, Anne-Carole Honfoga, y Patrick Sotindjo. 2023. «Security of digital agriculture networks: A review and bibliometric analysis». Pp. 1-9 en *2023 6th International Conference on Advanced Communication Technologies and Networking (CommNet)*. Rabat, Morocco: IEEE.

Alahe, Mohammad Ashik, Lin Wei, Young Chang, Sainath Reddy Gummi, James Kemeshi, Xufei Yang, Kwanghee Won, y Mazhar Sher. 2024a. «Cyber Security in Smart Agriculture: Threat Types, Current Status, and Future Trends». *Computers and Electronics in Agriculture* 226:109401. doi:10.1016/j.compag.2024.109401.

Alahe, Mohammad Ashik, Lin Wei, Young Chang, Sainath Reddy Gummi, James Kemeshi, Xufei Yang, Kwanghee Won, y Mazhar Sher. 2024b. «Cyber Security in Smart Agriculture: Threat Types, Current Status, and Future Trends». *Computers and Electronics in Agriculture* 226:109401. doi:10.1016/j.compag.2024.109401.

Alahmadi, Adel N., Saeed Ur Rehman, Husain S. Alhazmi, David G. Glynn, Hatoon Shoaib, y Patrick Solé. 2022. «Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture». *Sensors* 22(9):3520. doi:10.3390/s22093520.

Alshammari, Abeer, Qamra Alharbi, Rawan Alonazi, Nora Aljomaih, y Zainab Malik. 2021. «Smart Agriculture and Cybersecurity». 5:24-31.

Arias Ariza, Abimelec Antek, y Miguel Vargas-Lombardo. 2025. «Introducción a la Inteligencia Artificial y el Aprendizaje Automático en Ciberseguridad». *Revista Colón Ciencias, Tecnología y Negocios* 12(1):32-48. doi:10.48204/j.colonciencias.v12n1.a6824.

Barreto, Luis, y Antonio Amaral. 2018. «Smart Farming: Cyber Security Challenges». Pp. 870-76 en *2018 International Conference on Intelligent Systems (IS)*. Funchal - Madeira, Portugal: IEEE.

Bissadu, Kossi, Gahangir Hossain, y Leela Pavani Velagala. 2024. «A Enhancing Cybersecurity Resilience for Low-Income Farmers in Developing Nations: A Fuzzy Cognitive Mapping Approach». Pp. 1-6 en *2024 IEEE International Conference on Consumer Electronics (ICCE)*. Las Vegas, NV, USA: IEEE.

Castillo Gómez, José. 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. doi:10.64041/riidg.v2i2.40.

Cedeño Zamora, Karen Gabriela, Luis Daniel Nauta Padilla, y Eduardo Fabricio Cabrera Toscano. 2025. «Análisis de rentabilidad y eficiencia financiera del sector bananero del cantón La Maná. Estudio comparativo entre productores tradicionales y prácticas de agricultura de precisión». *Alpha International Journal* 3(2):5-26. doi:10.63380/aij.v3n2.2025.119.

Chávez García, Henry Alberto, Andy Paul Guacán Nepas, y Henry Marcelo Recalde Araujo. 2025. «Ciberseguridad en la era del IoT: Riesgos, desafíos y soluciones para la protección de redes domésticas y empresariales». *Revista Ingeniería e Innovación del Futuro* 4(1):101-15. doi:10.62465/riif.v4n1.2025.119.

De Salvo, Carmine Paolo, Lina Salazar, Mario González, Maja Schling, Gonzalo Muñoz, Gonzalo Rondinone, y Marion Le Pommellec. 2025. *Desarrollo sostenible de la agricultura en América Latina y el Caribe: desafíos y oportunidades*. Inter-American Development Bank. doi:10.18235/0013382.

Douzet, Frédérick. 2018a. *Cyber-Security Challenges*. Vol. 1. Oxford University Press.

Douzet, Frédérick. 2018b. *Cyber-Security Challenges*. Vol. 1. Oxford University Press.

Facuy Toledo, Dylan Paul. 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. doi:10.64041/riidg.v3i2.23.

Ferrag, Mohamed Amine, Lei Shu, Othmane Friha, y Xing Yang. 2022. «Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions». *IEEE/CAA Journal of Automatica Sinica* 9(3):407-36. doi:10.1109/JAS.2021.1004344.

Flórez-Martínez, Diego Hernando. 2024. «Una mirada al legado de los 25 años de la revista Ciencia y Tecnología Agropecuaria: una aproximación cienciométrica». *Ciencia y Tecnología Agropecuaria* 25(1). doi:10.21930/rcta.vol25_num1_art:3273.

Freyhof, Mark, George Grispos, Santosh Pitla, y William Mahoney. 2025. «Investigating The Implications of Cyberattacks Against Precision Agricultural Equipment». *International Conference on Cyber Warfare and Security* 20:93-104. doi:10.34190/iccws.20.1.3229.

Goldenits, Georg, y Thomas Neubauer. 2025. «Taxonomy of Cybersecurity Considerations in Agriculture». *Computers and Electronics in Agriculture* 237:110724. doi:10.1016/j.compag.2025.110724.

Guerra Dávila, Frank Eduardo, Eric Oswaldo Guerra Dávila, Diego Oswaldo Dávila Otero, Katherine Estefanía Chuquín Solís, y María Fernanda Guerrero Bolaños. 2024. «Adaptación de empresas imbabureñas a la cuarta revolución industrial en el contexto COVID-19: Adaptation of Imbaburan companies to the fourth industrial revolution in the context of COVID-19». *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades* 5(1). doi:10.56712/latam.v5i1.1613.

Hastuti, Puji, Nourma Islam Dewi Cantika, Aditya Pratama, y Dhanar Intan Surya Saputra. 2025. «Evaluating ERP Information Security Using ISO/IEC 27001:2013 Standard in Agricultural Technology Enterprises». *Inspiration: Jurnal Teknologi Informasi dan Komunikasi* 15(1):78-89. doi:10.35585/inspir.v15i1.120.

Hou, Kun Mean, Xunxing Diao, Hongling Shi, Hao Ding, Haiying Zhou, y Christophe De Vaulx. 2023. «Trends and Challenges in AIoT/IIoT/IoT Implementation». *Sensors* 23(11):5074. doi:10.3390/s23115074.

Huo, Dongyang, Asad Waqar Malik, Sri Devi Ravana, Anis Ur Rahman, y Ismail Ahmedy. 2024. «Mapping Smart Farming: Addressing Agricultural Challenges in Data-Driven Era». *Renewable and Sustainable Energy Reviews* 189:113858. doi:10.1016/j.rser.2023.113858.

Kjønås, Karianne, y Gaute Wangen. 2023. «A Survey on Cyber Security Research in the Field of Agriculture Technology». Pp. 1-8 en *2023 IEEE International Symposium on Technology and Society (ISTAS)*. Swansea, United Kingdom: IEEE.

Kristen, Erwin, Reinhard Kloibhofer, Vicente Hernández Díaz, y Pedro Castillejo. 2021. «Security Assessment of Agriculture IoT (AIoT) Applications». *Applied Sciences* 11(13):5841. doi:10.3390/app11135841.

Mancero-Castillo, Daniel, Yoansy Garcia, Maritza Aguirre-Munizaga, Daniel Ponce De Leon, Diego Portalanza, y Jorge Avila-Santamaria. 2024. «Dynamic Perspectives into Tropical Fruit Production: A Review of Modeling Techniques». *Frontiers in Agronomy* 6. doi:10.3389/fagro.2024.1482893.

Maraveas, Chrysanthos, Muttukrishnan Rajarajan, Konstantinos G. Arvanitis, y Anna Vatsanidou. 2024. «Cybersecurity Threats and Mitigation Measures in Agriculture 4.0 and 5.0». *Smart Agricultural Technology* 9:100616. doi:10.1016/j.atech.2024.100616.

Mishra, Shailendra, Aiman Albarakati, y Sunil Kumar Sharma. 2022. «Cyber Threat Intelligence for IoT Using Machine Learning». *Processes* 10(12):2673. doi:10.3390/pr10122673.

Neira, Evelin Giomara Criollo, Cristhian Humberto Flores Urgilés, Cristina Mariuxi Flores Urgilés, Julio Jhovany Santacruz Espinoza, y Mario Bernabé Ron Egas. 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):101-19. doi:10.29018/issn.2588-1000vol7iss49.2023pp101-119.

Nurbojatmiko, Nurbojatmiko, Muhammad Sharhan Khatami Karimiyah, Nur Muhammad Asnadi, y Rifka Anisyah. 2025. «ISO 27001 As Information Security Solution In Society 5.0 Era: Systematic Literature Review». *Sinkron* 9(1):484-92. doi:10.33395/sinkron.v9i1.14448.

Ocampo Alvarado, Andrés Marcelo. 2024. «Efectos de la transformación digital en el sector contable y financiero en Ecuador». *ACADEMO Revista de Investigación en Ciencias Sociales y Humanidades* 11(3):233-41. doi:10.30545/academo.2024.set-dic.2.

Padilla Díaz, Maria Ines, Ian David Criolla Cruz, Humberto García Viloria, y Martha Ceciliafranco Pacheco. 2024. «Producción científica sobre tendencias de innovación turística: Análisis bibliométrico de los aportes de la industria 4.0 en los períodos 2019-2023». *Revista Boletín Redipe* 13(6):114-32. doi:10.36260/v8f04k97.

Palugula, Nagendra Reddy, y Savitri Bevinakoppa. 2024a. «IoT Based Secure Data Sharing for Precision Agriculture with Optimal Clustering and Hybrid Encryption Algorithm». Pp. 1-6 en *2024 IEEE 9th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*. Bahrain, Bahrain: IEEE.

Palugula, Nagendra Reddy, y Savitri Bevinakoppa. 2024b. «IoT Based Secure Data Sharing for Precision Agriculture with Optimal Clustering and Hybrid Encryption Algorithm». Pp. 1-6 en *2024 IEEE 9th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*. Bahrain, Bahrain: IEEE.

Pinargote Bravo, Víctor Joel. 2023. «Desarrollo de arquitecturas de software para la gestión eficiente de grandes volúmenes de datos». *Innova Science Journal* 1(4):48-60. doi:10.63618/omd/isj/v1/n4/27.

Rahmouni, Mouad, Majdoulayne Hanifi, Claudio Savaglio, Giancarlo Fortino, y Mounir Ghogho. 2022. «An AIoT Framework for Precision Agriculture». Pp. 1-6 en *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. Falerna, Italy: IEEE.

Rodríguez Perea, Odalys. 2024a. «Comparación de modelos de comercialización directa e intermediada en el sector hortícola: análisis de márgenes de ganancia.» *Revista internacional de Investigación y Desarrollo Global* 3(3):17-33. doi:10.64041/riidg.v3i3.25.

Rodríguez Perea, Odalys. 2024b. «Comparación de modelos de comercialización directa e intermediada en el sector hortícola: análisis de márgenes de ganancia.» *Revista internacional de Investigación y Desarrollo Global* 3(3):17-33. doi:10.64041/riidg.v3i3.25.

Rodríguez-Correa, Paula Andrea, Camilo Andrés Echeverri-Gutiérrez, Alejandro Valencia-Arias, Leidy Catalina Acosta-Agudelo, y Mauricio Echeverri-Gutiérrez. 2023. «Tendencias en tecnologías convergentes en la industria 4.0: una revisión de literatura». *Revista ION* 36(2). doi:10.18273/revion.v36n2-2023006.

Rudrakar, Santoshi, y Parag Rughani. 2024. «IoT Based Agriculture (Ag-IoT): A Detailed Study on Architecture, Security and Forensics». *Information Processing in Agriculture* 11(4):524-41. doi:10.1016/j.inpa.2023.09.002.

Rueda Barrios, Gladys Elena, Jairo Alexander González Bueno, y Marianela Luzardo Briceño. 2022. *Factores determinantes de la competitividad y sostenibilidad de las empresas del sector agrícola en Santander*. Editorial Universidad Pontificia Bolivariana.

Sánchez, Hugo, y Jose Zambrano Mendoza. 2019. «Adopción e impacto de las tecnologías agropecuarias generadas en el Ecuador». *La Granja* 30(2):28-39. doi:10.17163/lgr.n30.2019.03.

Thilakarathne, Navod Neranjan, Muhammad Saifullah Abu Bakar, Pg Emeroylariffion Abas, y Hayati Yassin. 2025. «A Novel Cyber Threat Intelligence Platform for Evaluating the Risk Associated with Smart Agriculture». *Scientific Reports* 15(1). doi:10.1038/s41598-025-85320-8.

Urjilez, Hypatia, Danilo Valdez, Yoansy García, Maritza Aguirre, y Daniel Mancero. 2025. «Advances in Predictive Modeling in Fruit Crops: Mobile Applications». Pp. 354-63 en *Information Technology and Systems*. Vol. 1447, *Lecture Notes in Networks and Systems*, editado por A. Rocha, C. Ferrás, y H. Calvo. Cham: Springer Nature Switzerland.

Wiseman, Leanne, Jay Sanderson, Airong Zhang, y Emma Jakku. 2019. «Farmers and their data: An examination of farmers' reluctance to share their data through the lens of the laws impacting smart farming». *NJAS - Wageningen Journal of Life Sciences* 90-91:100301. doi:10.1016/j.njas.2019.04.007.

Zambrano Burgos, Velasco Rigoberto, Jael Dolores Zambrano Mieles, y Dolores Mieles Cevallos. 2025. «El rol de la inteligencia artificial en la automatización y la gestión de la cadena de suministro». *GADE: Revista Científica* 5(1):390-414. doi:10.63549/rg.v5i1.607.

Zamora Boza, Solange, Xavier Espinoza Herrera, Pablo San Andrés Reyes, y Adrián Moreno Silva. 2021. «Sistemas de innovación agrícola: una mirada a la situación del sector agrícola ecuatoriano: Agricultural innovation systems: a look to the situation of the ecuadorian agricultural sector». *REVISTA CIENTÍFICA ECOCIENCIA* 8:237-54. doi:10.21855/ecociencia.80.647.

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.