Agroecología Global
Revista Electrónica de Ciencias del Agro y Mar
Año VI. Vol. 6. N°10. Enero – Junio. 2024
Hecho el depósito legal: FA2019000051
FUNDACIÓN KOINONIA (F.K).
Santa Ana de Coro, Venezuela.

https://doi.org/10.35381/i.p.v8i15.5182

Gestión de riesgos de seguridad en dispositivos IoT en el sector agrícola

Security risk management for IoT devices in the agricultural sector

Steven Javier Gomez-Yumbo
sgomez5@utmachala.edu.ec
Universidad Técnica de Machala, Machala, El Oro
Ecuador
https://orcid.org/0009-0008-0411-9822

Jeremy Joel Riofrio-Valverde
jriofrio5@utmachala.edu.ec
Universidad Técnica de Machala, Machala, El Oro
Ecuador
https://orcid.org/0009-0008-6504-772X

Nancy Magaly Loja-Mora
nmloja@utmachala.edu.ec
Universidad Técnica de Machala, Machala, El Oro
Ecuador
https://orcid.org/0000-0002-5583-4278

Walter Marcelo Fuertes-Díaz
wmfuertes@espe.edu.ec
Universidad de las Fuerzas Armadas ESPE, Sangolquí, Pichincha
Ecuador
https://orcid.org/0000-0001-9427-5766

Recepción: 13 de abril 2026
Revisado: 16 de mayo 2026
Aprobación: 18 de junio 2026
Publicado: 01 de julio 2026

RESUMEN

El estudio tuvo como objetivo desarrollar un propuesta de gestión de riesgos de seguridad en dispositivos basados en internet de las cosas para el sector agrícola, orientada a una propuesta de controles técnicos para su tratamiento. La metodología se fundamentó en la norma ISO/IEC 27005:2022 para la identificación de activos, amenazas y vulnerabilidades en las capas de percepción, red, procesamiento y aplicación. El análisis integró los marcos normativos NIST SP 800-53, ETSI EN 303 645 y NISTIR 8259A para establecer criterios técnicos de seguridad y privacidad, valorando el impacto y la probabilidad según la normativa legal ecuatoriana de protección de datos personales. Los resultados evidenciaron que las capas de red y aplicación concentraron los escenarios de mayor criticidad frente a posibles ataques. Se concluyó que el proceso permitió identificar los activos con mayor exposición y fundamentar la propuesta de controles técnicos específicos para fortalecer la resiliencia en entornos agrícolas conectados.

Descriptores: Internet de las cosas; agricultura inteligente; gestión de riesgos; ciberseguridad; controles de seguridad. (Fuente: DeCS).

ABSTRACT

The study aimed to develop a proposal for the management of security risks in devices based on the Internet of Things for the agricultural sector, aimed at a proposal of technical controls for their treatment. The methodology was based on the ISO/IEC 27005:2022 standard for the identification of assets, threats, and vulnerabilities at the perception, network, processing, and application layers. The analysis integrated the regulatory frameworks NIST SP 800-53, ETSI EN 303 645 and NISTIR 8259A to establish technical security and privacy criteria, assessing the impact and probability according to the Ecuadorian legal regulations on the protection of personal data. The results showed that the network and application layers concentrated the most critical scenarios against possible attacks. It was concluded that the process made it possible to identify the assets with the greatest exposure and to inform the proposal of specific technical controls to strengthen resilience in connected agricultural environments.

Descriptors: Internet of things; smart agriculture; risk management; cybersecurity; security controls. (Source: DeCS).

INTRODUCCIÓN

El internet de las cosas (IoT) ha revolucionado las prácticas tradicionales de cultivo y ganadería, permitiendo automatizar procesos, recolectar datos en tiempo real y optimizar recursos (Loza González, 2021). Sin embargo, esta evolución tecnológica conlleva importantes desafíos de ciberseguridad, que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos. Los dispositivos IoT en agricultura presentan vulnerabilidades significativas debido a la falta de estándares de seguridad, mecanismos de autenticación débiles y actualizaciones de firmware deficientes (Campoverde-Molina y Luján-Mora, 2025).

La arquitectura IoT se compone por cuatro capas interconectadas que trabajan de manera coordinada. La capa de percepción incluye, en el sector agrícola, sensores y actuadores; la capa de red es la responsable de la transmisión de datos; la capa de procesamiento en donde los datos son almacenados y analizados; y la capa de aplicación que proporciona la interfaz al usuario final (Rudrakar y Rughani, 2024), cada una de estas capas presentan vulnerabilidades especificas que deben ser identificadas y mitigadas con controles de seguridad adecuados para proteger toda la arquitectura.

Investigaciones recientes evidencian que los agricultores que adoptaron estas tecnologías perciben mejoras en el rendimiento, reducción de tiempos de producción y mayor calidad de los productos (Izquierdo et al., 2025). Sin embargo, la implementación sin un adecuado control de seguridad expone a las explotaciones a riesgos críticos relacionados con la transmisión y almacenamiento de datos. Estudios especializados han identificado que la capa de percepción es particularmente vulnerable debido a la heterogeneidad de dispositivos, la diversidad de protocolos de comunicación y las limitaciones de recursos computacionales de los sensores y actuadores (Khattak et al., 2019).

De la misma manera, la naturaleza de cómo se distribuyen los sistemas agrícolas inteligentes amplían considerablemente los puntos débiles para posibles ataques en

donde no solo se encuentran en riesgo los equipos físicos en el terreno, sino también las señales inalámbricas que los conectan, quedando expuestos a diversas amenazas (Yazdinejad et al., 2021).

Para abordar estos desafíos, el marco normativo internacional proporciona diversas guías y estándares orientados a la gestión de riesgos y la seguridad en entornos IoT. La norma ISO/IEC 27005:2022 establece directrices para la gestión de riesgos de seguridad de la información, mientras que estándares como NIST SP 800-53, ETSI EN 303 645 y NISTIR 8259A ofrecen lineamientos y controles técnicos específicos para fortalecer la seguridad y la privacidad en dispositivos y sistemas IoT. En el contexto ecuatoriano, la Ley Orgánica de Protección de Datos Personales (LOPDP) establece criterios relacionados con la protección y el tratamiento de datos personales, considerados en la valoración del impacto dentro del análisis de riesgos.

La aplicación de controles técnicos y criterios normativos contribuye a fortalecer la protección de la información y reducir la probabilidad de incidentes de seguridad en entornos donde se manejan datos sensibles (Vega et al., 2025). Además, es importante incorporar la protección de la información desde las etapas iniciales en el desarrollo de las soluciones tecnológicas, ya que al integrar requisitos de seguridad y el cumplimiento normativo, se busca anticipar posibles problemas (Castro-Paredes et al., 2025). En entornos IoT esta relación es crítica debido a que la naturaleza de estos dispositivos exige combinar la seguridad técnica y el cuidado de datos sensibles.

Este artículo tuvo como objetivo desarrollar un propuesta de gestión de riesgos de seguridad en dispositivos basados en internet de las cosas para el sector agrícola, orientada a una propuesta de controles técnicos para su tratamiento

MÉTODO

La investigación adoptó un enfoque cualitativo con alcance exploratorio y descriptivo, orientado al análisis de los riesgos de seguridad presentes en dispositivos de Internet de

las Cosas (IoT) aplicados en el sector agrícola. El propósito fue desarrollar una gestión de riesgos de seguridad que permitiera identificar los activos más relevantes, valorar su impacto y probabilidad, evaluar su nivel de riesgo y proponer controles técnicos para su tratamiento.

El estudio se desarrolló bajo los lineamientos de la norma ISO/IEC 27005:2022, la cual sirvió como base para estructurar el proceso metodológico. La propuesta de controles se respaldó documentalmente mediante referencias como NIST SP 800-53, ETSI EN 303 645 y NISTIR 8259A, considerando además el contexto agrícola ecuatoriano y la normativa nacional de protección de datos.

En la primera fase se realizó la identificación y clasificación de los activos IoT agrícolas, organizándolos en las capas de percepción, red, procesamiento y aplicación. En la segunda fase se establecieron los criterios de valoración del impacto mediante los componentes de confidencialidad, integridad, disponibilidad y cumplimiento legal, considerando la LOPDP del Ecuador cuando el tratamiento involucró datos personales o información vinculable a personas. La tercera fase consistió en definir criterios de valoración de la probabilidad considerando la amenaza y la vulnerabilidad de cada escenario analizado. En la cuarta fase se realizó la evaluación del riesgo y su representación en un mapa de calor partiendo de la relación entre impacto y probabilidad, lo que permitió la clasificación de los riesgos según su nivel de criticidad. Como último paso en la quinta fase se propusieron los controles técnicos de seguridad necesarios para mitigar los riesgos identificados, respaldados documentalmente por referencias normativas, en esta misma fase: se planteó el tratamiento del riesgo, relacionando cada escenario evaluado con los controles propuestos y estimando el riesgo residual esperado tras su aplicación. La Figura 1 presenta de manera esquemática la secuencia metodológica aplicada.

Figura 1. Metodología aplicada para el análisis de riesgos.
Elaboración: Los autores.

RESULTADOS

Fase 1. Identificación y clasificación de activos IoT

Se identificaron los principales dispositivos IoT utilizados en el sector agrícola, de acuerdo con su función en actividades de monitoreo, automatización, conectividad, procesamiento y supervisión. Esta revisión permitió organizar la arquitectura IoT agrícola en las categorías de percepción, red, procesamiento y aplicación, estableciendo una base estructurada para el análisis posterior de seguridad.

La Tabla 1 reúne los dispositivos IoT identificados, su categoría, su uso agrícola principal y las fuentes bibliográficas que sustentan su inclusión. Este inventario permitió definir los

activos considerados en el estudio y sirvió como punto de partida para la valoración del impacto, la probabilidad, la evaluación del riesgo y la propuesta de controles técnicos.

Tabla 1.
Clasificación de los dispositivos IoT agrícolas.

ID	Categoría	Dispositivo	Uso agrícola principal	Fuentes
A1	Percepción	Sensores de humedad de suelo	Medir humedad del suelo para control de riego automático	(Montaño-Blacio et al., 2023) (Laverde Mena et al., 2021)
A2	Percepción	Sensores ambientales	Monitorear temperatura, humedad ambiental, luminosidad o radiación para la gestión de cultivos e invernaderos	(Montaño-Blacio et al., 2023); (Mosquera Meléndrez & Cevallos Rojas, 2022)
A3	Percepción	Sensores de pH y nutrientes	Controlar acidez y nutrientes en agua de riego o invernadero	(Montaño-Blacio et al., 2023)
A4	Percepción	Actuadores de riego	Automatizar el flujo de agua o fertilizantes en sistemas de riego	(Larrea et al., 2024)
A5	Red	Gateways LPWAN	Comunicar nodos remotos de sensores hacia otros componentes del sistema	(Rivera Guzmán et al., 2022)
A6	Red	Routers y tecnologías de comunicación de largo alcance	Proveer conectividad local o remota en entornos agrícolas con infraestructura limitada	(Novillo et al., 2022); (Tao et al., 2021)
A7	Procesamiento	Controladores y sistemas de procesamiento local	Ejecutar lógica de control, procesamiento y registro de datos de sensores en sistemas agrícolas	(Mosquera Meléndrez & Cevallos Rojas, 2022); (Novillo et al., 2022)
A8	Procesamiento	Módulos en maquinaria/UAV	Apoyar tareas automatizadas en drones, tractores conectados u otros equipos agrícolas	(Rejeb et al., 2022) (Boursianis et al., 2022)
A9	Aplicación	Dispositivos y estaciones de supervisión	Permitir la supervisión y el control operativo mediante interfaces móviles o estaciones locales	(Benyezza et al., 2023)
A10	Aplicación	Plataformas en la nube	Realizar almacenamiento, análisis y gestión centralizada de datos agrícolas	(Debauche et al., 2021) (Ivanochko et al., 2024)

Elaboración: Los autores.

Fase 2. Valoración del impacto

En esta fase se medió la gravedad del daño asociado a los activos IoT agrícolas, considerando los efectos que causarían en la seguridad, la operatividad y el cumplimiento legal. Para esta valoración se integraron los criterios de confidencialidad, integridad,

disponibilidad y el cumplimiento de la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP), teniendo como objetivo determinar cómo la afectación de un activo podría comprometer la producción, el acceso a la información agrícola o la exposición de datos personales vinculados con los productores.

Como se observa en la Tabla 2, el impacto se clasificó en cinco niveles: muy bajo, bajo, medio, alto y crítico, analizando tanto las consecuencias técnicas como las responsabilidades legales.

Tabla 2.
Criterios de impacto para la valoración.

Nivel	Valor	Confidencialidad (C)	Integridad (I)	Disponibilidad (D)	LOPDP (L)
Muy bajo	1	Divulgación sin importancia que no afecta ningún dato sensible ni operativo.	Cambios insignificantes en datos que no afectan decisiones.	Interrupciones menores sin repercusión operativa.	No existe infracción; no se tratan datos personales.
Bajo	2	Divulgación de información interna con efectos mínimos.	Alteraciones menores que requieren correcciones simples.	Interrupciones breves que afectan parcialmente la operación.	Gestión poco clara de datos genera leve afectación a transparencia y responsabilidad.
Medio	3	Divulgación no autorizada de información sensible agrícola o de operación.	Modificación de datos que alteran decisiones operativas	Interrupciones que retrasan procesos o afectan cultivos.	Acceso no autorizado a datos provoca incumplimiento de calidad, confidencialidad y seguridad.
Alto	4	Exposición de credenciales, claves, configuraciones de dispositivos IoT.	Modificación severa de registros que compromete la producción.	Interrupciones prolongadas con pérdidas económicas significativas.	Exposición de credenciales evidencia fallas de control, afectando confidencialidad, seguridad y responsabilidad.
Crítico	5	Fuga masiva de datos personales, datos biométricos o datos sensibles del productor.	Manipulación total de información, pérdida irreparable o falsificación deliberada.	Caída total del sistema que detiene siembras, riego o procesos críticos.	La fuga o manipulación de datos vulnera la confidencialidad, seguridad y juridicidad.

Elaboración: Los autores.

Para calcular el impacto base de cada activo se utilizó la siguiente fórmula:

$$CIDL = \frac{C+I+D+L}{4} \qquad [1]$$

donde:

C representa la confidencialidad, I la integridad, D la disponibilidad y L el cumplimiento legal asociado a la LOPDP. El valor obtenido corresponde al impacto promedio del activo y se emplea posteriormente en la evaluación del riesgo.

Fase 3. Valoración de la probabilidad

En esta fase se evaluó las posibilidades de que un ataque se materializara, considerando tanto la condición de la amenaza como las vulnerabilidades de cada activo IoT. Esta valoración permitió identificar qué situaciones presentan mayor probabilidad de suceder utilizando criterios cualitativos y semicuantitativos. Como se observa en la Tabla 3, la probabilidad se clasificó en cinco niveles: muy baja, baja, media, alta y crítica, a partir de la valoración de la amenaza y la vulnerabilidad.

Tabla 3.
Criterios de probabilidad de amenazas y vulnerabilidades.

Nivel	Valor	Amenazas	Vulnerabilidad
Muy bajo	1	La amenaza es remota y su materialización tendría poca posibilidad de afectar el activo.	El activo presenta controles adecuados y pocas debilidades explotables.
Bajo	2	La amenaza puede ocurrir en condiciones poco frecuentes, pero con un impacto limitado.	El activo presenta debilidades menores o medianamente mitigadas.
Medio	3	La amenaza representa un riesgo real y es capaz de afectar la operatividad o integridad de los datos.	El activo presenta protecciones básicas o incompletas.
Alto	4	La amenaza es probable y puede afectar a los datos, servicios o procesos del entorno agrícola.	El activo presenta fallos críticos de seguridad, cifrado o contiene configuraciones débiles.
Crítico	5	La amenaza es altamente probable y puede comprometer el control del activo o afectar varios componentes del sistema.	El activo presenta vulnerabilidades severas, explotables de forma directa y con escasas barreras de protección.

Elaboración: Los autores.

Fase 4. Evaluación del riesgo y mapa de calor

En esta fase se efectuó la evaluación del riesgo a partir de la relación entre el impacto y la probabilidad de cada escenario identificado, mediante la expresión:

$$R = I \times A \times V \qquad [2]$$

donde R, representa el nivel de riesgo; I, corresponde al impacto del activo; A, la amenaza; y V, la vulnerabilidad. Este cálculo, alineado con el enfoque de la ISO/IEC 27005, permitió determinar el nivel de riesgo asociado a cada activo IoT agrícola evaluado y establecer su grado de criticidad dentro del entorno analizado.

La Tabla 4 muestra la escala de interpretación del riesgo empleada para clasificar los valores obtenidos en cinco niveles: Muy bajo (1–25), Bajo (26–50), Medio (51–75), Alto (76–100) y Crítico (101–125). Esta escala establece que, si los riesgos son muy bajos se consideran insignificantes y no requieren acciones adicionales, los riesgos de nivel bajo son aceptables y requieren un monitoreo básico, los riesgos de nivel medio requieren mejoras técnicas, los riesgos de nivel alto requieren un tratamiento prioritario y los riesgos críticos se consideran inaceptables y requieren de una acción inmediata. Esta clasificación permitió interpretar los resultados obtenidos en la matriz de evaluación del riesgo de forma coherente y alineada con los criterios definidos al inicio.

Tabla 4.
Criterios de probabilidad de amenazas y vulnerabilidades.

Nivel	Valor	Descripción
1. Muy bajo	**1 – 25**	Riesgo insignificante; no requiere acción
2. Bajo	**26 – 50**	Riesgo aceptable; monitoreo básico
3. Medio	**51 – 75**	Requiere mejoras moderadas
4. Alto	**76 – 100**	Necesita tratamiento prioritario
5. Crítico	**101 – 125**	No aceptable; requiere acción inmediata

Elaboración: Los autores.

La Tabla 5 detalla la valoración del impacto de los activos IoT agrícolas identificados. El CIDL se calculó a partir de los criterios de Confidencialidad (C), Integridad (I), Disponibilidad (D) y Cumplimiento legal (L). El promedio de los componentes permitió determinar el impacto base de cada activo, el cual se empleó en la evaluación del riesgo.

Tabla 5.
Valoración del impacto de los activos IoT agrícolas.

ID	Activo	C	I	D	L	CIDL
A1	Sensores de humedad de suelo	3	4	4	2	3.25
A2	Sensores ambientales	3	4	4	2	3.25
A3	Sensores de pH y nutrientes	3	4	4	2	3.25
A4	Actuadores de riego	2	5	5	2	3.50
A5	Gateways LPWAN	5	5	5	4	4.75
A6	Routers y tecnologías de comunicación de largo alcance	4	4	5	3	4.00
A7	Controladores y sistemas de procesamiento local	4	5	5	3	4.25
A8	Módulos en maquinaria/UAV	4	5	4	3	4.00
A9	Dispositivos y estaciones de supervisión	4	4	3	4	3.75
A10	Plataformas en la nube	5	5	5	5	5.00

Elaboración: Los autores.

La Tabla 6 presenta la evaluación del riesgo por activos IoT agrícolas, considerando el impacto estimado mediante el valor CIDL, las amenazas y las vulnerabilidades asociadas a cada escenario. En la matriz, I representa el impacto; A, el nivel de amenaza; V, el nivel de vulnerabilidad y R, el valor final del riesgo. Debido a que un mismo activo puede estar expuesto a más de una amenaza, algunos dispositivos se repiten en distintas filas.

Los resultados muestran que los riesgos más relevantes se concentran en activos de conectividad, control y gestión de información, como gateways LPWAN, controladores locales y plataformas en la nube, donde se alcanzan niveles de riesgo altos. Por su parte, los sensores y dispositivos de percepción presentan principalmente riesgos bajos y medios, asociados con la manipulación de lecturas, exposición de datos y accesos no autorizados. Se identificaron y priorizaron los escenarios que requieren tratamiento y se definió controles orientados a la protección del dispositivo.

Tabla 6.
Evaluación del riesgo por activos IoT agrícolas.

ID	Activo	Amenaza	Vulnerabilidad	I	A	V	R	Nivel
R1	Sensores de humedad de suelo	Interceptación o alteración de lecturas	Transferencia y almacenamiento inseguro de datos	3.25	3	3	29.25	Bajo
R2	Sensores de humedad de suelo	Acceso no autorizado al sensor	Credenciales débiles, predecibles o embebidas	3.25	4	4	52.00	Medio
R3	Sensores ambientales	Manipulación de datos ambientales	Transferencia y almacenamiento inseguro de datos	3.25	3	3	29.25	Bajo
R4	Sensores ambientales	Control remoto no autorizado	Credenciales débiles, predecibles o embebidas	3.25	4	4	52.00	Medio
R5	Sensores de pH y nutrientes	Manipulación de datos de calidad del agua	Transferencia y almacenamiento inseguro de datos	3.25	3	4	39.00	Bajo
R6	Actuadores de riego	Ejecución de comandos maliciosos	Interfaces del ecosistema inseguras	3.50	4	4	56.00	Medio
R7	Gateways LPWAN	Acceso no autorizado al gateway	Credenciales débiles, predecibles o embebidas	4.75	5	4	95.00	Alto
R8	Gateways LPWAN	Denegación de servicio sobre comunicaciones	Servicios de red inseguros o innecesarios expuestos	4.75	4	4	76.00	Alto
R9	Routers y tecnologías de comunicación de largo alcance	Interrupción de la conectividad	Servicios de red inseguros o innecesarios expuestos	4.00	4	4	64.00	Medio
R10	Routers y tecnologías de comunicación de largo alcance	Exposición por configuración insegura	Configuración por defecto insegura o no endurecida	4.00	4	4	64.00	Medio
R11	Controladores y sistemas de procesamiento local	Instalación de firmware malicioso	Falta de un mecanismo seguro de actualización	4.25	4	5	85.00	Alto
R12	Controladores y sistemas de procesamiento local	Exposición por gestión deficiente del dispositivo	Gestión deficiente del dispositivo	4.25	3	3	38.25	Bajo
R13	Módulos en maquinaria/UAV	Toma de control o manipulación remota	Interfaces del ecosistema inseguras	4.00	4	4	64.00	Medio
R14	Módulos en maquinaria/UAV	Explotación de componentes obsoletos	Uso de componentes inseguros u obsoletos	4.00	3	4	48.00	Bajo
R15	Dispositivos y estaciones de supervisión	Exposición de credenciales o acceso no autorizado	Credenciales débiles, predecibles o embebidas	3.75	4	4	60.00	Medio
R16	Dispositivos y estaciones de supervisión	Manipulación de la interfaz de operación	Interfaces del ecosistema inseguras	3.75	4	4	60.00	Medio
R17	Plataformas en la nube	Administración no autorizada de la plataforma	Configuración por defecto insegura o no endurecida	5.00	5	4	100.00	Alto
R18	Plataformas en la nube	Fuga de datos o credenciales	Protección insuficiente de privacidad	5.00	4	5	100.00	Alto

Elaboración: Los autores.

Fase 5. Plan de tratamiento del riesgo

En esta fase se proponen los controles técnicos para el tratamiento de los riesgos identificados en los activos IoT agrícolas. La selección de estos controles se sustentó documentalmente en la ISO/IEC 27005:2022 como marco para el tratamiento del riesgo, en NIST SP 800-53 como catálogo de controles de seguridad, en NISTIR 8259A como referencia de capacidades básicas de ciberseguridad para dispositivos IoT y en ETSI EN 303 645 como guía práctica para dispositivos conectados. La Tabla 7 presenta los controles técnicos propuestos y una descripción de su función en del tratamiento del riesgo.

Tabla 7.
Controles técnicos propuestos para el tratamiento del riesgo.

ID	Control técnico	Descripción del control
CT1	Autenticación fuerte.	Implementar mecanismos de autenticación robusta en dispositivos, plataformas y servicios, eliminando credenciales por defecto y estableciendo credenciales únicas y seguras para cada activo.
CT2	Gestión segura de credenciales.	Proteger el almacenamiento, uso, renovación y revocación de contraseñas, claves y secretos, evitando su reutilización o exposición no autorizada.
CT3	Cifrado de datos en tránsito.	Proteger la telemetría, comandos y credenciales durante la comunicación entre sensores, gateways, controladores y aplicaciones mediante mecanismos adecuados.
CT4	Cifrado de datos en reposo.	Asegurar la confidencialidad de la información sensible almacenada en el hardware o la nube, incluyendo registros, claves, configuraciones y datos operativos de accesos no autorizados.
CT5	Actualización segura de firmware y software.	Implementar procesos de actualización que validen su autenticidad, sean íntegras y verificables, evitando la instalación de firmware malicioso.
CT6	Hardening de configuración.	Desactivar puertos, servicios, cuentas y funciones innecesarias para reducir la superficie de exposición y eliminar configuraciones débiles de fábrica.
CT7	Protección de interfaces físicas.	Bloquear el acceso a puertos físicos como UART, JTAG, USB para prevenir la manipulación directa del hardware o la extracción de datos.
CT8	Seguridad física del dispositivo.	Proteger físicamente sensores, actuadores, gateways y controladores mediante cerramientos o cajas seguras para evitar sabotajes, robos o daños intencionados.
CT9	Seguridad de red y segmentación.	Implementar aislamiento lógico, segmentación y control de tráfico, evitando que una intrusión en alguna capa se propague al resto del sistema.
CT10	Integridad de datos y comandos.	Garantizar que las órdenes de control y datos recolectados no hayan sido alteradas durante la transmisión utilizando firmas digitales o validaciones criptográficas.
CT11	Monitoreo técnico y registros de seguridad.	Mantener una vigilancia mediante logs y alertas en tiempo real que permitan identificar intentos de intrusión o fallos de configuración.
CT12	Detección de anomalías.	Evaluar patrones del comportamiento del trafico y telemetría para detectar desviaciones maliciosas.

CT13	Protección de privacidad y minimización de datos.	Priorizar la privacidad limitando la recolección de información a datos estrictamente usados para la operación, bajo criterios de protección de datos sensibles.
CT14	Redundancia y tolerancia a fallos.	Incorporar mecanismos de respaldo que aseguren la continuidad del dispositivo ante cortes de energía, caídas de red o fallos en la comunicación.
CT15	Gestión segura del fin de vida.	Asegurar el borrado de datos, la eliminación de credenciales y el retiro confiable de los dispositivos cuando sean reemplazados o desincorporados.

Elaboración: Los autores.

La Tabla 8 presenta los controles implementados, el tipo de control, el impacto del activo I, los valores residuales de amenaza A y vulnerabilidad V, el riesgo residual R, el nivel resultante y el criterio de aceptación. Los resultados muestran una reducción clara de los riesgos a niveles residuales mínimos lo que demuestra la efectividad de los controles. Sin embargo, en escenarios relacionados con gateways LPWAN, controladores y plataformas en la nube se encuentran en un nivel aceptable bajo monitoreo, debido a la importancia que presentan dentro de la arquitectura IoT y el impacto que tienen en la operación agrícola.

Tabla 8.
Matriz del tratamiento del riesgo.

ID	Controles implementados	Tipo de control	I	A	V	R	Nivel	Criterio de aceptación
R1	CT3, CT10, CT11	Preventivo / Detectivo	3.25	2	2	13.00	Muy bajo	Aceptable
R2	CT1, CT2, CT6, CT11	Preventivo / Detectivo	3.25	2	3	19.50	Muy bajo	Aceptable
R3	CT3, CT10, CT11	Preventivo / Detectivo	3.25	2	2	13.00	Muy bajo	Aceptable
R4	CT1, CT2, CT6, CT11	Preventivo / Detectivo	3.25	2	3	19.50	Muy bajo	Aceptable
R5	CT3, CT10, CT11	Preventivo / Detectivo	3.25	2	2	13.00	Muy bajo	Aceptable
R6	CT1, CT7, CT8, CT10	Preventivo	3.50	3	2	21.00	Muy bajo	Aceptable
R7	CT1, CT2, CT6, CT9, CT11	Preventivo / Detectivo	4.75	3	3	42.75	Bajo	Aceptable con monitoreo
R8	CT9, CT11, CT14	Preventivo / Detectivo / Correctivo	4.75	3	2	28.50	Bajo	Aceptable con monitoreo

R9	CT9, CT11, CT14	Preventivo / Detectivo / Correctivo	4.00	3	2	24.00	Muy bajo	Aceptable
R10	CT6, CT9, CT11	Preventivo / Detectivo	4.00	2	3	24.00	Muy bajo	Aceptable
R11	CT5, CT6, CT11	Preventivo / Detectivo	4.25	3	2	25.50	Bajo	Aceptable con monitoreo
R12	CT6, CT11, CT15	Preventivo / Detectivo / Correctivo	4.25	2	3	25.50	Bajo	Aceptable con monitoreo
R13	CT1, CT6, CT8, CT9, CT11	Preventivo / Detectivo	4.00	3	2	24.00	Muy bajo	Aceptable
R14	CT5, CT6, CT11	Preventivo / Detectivo	4.00	2	3	24.00	Muy bajo	Aceptable
R15	CT1, CT2, CT4, CT11, CT13	Preventivo / Detectivo	3.75	2	2	15.00	Muy bajo	Aceptable
R16	CT1, CT6, CT10, CT11	Preventivo / Detectivo	3.75	2	3	22.50	Muy bajo	Aceptable
R17	CT1, CT2, CT6, CT11, CT13	Preventivo / Detectivo	5.00	3	3	45.00	Bajo	Aceptable con monitoreo
R18	CT4, CT11, CT13	Preventivo / Detectivo	5.00	3	2	30.00	Bajo	Aceptable con monitoreo

Elaboración: Los autores.

Los resultados del tratamiento muestran que la propuesta de controles técnicos permitió reducir la criticidad de los riesgos identificados. Los escenarios que inicialmente presentaban niveles medios y altos pasaron a niveles residuales muy bajos y bajos, lo que refleja una disminución esperada en la probabilidad de materialización de las amenazas y en la exposición asociada a las vulnerabilidades.

No obstante, algunos escenarios relacionados con gateways LPWAN, routers y tecnologías de comunicación de largo alcance, controladores y sistemas de procesamiento local, y plataformas en la nube mantienen un criterio de aceptable con monitoreo. Esto indica que, aunque el riesgo residual disminuye, estos activos continúan requiriendo seguimiento periódico debido a su importancia dentro de la arquitectura IoT agrícola y al impacto potencial que tendría su afectación sobre la operación del sistema.

Tabla 9.
Distribución de riesgos por capa de la arquitectura IoT agrícola.

Capa	Riesgos	Bajos	Medios	Altos	Críticos	Nivel general de riesgo
Percepción	6	3	3	0	0	Bajo–Medio
Red	4	0	2	2	0	Medio–Alto
Procesamiento	4	2	1	1	0	Bajo–Alto
Aplicación	4	0	2	2	0	Medio–Alto

Elaboración: Los autores.

La Tabla 9 presenta la distribución de los riesgos identificados según las capas de la arquitectura IoT agrícola. Los resultados muestran que la capa de percepción concentra la mayor cantidad de escenarios evaluados; sin embargo, estos se ubican principalmente entre niveles bajos y medios, asociados con la alteración de lecturas, exposición de telemetría, acceso no autorizado y manipulación de dispositivos.

Por otro lado, aunque las capas de red y de aplicación se encuentran con menor cantidad de riesgos concentran escenarios más delicados en especial activos que se relacionan con la conectividad, administración y gestión de la información. En la capa de procesamiento se encuentra una mezcla de niveles de riesgos bajos, medios y altos que se vinculan con actualizaciones de firmware y el procesamiento de datos. Esto demuestra que la gravedad de un riesgo no se mide en el número de amenazas, sino del papel fundamental que cumplen estos activos dentro del sistema agrícola.

CONCLUSIONES

Se cumplió el objetivo de la investigación al proponer controles técnicos de seguridad para las diferentes categorías de activos IoT agrícolas, a partir de un proceso de gestión de riesgos estructurado conforme a la ISO/IEC 27005:2022.

La evaluación del riesgo evidenció que la mayor criticidad se concentra en las capas de red y aplicación, donde se ubicaron los escenarios altos y críticos asociados principalmente con conectividad, administración y gestión de información. Si bien la capa

de percepción concentra un mayor número de riesgos, en su mayoría se encuentra en niveles medios. Al valorar el impacto CIDL junto a la probabilidad de las amenazas, queda claro que los activos asociados al control, comunicación y gestión de información son los que requieren mayor cuidado.

La propuesta de controles técnicos como la autenticación fuerte, hardening, segmentación de red, monitoreo e integridad de datos ayudaron principalmente que los activos con un nivel de riesgo alto bajaran a niveles mínimos.

Para futuras investigaciones, resulta pertinente desarrollar estudios comparativos entre distintos entornos agrícolas conectados, con el propósito de analizar cómo varían los niveles de riesgo y la pertinencia de los controles técnicos según el contexto operativo.

CONFLICTO DE INTERÉS

Los autores declaran que no tienen conflicto de interés en la publicación de este artículo.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A todos los agentes sociales involucrados en el proceso investigativo.

REFERENCIAS CONSULTADAS

Benyezza, H., Bouhedda, M., Kara, R., & Rebouh, S. (2023). Smart platform based on IoT and WSN for monitoring and control of a greenhouse in the context of precision agriculture. *Internet of Things*, *23*, 100830. https://doi.org/10.1016/j.iot.2023.100830

Boursianis, A. D., Papadopoulou, M. S., Diamantoulakis, P., Liopa-Tsakalidi, A., Barouchas, P., Salahas, G., Karagiannidis, G., Wan, S., & Goudos, S. K. (2022). Internet of Things (IoT) and Agricultural Unmanned Aerial Vehicles (UAVs) in smart farming: A comprehensive review. *Internet of Things*, *18*, 100187. https://doi.org/10.1016/j.iot.2020.100187

Campoverde-Molina, M., y Luján-Mora, S. (2025). Cybersecurity in smart agriculture: A systematic literature review. *Computers & Security*, *150*, 104284. https://doi.org/10.1016/j.cose.2024.104284

Castro-Paredes, J. G., Mendoza-Masache, G. R., Loja-Mora, N. M., Loján-Alvarado, H. P., Castro-Paredes, J. G., Mendoza-Masache, G. R., Loja-Mora, N. M., y Loján-Alvarado, H. P. (2025). Protección de datos por diseño y por defecto. Implicaciones legales en el desarrollo de software. *Ingenium et Potentia. Revista Electrónica Multidisciplinaria de Ciencias Básicas, Ingeniería y Arquitectura*, *7*(12), 77-96. https://doi.org/10.35381/i.p.v7i12.4471

Debauche, O., Trani, J. P., Mahmoudi, S., Manneback, P., Bindelle, J., Mahmoudi, S. A., Guttadauria, A., & Lebeau, F. (2021). Data management and internet of things: A methodological review in smart farming. *Internet of Things*, *14*, 100378. https://doi.org/10.1016/j.iot.2021.100378

Ivanochko, I., Greguš, M. jr., & Melnyk, O. (2024). Smart Farming System Based on Cloud Computing Technologies. *Procedia Computer Science, The 15th International Conference on Ambient Systems, Networks and Technologies Networks (ANT) / The 7th International Conference on Emerging Data and Industry 4.0 (EDI40), April 23-25, 2024, Hasselt University, Belgium*, *238*, 857-862. https://doi.org/10.1016/j.procs.2024.06.103

Izquierdo, J. A., Jaramillo, J. F., Loja, N. M., y Mazon-Olivo, B. (2025). Modelo integrado de adopción de tecnologías en la agricultura. Caso de estudio: IA e IoT aplicadas en producción de cacao. *Revista ESPACIOS*, *46*(03). https://doi.org/10.48082/espacios-a25v46n03pXX

Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in Internet of Things. *Future Generation Computer Systems*, *100*, 144-164. https://doi.org/10.1016/j.future.2019.04.038

Larrea, J. W. H., Bermúdez, M. J. V., Balarezo, L. C. B., y Holguin, J. M. Y. (2024). Monitoreo IOT utilizando una red de sensores inalámbricos para el cultivo de cacao. *Polo del Conocimiento*, *9*(11), 826-844. https://doi.org/10.23857/pc.v9i11.8343

Laverde Mena, J. A., Laverde Mena, C. G., Laverde Mena, J. A., y Laverde Mena, C. G. (2021). Internet de las cosas aplicado en la agricultura ecuatoriana: Una propuesta para sistemas de riego. *Dilemas contemporáneos: educación, política y valores*, *8*(2). https://doi.org/10.46377/dilemas.v8i2.2542

Loza González, G. A. (2021). *Factores críticos de éxito en la aplicación de la IOT al Sector Agropecuario* [Tesis de Grado, Universidad Politécnica Salesiana]. http://dspace.ups.edu.ec/handle/123456789/20955

Montaño-Blacio, M., González-Escarabay, J., Jiménez-Sarango, Ó., Mingo-Morocho, L., y Carrión-Aguirre, C. (2023). Diseño y despliegue de un sistema de monitoreo basado en IoT para cultivos hidropónicos. *Ingenius*, (30), 9-18. https://doi.org/10.17163/ings.n30.2023.01

Mosquera Meléndrez, L. M., y Cevallos Rojas, C. D. (2022). *Diseño e implementación de un Prototipo IoT para el monitoreo de parámetros ambientales aplicados al cultivo de arroz utilizando ESP32 y Thingspeak* [Tesis de Grado, Universidad Politécnica Salesiana]. http://dspace.ups.edu.ec/handle/123456789/22884

Novillo, G. L., Macancela, A., Tacuri, E., y Lupercio, L. (2022). Estación meteorológica inteligente para control de riego y mitigación de heladas. *Revista Tecnológica - ESPOL*, *34*(3), 46-57. https://doi.org/10.37815/rte.v34n3.948

Rejeb, A., Abdollahi, A., Rejeb, K., & Treiblmaier, H. (2022). Drones in agriculture: A review and bibliometric analysis. *Computers and Electronics in Agriculture*, *198*, 107017. https://doi.org/10.1016/j.compag.2022.107017

Rivera Guzmán, E. F., Mañay Chochos, E. D., Chiliquinga Malliquinga, M. D., Baldeón Egas, P. F., y Toasa Guachi, R. M. (2022). LoRa Network-Based System for Monitoring the Agricultural Sector in Andean Areas: Case Study Ecuador. *Sensors*, *22*(18), 6743. https://doi.org/10.3390/s22186743

Rudrakar, S., & Rughani, P. (2024). IoT based Agriculture (Ag-IoT): A detailed study on Architecture, Security and Forensics. *Information Processing in Agriculture*, *11*(4), 524-541. https://doi.org/10.1016/j.inpa.2023.09.002

Tao, W., Zhao, L., Wang, G., & Liang, R. (2021). Review of the internet of things communication technologies in smart agriculture and challenges. *Computers and Electronics in Agriculture*, *189*, 106352. https://doi.org/10.1016/j.compag.2021.106352

Vega, D. D. C., Ramírez, K. A. B., Mora, N. M. L., y Alvarado, H. P. L. (2025). Gestión de riesgos para el tratamiento de datos personales sensibles en el movimiento de mujeres de El Oro. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, *7*(3), 389-406. https://doi.org/10.59169/pentaciencias.v7i3.1505

Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., Green, A. G., Russell, C., & Duncan, E. (2021). A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures. Applied Sciences, 11(16), 7518. https://doi.org/10.3390/app11167518