REVISTA ISTE SCIENTIST/ Vol. 5, N.02, 2026 (pág. xx-xx)
ISSN: 2953-6618 / Unidad de Investigación
Instituto Superior Tecnológico España

EVALUACIÓN DE RIESGOS DE CIBERSEGURIDAD EN SISTEMAS IOT APLICADOS A LA AGRICULTURA TROPICAL EN LA PROVINCIA DE MANABÍ

Rocio Alexandra Mendoza Villamar
https://orcid.org/0000-0002-1277-7162

Juana Isabel Salavarria Loor
https://orcid.org/0009-0002-9984-3106

Carmen Capitu Mendoza Armendariz
https://orcid.org/0000-0002-1277-7162

Jessenia Margarita Zambrano Zambrano
https://orcid.org/0009-0008-6003-5092

Universidad Laica Eloy Alfaro de Manabí (ULEAM), El Carmen, Ecuador
Correo autor principal: rocio.mendoza@uleam.edu.ec

Recibido: 11 de marzo de 2026 / Aprobado: 11 de mayo de 2026 / Publicado: día de mes de 2026

Resumen:
En los últimos años, los agricultores de Manabí han empezado a incorporar dispositivos IoT en sus cultivos de cacao, maíz y banano, una apuesta tecnológica que abre puertas reales para producir mejor y con más eficiencia. Pero esta transición también trae consigo un riesgo que muchas veces pasa desapercibido: la exposición a amenazas cibernéticas capaces de alterar datos de cultivo, interrumpir el riego automatizado o detener la producción en el peor momento. Este artículo nace precisamente de esa preocupación. Buscamos entender cuáles son los principales peligros de ciberseguridad en estos sistemas, qué tipos de ataques son más frecuentes en este contexto y cómo marcos internacionales como el NIST Cybersecurity Framework 2.0, la ISO/IEC 27001 y el IEC 62443 pueden orientar soluciones concretas para la realidad del campo manabita. Lo que encontramos no es menor: los ataques Man-in-the-Middle, los DDoS y la manipulación de firmware son las amenazas más serias en zonas tropicales donde la conectividad suele ser limitada e irregular. Y la conclusión apunta a algo que está al alcance de cualquier productor organizado: cifrar los datos, separar las redes y, sobre todo, formar a las personas que operan estos sistemas cada día.

Palabras Clave: Ciberseguridad, Internet de las Cosas, agricultura inteligente, Manabí, evaluación de riesgos, IoT agrícola.

REVISTA ISTE SCIENTIST/ Vol. 5, N.02, 2026 (pág. xx-xx)
ISSN: 2953-6618 / Unidad de Investigación
Instituto Superior Tecnológico España

Cybersecurity Risk Assessment in IoT Systems Applied to Tropical Agriculture in the Province of Manabí

Abstract: In recent years, farmers in Manabí have begun incorporating IoT devices into their cacao, corn, and banana crops a technological shift that opens real doors for smarter, more efficient production. But this transition also brings a risk that often goes unnoticed: exposure to cyber threats capable of corrupting crop data, disrupting automated irrigation, or halting production at the worst possible moment. This article grows out of exactly that concern. We set out to understand what the main cybersecurity dangers are in these systems, which types of attacks are most common in this context, and how international frameworks like the NIST Cybersecurity Framework 2.0, ISO/IEC 27001, and IEC 62443 can point toward concrete solutions for the real conditions of Manabí's farmland. What we found is not trivial: Man-in-the-Middle attacks, DDoS, and firmware manipulation are the most serious threats in tropical areas where connectivity tends to be limited and unreliable. And the conclusion points to something within reach of any organized producer: encrypt the data, segment the networks, and above all, train the people who operate these systems every single day.

Keywords: Cybersecurity, Internet of Things, smart agriculture, Manabí, risk assessment, agricultural IoT

Introducción

Manabí es mucho más que una provincia costera: es uno de los motores agrícolas del Ecuador, con cultivos como el cacao fino de aroma, el maíz, el banano y una ganadería que sostiene a miles de familias. En los últimos años, algo ha cambiado en el campo manabita. Los agricultores han empezado a adoptar tecnologías que antes parecían exclusivas de laboratorios o grandes industrias: sensores que miden la humedad del suelo, sistemas de riego que se activan solos, redes inalámbricas que transmiten datos en tiempo real. Todo esto, impulsado por la llamada Industria 4.0, ha mejorado notablemente la forma en que se usa el agua, se rastrea el estado de los cultivos y se toman decisiones en el día a día (Gallegos Zurita et al., 2023).

Pero esta modernización tiene una cara menos visible y bastante preocupante. Conectarse al mundo digital también significa quedar expuesto a sus riesgos, y en el caso de Manabí, esos riesgos se multiplican por condiciones muy concretas: redes de internet irregulares, dispositivos con poca capacidad para defenderse por sí solos, operadores que nadie ha capacitado en ciberseguridad, y una infraestructura tecnológica que muchas veces mezcla lo nuevo con lo viejo sin mayor planificación (Adewusi et al., 2022).

Los datos a nivel mundial no dejan mucho margen para la incertidumbre. Berghout et al. (2024) hallaron que el 80% de los sistemas de agricultura de precisión presentan fallos susceptibles a ser utilizados por atacantes y que los ataques de ransomware en fincas agrícolas se han cuadruplicado desde 2020 hasta ahora. No son números abstractos tras cada porcentaje se encuentra cosechas perdidas, sistemas detenidos y productos que no sabían que eran un objetivo. Eso nos llevó a preguntarnos algo muy concreto: ¿qué tan expuestos están los agricultores de Manabí que ya usan estas tecnologías, y qué opciones reales tienen para protegerse sin necesidad de grandes inversiones ni infraestructura que la región todavía no tiene?

Metodología

Para llevar a cabo este estudio, combinamos dos enfoques que se complementan bien. Por un lado, hicimos una revisión sistemática de la literatura siguiendo el protocolo PRISMA, que básicamente es una guía rigurosa para seleccionar y analizar estudios de forma ordenada y transparente. Revisamos investigaciones publicadas entre 2020 y 2025 en bases de datos como Scopus, Web of Science y Google Scholar, todas enfocadas en ciberseguridad aplicada a sistemas IoT agrícolas.

Un análisis de riesgo basado en el marco NIST CSF 2.0 costituyo la segunda parte del estudio. Lo estructuramos en cuatro fases que a pesar de sonar técnicas siguen una lógica muy programática. Comenzamos con lo más elemental conocer los dispositivos IoT que se utilizan efectivamente en las granjas de Manabí. Sin ese inventario seria hablar en vacío si se habla de riesgos. Luego llego la etapa más trabajosa identificar qué clase de ataques impactan a esos equipos en particular, acotejando los datos de la literatura con las anotaciones registradas de vulnerabilidad en bases como CVE y NVD. Con ese mapa de amenazas analizamos cada riesgo desde dos perspectivas la probabilidad de que suceda y que tan grave seria se lo hiciera utilizando una matriz 3x3 que facilita una rápita visualización de los puntos más críticos. Finalmente, con ese panorama claro, priorizamos las estrategias de protección según el nivel de riesgo que quedaba después de aplicar cada medida.

La idea detrás de este diseño fue no quedarse solo en la teoría, sino conectar lo que dice la literatura global con lo que realmente pasa en los sistemas agrícolas de Manabí.

Resultados

Al revisar la literatura, encontramos un inventario bastante representativo de los dispositivos que hoy forman parte del campo manabita conectado. Los más comunes son los sensores de humedad y temperatura DHT22, microcontroladores como el ESP32 y el Arduino Mega, módulos LoRa y GSM para la comunicación, sistemas de riego automatizado, estaciones meteorológicas enlazadas a plataformas en la nube como

ThingSpeak y AWS IoT, y los gateways LoRaWAN que hacen de puente entre el campo y el internet.El problema es que tanta variedad de equipos, cada uno hablando su propio idioma digital MQTT, HTTP, CoAP, LoRaWAN crea un sistema difícil de proteger de manera uniforme.Cada protocolo, cada dispositivo, es una puerta potencial para quien quiera entrar sin permiso.Y cuando miramos qué puertas aprovechan más los atacantes, el patrón fue claro.

El ataque más frecuente es el Man-in-the-Middle, donde alguien se mete silenciosamente en medio de la comunicación entre dispositivos y puede leer o alterar los datos sin que nadie lo note. Le siguen los ataques DDoS, que básicamente ahogan el sistema a punta de tráfico hasta dejarlo paralizado, y la modificación maliciosa de firmware, que es quizás la más peligrosa de todas porque cambia cómo se comporta el dispositivo desde adentro. Todo esto queda resumido en la Tabla 1.

Tipo de Riesgo	**Descripción**	**Vector de Ataque**	**Probabilidad**	**Impacto**
Intercepción de datos	Captura no autorizada de datos de sensores	Man-in-the-Middle (MitM)	Alta	Crítico
Acceso no autorizado	Intrusión en sistemas de control de riego	Credenciales débiles	Alta	Alto
Ataques DDoS	Saturación de la red agrícola IoT	Botnets sobre dispositivos IoT	Media	Alto
Firmware malicioso	Modificación de firmware en sensores	Actualización comprometida	Media	Crítico
Ransomware	Cifrado de datos agropecuarios	Phishing / enlace malicioso	Baja	Crítico
Spoofing de sensores	Falsificación de lecturas ambientales	Señal RF manipulada	Media	Alto

Tabla 1 Matriz de evaluación de riesgos de ciberseguridad en sistemas IoT agrícolas de Manabí

Estos riesgos no son solo teóricos. Pham et al. (2025) documentaron casos reales donde la falta de autenticación entre sensores y gateways permitió que atacantes manipularan datos de humedad del suelo, engañando al sistema de riego para que tomara decisiones equivocadas. Alharbi et al. (2023) mostraron cómo dispositivos con firmware desactualizado fueron secuestrados para lanzar ataques DDoS contra servidores agrícolas. Y Zidi et al. (2024) demostraron que un sistema de detección de intrusiones bien diseñado puede identificar estas amenazas con más del 94 % de precisión, incluso en entornos de agricultura inteligente.

Discusión

Lo que encontramos no sorprende a quienes conocen el campo manabita, pero sí preocupa. Los sistemas IoT agrícolas de la región están expuestos porque se combinan tres factores complicados al mismo tiempo: dispositivos con poca capacidad para defenderse solos, comunicaciones que viajan sin cifrar y operadores que nadie ha formado en ciberseguridad. No es culpa de nadie en particular, es el resultado de una digitalización que avanzó más rápido que la preparación para protegerla. Y esto, según la literatura, no es exclusivo de Manabí: es un patrón que se repite en la agricultura de precisión de muchos países en desarrollo (Kavallieratos et al., 2022; Rizvi et al., 2020).

Los marcos internacionales como el NIST CSF 2.0, la ISO/IEC 27001 y el IEC 62443 son herramientas útiles y bien estructuradas, pero hay que ser honestos: fueron pensados para industrias con recursos, personal especializado y conectividad estable. Aplicarlos al campo manabita requiere adaptarlos a una realidad donde el internet llega mal, los presupuestos son ajustados y los técnicos no siempre están disponibles. Las soluciones que mejor funcionan en este contexto son las que combinan tecnología de bajo costo y bajo consumo, como la criptografía ligera y los sistemas de detección embebidos, con capacitación real a las personas que operan estos equipos cada día (Drape et al., 2021; Moh'd Alia et al., 2023).

Hay que ser transparentes también sobre lo que este estudio no pudo hacer: todo se basó en revisión bibliográfica, sin trabajo de campo propio en la región. Lo que viene después debería incluir pruebas reales de penetración en dispositivos IoT usados en fincas de Manabí, y el diseño de sistemas de detección ajustados a las condiciones rurales del Ecuador.

Conclusión

Los sistemas IoT que están transformando la agricultura de Manabí también la están exponiendo a riesgos que no pueden seguir ignorándose. De todo lo que encontramos, tres amenazas concentran el mayor riesgo: los ataques MitM, los DDoS y la manipulación de firmware. No son las únicas, pero sí las que más daño pueden hacer en un entorno como el de Manabí, donde detectarlas a tiempo es difícil y recuperarse de ellas puede costar una temporada entera de producción. Frente a eso, no existe una solución mágica ni un solo botón que lo resuelva: lo que funciona es combinar varias cosas a la vez cifrado liviano, redes bien separadas, sistemas que detecten intrusiones y, quizás lo más importante, gente capacitada que sepa reconocer cuándo algo no está bien.

Los marcos internacionales como el NIST o la ISO son un buen punto de partida, pero leerlos desde Manta o El Carmen es otra cosa. Fueron escritos pensando en empresas con departamentos de IT, presupuestos holgados y fibra óptica estable. Adaptarlos al campo ecuatoriano es un trabajo que todavía está pendiente. Este artículo no pretende haberlo resuelto, pero sí haber abierto una puerta: la idea es que otros investigadores puedan tomar esto, salir al campo, probar con dispositivos reales y construir algo que de verdad le sirva al agricultor de Manabí, y con suerte también al de Esmeraldas, Los Ríos o cualquier otra provincia costera que está viviendo la misma transformación.

Referencias Bibliográficas

Adewusi, A. O., Chiekezie, N. R., & Eyo-Udo, N. L. (2022). Securing smart agriculture: Cybersecurity challenges and solutions in IoT-driven farms. World Journal of Advanced Research and Reviews, 15(3), 480–489. https://doi.org/10.30574/wjarr.2022.15.3.0887

Alharbi, A., Alsubhi, K., & Alsolami, F. (2023). Prediction of DDoS attacks in agriculture 4.0 with the help of prairie dog optimization algorithm with IDSNet. PLOS ONE, 18(9), e0291063. https://doi.org/10.1371/journal.pone.0291063

Berghout, T., Benbouzid, M., & Muyeen, S. M. (2024). Cybersecurity in smart agriculture: A systematic literature review. Computers & Security, 150, 104284. https://doi.org/10.1016/j.cose.2024.104284

Drape, T., Magerkorth, N., Sen, A., Simpson, J., Seibel, M., Murch, R. S., & Duncan, S. E. (2021). Assessing the role of cyberbiosecurity in agriculture: A case study. Frontiers in Bioengineering and Biotechnology, 9, 737927. https://doi.org/10.3389/fbioe.2021.737927

Gallegos Zurita, D. E., Rodriguez Castillo, K. B., & Ortiz Mosquera, N. S. (2023). Digitalización en el riego 4.0 y la captación de variables climáticas con dispositivos IoT, para optimizar la producción de maíz en un sector de Manabí. RECIAMUC, 7(2), 219–228. https://doi.org/10.26820/reciamuc/7.(2).abril.2023.219-228

Gloria, A., Cardoso, J., & Sebastião, P. (2021). Sustainable irrigation system for farming supported by machine learning and real-time sensor data. Sensors, 21(9), 3079. https://doi.org/10.3390/s21093079

Hamdan, S., Ayyash, M., & Almajali, S. (2023). Comprehensive study of IoT vulnerabilities and countermeasures. Applied Sciences, 15(6), 3036. https://doi.org/10.3390/app15063036

Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2022). Cyber-security threats and side-channel attacks for digital agriculture. Sensors, 22(9), 3520. https://doi.org/10.3390/s22093520

Moh'd Alia, O., Al-Ajmi, M., Al-Dmour, N., & Alqahtani, A. (2023). A secure IoT-based irrigation system for precision agriculture using the expeditious cipher. Sensors, 23(4), 2091. https://doi.org/10.3390/s23042091

National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0: Resource & overview guide (NIST SP 1299). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.1299

Neethirajan, S. (2025). Safeguarding digital livestock farming: A comprehensive cybersecurity roadmap for dairy and poultry industries. Frontiers in Big Data, 8, 1556157. https://doi.org/10.3389/fdata.2025.1556157

Oikonomou, G., & Nikoloudakis, Y. (2023). DDoS attack detection in IoT-based networks using machine learning models: A survey and research directions. Electronics, 12(14), 3103. https://doi.org/10.3390/electronics12143103

Pham, M. T., Nguyen, T. H., & Le, V. T. (2025). A novel cyber threat intelligence platform for evaluating the risk associated with smart agriculture. Scientific Reports, 15, 3820. https://doi.org/10.1038/s41598-025-85320-8

Rizvi, S., Pipetti, R., McIntyre, N., Todd, J., & Williams, I. (2020). Survey on security threats in agricultural IoT and smart farming. Sensors, 20(22), 6568. https://doi.org/10.3390/s20226568

Zidi, K., Ben Abdellafou, K., Aljuhani, A., Taouali, O., & Harkat, M. F. (2024). Novel intrusion detection system based on a downsized kernel method for cybersecurity in smart agriculture. Engineering Applications of Artificial Intelligence, 133, 107996. https://doi.org/10.1016/j.engappai.2024.107996