Fortalecimiento de la seguridad en el internet de las cosas (IoT): estrategias y propuestas para mitigar riesgos de vulnerabilidad en sensores de agua con tecnología IoT

Elder Orlando De Lima Rosado

Asesor

Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

Dedico este trabajo de investigación a mi familia, cuyo amor y apoyo incondicional han sido mi mayor fuente de inspiración; a mis profesores, por su valiosa orientación y por fomentar en mí la curiosidad intelectual; y a todos los profesionales y expertos que se esfuerzan día a día por fortalecer la seguridad en el Internet de las Cosas, contribuyendo así a un entorno digital más seguro y confiable para todos.

Agradecimientos

Agradezco profundamente a mis tutores, por su invaluable guía, paciencia y las acertadas sugerencias que fueron fundamentales para la culminación de esta investigación. Extiendo mi gratitud al Escuela de Ciencias Básicas, Tecnología e Ingeniería, por brindarme el espacio, los recursos y el acceso a las herramientas necesarias para llevar a cabo este trabajo. Finalmente, quiero expresar mi sincero agradecimiento a mis compañeros de estudio, por su colaboración, apoyo técnico, valiosas perspectivas y las incontables horas de discusión que enriquecieron significativamente el contenido de esta monografía sobre el fortalecimiento de la seguridad en el Internet de las Cosas.

Resumen

El Internet de las Cosas (IoT) se ha consolidado como un pilar esencial en la gestión de infraestructuras críticas, integrando sistemas como SCADA y redes de sensores inalámbricos (WSN) en sectores estratégicos como energía, manufactura y recursos hídricos. Sin embargo, esta interconexión ha incrementado los riesgos de ciberseguridad, especialmente en los sensores de agua IoT empleados para el monitoreo y control ambiental, que presentan deficiencias en sus protocolos de protección, comprometiendo la integridad de los datos y la confiabilidad operativa.

Este estudio analiza las principales vulnerabilidades y propone una arquitectura híbrida que combina Blockchain y Machine Learning como mecanismo de detección y prevención de intrusiones. Blockchain garantiza la inmutabilidad y trazabilidad de los registros, mientras que Machine Learning permite identificar patrones anómalos en tiempo real, fortaleciendo la defensa ante ataques como inyección de código o denegación de servicio. A diferencia de los sistemas tradicionales basados en reglas estáticas, la propuesta plantea un modelo adaptable, descentralizado y eficiente en recursos, adecuado para dispositivos con capacidades limitadas.

Los resultados demuestran mejoras significativas en precisión de detección, reducción de falsos positivos y escalabilidad operativa en entornos industriales y ambientales. Además, el enfoque descentralizado reduce los puntos únicos de fallo y mejora la resiliencia en redes fragmentadas o con baja conectividad.

La investigación aporta un análisis técnico y bibliográfico sobre la seguridad en sensores de agua IoT, evaluando debilidades como la dependencia de firmas conocidas, la falta de adaptabilidad y las limitaciones de procesamiento. Se concluye que la integración de Blockchain y Machine Learning ofrece una solución viable para fortalecer la ciberseguridad en entornos IoT

críticos, promoviendo la protección de datos, la continuidad de servicio y la confianza tecnológica en sistemas inteligentes de gestión hídrica.

Palabras clave: Internet de las Cosas, Blockchain, Machine Learning, sensores de agua, ciberseguridad.

Abstract

The Internet of Things (IoT) has become a fundamental component in the management of critical infrastructures, integrating SCADA systems and Wireless Sensor Networks (WSN) into strategic sectors such as energy, manufacturing, and water resources. However, this interconnection has significantly increased cybersecurity risks, particularly in IoT-based water sensors used for environmental monitoring and resource management. These devices often present deficiencies in their security protocols, compromising data integrity, availability, and system reliability.

This research analyzes the main vulnerabilities and proposes a hybrid cybersecurity architecture that combines Blockchain and Machine Learning to enhance intrusion detection and resilience in IoT environments. Blockchain technology ensures data immutability and traceability through decentralized verification, while Machine Learning enables real-time anomaly detection, improving responsiveness to advanced threats such as code injection, spoofing, or denial-of-service (DoS/DDoS) attacks. Unlike traditional intrusion detection systems based on static rules, this approach introduces a scalable, adaptive, and lightweight model designed for resource-constrained IoT devices operating in distributed or isolated networks.

The results demonstrate that the proposed model improves detection accuracy, reduces false positives, and strengthens system scalability and reliability in both industrial and environmental applications. Its decentralized design minimizes single points of failure and provides continuous verification of security events, increasing operational continuity in fragmented networks or with heterogeneous devices.

The study contributes a technical and bibliographic framework that identifies and mitigates weaknesses in IoT water sensor cybersecurity, such as dependency on known signatures, limited adaptability, and high false-positive rates. It concludes that integrating Blockchain and Machine Learning offers an effective and sustainable approach to protecting IoT infrastructures, improving resilience, data integrity, and user trust in intelligent water management systems.

Keywords: Internet of Things, Blockchain, Machine Learning, Water Sensors, Cybersecurity.

Tabla de Contenido

LISTA DE TABLAS

Glosario

Autenticación Multifactor (MFA): Proceso de verificación de la identidad de un usuario mediante la combinación de dos o más factores de autenticación independientes, como algo que el usuario sabe (contraseña), algo que el usuario tiene (token) o algo que el usuario es (biometría) (Malik & Singh, 2020).

Blockchain: Estructura de datos distribuida y descentralizada que registra transacciones de manera secuencial y en bloques enlazados criptográficamente, garantizando la integridad y transparencia de la información (De Lima Rosado, 2025).

Ciberseguridad: Conjunto de políticas, tecnologías, procesos y prácticas diseñadas para proteger los sistemas informáticos, redes, dispositivos y datos contra ataques cibernéticos, daños, robos o accesos no autorizados (Nurse et al., 2017).

Criptografía: Ciencia y arte de cifrar y descifrar información para proteger su confidencialidad e integridad durante el almacenamiento y la transmisión (Rueda & Talavera, 2017).

Firewall: Dispositivo de seguridad de red que controla el tráfico entrante y saliente, bloqueando accesos no autorizados y previniendo ataques maliciosos (INCIBE, 2015).

Inteligencia Artificial (IA): Capacidad de las máquinas para simular procesos de pensamiento humano, como el aprendizaje, el razonamiento y la resolución de problemas, aplicada en ciberseguridad para detectar anomalías y amenazas (Kaspersky, 2019).

Internet de las Cosas (IoT): Red de dispositivos físicos interconectados que recopilan e intercambian datos a través de internet, permitiendo la automatización y el control remoto de diversos procesos y sistemas (Rueda J., 2021).

Machine Learning (ML): Subcampo de la inteligencia artificial que permite a los sistemas aprender de los datos sin ser programados explícitamente, utilizado para identificar patrones y predecir comportamientos maliciosos en redes IoT (Petrov, 2023).

Prueba de Penetración (Pentest): Simulación de ataques cibernéticos controlados para evaluar la seguridad de un sistema o red, identificando vulnerabilidades y debilidades explotables (Torrijos, 2021).

Vulnerabilidad: Debilidad o fallo en un sistema, aplicación o red que puede ser explotado por un atacante para comprometer la seguridad y la integridad de la información (Campos, 2020).

Introducción

En la última década, el Internet de las Cosas (IoT) ha transformado radicalmente la forma en que interactuamos con el entorno, integrándose en dispositivos domésticos inteligentes y sistemas industriales interconectados. Esta revolución tecnológica ha traído consigo numerosos beneficios, desde la automatización de procesos hasta la mejora en la eficiencia operativa. Sin embargo, esta creciente conectividad también ha expuesto nuevas superficies de ataque, incrementando los riesgos en materia de ciberseguridad.

Los dispositivos IoT, incluidos los sensores de agua inteligentes, se han convertido en objetivos prioritarios para actores maliciosos. Según Check Point Research, el 34% de las empresas que sufrieron brechas a través de dispositivos IoT enfrentaron pérdidas superiores a las generadas por ataques a dispositivos tradicionales, con costos que oscilaron entre 5 y 10 millones de dólares. Además, un porcentaje igual de organizaciones reportó daños reputacionales y sanciones significativas.

Estudios recientes señalan que los ciberataques dirigidos a dispositivos IoT han crecido más del 400%. Esta vulnerabilidad está especialmente presente en aquellos dispositivos que no implementan principios de “confianza cero” (Zero Trust) para su protección (Rosalía, 2023). En comparación con 2022, el año 2023 registró un aumento del 41% en ataques a dispositivos IoT (Mireya, 2024), y para 2024, el 86% de los incidentes cibernéticos ocasionaron graves daños económicos. Un informe sobre 500 incidentes importantes en 38 países reveló una nueva tendencia: los ciber atacantes motivados financieramente están priorizando la interrupción operativa deliberada, utilizando tácticas de sabotaje, bloqueo de clientes y destrucción de sistemas para maximizar el impacto y forzar pagos por extorsión (Alirio, 2025).

A medida que más dispositivos se integran a las redes, se vuelve urgente abordar los desafíos de ciberseguridad en el IoT. La web oscura ha intensificado esta amenaza al explotar las vulnerabilidades de estos dispositivos, utilizando IA adversaria para ejecutar ataques automatizados. De acuerdo con Kaspersky, el 70% de los dispositivos IoT comprometidos son utilizados como proxies para actividades ilícitas o para propagar malware. En el sector de maquinaria y equipos industriales, el 50% de las alertas de seguridad corresponden a solicitudes de parámetros ilegales, una amenaza crítica en el ámbito de tecnologías operativas (OT).

Este trabajo de investigación se enfoca en el fortalecimiento de la seguridad en dispositivos IoT, con énfasis en los sensores de agua, analizando las vulnerabilidades más comunes y proponiendo estrategias para su mitigación. Desde ataques técnicos como DDoS, malware o la explotación de interfaces inseguras, hasta debilidades organizativas como la ausencia de protocolos de autenticación o una gestión inadecuada de datos sensibles, se abordará el fenómeno desde una perspectiva integral y multidisciplinaria.

Con más del 90% de las organizaciones experimentando al menos una amenaza cibernética en 2024, se hace evidente la necesidad de implementar soluciones sólidas y proactivas. Este estudio busca aportar al conocimiento en ciberseguridad IoT y proporcionar herramientas prácticas que fortalezcan la confianza en este ecosistema digital en expansión.

Planteamiento del Problema

Las redes de sensores constituyen un sistema compuesto en el que se conectan nodos capaces de intercambiar datos a través de comunicación cableada o inalámbrica. Desde la década de 1980, estas redes, inicialmente conocidas como Redes de Sensores Distribuidas (DSN), han evolucionado hacia lo que hoy conocemos como Redes de Sensores Inalámbricos (WSN), una tecnología crítica para múltiples aplicaciones, incluyendo el monitoreo ambiental, agrícola, industrial y doméstico (Rueda & Talavera, 2017; Rueda, 2021).

Entre estas aplicaciones, los sensores de agua IoT destacan por su papel esencial en la supervisión de recursos hídricos, calidad del agua, detección de fugas y control de consumo. Estos dispositivos, al estar conectados a redes WSN, permiten la recopilación y transmisión de datos en tiempo real, facilitando la toma de decisiones automatizada y eficiente. No obstante, la creciente dependencia de estos sensores trae consigo serias preocupaciones en materia de ciberseguridad.

En un contexto donde se generan cantidades masivas de datos —con proyecciones de hasta 35 zettabytes almacenados globalmente en 2020 y un promedio de 1.7 megabytes generados por segundo por individuo (Petrov, 2023; Brown, 2022)—, garantizar la seguridad de la información resulta prioritario. Esto es aún más relevante en entornos donde los sensores IoT, como los de agua, se integran en infraestructuras críticas susceptibles a ataques cibernéticos.

Estos dispositivos pueden ser blanco de múltiples amenazas: acceso no autorizado, manipulación de datos, denegación de servicio (DoS), espionaje, o control remoto por parte de atacantes. En 2019, por ejemplo, Kaspersky identificó más de 100 millones de ataques a dispositivos IoT desde más de 276,000 IPs públicas en solo seis meses, ilustrando la magnitud del problema (Kaspersky, 2019). Si un sensor de agua comprometido forma parte de un sistema

mayor, el atacante podría acceder a toda la red, afectando la privacidad de los usuarios, la disponibilidad del servicio e incluso la integridad de los recursos hídricos monitoreados.

Además, los dispositivos IoT suelen tener limitaciones en capacidad de procesamiento y almacenamiento, lo que restringe la implementación de mecanismos de seguridad avanzados. Esto agrava el problema, pues las brechas de seguridad pueden ser explotadas con facilidad por ciberdelincuentes motivados por beneficios económicos (García & Lee, 2025). Como consecuencia, el usuario final se enfrenta a riesgos de robo de identidad, extorsión, espionaje o pérdida financiera (INCIBE, 2015; Europol, 2021).

Ante esta problemática, surge la necesidad urgente de fortalecer la seguridad de los dispositivos IoT, y en particular de los sensores de agua, mediante estrategias y propuestas concretas que permitan mitigar riesgos de vulnerabilidad. La pregunta clave que guía esta investigación es:

¿Cómo fortalecer la seguridad en el Internet de las Cosas (IoT), particularmente en sensores de agua conectados a Redes de Sensores Inalámbricos (WSN), mediante estrategias y propuestas eficaces para mitigar riesgos de vulnerabilidad?

Para abordar esta cuestión, se propone una metodología de auditoría de seguridad intrusiva que permita simular ataques controlados sobre redes WSN reales. Dado que no todas las técnicas de auditoría existentes son directamente aplicables a sensores IoT, se realizará un análisis comparativo de metodologías reconocidas (como OWASP, PHVA, NIST o NUTRIA), para seleccionar un conjunto de pruebas adaptadas al entorno evaluado. Esta estrategia permitirá identificar y documentar vulnerabilidades específicas, facilitando el diseño de mecanismos de mitigación, detección y respuesta ante incidentes más robustos y adaptados a este tipo de tecnologías.

En definitiva, lograr un entorno seguro para sensores de agua IoT en WSN es fundamental para asegurar el buen funcionamiento de infraestructuras críticas, preservar la confianza de los usuarios, y fomentar una evolución segura del ecosistema digital.

Justificación

La problemática en la seguridad en el internet de las cosas (IoT), presenta inconvenientes a los ataques cibernéticos que se hacen en sensores de Agua con Tecnología IoT. En la actualidad digital las organizaciones están buscando herramientas cuyos procesos emergentes de sistemas informáticos, personal y productos se integren en una única cadena de análisis y recopilación de información.

El crecimiento exponencial del Internet de las Cosas (IoT) ha traído consigo una serie de desafíos en materia de seguridad, lo que hace imprescindible el desarrollo de metodologías efectivas para mitigar riesgos. Según Rueda (2021), las redes de sensores inalámbricos, que son fundamentales en la infraestructura del IoT , incluyendo sensores de agua conectados, requieren una evaluación constante de su seguridad debido a su alta vulnerabilidad a ataques cibernéticos. Esto subraya la necesidad de implementar auditorías intrusivas que no solo identifiquen vulnerabilidades, sino que también fortalezcan la confianza en el uso de estos dispositivos conectados.

Por otra parte las entidades gubernamentales y organizaciones, buscan proteger contra riesgos emergentes. En este marco, la creciente adopción de metodologías para la evaluación de sistemas IoT presenta un reto considerable, dado que los nuevos riesgos asociados a estos entornos pueden estar relacionados con un alto nivel de conectividad o la fusión de sistemas digitales, ciber físicos y sociales.

En consecuencia, es esencial destacar que varias instituciones públicas han progresado en la implementación del Modelo de Seguridad y Protección de la Información (MSPI), desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC). Se espera crear un valor añadido para los grupos de interés de la

organización que adopten la guía de gestión de riesgos aplicada a dispositivos IoT, siguiendo las pautas establecidas por la norma ISO 27001.

Por lo expuesto en la información, resulta esencial llevar a cabo una investigación que facilite la identificación de amenazas y vulnerabilidades, así como de las particularidades de diseño en los dispositivos y la definición de los riesgos asociados a la ciberseguridad en la tecnología.

Es importante tener en cuenta, los riesgos que se corren en la tecnología de sensores de agua IoT, como el uso indebido o la pérdida de datos. Para el uso de estas tecnologías, se vuelve importante desarrollar proyectos de investigación, como este documento, que evidencia propuestas que puedan establecer soluciones para el fortalecimiento de la Seguridad en el Internet de las Cosas (IoT): Estrategias y Propuestas para Mitigar Riesgos de Vulnerabilidad en Sensores de Agua con Tecnología IoT.

Objetivos

Objetivo General

Analizar las deficiencias de ciberseguridad en los sensores de agua de las tecnologías IoT, mediante un estudio basado en literatura académica y casos documentados, que garanticen su implementación y operación segura.

Objetivos Específicos

Identificar los riesgos y vulnerabilidades, en términos de deficiencias de ciberseguridad para los sensores de agua IoT.

Evaluar, a partir de casos documentados en literatura académica, los riesgos y vulnerabilidades en ciberseguridad aplicando métricas de impacto (VEI, MTTE, IOI, KNR).

Proponer lineamientos de ciberseguridad, en la implementación y operación segura de sensores de agua con tecnologías IoT.

Marco Referencial

Marco Teórico

En relación con la clasificación de Protocolos de Seguridad, Kondoro y colaboradores llevaron a cabo un estudio que facilita el examen en tiempo real de los protocolos de seguridad asociados al Internet de las Cosas (IoT), incluyendo CoAP, MQTT y XMPP, para la comunicación en microrredes. Este análisis permitió identificar los requisitos que deben satisfacer los protocolos de seguridad y su influencia en las exigencias en tiempo real de las funciones de redes inteligentes, tales como protección, control y supervisión (Kondoro et al., 2021). DTLS, tiene como fortaleza proporcionar la confidencialidad, la autenticación y protección a la manipulación de la información sobre redes UDP (Raza et al., 2017).

Dentro de los protocolos CoAP, una debilidad, es que no se tiene en cuenta la actualización automática de la clave, esto crea vulnerabilidad a las sesiones de ataques de formas constante (Bertín et al., 2019). Los protocolos de seguridadLightweight Security Protocols: EDHOC y LAKE, EDHOC (Ephemeral Diffie-Hellman Over COSE) cuenta con un protocolo de asignación de claves de baja sobrecarga, se utiliza, para dispositivos bastante restringidos (Selander et al., 2020).

Sensores de Agua Iot en el Contexto de Redes Inteligentes y Protocolos de Seguridad

En la evolución de las tecnologías IoT aplicadas al monitoreo ambiental y de recursos, los sensores de agua han emergido como componentes clave para la gestión eficiente y sostenible de los recursos hídricos. Estos sensores, integrados en plataformas IoT, permiten la medición en tiempo real de parámetros críticos como el nivel del agua, calidad, presión, caudal y parámetros fisicoquímicos, facilitando la toma de decisiones basada en datos precisos y oportunos.

Respecto a la seguridad en las comunicaciones de sensores de agua IoT, Kondoro et al. (2021) destacan que los protocolos CoAP, MQTT y XMPP, ampliamente usados en microrredes inteligentes, deben cumplir requisitos rigurosos para garantizar la protección, control y supervisión en tiempo real. En particular, el protocolo DTLS ha demostrado ser eficaz al proporcionar confidencialidad, autenticación y protección contra la manipulación de datos en redes UDP (Raza et al., 2017), lo cual es vital para mantener la integridad de la información transmitida por sensores de agua en entornos críticos.

No obstante, vulnerabilidades persisten; por ejemplo, CoAP carece de mecanismos para la actualización automática de claves, lo que lo hace susceptible a ataques de sesión prolongada (Bertín et al., 2019). Para dispositivos con recursos limitados, como muchos sensores de agua IoT desplegados en zonas remotas, los protocolos Lightweight Security Protocols como EDHOC (Ephemeral Diffie-Hellman Over COSE) y LAKE ofrecen una asignación eficiente y segura de claves, minimizando la sobrecarga computacional (Selander et al., 2020).

En la implementación práctica de sensores de agua, investigaciones como las de Ochoa Duarte et al. (2018) han desarrollado modelos de supervisión para evaluar la calidad ambiental, que podrían adaptarse para la supervisión del recurso hídrico, notificando a los usuarios sobre condiciones críticas como contaminación o niveles anómalos. Asimismo, Arias Hurtado et al. (2018) enfatizan la importancia de interfaces accesibles y transparentes para gestionar APIs de dispositivos IoT, facilitando el manejo de sensores de agua por parte de técnicos y usuarios no especializados.

Para enfrentar amenazas a la integridad y disponibilidad de los datos, Djedjig et al. (2020) proponen un modelo seguro de enrutamiento basado en RPL (MRTS), que puede

aplicarse en redes de sensores de agua para asegurar la transmisión confiable y segura de información, especialmente en sistemas de bajo consumo energético.

Por otro lado, la implementación de bancos de prueba estandarizados, como la tesis doctoral de Martínez Carreras (2016), resulta fundamental para evaluar y mejorar el firmware de sensores IoT, incluyendo aquellos dedicados a la medición y control de recursos hídricos. Un ejemplo aplicado es el sistema diseñado por Gómez Moreno (2020), que integra sensores para medir temperatura y humedad durante el transporte de mercancías, y que puede extenderse para monitorear condiciones ambientales en estaciones de monitoreo hídrico, con acceso remoto mediante plataformas en la nube.

Finalmente, la seguridad en dispositivos IoT, incluidos los sensores de agua, enfrenta desafíos importantes. Jha et al. (2020) analizaron ataques en sistemas de hogares inteligentes conectados por NB-IoT, señalando la necesidad de robustecer la arquitectura de comunicación para garantizar la confidencialidad y la disponibilidad. Similarmente, Al-Turjman y Lemayian (2020) evaluaron las vulnerabilidades de sensores en vehículos, destacando la importancia de implementar mecanismos de protección frente a ataques cibernéticos, lecciones que son transferibles a la infraestructura de sensores de agua IoT.

En el contexto de sensores de agua IoT, las vulnerabilidades de seguridad también representan un desafío crítico, dada la sensibilidad y relevancia de los datos recolectados para la gestión hídrica. Los sensores de agua conectados a redes NB-IoT o IoT convencionales pueden ser blanco de ataques cibernéticos similares a los identificados por Jha et al. (2020) en sistemas de hogares inteligentes, donde se evaluaron métricas como la tasa de secreto (SR) y la probabilidad de interrupción del secreto (SOP). La exposición de datos de sensores de agua a interceptaciones o manipulaciones maliciosas puede comprometer la integridad y disponibilidad

de información vital para la supervisión y control de recursos hídricos. Por otra parte, el análisis de Al-Turjman y Lemayian (2020) sobre dispositivos con sensores en automóviles evidencia la necesidad de robustecer los mecanismos de seguridad en sensores IoT, un principio que debe aplicarse rigurosamente a los sensores de agua para protegerlos frente a amenazas cibernéticas que podrían afectar la confiabilidad de sistemas inteligentes de gestión hídrica.

En el ámbito de los sensores, Ochoa y sus colegas desarrollaron un modelo de sistema para la medición y supervisión, que posibilita la evaluación de la calidad del aire, con el objetivo de notificar a los usuarios sobre la situación actual y, al mismo tiempo, adoptar precauciones ante la problemática existente (Ochoa Duarte et al., 2018).Los sensores, Arias y sus coautores llevaron a cabo una investigación con el propósito de crear un software accesible para los usuarios, adaptado a sus requerimientos. Propusieron técnicas para gestionar la Interfaz de Programación de Aplicaciones (API) proporcionada por los fabricantes de transceptores de radio, de manera que la comunicación a través de las capas inferiores del modelo de interconexión abierto sea clara y comprensible para los usuarios (Arias Hurtado et al., 2018).

En la sección de Protocolos de Seguridad, Djedjig y sus colegas proponen un modelo seguro para los protocolos de enrutamiento destinados a redes de bajo consumo de datos que son susceptibles a amenazas. Han diseñado un esquema de RPL (MRTS) que proporciona un enrutamiento seguro, considerando la MRTS como una solución para abordar esta problemática (Djedjig et al., 2020).

En el ámbito de los sensores, se mencionó la tesis doctoral de Martínez, que se centra en la creación de un banco de pruebas estándar. Este desarrollo permitió reconocer las características y elementos clave del firmware utilizado en dispositivos para la recolección de productos hortícolas en el sureste de España. Su finalidad es mejorar la eficiencia del proceso

agrícola mediante el análisis de los datos obtenidos (Martínez Carreras, 2016). Desde el diseñó se implementó una red de dispositivos que permite detectar y evaluar el estado de la carga durante su transporte. Este sistema es capaz de medir tanto la temperatura como la humedad a las que se transporta la mercancía. Además, facilita el seguimiento del envío mediante GPS, otorgando acceso a los datos del transporte a través de Internet en un servidor en la nube (Gómez Moreno, 2020

Las vulnerabilidades, Jha y sus colaboradores examinan la arquitectura en capas del IoT y NB-IoT mediante un ataque de seguridad dirigido a un sistema de hogar inteligente que incorpora dispositivos conectados a estas tecnologías. El objetivo de su análisis es establecer la tasa de secreto (SR) y la probabilidad de interrupción del secreto (SOP) (Jha et al., 2020). Al-Turjman y sus colegas ofrecen un análisis sobre los niveles de seguridad de los dispositivos equipados con sensores en automóviles, con el propósito de identificar sus debilidades frente a ataques cibernéticos (Al-Turjman & Lemayian, 2020).

Los protocolos de seguridad, Yugha lleva a cabo una investigación cuyo propósito es analizar los problemas asociados a la seguridad y la implementación de protocolos de seguridad en el Internet de las Cosas (IoT) (Yugha & Chithra, 2020).En la publicación Computer Science Review, Mark Mbock Ogonji, George Okeyo y Joseph Muliaro Wafula presentan en 2020 el artículo titulado “Una encuesta sobre privacidad y seguridad en el Internet de las Cosas” (Ogonji et al., 2020). En este trabajo el autor argumenta que el Internet de las Cosas ha influido en la dinámica operativa de las tecnologías de la información y los entornos comunicativos, ofreciendo diversas opciones de interacción y beneficios para los usuarios potenciales a través de la implementación de sensores inalámbricos. No obstante, a pesar del rápido avance en la infraestructura física y de software, se ha observado una escasa integración de esta tecnología

con aspectos de seguridad y privacidad de la información gestionada, lo que ha generado un amplio rango de vulnerabilidades relacionadas con la exposición de datos sensibles de los usuarios.

En 2018, en España, se llevó a cabo un estudio titulado: “Seguridad en el Internet de las Cosas: firmwares, vulnerabilidades y riesgos asociados al rápido desarrollo y uso del Internet de las Cosas” (Calvo del Olmo, 2018). Este trabajo se inscribe dentro de la categoría de vulnerabilidades en IoT, donde el autor inicia su investigación aplicando una metodología experimental. Analiza dispositivos IoT de su propiedad, identificando sus posibles debilidades, las cuales contrasta con una revisión bibliográfica pertinente. El objetivo es definir las principales vulnerabilidades que podrían comprometer la red IoT a la que están conectados.

En el ámbito de las vulnerabilidades, Rivera se centró en la recopilación, identificación y análisis de los ataques y amenazas en el Internet de las Cosas (IoT). Su objetivo fue establecer las ventajas de herramientas como SDR y GNU RADIO para examinar las vulnerabilidades en dispositivos que utilizan protocolos de Radio Frecuencia (RF). Esto incluyó el análisis de frecuencias, modulación, decodificación de señales y reproducción de paquetes de radio, con el fin de identificar debilidades en las comunicaciones entre dispositivos IoT (Rivera Arellano, 2020). El estudio titulado “Desafíos del estándar de cifrado avanzado para proteger las redes de sensores del Internet de las Cosas” (Arpaia et al., 2020) se encuadró en los tres criterios de análisis establecidos en esta investigación, y se llevó a cabo en el Reino Unido durante el año 2020. Los autores, Páscuale Arpaia, Francesco Bonavolontá y Antonella Cioffi, desarrollaron una metodología que se basa en un modelo experimental para evaluar las vulnerabilidades presentes en una red de sensores IoT.

En 2015, en el Reino Unido, Yousuf, T. Mahmoud, R., Aloul, F., y Zualkernan, I. llevaron a cabo un estudio titulado “Seguridad del Internet de las Cosas (IoT): situación actual y medidas futuras” (Mahmoud et al., 2015), que se clasifica bajo el tema de vulnerabilidades en IoT. En este trabajo, los autores proponen una metodología de análisis estructurada en varias fases: evaluación de la arquitectura IoT, identificación de problemas de seguridad en IoT, implementación de contramedidas de seguridad y un examen del estado actual de la problemática.

En 2020, en los Países Bajos, los autores Sakshi Anand y Avinash Sharma llevaron a cabo un estudio titulado “Evaluación de amenazas a la seguridad en aplicaciones basadas en IoT”, que se clasifica en el ámbito de vulnerabilidades de IoT (Anand & Sharma, 2020). Este trabajo se fundamentó en una revisión inicial de la literatura relacionada con el tema, a partir de la cual se contextualizaron los elementos esenciales del IoT, sus áreas de aplicación, y la arquitectura de las distintas capas que permiten su funcionamiento. Además, se identificaron las amenazas a la seguridad categorizadas según el tipo de aplicación, culminando en propuestas para mejorar la seguridad en el entorno IoT.

De las vulnerabilidades de IoT, Daniel Rodríguez Margareto llevó a cabo en España, durante el año 2020, un estudio titulado “Ciberseguridad en el Internet de las Cosas: análisis, riesgos y vulnerabilidades” (Margareto, 2020). El propósito de este trabajo fue destacar la relevancia de la seguridad en las redes de IoT como una defensa contra los posibles ciberataques que podrían surgir debido a sus debilidades. Para lograr esto, el autor presenta un caso específico que ilustra las problemáticas y fallos en los protocolos de seguridad, así como las estrategias propuestas para mitigar estos riesgos y mejorar el diseño e implementación de dichos protocolos.

En 2018, en México, Norma Pérez y Miguel Bustos llevaron a cabo un estudio titulado "Análisis sistemático de la seguridad en el Internet de las Cosas" (Pérez et al., 2018). El objetivo principal de este trabajo fue enfatizar la relevancia de la seguridad en las redes de IoT como una defensa contra los ciberataques potenciales que podrían surgir debido a sus vulnerabilidades. Para ello, los autores presentan un análisis detallado que ilustra las problemáticas y deficiencias en los protocolos de seguridad existentes, así como las estrategias propuestas para mitigar estos riesgos y mejorar el diseño e implementación de dichos protocolos.

En 2019, en Colombia, Alexander Arias Silva llevó a cabo un estudio en la Universidad Nacional Abierta y a Distancia (UNAD) titulado "Análisis de seguridad de vulnerabilidades y ataques en cuatro dispositivos del Internet de las Cosas" (Silva & Alexander, 2019), que se clasifica dentro del tema de vulnerabilidades de IoT. En este trabajo, el autor realiza un examen exhaustivo sobre la seguridad de los dispositivos conectados a IoT, identificando fallos y debilidades en las redes asociadas a esta tecnología. El objetivo es establecer recomendaciones sobre prácticas adecuadas que ayuden a reducir las deficiencias detectadas, garantizando una gestión eficiente de estas redes y minimizando así el riesgo de ciberataques, al tiempo que se asegura la confiabilidad en sus diversas aplicaciones.El Journal Networks and Communications de Estados Unidos, Mobasshir Mahbud publicó un estudio titulado "Investigaciones avanzadas sobre la seguridad del IoT: un análisis completo desde la perspectiva de los protocolos, vulnerabilidades y arquitecturas preventivas" (Mahbub, 2020a).

En este trabajo, el autor subraya la necesidad de llevar a cabo una investigación exhaustiva sobre las problemáticas significativas relacionadas con la seguridad y las fuentes de amenazas que afectan los recursos y aplicaciones de la tecnología IoT, con el objetivo de desarrollar arquitecturas que prevengan estas problemáticas. La investigación se basó en una

metodología que abarcó varias áreas temáticas: caracterización de los componentes del IoT, identificación de aplicaciones vulnerables, revisión de estándares y protocolos del IoT, análisis de las capas arquitectónicas del IoT, modelado de amenazas, fuentes de riesgo y técnicas para garantizar la seguridad.

En China, Xuanxia Yao, Fadi Farha, Rongyang Li, Ismini Psychoula, Liming Chen y Huansehg Ning publicaron en la revista Digital Communications and Networks un artículo titulado “Desafíos y oportunidades en la seguridad y privacidad de los objetos físicos en IoT” (Yao et al., 2020), que se clasifica dentro de los protocolos de seguridad. En este trabajo, los autores destacan la necesidad de investigar las problemáticas relacionadas con la seguridad y la privacidad de los objetos físicos en las aplicaciones de IoT, haciendo referencia al desarrollo de esta tecnología y a los numerosos desafíos que surgen, así como a las alternativas para su manejo y prevención. La metodología empleada se basa en caracterizar la arquitectura de seguridad de los objetos físicos utilizados en IoT, analizando las distintas etapas de su funcionamiento y contrastándolas con características como la descripción de dichos objetos, las cuestiones de seguridad y privacidad que enfrentan, y los mecanismos de protección disponibles para ellos.

El término “IoT” ha ganado considerable popularidad en los últimos años gracias a los avances tecnológicos que han facilitado una mayor producción e implementación de estos dispositivos. Sin embargo, este crecimiento también ha propiciado un incremento en los ataques cibernéticos. Por estas razones, es fundamental definir algunos conceptos clave para una adecuada comprensión de esta investigación. Estos incluyen el IoT y los dispositivos que lo integran, la ciberseguridad, los ciberataques, los ciberdelincuentes, securIT y las vulnerabilidades asociadas a esta tecnología emergente. Esta definición de "IoT", que proviene del inglés "Internet of Things" y se traduce al español como "Internet de las Cosas", hace referencia a una

red creciente de dispositivos físicos que poseen capacidades computacionales, permitiendo su comunicación entre sí, el almacenamiento de datos y el control remoto, así como su conexión a Internet, lo que les otorga la capacidad de interactuar con otros dispositivos y sistemas a través de redes inalámbricas, facilitando así una amplia gama de aplicaciones en la vida cotidiana y en entornos industriales (Vinton, 2016). La conectividad es un aspecto crucial al utilizar dispositivos IoT; según Oracle, se define como “un conjunto de protocolos de red para Internet que facilita la conexión de sensores a la nube y a otros 'elementos' para lograr una transmisión de datos efectiva” (Oracle, 2020). Por lo tanto, es fundamental comprender las diversas formas en que cada persona puede conectarse a una red. La primera opción es el Wi-Fi, una tecnología esencial hoy en día que permite a los usuarios conectarse de manera inalámbrica a través de dispositivos móviles, laptops y otros equipos que necesitan ser compartidos, como impresoras o cámaras de seguridad, estableciendo así una red mediante un router, todo bajo la regulación del estándar IEEE 802.11. Otra opción común es el ethernet, que se refiere a las conexiones de red de área local, reguladas por el estándar IEEE 802.3, siendo el medio principal para que hogares o empresas accedan a Internet a través de cable coaxial, fibra óptica o cable de par trenzado (Cisco, 2020).

El Internet de las Cosas (IoT) permite clasificar varios dispositivos debido a su habilidad para conectarse a la red. En la actualidad, hay una amplia gama de aparatos que pueden ser considerados como dispositivos IoT, incluyendo electrodomésticos como sistemas de calefacción, aire acondicionado, ventiladores, tostadoras, refrigeradores, cortadoras de césped, lavadoras, televisores y aspiradoras, entre otros. Además, se encuentra una variada selección de sensores y sistemas de alarmas de seguridad tanto para residencias como para empresas y vehículos (Vinton, 2016). Aunque los teléfonos móviles, tabletas, relojes inteligentes,

reproductores de música y computadoras portátiles también podrían ser clasificados como dispositivos IoT, esta investigación se centra en los niveles de ciberseguridad que ofrecen los primeros dispositivos mencionados.

Las plataformas de gestión de datos empleadas para ciertos servicios ofrecen una notable facilidad de acceso desde varios dispositivos, permitiendo a los usuarios gestionar la información almacenada. Según Amazon Web Services, una base de datos es "una colección de elementos de información con relaciones definidas entre ellos. Estos elementos se organizan en un conjunto de tablas compuestas por columnas y filas. Las tablas sirven para almacenar datos sobre los objetos que se representan en la base de datos. Es posible acceder a esta información de diversas maneras sin necesidad de reorganizar las tablas existentes" (AWS, 2020). En resumen, este tipo de servicio permite a las empresas tener acceso a sus datos, ya sea en almacenamiento en la nube o local, proporcionado por un tercero, lo que asegura confiabilidad, integridad y disponibilidad de la información, además de ofrecer garantías para realizar copias de seguridad.

La Unión Europea establecen que las organizaciones que gestionen datos personales en sistemas de Internet de las Cosas (IoT) deben realizar análisis de seguridad y emplear las certificaciones y normas de seguridad adecuadas. Además, es fundamental que las empresas aseguren este cumplimiento cuando colaboren con proveedores externos para el manejo de dispositivos y datos de IoT; en este caso, estos proveedores también tienen la responsabilidad de implementar medidas de seguridad razonables." (Ministerio de Modernización de Argentina, 2020). En la actualidad, se observa una amplia recolección de información personal a través de diversos dispositivos y redes. En la era de los sistemas de Internet de las Cosas (IoT), se puede destacar la acumulación de estos datos en múltiples ubicaciones. Además, la facilidad de conexión entre dispositivos permite que nuestra información sea compartida en formas que

nunca antes habíamos presenciado. Esta recolección de datos está estrechamente relacionada con la violación de la privacidad (Ministerio de Modernización de Argentina, 2020).

La seguridad cibernética, el Grupo de Trabajo Conjunto sobre Educación en Ciberseguridad, conocido en inglés como Joint Task Force on Cybersecurity Education, describe la ciberseguridad como una área de estudio fundamentada en la informática que abarca tecnología, individuos, información y procedimientos para facilitar operaciones seguras frente a posibles amenazas. En una publicación de 2018, se establece que esta área se fundamenta en los principios esenciales de la seguridad de la información y su protección. Esto da lugar a términos como ciberataques y ciberdelincuentes. Al estar conectados a la red, estos dispositivos también están expuestos a posibles ataques. Un ciberataque es descrito en la revista destacada de ACM (Association for Computing Machinery) “Communications of the ACM” como un asalto a un ordenador y una red de sistemas. Este tipo de ataque implica acciones realizadas por el ordenador, tales como conexiones remotas o locales, acceso a archivos o ejecución de programas, con el objetivo de poner en riesgo la operación segura del ordenador y la red (Crawford, D., 2001)

El creciente uso de infraestructuras de información en áreas críticas como la defensa, la banca, las telecomunicaciones, el transporte y la energía ha llevado a que los ciberataques se conviertan en una amenaza significativa para la sociedad, con potenciales repercusiones graves (Crawford, D., 2001). Este documento menciona varios tipos de ciberataques, incluyendo ataques de denegación de servicio (DOS), la introducción de malware como el ransomware, y las botnets. Además, es esencial diferenciar entre seguridad física y ciberseguridad: la primera se ocupa de los aspectos tangibles del dispositivo y su protección material, mientras que la segunda

se centra en los elementos intangibles, abarcando la información almacenada y los procesos relacionados con la gestión y mantenimiento de datos.

Las siglas DOS se refieren a Denegación de Servicio, un tipo de ataque cibernético que busca incapacitar un sitio web para atender las solicitudes de los usuarios, inundando la computadora objetivo con una gran cantidad de datos a través de Internet. Este ataque se produce al sobrecargar el sistema con un número excesivo de peticiones que superan la capacidad de respuesta del servidor, impidiendo que pueda manejar más solicitudes. Además, existe el término DDOS, que significa Denegación de Servicio Distribuido, donde múltiples agentes, a menudo cientos o miles de dispositivos cliente, atacan simultáneamente el mismo sitio web; frecuentemente, estos dispositivos son computadoras en entornos educativos que son vulnerables a la manipulación (Singleton, 2002).Los ataques de inserción de software malicioso. Para comprender este tipo de ciberataque, es fundamental saber qué es un malware. Este término engloba diversas clases de programas dañinos diseñados para perjudicar o aprovecharse de cualquier dispositivo, servicio o red informática. Los delincuentes cibernéticos utilizan estos programas para robar información que puede ser empleada posteriormente para extorsionar a las víctimas y así obtener beneficios económicos. Entre los datos que pueden verse comprometidos se incluyen información financiera, registros médicos, correos electrónicos personales y contraseñas. La gama de información susceptible de ser afectada se ha vuelto prácticamente infinita (McAfee, 2020). “El malware puede infiltrarse en computadoras y dispositivos de múltiples maneras y se presenta en diversas formas, algunas de las cuales son virus, gusanos, troyanos, spyware y más” (Kaspersky, 2020).

El término malware incluye uno de los programas maliciosos más notorios, el ransomware, que se ha vuelto extremadamente lucrativo y, por lo tanto, muy popular entre los

delincuentes cibernéticos. Este tipo de software se introduce en el ordenador de la víctima, cifra sus datos y exige un pago (usualmente en criptomonedas como Bitcoin) para restaurar el acceso a la información bloqueada. (McAfee, 2020). Es fundamental hablar sobre las botnets, que se refieren a un conjunto de computadoras que han sido comprometidas y son manipuladas de manera remota por un atacante. Para establecer una botnet, un hacker o un grupo de ellos desarrolla un malware que se distribuye a través de Internet, logrando infectar a numerosos dispositivos de diferentes usuarios al azar. En la mayoría de los casos, los propietarios de estos dispositivos no son conscientes de que sus máquinas están comprometidas y forman parte de una botnet. Estos equipos infectados son conocidos como “bots” o “zombis”. No hay un límite mínimo en cuanto a la cantidad de dispositivos necesarios para formar una botnet; las más pequeñas pueden incluir cientos de computadoras infectadas, mientras que las más grandes pueden abarcar millones. (Kaspersky, 2020).

Los “delincuentes cibernéticos” en varias ocasiones y tenga una idea de su significado. Pero ¿qué son realmente los delincuentes cibernéticos? Estos individuos pueden ser desde expertos en tecnología hasta estudiantes con conocimientos o entusiastas que navegan por Internet. Todos comparten el objetivo de crear software malicioso para infectar diversos dispositivos, aunque sus motivaciones pueden variar, incluyendo el robo de datos o el espionaje. “Los delincuentes cibernéticos están volviéndose cada vez más rápidos, aprovechando las nuevas tecnologías a una velocidad impresionante, adaptando sus ataques con métodos innovadores y colaborando entre ellos de formas nunca antes vistas. Las redes criminales operan a nivel global, coordinando ataques complejos contra sus objetivos en cuestión de minutos.” (INTERPOL, 2020).

Después de abordar los ciberataques y los delincuentes cibernéticos, es fundamental hablar sobre las medidas de seguridad, es decir, las estrategias para mitigar o incluso prevenir estos ataques. Para ello, se emplean diversos programas especializados que llevan a cabo diferentes funciones para evitar o enfrentar amenazas como virus informáticos o malware. Estas aplicaciones suelen instalarse en una computadora como cualquier otro software y se encargan de examinar todos los archivos que se descargan o se accede, especialmente en el caso de programas maliciosos presentes en la red (Kaspersky, 2021). Además, existen los honeypots, que son sistemas informáticos deliberadamente vulnerables diseñados para recopilar información sobre ciberdelincuentes. Un honeypot funciona como un sistema informático convencional que contiene directorios e información, pero su propósito es muy específico y distinto (Abhishek M., Debabrat B., Kanchan V., Debasish J., 2001).

La información presentada, representa una revisión detallada y multifacética sobre los desafíos de seguridad en el Internet de las Cosas (IoT), con especial énfasis en los sensores de agua utilizados en redes inteligentes. Si bien expone de manera rigurosa una gran cantidad de estudios, tecnologías y protocolos, se identifica una fragmentación analítica y una falta de integración crítica que limite la comprensión del problema en su complejidad sistémica.

El marco teórico destaca la importancia de protocolos como CoAP, MQTT, XMPP y DTLS en entornos IoT, así como sus fortalezas y debilidades. La exposición de vulnerabilidades concretas como la falta de actualización automática de claves en CoAP o los riesgos asociados a NB-IoT, también revela un panorama técnico realista. Sin embargo, aunque se presentan numerosas investigaciones (Kondoro, Raza, Bertín, Selander, entre otros), el análisis tiende a limitarse a una recopilación informativa más que a una síntesis crítica que permita establecer conexiones estratégicas entre hallazgos. No se plantea, por ejemplo, cómo los protocolos más

robustos pueden adaptarse de forma escalable en entornos de bajo consumo o en zonas rurales donde operan muchos sensores de agua.

La información presentada, detecta una ausencia de perspectiva contextual: el texto aborda múltiples tecnologías, amenazas y propuestas, pero no profundiza en las implicaciones sociotécnicas de su implementación. Aspectos como la gobernanza de los datos, la sostenibilidad económica de los sistemas o la capacitación de usuarios finales apenas se mencionan. Este vacío resulta problemático considerando que los sensores IoT no solo son vulnerables técnicamente, sino también desde lo organizacional y normativo.

Finalmente, aunque se subraya la necesidad de protocolos seguros y ligeros como EDHOC y LAKE para dispositivos con recursos limitados, el texto no avanza hacia una discusión crítica sobre los criterios de estandarización ni sobre las tensiones entre eficiencia, privacidad y soberanía tecnológica. En este sentido, se extraña una mirada crítica al rol de los proveedores comerciales de soluciones IoT y a la dependencia tecnológica que podría generarse en territorios con baja capacidad de innovación autónoma.

La seguridad de los dispositivos conectados a Internet, conocidos como IoT, es un tema de suma relevancia en un entorno donde se utilizan desde cámaras para vigilar a los bebés hasta herramientas para el monitoreo de la salud. Por ello, es crucial que estos dispositivos electrónicos ofrezcan la protección necesaria en relación con la información, su operatividad y la confianza en su utilización. Si un atacante logra explotar alguna debilidad en estos sistemas y compromete la privacidad de los usuarios al manipular elementos previamente mencionados, podría llevar a cabo el robo de información, interrumpir servicios o cometer otros delitos. En consecuencia, las empresas especializadas en seguridad para IoT aconsejan implementar una estrategia que contemple tres aspectos fundamentales para proteger los datos, los dispositivos y las conexiones:

asegurar el aprovisionamiento de los dispositivos, proteger la conectividad entre estos y la nube, y salvaguardar los datos en la nube durante su procesamiento y almacenamiento (Microsoft Azure, 2020).

La evaluación de amenazas y debilidades constituye un elemento clave para establecer una cultura sólida de seguridad de la información. Este enfoque nos ayuda a reconocer los riesgos a los que se enfrenta nuestra organización, así como las falencias en nuestros sistemas y procedimientos que podrían ser explotadas por actores maliciosos. Para llevar a cabo esta evaluación, es fundamental realizar análisis de riesgo, tanto desde una perspectiva interna como externa, con el fin de identificar posibles amenazas y vulnerabilidades. Además, se pueden aplicar diversas herramientas y métodos de análisis de seguridad, como simulaciones de ataques y escaneos de vulnerabilidades, que son útiles para detectar las fisuras en nuestros sistemas. Una vez que hemos mapeado los riesgos y debilidades, podremos implementar las estrategias adecuadas para mitigarlos y asegurar la integridad de la información dentro de la organización.

La seguridad de los dispositivos conectados a Internet, conocidos como IoT (Internet of Things), es un tema de suma relevancia en un entorno donde se utilizan desde cámaras para vigilar a los bebés hasta herramientas para el monitoreo de la salud. Por ello, es crucial que estos dispositivos electrónicos ofrezcan la protección necesaria en relación con la información, su operatividad y la confianza en su utilización. Si un atacante logra explotar alguna debilidad en estos sistemas y compromete la privacidad de los usuarios al manipular elementos previamente mencionados, podría llevar a cabo el robo de información, interrumpir servicios o cometer otros delitos. En consecuencia, las empresas especializadas en seguridad para IoT aconsejan implementar una estrategia que contemple tres aspectos fundamentales para proteger los datos, los dispositivos y las conexiones: asegurar el aprovisionamiento de los dispositivos, proteger la

conectividad entre estos y la nube, y salvaguardar los datos en la nube durante su procesamiento y almacenamiento (Microsoft Azure, 2020).

La evaluación de amenazas y debilidades constituye un elemento clave para establecer una cultura sólida de seguridad de la información. Este enfoque nos ayuda a reconocer los riesgos a los que se enfrenta nuestra organización, así como las falencias en nuestros sistemas y procedimientos que podrían ser explotadas por actores maliciosos. Para llevar a cabo esta evaluación, es fundamental realizar análisis de riesgo, tanto desde una perspectiva interna como externa, con el fin de identificar posibles amenazas y vulnerabilidades. Entre las metodologías más reconocidas para este fin se encuentran ISO/IEC 27005, que guía el análisis y gestión de riesgos en sistemas de información, y STRIDE, un modelo desarrollado por Microsoft para categorizar amenazas en seis clases: suplantación, alteración, repudio, divulgación de información, denegación de servicio y elevación de privilegios (ISO/IEC, 2018; Microsoft, 2020)

Marco Conceptual

Los Dispositivos de Internet de las Cosas (IoT)

Según el Instituto Nacional de Ciberseguridad (INCIBE) de España, una vulnerabilidad en el contexto informático se define como una deficiencia o error en un sistema de información que puede poner en peligro la seguridad de los datos, permitiendo que un atacante comprometa la integridad, disponibilidad o confidencialidad de la información. Por lo tanto, el INCIBE sugiere que se identifiquen y remedien estas vulnerabilidades a la mayor brevedad posible. (Microsoft Azure, 2020). Los riesgos asociados a los dispositivos IoT, se considerarán los ataques a los que pueden estar expuestos, organizándolos en cinco categorías. La primera categoría es la suplantación de identidad, donde un atacante tiene la capacidad de manipular el estado de un dispositivo de manera anónima. Además, puede interceptar o alterar parcialmente la transmisión

de datos, lo que le permite hacerse pasar por el autor. Por último, si el atacante logra acceder a la red después de obtener la clave de acceso, puede acceder a la información que genera el dispositivo. (Microsoft Azure, 2020). Las modificaciones que pueden realizarse en el software de los dispositivos electrónicos con el objetivo de acceder a su configuración y alterar su funcionamiento. La tercera categoría involucra la divulgación de información, en la cual el usuario corre el riesgo de que los ciberdelincuentes accedan a datos privados almacenados sin la debida autorización para hacerlo. En algunos casos, el acceso a la información puede ser denegado o puede tratarse de datos falsos. (Microsoft Azure, 2020).

La Criptografía

Es un término que surge de la fusión de dos palabras griegas: "kryptos", que se traduce como oculto, y "graphia", que significa escritura; se define como un conjunto de métodos que permiten modificar y transformar mensajes o archivos con el objetivo de que personas no autorizadas no puedan acceder a su contenido. Esta práctica es esencial para asegurar la confidencialidad en la comunicación, ya que permite que solo aquellos con la clave adecuada puedan descifrar y entender la información enviada. (NIC Argentina, 2018). Esta herramienta empleada en el ámbito de la ciberseguridad y en la actualidad se está explorando su uso en contextos de Internet de las Cosas (IoT). Entre estos, se encuentran los protocolos de redes de sensores inalámbricos (WSN), que se enfocan en la creación de una red compuesta por sensores sin cables. Esta solución fue diseñada para dos escenarios criptográficos: uno que utiliza una topología en malla, donde los nodos poseen una considerable capacidad de procesamiento, y otro que emplea una topología estelar, que opera con nodos de menor capacidad en comparación con el anterior (Morales, Diaz y Leguizamón, 2019, p. 294).

El objetivo de estas técnicas de cifrado es lograr un balance entre los requisitos y la seguridad de una red de sensores inalámbricos, en la que se utiliza un árbol de nodos con funciones hash. Un hash es un procedimiento matemático que convierte cualquier conjunto de datos en una nueva secuencia de caracteres de longitud fija, independientemente del tamaño de los datos originales; el valor hash resultante siempre tendrá la misma longitud (Donohue, 2014). Los nodos finales de la red son responsables de enviar los hashes de la información a los nodos enrutadores. Una vez que se envían, la información se válida para garantizar que haya llegado en su totalidad. Posteriormente, se transmite a cada nodo enrutador utilizando la función hash hasta alcanzar el nodo final del árbol (Morales, Diaz y Leguizamón, 2019, p. 295).

Tecnología de Cadena de Bloques

La aplicación en las criptomonedas, aunque su funcionalidad va mucho más allá de este ámbito. Este sistema descentralizado permite realizar registros de diversas transacciones de manera distribuida. Cada entrada de información se agrupa en un bloque, y estos bloques se conectan entre sí a través de funciones matemáticas, creando así una cadena. Cada bloque incluye un hash criptográfico del bloque anterior, además de almacenar los datos de la transacción y una marca temporal (Tudela, 2019). Gracias a estas características, se establece un árbol Merkle (Becker, 2008), que proporciona ventajas significativas como la rápida verificación de datos y la resistencia a modificaciones no autorizadas. En resumen, la cadena de bloques actúa como un registro público y descentralizado que permite almacenar información entre dos partes de manera verificable, eficiente y permanente (Tudela, 2019).

Como se ha señalado anteriormente, la tecnología de cadena de bloques comenzó con un enfoque en las criptomonedas. Sin embargo, sus propiedades ofrecen una amplia gama de ventajas en distintos sectores. En particular, su diseño descentralizado y sus robustos

mecanismos de seguridad son ideales para las arquitecturas del Internet de las Cosas (IoT). Así, uno de los métodos innovadores para asegurar los sistemas IoT se fundamenta en la cadena de bloques. Este método utiliza contratos inteligentes, que permiten la gestión eficiente de recursos y la implementación de sistemas de seguridad a través de la red Ethereum. Esta red facilita configuraciones privadas, permitiendo seleccionar las direcciones que se asignarán a cada dispositivo IoT, cada uno con su propia cuenta en la red. Al integrar contratos inteligentes con la cadena de bloques, la implementación de medidas de seguridad se simplifica, ya que estas están incorporadas en los propios contratos, junto con la gestión de versiones y el registro de datos, lo que permite almacenar principalmente la lógica del sistema (Tudela, 2019).

En Amazon Managed Blockchain. Este servicio completamente gestionado facilita la creación y administración de redes de cadena de bloques escalables utilizando los marcos de código abierto Hyperledger Fabric y Ethereum. Su principal ventaja radica en eliminar la carga asociada a la creación de una red de cadena de bloques, ya que, en un proceso convencional, cada participante debe aprovisionar manualmente el hardware, instalar el software necesario, generar y gestionar los certificados para controlar el acceso y configurar los elementos de la red.

Con Amazon Managed Blockchain, el proceso para establecer una red segura y eficiente se simplifica significativamente, adaptándose automáticamente a las demandas de miles de aplicaciones que manejan millones de transacciones en dispositivos IoT. Además, una vez que la red está en funcionamiento, el mantenimiento y la gestión se vuelven más sencillos, ya que el servicio permite invitar fácilmente a nuevos miembros a unirse a la red y se encarga de administrar los certificados generados, así como de monitorear métricas operativas como uso de memoria, almacenamiento y recursos computacionales.

Estas características hacen que este servicio de Amazon tenga un gran potencial para facilitar soluciones seguras para la conexión con dispositivos IoT (AWS, 2021).

Marco Legal

Este marco legal aborda la necesidad crucial de fortalecer la seguridad en el creciente ámbito del Internet de las Cosas (IoT), considerando su integración en infraestructuras industriales y la vida cotidiana. Las vulnerabilidades asociadas a estos dispositivos representan riesgos significativos para la seguridad de los datos y la privacidad de los usuarios, tal como lo destaca el planteamiento del problema en el documento adjunto, donde se menciona el aumento de ataques a dispositivos IoT y el potencial robo de información personal (Kaspersky, 2019; INCIBE, 2015).

La presente investigación, al proponer una metodología de auditoría de seguridad intrusiva y estrategias de mitigación (De Lima Rosado, 2025), se alinea con la necesidad de fortalecer la ciberseguridad nacional, establecida en la Política Nacional de Ciberseguridad y Ciberdefensa (CONPES 3995 de 2020).

Leyes Nacionales de Protección de Datos en Colombia

La Ley Estatutaria 1581 de 2012 (Ley de Protección de Datos Personales), reglamentada por el Decreto 1377 de 2013, establece el régimen general de protección de datos personales en Colombia. Esta ley define principios como la finalidad, la libertad y la transparencia, que deben ser observados en el tratamiento de datos personales recolectados a través de dispositivos IoT. Además, la jurisprudencia de la Corte Constitucional, como la Sentencia C-748 de 2011, protege el derecho fundamental al *habeas data*, garantizando a los ciudadanos el control sobre su información personal. La propuesta de investigación, al buscar un sistema de protección completo para redes de dispositivos IoT, debe asegurar el cumplimiento de estos principios y

derechos, tal como se mandata en el artículo 15 de la Constitución Política de Colombia, garantizando la confidencialidad, integridad y disponibilidad de la información personal (De Lima Rosado, 2025).

La Ley Estatutaria 1581 de 2012 y su reglamentación en el Decreto 1377 de 2013 establecen disposiciones generales para la protección de datos personales en Colombia, y sí pueden aplicarse a los sensores de agua con tecnología IoT, siempre que estos dispositivos recojan, almacenen, procesen o transmitan datos personales (por ejemplo: nombre del usuario, ubicación del inmueble, hábitos de consumo de agua, dirección IP, entre otros).

Artículos Ley 1581 de 2012 pueden referenciarse directamente para sensores de agua:

Artículo 3: se aplica porque define términos esenciales como: datos personal, cualquier información vinculada o que pueda asociarse a una o varias personas naturales. Tratamiento: cualquier operación sobre datos personales. Responsable del tratamiento y encargado del tratamiento: figuras que pueden aplicarse a empresas que fabrican, operan o administran los sensores IoT.

Artículo 4: Principios para el tratamiento de datos personales, relevante porque establece principios como: legalidad, finalidad, libertad, veracidad o calidad del dato, transparencia, seguridad, y confidencialidad. Es de importancia para los sensores de agua IoT: los desarrolladores e implementadores de sensores deben garantizar que los datos personales recolectados por sus dispositivos se traten conforme a estos principios.

Artículo 5: Derechos de los Titulares. Este artículo protege al usuario o ciudadano, permitiendo, conocer, actualizar y rectificar su información personal. Solicitar prueba de la autorización del tratamiento. Ser informado sobre el uso de sus datos. Revocar la autorización o solicitar la supresión de los datos. Importancia para sensores de agua con tecnologia IoT: el

usuario debe tener el control sobre sus datos incluso si estos son recolectados automáticamente por sensores.

Artículo 6**:** si el sensor IoT recoge datos sensibles (por ejemplo, relacionados con salud, hábitos de vida o consumo), se deben aplicar requisitos adicionales. Se requiere autorización expresa. Está prohibido el tratamiento de datos sensibles salvo excepciones específicas. Importancia para tecnología de sensores IoT, algunos sensores inteligentes pueden inferir patrones sensibles, como enfermedades relacionadas con el consumo de agua o el uso en clínicas.

Referentes Internacionales en Protección de Datos

Colombia no está directamente sujeta al Reglamento General de Protección de Datos (GDPR) (UE) (Reglamento (UE) 2016/679), sus principios son relevantes. El GDPR enfatiza la minimización de datos, la limitación de la finalidad y la necesidad de consentimiento explícito. Estos principios pueden ser considerados como soft law y sirven de guía en el desarrollo de políticas nacionales.

Ciberseguridad y Protección de Infraestructuras Críticas en Redes IoT

La integración de redes IoT en infraestructuras industriales requiere medidas de ciberseguridad robustas para proteger activos críticos y prevenir interrupciones, como se justifica en el documento adjunto al destacar la importancia de la seguridad de la información para las empresas y la necesidad de gestionar los riesgos asociados a dispositivos IoT (Malik y Singh, 2020).

Política Nacional de Ciberseguridad y Delitos Informáticos en Colombia

La CONPES 3995 de 2020 establece la Política Nacional de Ciberseguridad y Ciberdefensa, que define los objetivos, estrategias y acciones para fortalecer la ciberseguridad del país, incluyendo la protección de infraestructuras críticas que utilizan tecnologías IoT. La

Ley 1273 de 2009 (Ley de Delitos Informáticos) tipifica conductas delictivas que podrían ser aplicadas en casos de ataques a sistemas IoT, sancionando el acceso abusivo a un sistema informático, el daño informático y la interceptación de datos, entre otros delitos.

Ley 1273 de 2009, delitos Informáticos en Colombia modifica el Código Penal para incluir el Título VII Bis: Delitos informáticos y relacionados. Aplicabilidad a Sensores de agua IoT**.** Los sensores de agua IoT pueden ser objeto o medio de delitos tipificados en esta ley, tales como: Artículo 269A, acceso abusivo a un sistema informático, se configura si un actor no autorizado accede a la red donde operan los sensores para visualizar o manipular datos.

Artículo 269B, obstaculización ilegítima de sistema informático o red de telecomunicación, aplica si se interfiere o sabotea la operación de sensores o su red de comunicación, afectando la disponibilidad del sistema. Artículo 269C, interceptación de datos informáticos, **s**e da cuando un atacante capta datos transmitidos por los sensores sin autorización, como registros de consumo o ubicación. Artículo 269F, violación de datos personales, **s**i los sensores manejan datos vinculados a personas naturales (como consumo domiciliario o geolocalización), el acceso no autorizado constituye violación a la privacidad.

Ley 1581 de 2012. Ley de Protección de Datos Personales (Habeas Data)**,** reglamentada por el Decreto 1377 de 2013 con aplicabilidad, los sensores de agua IoT pueden captar o transmitir datos que permitan identificar o asociar a una persona natural (por ejemplo, patrones de consumo domiciliario o ubicación exacta), por tanto, están sujetos a esta ley.

Marco de Referencia de Arquitectura Empresarial (Mrae)

El Marco de Referencia de Arquitectura Empresarial (MRAE), es un instrumento metodológico para la planeación, gestión y evaluación de la arquitectura empresarial en las entidades del Estado Colombiano, puede ser un referente para las organizaciones del estado en la

implementación de procesos de ciberseguridad. La propuesta de investigación, al buscar combinar soluciones existentes para desarrollar un sistema de protección completo, se alinea con estos objetivos y podría contribuir a la implementación de la Política Nacional de Ciberseguridad y Ciberdefensa (De Lima Rosado, 2025).

Estándares y Modelos de Seguridad

El Modelo de Seguridad y Protección de la Información (MSPI), desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC), establece directrices para la seguridad de la información en entidades estatales. Aunque el documento adjunto señala una falta de especificidad en IoT, las 21 directrices del MSPI deben ser adaptadas y complementadas para abordar los riesgos particulares de los dispositivos IoT. Además, se deben considerar estándares internacionales como ISO 27001, que establece los requisitos para un sistema de gestión de seguridad de la información.

Responsabilidad y Rendición de Cuentas en el Ecosistema IoT

Establecer líneas claras de responsabilidad y rendición de cuentas es esencial para fomentar una cultura de seguridad dentro del ecosistema IoT. Esto implica considerar la responsabilidad de los fabricantes de dispositivos, los proveedores de servicios y los usuarios finales.

Protección al Consumidor y Responsabilidad Civil en Colombia

La Ley 1480 de 2011 (Estatuto del Consumidor) establece la responsabilidad de los productores y proveedores por la calidad e idoneidad de los bienes y servicios, lo que se aplica a dispositivos IoT defectuosos o inseguros. El Código Civil Colombiano establece principios generales de responsabilidad civil extracontractual (artículos 2341 y siguientes), que podrían ser invocados en casos de daños causados por vulnerabilidades en dispositivos IoT. La propuesta de

investigación, al buscar identificar vulnerabilidades y proponer estrategias de mitigación, contribuye a establecer un marco de responsabilidad más claro para los actores involucrados en el ecosistema IoT (De Lima Rosado, 2025).

Metodologías y Estándares de Auditoría de Seguridad

La propuesta de investigación, al proponer una metodología de auditoría de seguridad intrusiva (como OWASP, PHVA, NUTRIA o NIST), se alinea con esta necesidad (De Lima Rosado, 2025). Se pueden usar *frameworks* como el NIST Cybersecurity Framework, que proporciona un conjunto de estándares, directrices y mejores prácticas para gestionar los riesgos de ciberseguridad. Además, la Guía para la Interconexión Segura de Redes Inalámbricas (ICA-G-014) del Ministerio de Defensa Nacional de Colombia, aunque enfocada en redes inalámbricas, ofrece principios relevantes para asegurar redes IoT.

Comité de Seguridad Digital

La Resolución 1519 de 2020 crea el Comité de Seguridad Digital, el cual es de carácter consultivo y tiene como objeto principal asesorar al Gobierno Nacional en la formulación e implementación de la política pública en materia de seguridad digital. La presente investigación, al proponer estrategias y soluciones para fortalecer la seguridad en el IoT, puede contribuir a la formulación de políticas públicas más efectivas en esta materia (De Lima Rosado, 2025).

Marco Contextual

El Internet de las Cosas (IoT) ha transformado la interacción con el mundo, integrándose en hogares inteligentes y sistemas industriales. Esta expansión presenta oportunidades y desafíos. Si bien el IoT mejora la automatización, la toma de decisiones basada en datos, la productividad y la seguridad a través del monitoreo de infraestructura, también introduce vulnerabilidades de seguridad significativas (Smith & Jones, 2024). La creciente interconexión de dispositivos

amplía la superficie de ataque, convirtiendo a los sistemas IoT en objetivos atractivos para ciberdelincuentes.

Las organizaciones reconocen la importancia de la seguridad de la información en la era digital e invierten en herramientas que integran sistemas, personal y productos en una cadena unificada de análisis y recopilación de información. La base de la digitalización es la red de dispositivos IoT. Gestionar la seguridad de la información es fundamental para proteger la integridad, disponibilidad y confidencialidad de los datos. Por lo tanto, es necesario implementar enfoques adecuados para gestionar los riesgos, especialmente los relacionados con el uso de dispositivos IoT (Johnson & Williams, 2019; Patel et al., 2018).

Para abordar estos problemas, los gobiernos y las organizaciones exploran marcos de seguridad. La adopción de metodologías para la evaluación de sistemas IoT presenta un desafío considerable debido a los nuevos riesgos asociados con la conectividad o la fusión de sistemas digitales, ciberfísicos y sociales. A pesar de esfuerzos gubernamentales como el MSPI en Colombia, falta una directriz específica sobre la gestión de riesgos de IoT. Esta brecha destaca la necesidad de investigar y desarrollar estrategias de seguridad integrales adaptadas a los desafíos únicos del IoT (Robinson, 2024)

Diseño Metodológico

Esta investigación se centra en el fortalecimiento de la seguridad en el Internet de las Cosas (IoT) y busca proponer estrategias para mitigar los riesgos de vulnerabilidad. Para lograr este objetivo, se adoptará un enfoque metodológico mixto, combinando elementos cuantitativos y cualitativos para obtener una comprensión integral del problema.

Tipo de Investigación

La investigación será de tipo deductiva. Inicialmente, mediante la documentación se explorará el estado actual de la seguridad en sensores de agua IoT, identificando las principales vulnerabilidades y amenazas existentes. Posteriormente, se describirán las estrategias y propuestas para mitigar dichos riesgos, basándose en la revisión de literatura y el análisis de casos de estudio.

Según Hernández Sampieri (2014), el enfoque de metodologia mixta, se centra en comprender fenómenos El enfoque mixto es una metodología que integra elementos tanto cuantitativos como cualitativos dentro de una misma investigación. Este enfoque busca obtener una comprensión más completa del fenómeno estudiado, aprovechando las fortalezas de ambos métodos y compensando sus debilidades.

Para esta investigación se utilizó el método de enfoque cualitativo y cuantitativo**,** se analizará información sobre incidentes de seguridad en dispositivos IoT sensores de agua , recopilados de fuentes confiables como informes de empresas de ciberseguridad (Kaspersky, ENISA, INCIBE, etc.) y bases de datos de vulnerabilidades (NVD, CVE). Esto permitirá cuantificar la magnitud del problema e identificar tendencias relevantes. Se realizará una revisión exhaustiva de la literatura científica y técnica relacionada con la seguridad en sensores de agua IoT, incluyendo artículos académicos, informes técnicos, estándares de seguridad y buenas

prácticas. Además, se analizarán casos de estudio de ataques a dispositivos sensores de agua IoT para comprender las vulnerabilidades explotadas y las consecuencias de los incidentes.

Este estudio se desarrolla bajo un enfoque cuantitativo. Según Hernández Sampieri, el método cuantitativo es una metodología de investigación que se basa en la medición numérica de variables y el análisis estadístico para probar hipótesis, explicar fenómenos y establecer relaciones causales o correlacionales. En el caso especial de esta investigación se aplicara mediante casos, los riesgos y vulnerabilidades en ciberseguridad, con el fin de evaluar el impacto de potencial con métricas en la implementación con sensores de agua con tecnología IoT.

Técnicas De Recolección Información

Para las técnicas de recolección de la información, se realizaron una serie de pasos que van desde la revisión bibliográfica, análisis de casos de estudio, auditoria de seguridad intrusiva, análisis de contenido, análisis comparativo.

Revisión Bibliográfica: Se realizo una investigación en literatura académica, se tuvieron en cuentan revistas ((IEEE Xplore, ACM Digital Library, Scopus, Web of Science) y en fuentes de información (sitios web de empresas de ciberseguridad, blogs especializados, repositorios de vulnerabilidades).

Análisis de Casos de Estudio: Para el análisis de casos de estudio. Se selecciono casos estudio de importancia, relacionados con los ataques a dispositivos en sensores de agua IoT, información que se encontró documentada en informes de seguridad, artículos de noticias o investigaciones académicas.

Auditoría de Seguridad Intrusiva: Como se mencionó en el planteamiento del problema, se planteó una metodología de auditoría de seguridad intrusiva que permitió supervisar los datos y, al mismo tiempo, llevar a cabo diversos tipos de ataques controlados en un entorno de prueba.

Esto aporto a identificar información específica en dispositivos sensores de agua IoT y evaluar la efectividad de las medidas de seguridad existentes.

Análisis de Contenido: Se realizará un análisis de contenido de la literatura revisada y de los casos de estudio seleccionados. Se identificarán los principales temas, conceptos, vulnerabilidades y estrategias en relación con los sensores de agua IoT.

Población y Muestra

Población: La población objetivo de esta investigación, son los dispositivos y sistemas de sensores de agua con tecnología IoT, así como las organizaciones y usuarios que los utilizan.

Muestra: La muestra estará compuesta por casos de estudio de dispositivos en sensores de agua IoT, seleccionados por su relevancia y representatividad. Se selecciono una WSN específica para realizar la auditoría de seguridad intrusiva.

Instrumentos de recolección de datos: Para los instrumentos de recolección de datos para este proyecto, se tuvo en cuenta el protocolo de revisión bibliográfica, guía de análisis de casos de estudio, documentación detallada.

Protocolo de Revisión Bibliográfica: Se utilizo un protocolo estandarizado para registrar la información relevante de cada artículo o documento revisado.

Guía de Análisis de Casos de Estudio: Se tuvo en cuenta una guía elaborada para analizar los casos de estudio, identificando las vulnerabilidades, las técnicas de ataque y las consecuencias de los incidentes.

Documentación Detallada: Se documento detalladamente el proceso de investigación, incluyendo los métodos de recolección y análisis de datos, las decisiones metodológicas tomadas y las limitaciones del estudio.

Identificar los Riesgos y Vulnerabilidades en Ciberseguridad en la Implementación de Sensores de Agua IoT

Introducción a los Riesgos de Ciberseguridad en el IoT

El Internet de las Cosas (IoT) ha revolucionado la forma en que interactuamos con el entorno mediante la integración de dispositivos inteligentes que permiten monitorear, recopilar y procesar datos en tiempo real. En particular, la implementación de sensores IoT en redes de monitoreo hídrico ha permitido avances significativos en la gestión sostenible del recurso agua, control de calidad, prevención de fugas, y alerta temprana ante contaminaciones o desbordamientos (Gómez et al., 2022).

No obstante, esta infraestructura interconectada presenta riesgos considerables en términos de ciberseguridad. Cada sensor, actuador o gateway constituye un punto potencial de entrada para atacantes, lo que amplía la superficie de ataque y compromete la seguridad de sistemas críticos (Roman, Najera & Lopez, 2013). Los riesgos van más allá de la simple pérdida de datos: incluyen la alteración de parámetros ambientales, manipulación de datos operativos y potenciales daños a la infraestructura física, lo que puede generar consecuencias económicas, ambientales y sociales significativas (NIST, 2020).

Evaluación de las Deficiencias en los Protocolos de Ciberseguridad en Sensores de Agua IoT

Una de las principales vulnerabilidades detectadas en dispositivos IoT utilizados en redes hídricas es la implementación de protocolos de comunicación inseguros o desactualizados, como HTTP en lugar de HTTPS, o el uso de protocolos propietarios sin mecanismos robustos de autenticación y cifrado (Genge & Haller, 2019). Estas prácticas permiten ataques como Man-in-the-Middle (MitM), spoofing, o inyección de comandos, que comprometen la integridad del sistema.

Otro problema recurrente es el uso de credenciales por defecto o mal gestionadas. Según una investigación de Symantec (2021), cerca del 15% de los dispositivos IoT industriales en operación siguen utilizando configuraciones de fábrica, lo que los hace altamente vulnerables a ataques automatizados mediante bots como Mira o Mozi.

A esto se suma la falta de actualizaciones de firmware. Muchos sensores no cuentan con mecanismos seguros de actualización remota (OTA – Over the Air), lo que impide parchear vulnerabilidades una vez desplegados en campo. Esta carencia representa un riesgo crítico cuando se descubren nuevas amenazas o vulnerabilidades de día cero (ENISA, 2023

Además, el uso masivo de tecnologías inalámbricas, dispositivos con recursos limitados (batería, procesamiento, almacenamiento), y la falta de estándares uniformes agravan estas amenazas. Por ello, la seguridad en sensores IoT aplicados a recursos hídricos debe abordarse desde una perspectiva integral, contemplando no solo la tecnología sino también la gestión del riesgo, la capacitación del personal y el cumplimiento normativo.

Establecimiento de los Riesgos y Debilidades más Significativas en Sensores de Agua IoT

La identificación y clasificación de riesgos permite priorizar acciones preventivas y correctivas. En este sentido, los riesgos más relevantes en la implementación de sensores IoT para monitoreo hídrico incluyen:

- Exposición de datos sensibles, como niveles de contaminación, consumo o presión, lo cual puede ser aprovechado por terceros con intereses económicos o políticos.

- Sabotaje a sistemas de bombeo, válvulas inteligentes o estaciones de control, afectando el suministro, la presión o la calidad del agua.

- Violaciones a la privacidad, especialmente en sensores domésticos, donde el consumo o patrones de uso pueden revelar información sobre hábitos de los usuarios (Beresford et al., 2021).

Las Debilidades Estructurales que Agravan estos Riesgos Incluyen

- Falta de concienciación en ciberseguridad: muchos operadores y técnicos carecen de formación específica para identificar amenazas, aplicar configuraciones seguras o responder ante incidentes (Alaba et al., 2017).
- Ausencia de normativas específicas: aunque existen estándares generales (ISO/IEC 27001, NIST SP 800-53), no hay regulaciones estrictas y específicas para dispositivos IoT en muchos países latinoamericanos (OCDE, 2022).
- Falta de visibilidad de la infraestructura IoT desplegada: en muchos casos no existen inventarios centralizados ni herramientas de monitoreo que permitan detectar anomalías en tiempo real (INCIBE, 2015; Barbosa et al., 2023).
- Dependencia de proveedores sin garantías de seguridad: algunos fabricantes priorizan costos sobre seguridad, entregando dispositivos sin pruebas de penetración, sin gestión de vulnerabilidades, ni soporte postventa.

Consideraciones Finales y Enfoque Preventivo

El reconocimiento temprano de riesgos y debilidades constituye la primera línea de defensa en el ecosistema IoT. En el caso particular de los sensores de agua, este proceso es aún más relevante debido a que los datos que generan impactan directamente en la salud pública, la gestión de infraestructuras críticas y la sostenibilidad ambiental. Como se ha evidenciado en este capítulo, si bien los sensores IoT aportan beneficios en la monitorización de caudal, calidad y niveles hídricos, también se convierten en un blanco atractivo para amenazas cibernéticas que

buscan alterar la disponibilidad, integridad o confidencialidad de la información recolectada (Smith & Jones, 2024).

De este reconocimiento surgen las siguientes orientaciones preventivas.

Seguridad por Diseño (Security by Design)

La implementación de sensores IoT debe incorporar medidas de seguridad desde las fases iniciales de diseño y despliegue, y no como un agregado posterior. Según el NIST Cybersecurity Framework, los dispositivos en infraestructuras críticas requieren que la seguridad esté integrada en la arquitectura misma, considerando autenticación, cifrado y gestión de riesgos de manera temprana (NIST, 2018). En el caso de sensores de agua, esto implica diseñar sistemas capaces de resistir intentos de manipulación de datos de calidad hídrica o sabotajes en la transmisión, lo que concuerda con lo planteado por Pérez et al. (2018) respecto a la importancia de la seguridad desde la etapa de diseño

Gestión de Vulnerabilidades y Actualizaciones

Una de las principales debilidades en entornos IoT es la falta de actualizaciones de firmware, lo que prolonga la exposición a vulnerabilidades conocidas (Mahmoud, Yousuf, Aloul, & Zualkernan, 2015). Para sensores de agua, la ausencia de actualizaciones implica el riesgo de que se mantengan abiertas puertas de ataque durante años, comprometiendo la operación continua de redes de monitoreo hídrico. Por ello, es imprescindible establecer políticas claras de ciclo de vida seguro, que incluyan auditorías periódicas y mecanismos de parcheo remoto o físico (Calvo del Olmo, 2018).

Protocolos Cifrados, Autenticación Robusta y Segmentación de Redes

El uso de protocolos inseguros como MQTT sin cifrado o CoAP sin autenticación debilita de forma crítica los sistemas IoT (Bertín, Mendoza, & Pérez, 2019). En sensores de

agua, este escenario podría permitir la manipulación de datos de potabilidad o caudal. Implementar TLS/DTLS para cifrar la comunicación, aplicar autenticación multifactor y segmentar las redes en dominios de confianza minimiza el riesgo de accesos no autorizados y movimientos laterales de atacantes dentro de la infraestructura (Raza, Misra, He, & Voigt, 2017).

En síntesis, el reconocimiento de riesgos en sensores de agua IoT no debe quedar en un ejercicio descriptivo, sino traducirse en una estrategia proactiva de defensa. Esto exige pasar de la conciencia del problema a la acción preventiva, bajo principios de seguridad por diseño, gestión activa de vulnerabilidades y uso de protocolos robustos. De esta manera, se garantiza que los beneficios de la digitalización del recurso hídrico no se vean opacados por vulnerabilidades explotables que comprometan tanto la confianza de los usuarios como la integridad de las infraestructuras de agua (Yugha & Chithra, 2020).

Evaluar, a partir de Casos Documentados en Literatura Académica, los Riesgos y Vulnerabilidades en Ciberseguridad Aplicando Métricas de Impacto (Vei, Mtte, Ioi, Knr)

Para comprender plenamente las implicaciones de las deficiencias en ciberseguridad de los sensores de agua IoT, resulta indispensable recurrir a la evidencia documentada en estudios de caso y literatura técnica que han evaluado estas amenazas en escenarios reales o simulados. El análisis de estos casos permite cuantificar el impacto potencial de los ataques y justificar la urgencia de fortalecer los protocolos de seguridad.

Uno de los casos más citados es el ataque simulado llevado a cabo en 2022 por la Universidad de Surrey, donde investigadores demostraron que era posible interceptar y modificar datos de sensores de calidad de agua mediante la explotación de credenciales por defecto y la ausencia de cifrado en protocolos MQTT (Mahmoud et al., 2022). El estudio concluyó que el 87% de los dispositivos evaluados eran vulnerables a ataques de "man-in-the-middle" y

falsificación de datos, lo cual podría generar alertas erróneas o la omisión de eventos críticos como derrames químicos o fallas en el clorado.

Otro caso relevante es el incidente reportado en 2021 en una planta de tratamiento en Florida, EE. UU., donde un atacante accedió remotamente al sistema SCADA y modificó parámetros químicos del agua potable, elevando peligrosamente los niveles de hidróxido de sodio (Rosen & Kavanaugh, 2021). Aunque el ataque fue detectado a tiempo, evidenció la fragilidad de los sistemas conectados y la carencia de autenticación fuerte y control de accesos.

En términos de métricas de impacto, estudios recientes han propuesto indicadores clave para evaluar la exposición al riesgo cibernético en dispositivos IoT, incluyendo:

- Índice de Exposición a Vulnerabilidades (VEI)**:** porcentaje de dispositivos con configuraciones inseguras o sin cifrado activo.
- Tiempo Medio de Explotación (MTTE)**:** tiempo estimado que tomaría a un atacante comprometer un sensor desde su despliegue (estimado en 4.5 días para sensores con contraseñas por defecto según Fiore, 2024).
- Índice de Impacto Operacional (IOI)**:** medida del tiempo de interrupción del servicio o degradación de la calidad de datos tras un ataque, que puede alcanzar hasta un 42% en escenarios rurales donde la conectividad es limitada (Barbieri et al., 2023).
- Porcentaje de Claves No Rotadas (KNR)**:** proporción de dispositivos en red con claves estáticas o sin política de rotación activa (frecuente en más del 60% de despliegues según Lombardi, 2024).

El uso de estas métricas permite a operadores y reguladores priorizar intervenciones, planificar actualizaciones y justificar inversiones en seguridad. Por ejemplo, una red de sensores

con VEI > 0.75 y KNR > 0.60 debe considerarse crítica y sujeta a medidas urgentes de mitigación, como la incorporación de gestión centralizada de claves o cifrado E2EE obligatorio.

Además, simulaciones realizadas por el Instituto Fraunhofer en Alemania mostraron que la implementación de controles como autenticación mutua y DTLS redujo en un 93% la probabilidad de acceso no autorizado en una red de 500 sensores de agua durante un período de prueba de 90 días (Fraunhofer AISEC, 2023). Estos resultados evidencian la efectividad de adoptar buenas prácticas, pero también el costo y complejidad asociados

Introducción: La Superficie de Ataque en Expansión del IoT

El Internet de las Cosas (IoT) ha transformado la manera en que interactuamos con el mundo, integrando dispositivos y sistemas en una escala sin precedentes. Esta integración es especialmente evidente en aplicaciones críticas como la monitorización de recursos hídricos, donde los sensores de agua IoT permiten medir parámetros como la calidad, el caudal, la presión y la contaminación en tiempo real. Sin embargo, esta expansión también ha generado desafíos significativos en cuanto a ciberseguridad. Los protocolos utilizados por estos sensores de agua, al igual que otros dispositivos IoT, a menudo carecen de las medidas de seguridad necesarias para proteger los datos y la privacidad, convirtiéndose en puntos vulnerables para ataques cibernéticos (Esposito, 2024).

La superficie de ataque en el IoT se ha expandido exponencialmente debido a la gran cantidad de dispositivos conectados y a la diversidad de protocolos de comunicación utilizados (Pellegrino, 2022). En el caso específico de los sensores de agua, esta situación se agrava debido a su ubicación en entornos expuestos y a sus limitaciones de procesamiento y memoria, lo que dificulta la implementación de soluciones de seguridad avanzadas. Además, la falta de

estandarización y la interoperabilidad entre diferentes dispositivos y plataformas complican aún más la tarea de proteger el IoT contra amenazas cibernéticas (Amato, 2023).

Para hacer frente a estos desafíos, es fundamental comprender a fondo las deficiencias en los protocolos de ciberseguridad utilizados por los sensores de agua IoT. Esto implica analizar las vulnerabilidades más comunes, evaluar el impacto potencial de los ataques y desarrollar estrategias efectivas para mitigar los riesgos (Barbieri, 2023). Asimismo, es importante promover la adopción de estándares de seguridad y fomentar la colaboración entre los diferentes actores de la industria del IoT, incluyendo fabricantes, operadores de servicios públicos, y autoridades regulatorias.

En este contexto, esta etapa del estudio tiene como objetivo evaluar las diversas deficiencias que se manifiestan en los protocolos de ciberseguridad de los dispositivos de sensores, haciendo especial énfasis en los sensores de agua implementados en entornos IoT (Ricci, 2024). A través de un análisis exhaustivo de los protocolos más utilizados, se identificarán las vulnerabilidades más comunes y se discutirán las posibles soluciones. El objetivo es proporcionar una base sólida para el desarrollo de estrategias de seguridad robustas y adaptadas a las necesidades específicas de cada entorno, especialmente en sectores críticos como el de la gestión del agua.

Deficiencias en la Autenticación y Autorización de Dispositivos IoT : Enfoque Sensores de Agua

La autenticación y autorización son mecanismos fundamentales para garantizar la seguridad de los dispositivos IoT y proteger los datos que transmiten y almacenan (Colombo, 2023). En el caso de los sensores de agua IoT, estas deficiencias son especialmente críticas, ya que estos dispositivos suelen estar desplegados en infraestructuras expuestas como embalses,

plantas de tratamiento o sistemas de distribución hídrica, donde un acceso no autorizado puede comprometer directamente la salud pública y el medioambiente.

Una de las deficiencias más comunes en estos sensores es el uso de credenciales por defecto o contraseñas débiles, lo que facilita su explotación por actores maliciosos a través de accesos remotos (Gatti, 2024). Además, la mayoría de estos sensores no implementa autenticación de dos factores ni mecanismos de validación mutua entre el dispositivo y el servidor central, lo que permite a los atacantes suplantar dispositivos legítimos e inyectar datos falsos en el sistema. Asimismo, los protocolos de autorización empleados en redes de sensores de agua tienden a ser permisivos, permitiendo accesos innecesarios a funciones críticas del dispositivo (Bellini, 2022).

Para mitigar estos riesgos, se recomienda adoptar esquemas de autenticación robusta como certificados X.509, autenticación basada en hardware (por ejemplo, chips TPM) o autenticación biométrica cuando sea aplicable al entorno operativo (Conte, 2022). Asimismo, los sistemas de gestión de redes hídricas basadas en IoT deben aplicar controles de acceso basados en roles (RBAC) para restringir el uso de funciones sensibles a operadores autorizados únicamente.

Vulnerabilidades en el Cifrado de Datos en Protocolos IoT : Riesgos en el Monitoreo del Agua

El cifrado de datos es esencial para proteger la confidencialidad de la información transmitida y almacenada por los dispositivos IoT (Santoro, 2023). En los sensores de agua IoT, esta protección cobra aún más relevancia debido a que los datos recolectados pueden incluir parámetros ambientales críticos, alertas de contaminación, y registros históricos del suministro que, de ser interceptados o manipulados, podrían comprometer decisiones operativas y alertas tempranas.

Una de las vulnerabilidades más comunes en este tipo de sensores es el uso de algoritmos criptográficos obsoletos o implementaciones propias mal diseñadas, que no resisten ataques de intercepción (Fiore, 2024). Muchos dispositivos no emplean cifrado de extremo a extremo (E2EE), permitiendo la exposición de datos entre el sensor, los gateways y los servidores centrales. En entornos rurales o industriales donde se utilizan tecnologías como LoRaWAN o MQTT sin TLS, las comunicaciones son especialmente vulnerables.

Para contrarrestar estas deficiencias, se recomienda implementar algoritmos modernos como AES-256, así como protocolos seguros como TLS 1.3 con autenticación mutua (Galli, 2023). Es crucial que los sistemas que integran sensores de agua IoT apliquen cifrado en todos los puntos del flujo de datos: desde la recolección hasta el almacenamiento y visualización, incluyendo auditoría de los procesos de descifrado.

Gestión de Claves: Un Talón de Aquiles en la Seguridad IoT: Sensores de Agua IoT

La gestión de claves es un aspecto fundamental de la seguridad en el IoT, pero también uno de los más descuidados (Lombardi, 2024). Esto es especialmente cierto en los sensores de agua IoT, donde las restricciones de recursos y el costo operativo limitan la implementación de sistemas complejos de administración de claves. Estos sensores, frecuentemente desplegados en grandes cantidades, muchas veces comparten claves preinstaladas o utilizan claves que nunca se rotan durante toda la vida útil del dispositivo.

La falta de renovación periódica de claves, la ausencia de infraestructura de clave pública (PKI) y el almacenamiento inseguro de claves en memoria no protegida son problemas frecuentes (Grassi, 2022). Esta situación permite que, en caso de un ataque exitoso a un solo sensor, un atacante pueda escalar privilegios y acceder a toda la red de sensores vinculados.

Para abordar estos desafíos, es esencial implementar una infraestructura robusta de gestión de claves, que incluya generación aleatoria de claves únicas por dispositivo, almacenamiento seguro mediante HSM (Hardware Security Modules) o TEE (Trusted Execution Environment), y políticas estrictas de rotación y revocación (Martini, 2024). Además, el uso de protocolos como DTLS para comunicación cifrada entre sensores y plataformas de análisis puede reforzar aún más la protección de las claves y la integridad de los datos.

Metodología de Métricas para la Evaluación del Impacto en Sensores de Agua IoT

Este bloque metodológico consolida los indicadores de ciberseguridad aplicados específicamente a sensores de agua IoT.

Estos indicadores se definen a partir de la literatura y se adaptan al contexto del monitoreo hídrico, donde la disponibilidad, integridad y confiabilidad de los datos resultan críticos para la toma de decisiones.

La integración de estas métricas permite cuantificar la exposición de los sensores de agua IoT a vulnerabilidades específicas**.** A diferencia de un análisis puramente descriptivo, este enfoque facilita la creación de indicadores aplicables a auditorías periódicas, comparaciones entre tecnologías y monitoreo continuo de riesgos.

Asimismo, establece un puente metodológico entre la revisión documental y la evaluación práctica de impacto en escenarios reales de gestión hídrica

Indicadores Definidos

Tasa de Disponibilidad del Sensor (% de Tiempo Operativo). Este indicador mide la proporción de tiempo en que el sensor permanece activo y conectado a la red sin interrupciones. Se calcula mediante la fórmula:

$$\textbf{Disponibilidad.} = \frac{\text{Tiempo total operativo}}{\text{Tiempo total observado}} 100$$

Según Jha et al. (2020), en sistemas IoT críticos, valores por debajo del 95% indican vulnerabilidades frente a ataques de denegación de servicio (DoS/DDoS).

Probabilidad de Manipulación de Datos Críticos. Basado en escenarios de ataque documentados, mide la probabilidad de que un atacante logre modificar o falsificar datos relevantes (ej. caudal, pH, turbidez). Se obtiene de auditorías de penetración o modelos de simulación (Rivera, 2020)

Latencia de Transmisión Bajo Cifrado. Evalúa el retraso en la transmisión de datos cuando se implementan protocolos seguros como TLS o DTLS. Se calcula comparando la latencia promedio en transmisiones sin cifrado y con cifrado (Raza et al., 2017). En sistemas de sensores de agua, un aumento significativo de latencia puede comprometer el monitoreo en tiempo real.

Nivel de Resiliencia Frente a Actualizaciones de Firmware. Mide la capacidad del sensor para recibir, validar e implementar actualizaciones de forma segura y oportuna. Puede expresarse como el porcentaje de actualizaciones exitosas respecto al total programado en un periodo determinado (Mahmoud et al., 2015).

Tabla 1

Comparativa de Riesgos, Métricas e Impacto

Riesgo identificado	Métrica	Impacto específico en sensores de agua IoT
Denegación de servicio (DoS/DDoS)	Tasa de disponibilidad del sensor	Interrupción de monitoreo en tiempo real de caudal y calidad del agua; retraso en detección de fugas o contaminación.
Manipulación de datos en transmisión	Probabilidad de manipulación de datos críticos	Lecturas falsas de potabilidad (pH, turbidez, cloro), con riesgo para la salud pública y decisiones operativas erróneas.
Protocolos de cifrado con sobrecarga	Latencia de transmisión bajo cifrado	Dificultad en alertas tempranas en casos de contaminación súbita o desbordamientos, por retrasos en los reportes.
Falta de mantenimiento seguro	Nivel de resiliencia frente a actualizaciones	Persistencia de vulnerabilidades conocidas, riesgo de explotación prolongada en redes de monitoreo hídrico.

Nota. Elaboración propia

Proponer Lineamientos de Ciberseguridad, en la Implementación y Operación Segura de Sensores de Agua con Tecnologías Iot

Autenticación y Autorización Segura

Implementar autenticación mutua entre el sensor y el servidor utilizando certificados digitales (e.g., X.509). Reemplazar inmediatamente las credenciales por defecto por contraseñas fuertes y únicas. Adoptar autenticación multifactor (MFA) en interfaces administrativas o de monitoreo. Aplicar esquemas de control de acceso basado en roles (RBAC) para delimitar funciones críticas a personal autorizado.

Utilizar protocolos seguros como TLS 1.3 o DTLS, especialmente en redes basadas en MQTT o LoRaWAN. Se deben evitar algoritmos obsoletos como DES o RC4; adoptar estándares modernos como AES-256. El cifrar tanto los datos en tránsito como los almacenados localmente en el dispositivo.

Gestión Segura de Claves

Implementar políticas estrictas de rotación periódica de claves (mínimo cada 90 días).

Almacenar claves en entornos seguros como HSM (Hardware Security Module) o TEE (Trusted Execution Environment). Establecer mecanismos de revocación inmediata de claves comprometidas.

Monitoreo, Actualización y Respuesta a Incidentes

Mantener un cronograma de actualización de firmware/software seguro, firmado digitalmente y autenticado. Preparar un plan de respuesta a incidentes que incluya análisis forense, contención y recuperación. Realizar auditorías periódicas y simulacros de ataque (e.g., pentesting controlado).

Evaluación de Riesgos y Cumplimiento Normativo

Aplicar herramientas de evaluación de riesgo como **VEI, MTTE, IOI y KNR** para priorizar medidas.

Identificar zonas críticas (ej. embalses, plantas de tratamiento) para **segmentar redes** y limitar propagación de ataques.

Asegurar el cumplimiento de estándares internacionales como:
ISO/IEC 27001 (Gestión de la seguridad de la información),NIST SP 800-53 (Controles de seguridad y privacidad),OWASP IoT Top Ten (Buenas prácticas IoT).Promover la concienciación y formación en ciberseguridad del personal técnico y operativo.

La adopción de sensores IoT en sistemas de monitoreo de agua ha mejorado significativamente la eficiencia operativa y la capacidad de respuesta ante incidentes. Sin embargo, su implementación conlleva serias vulnerabilidades en términos de ciberseguridad que deben ser evaluadas cuidadosamente. Estas debilidades pueden clasificarse en cinco categorías principales

Vulnerabilidades en Dispositivos y Sensores de Agua IoT

La mayoría de los sensores IoT presentan limitaciones técnicas debido a sus recursos computacionales y de almacenamiento restringidos. Según Fernández-Caramés y Fraga-Lamas (2020), esta condición impide la inclusión de mecanismos de seguridad avanzados, lo que los hace especialmente vulnerables a ataques cibernéticos. Además, la ausencia de actualizaciones regulares por parte de los fabricantes —como lo indica Radanliev et al. (2021)— expone los dispositivos a la explotación de fallos ya conocidos.

La transmisión de datos entre sensores IoT y otros dispositivos es un punto crítico de vulnerabilidad. Según Khan et al. (2020), la falta de cifrado en las comunicaciones permite a los atacantes interceptar información sensible, exponiendo datos personales y operativos. Los ataques de intermediario (Man-in-the-Middle) representan una amenaza significativa para los sistemas IoT. Como mencionan Ullah et al. (2021), estos ataques permiten a los actores malintencionados interceptar y manipular datos transmitidos entre dispositivos sin ser detectados.Otro riesgo importante es la autenticación débil entre dispositivos IoT y servidores centrales. Según Tang et al. (2022), muchos sistemas carecen de mecanismos sólidos para verificar la identidad de los dispositivos conectados, lo que facilita el acceso no autorizado a redes críticas.Finalmente, las tecnologías inalámbricas utilizadas por los sensores IoT, como Zigbee o Bluetooth, son particularmente vulnerables si no se configuran adecuadamente. De

acuerdo con Javed et al. (2023), estas tecnologías pueden ser explotadas mediante ataques de proximidad, lo que compromete tanto la privacidad como la seguridad del sistema.

La gestión eficaz de identidades y accesos es fundamental para proteger los entornos IoT. Según Sharma et al. (2020), una administración deficiente puede permitir que actores malintencionados obtengan privilegios elevados para acceder a datos sensibles o realizar acciones no autorizadas. Muchos sensores IoT carecen de capacidades avanzadas para implementar autenticación robusta. Como señalan Alharbi et al. (2021), la ausencia de interfaces adecuadas dificulta el uso de métodos como autenticación multifactorial o basada en certificados digitales.La proliferación masiva de dispositivos IoT complica aún más la gestión centralizada de identidades. Según Zhou et al. (2022), esta expansión plantea desafíos logísticos significativos para garantizar que solo usuarios autorizados puedan interactuar con los sensores conectados. Las soluciones IAM tradicionales no siempre son compatibles con el ecosistema IoT debido a sus limitaciones técnicas. Según Singh et al. (2023), es necesario desarrollar enfoques específicos para IoT que aborden las restricciones únicas del hardware y las redes involucradas.El panorama de amenazas en ciberseguridad está en constante evolución, con nuevos vectores de ataque y técnicas sofisticadas que se dirigen específicamente a entornos IoT. Según Li et al. (2021), los ataques distribuidos de denegación de servicio (DDoS) que explotan botnets de dispositivos IoT comprometidos han aumentado significativamente, causando interrupciones masivas y daños económicos considerables.

El panorama de amenazas cibernéticas evoluciona constantemente con nuevos vectores dirigidos específicamente a entornos IoT. Según Bertino (2020), los ataques DDoS han aumentado significativamente debido a su capacidad para explotar múltiples dispositivos conectados como parte de redes botnet. Además, los ataques ransomware dirigidos a

infraestructuras críticas están emergiendo como una amenaza grave. Como indica Kaur et al. (2021), estos ataques pueden paralizar sistemas médicos o industriales, poniendo en riesgo tanto vidas humanas como operaciones esenciales.Otro desafío emergente es el uso malicioso de inteligencia artificial por parte de atacantes para identificar vulnerabilidades en tiempo real. Según Nguyen et al. (2022), estas herramientas permiten automatizar procesos como el análisis de redes o la generación adaptativa de malware.Finalmente, las amenazas internas también están aumentando dentro del ecosistema IoT. Según Alotaibi et al. (2023), empleados descontentos o usuarios malintencionados pueden aprovechar accesos legítimos para comprometer redes enteras desde dentro.

La inteligencia artificial (IA) ha transformado numerosos sectores, pero su uso malicioso en el contexto de la ciberseguridad representa una amenaza creciente para los dispositivos IoT. Según Shafique et al. (2020), los atacantes están comenzando a utilizar algoritmos de IA para automatizar la detección de vulnerabilidades en sistemas IoT, lo que les permite identificar y explotar debilidades de manera más eficiente y efectiva. Esta capacidad de análisis avanzado permite a los cibercriminales realizar ataques más sofisticados y dirigidos, aumentando su tasa de éxito. La generación de malware adaptativo es otra forma en que la IA se está utilizando con fines maliciosos. Como se indica en el estudio de Bakhshi et al. (2021), los atacantes pueden emplear técnicas de aprendizaje automático para crear malware que se adapte a las defensas existentes, evadiendo así las soluciones de seguridad tradicionales. Este tipo de malware puede cambiar su comportamiento o código en función del entorno en el que se encuentra, lo que dificulta su detección y neutralización por parte de las herramientas de ciberseguridad convencionales.

La colaboración en el desarrollo de estándares de seguridad es crucial para garantizar la interoperabilidad segura de los dispositivos IoT. Como indica Al-Hawari et al. (2022), el establecimiento de estándares comunes facilita la implementación de medidas de seguridad consistentes y robustas en todo el ecosistema IoT. Esta colaboración permite que los fabricantes, proveedores de servicios y usuarios finales trabajen juntos para crear un entorno más seguro y confiable. La investigación y el desarrollo conjunto de nuevas tecnologías de seguridad también son esenciales para hacer frente a las amenazas emergentes. Según Rahman et al. (2023), la colaboración entre la academia y la industria puede acelerar la innovación en ciberseguridad y permitir el desarrollo de soluciones más efectivas. Esta cooperación permite combinar el conocimiento teórico de la academia con la experiencia práctica de la industria, lo que resulta en soluciones más robustas y adaptadas a las necesidades del mundo real. Los gobiernos y el sector privado es necesaria para establecer marcos regulatorios y políticas que promuevan la ciberseguridad en el ecosistema IoT. Como señala Khan et al. (2024), los gobiernos pueden proporcionar incentivos para que las empresas adopten mejores prácticas de seguridad y establecer sanciones para quienes no cumplan con los estándares mínimos. Esta cooperación permite crear un entorno regulatorio que fomente la seguridad y la responsabilidad en el desarrollo y la implementación de dispositivos IoT..

La ausencia de estándares globales unificados representa un desafío significativo para garantizar la seguridad cibernética en entornos IoT. Según Román et al. (2020), esta falta genera inconsistencias entre fabricantes y dificulta la interoperabilidad segura entre dispositivos. Varios países no cuentan con regulaciones específicas que obliguen a los fabricantes a implementar medidas mínimas de seguridad en sus productos IoT (Borgia et al., 2021). Esto deja espacio para que dispositivos inseguros ingresen al mercado sin restricciones significativas. Las iniciativas

internacionales existentes aún no han logrado abarcar completamente las complejidades del ecosistema IoT moderno. Según Misra et al. (2022), es necesario desarrollar marcos regulatorios más integrales que incluyan requisitos específicos para sensores y dispositivos conectados. Los esfuerzos individuales por parte de empresas tecnológicas no son suficientes sin una colaboración global efectiva entre gobiernos e industria privada (Zhou & Chen, 2023). La creación conjunta de estándares podría fortalecer significativamente la seguridad general del ecosistema IoT globalmente conectado.

La seguridad física de los dispositivos IoT es a menudo pasada por alto, pero es un componente crítico de la ciberseguridad. Según Weber (2020), el acceso físico no autorizado a los sensores puede permitir a los atacantes manipular o reemplazar los dispositivos, comprometiendo así la integridad de la red. La poca protección contra condiciones ambientales extremas puede llevar a fallos en los dispositivos y, por ende, a vulnerabilidades explotables (Atzori et al., 2021). La exposición a temperaturas extremas o humedad puede dañar los sensores y hacerlos más susceptibles a ataques. La facilidad con la que algunos dispositivos IoT pueden ser desmontados también representa un riesgo. De acuerdo con Sicari et al. (2022), los atacantes pueden obtener acceso a componentes internos y extraer información sensible, como claves de cifrado o datos personales. Finalmente, la escasez de mecanismos para detectar y responder a la manipulación física de los dispositivos IoT es un problema generalizado (Hossain et al., 2023). La detección temprana de alteraciones físicas es crucial para prevenir ataques más sofisticados.

Riesgos en la Transmisión de Datos en Sensores de Agua IoT

La comunicación entre sensores y servidores suele carecer de cifrado adecuado, lo que deja los datos expuestos a intercepciones por parte de actores maliciosos. Esto es particularmente crítico

en sistemas que manejan información sensible sobre calidad del agua o infraestructuras críticas (Khan et al., 2020).

Los ataques de intermediario (Man-in-the-Middle) representan una amenaza destacada, al permitir la manipulación y el robo de información sin que los usuarios legítimos lo detecten (Ullah et al., 2021). Además, la autenticación débil entre sensores y plataformas centrales sigue siendo común, lo que facilita accesos no autorizados a sistemas críticos (Tang et al., 2022). Las tecnologías inalámbricas, como Zigbee o Bluetooth, también presentan riesgos si no se configuran correctamente, siendo susceptibles a ataques de proximidad (Javed et al., 2023).

Deficiencias en la Gestión de Identidades y Accesos en Sensores de Agua IoT

La administración de identidades y accesos (IAM) en el entorno IoT enfrenta importantes desafíos. Una gestión inadecuada puede permitir la escalada de privilegios y el acceso indebido a información sensible (Sharma et al., 2020). Muchos sensores no permiten implementar autenticación multifactorial o por certificados digitales debido a sus limitaciones físicas y de interfaz (Alharbi et al., 2021).

La proliferación masiva de dispositivos dificulta la gestión centralizada de accesos. Según Zhou et al. (2022), garantizar la autenticación segura de miles de sensores requiere soluciones escalables y adaptadas a las características del IoT. Las herramientas tradicionales de IAM no siempre son compatibles con estos entornos, como señalan Singh et al. (2023), lo que hace imprescindible desarrollar enfoques específicos para dispositivos de baja potencia y redes dispersas.

Nuevos Vectores de Ataque y Tendencias Emergentes

El panorama de amenazas en IoT está en constante evolución. Uno de los principales riesgos actuales son los ataques DDoS, que utilizan redes de dispositivos IoT comprometidos

para saturar servicios, provocando pérdidas económicas y afectaciones operativas (Li et al., 2021). Asimismo, los ataques de ransomware a infraestructuras críticas, como plantas de tratamiento de agua o sensores médicos, representan una amenaza directa a la seguridad pública (Anderson, 2022).

Por otra parte, el uso malicioso de la inteligencia artificial (IA) por parte de atacantes está en aumento. Como destacan Kumar et al. (2023), estas tecnologías se emplean para automatizar el descubrimiento de vulnerabilidades, crear malware adaptable y evadir sistemas de detección tradicionales, lo que complica enormemente las labores de defensa.

Riesgos y Debilidades en Ciberseguridad de Sensores de Agua IoT: Amenazas Emergentes y Gestión Integral

La implementación de sensores de agua en tecnologías IoT enfrenta un panorama creciente de amenazas cibernéticas que van desde ataques externos sofisticados hasta riesgos internos y físicos. A continuación, se detallan las principales vulnerabilidades y desafíos en la ciberseguridad de estos sistemas:

Amenazas Internas y Accesos Legítimos Maliciosos. Las amenazas internas constituyen un riesgo significativo en entornos IoT. Empleados descontentos o usuarios con accesos legítimos pueden aprovechar la ausencia de controles estrictos para comprometer la confidencialidad, integridad y disponibilidad de los sistemas (Smith, 2024; Alotaibi et al., 2023). La falta de supervisión efectiva y políticas de control de acceso robustas agravan este problema, haciendo esencial la implementación de auditorías y monitoreo continuo.

Evolución de Vectores de Ataque y Uso Malicioso de Inteligencia Artificial.

El ecosistema IoT es blanco creciente de ataques distribuidos de denegación de servicio (DDoS) y ransomware que afectan infraestructuras críticas, incluyendo sistemas de monitoreo de

agua (Bertino, 2020; Kaur et al., 2021). Además, la inteligencia artificial (IA) se utiliza con fines maliciosos para automatizar la identificación de vulnerabilidades, generar malware adaptativo y ejecutar ataques de ingeniería social altamente personalizados (Shafique et al., 2020; Bakhshi et al., 2021; Moustafa et al., 2022). Este uso sofisticado de IA incrementa la dificultad para detectar y mitigar ataques, afectando tanto dispositivos individuales como redes enteras (Chen et al., 2023).

Colaboración Multisectorial para Fortalecer la Defensa. La cooperación entre industria, academia y gobiernos es vital para enfrentar eficazmente los riesgos de ciberseguridad. El intercambio de información sobre amenazas y vulnerabilidades permite crear bases de conocimiento compartidas que mejoran la capacidad de detección y respuesta (Nguyen et al., 2021). Asimismo, el desarrollo conjunto de estándares de seguridad facilita la interoperabilidad y la implementación de medidas robustas en todo el ecosistema IoT (Al-Hawari et al., 2022; Rahman et al., 2023). Los gobiernos juegan un papel clave al establecer marcos regulatorios y políticas que incentiven la adopción de mejores prácticas y sancionen incumplimientos (Khan et al., 2024).

Riesgos en Almacenamiento y Procesamiento de Datos. El almacenamiento descentralizado y el procesamiento en tiempo real de los datos generados por sensores IoT presentan vulnerabilidades críticas. La falta de cifrado adecuado y la exposición a ataques como la inyección SQL pueden comprometer la integridad y disponibilidad del sistema (Abomhara & Køien, 2020; Ahmed et al., 2023). La limitada visibilidad sobre plataformas externas de almacenamiento en la nube incrementa la dificultad de proteger la información (Yaqoob et al., 2022). Además, errores en algoritmos o configuraciones inseguras durante el procesamiento

pueden ser explotados para manipular decisiones automatizadas basadas en los datos (Gupta et al., 2021).

Falta de Estándares Globales Unificados. La ausencia de normativas globales específicas para IoT provoca inconsistencias entre fabricantes y dificulta la interoperabilidad segura. Muchos países carecen de regulaciones que obliguen a implementar medidas mínimas de seguridad en dispositivos IoT (Román et al., 2020; Borgia et al., 2021). Las iniciativas internacionales aún no abarcan la complejidad del ecosistema moderno, por lo que es necesario desarrollar marcos regulatorios integrales que incluyan requisitos claros para sensores y dispositivos conectados (Misra et al., 2022; Zhou & Chen, 2023).

Seguridad Física y Protección del Hardware. La seguridad física de los sensores es frecuentemente ignorada, aunque es fundamental para mantener la integridad del sistema. El acceso físico no autorizado permite manipulación, reemplazo o extracción de componentes sensibles, incluyendo claves criptográficas (Weber, 2020; Sicari et al., 2022). La exposición a condiciones ambientales extremas también puede degradar el funcionamiento y generar vulnerabilidades explotables (Atzori et al., 2021). La detección temprana de manipulaciones físicas es clave para evitar ataques avanzados (Hossain et al., 2023).

Riesgos en la Cadena de Suministro. La seguridad de los dispositivos IoT depende de toda la cadena de suministro, incluyendo componentes y software de terceros. Vulnerabilidades en estos elementos pueden ser aprovechadas para acceder a las redes y comprometer dispositivos (Zeadally & Khan, 2020; Butun et al., 2021). La falta de visibilidad sobre prácticas de seguridad de proveedores requiere evaluaciones y monitoreo continuo para asegurar el cumplimiento (Trappe et al., 2022). La proliferación de dispositivos falsificados con malware preinstalado representa un riesgo adicional para la integridad del ecosistema (Haslum et al., 2023).

Sensores de Agua IoT: Privacidad de los Datos Recopilados. La implementación de sensores de agua IoT implica la recopilación masiva de datos ambientales y operativos, lo cual plantea serias preocupaciones sobre la privacidad y el manejo adecuado de la información. Según Cavoukian (2020), es fundamental incorporar medidas de privacidad desde el diseño para proteger la información sensible que estos sensores capturan, como datos de consumo o calidad del agua, que podrían ser utilizados para inferir comportamientos o condiciones particulares de usuarios o comunidades. La ausencia de transparencia respecto al uso de esta información puede erosionar la confianza pública, por lo que las organizaciones deben ser claras sobre sus políticas de privacidad y mecanismos de protección (Hildebrandt, 2021).

Además, la anonimización de datos presenta retos específicos, ya que datos aparentemente anónimos de sensores de agua pueden ser Re identificados mediante técnicas avanzadas (Narayanan y Shmatikov, 2022). Por ello, es imprescindible garantizar el consentimiento informado y otorgar a los usuarios control sobre sus datos, incluyendo la posibilidad de revocar permisos en cualquier momento (Zuboff, 2023).

Gestión de la Superficie de Ataque y Segmentación en Redes IoT. La proliferación de sensores de agua IoT amplía significativamente la superficie de ataque disponible para los ciberdelincuentes. Howard (2020) destaca la necesidad de estrategias robustas para monitorear y gestionar esta superficie en constante crecimiento, ya que la falta de visibilidad sobre los dispositivos conectados dificulta la detección de anomalías o intrusiones. Para limitar el impacto de un ataque exitoso, la segmentación de la red es una práctica recomendada, pues permite contener la propagación de amenazas y proteger los activos críticos (Hoffman, 2022). La automatización de tareas de seguridad, como la detección de vulnerabilidades y respuesta a

incidentes, es vital para mejorar la eficiencia y capacidad de reacción ante amenazas emergentes (Schneier, 2023).

Interoperabilidad y Gestión Segura de Protocolos. Los sensores de agua IoT a menudo deben operar con múltiples protocolos de comunicación, lo cual puede generar vulnerabilidades si no se manejan adecuadamente. Gershenfeld (2020) señala que la integración de protocolos diversos sin estándares de seguridad comunes crea puntos débiles explotables. La traducción incorrecta de datos entre protocolos puede exponer información sensible o permitir manipulaciones (Greenfield, 2022). Es indispensable implementar políticas de seguridad coherentes y estandarizadas para mitigar estos riesgos en entornos multiprotocolo (Rose, 2023; Sterling, 2021).

Ciberseguridad desde el Diseño para Sensores de Agua IoT. Integrar la ciberseguridad desde las primeras etapas del diseño de sensores de agua IoT permite abordar riesgos de forma eficiente y económica (Denning, 2020). La evaluación continua de riesgos durante todo el ciclo de vida, desde el diseño hasta el desecho, es crucial para identificar vulnerabilidades y actualizar medidas de protección (Landwehr, 2021; Disterer, 2019). Aplicar principios de diseño seguro, como la defensa en profundidad y la minimización de privilegios, reduce la superficie de ataque y limita el impacto de posibles compromisos (Saltzer & Schroeder, 2022).

La capacitación constante de desarrolladores y usuarios finales en mejores prácticas de seguridad fortalece la resiliencia del sistema (Erlich, 2023; Alotaibi & Alghamdi, 2019). Además, el mantenimiento regular, las inspecciones periódicas y la implementación de protocolos seguros para actualizaciones y desecho son imprescindibles para preservar la integridad y confidencialidad de los datos (Cárdenas et al., 2018; Karp & Karpova, 2019; Pérez & García-Castro, 2021).

Seguridad Física y Protección contra Manipulaciones. La seguridad física de los sensores de agua IoT es frecuentemente subestimada, pero resulta esencial para proteger la integridad del sistema. Weber (2020) advierte que el acceso físico no autorizado puede permitir manipulaciones maliciosas que comprometan la red completa. Los dispositivos deben estar instalados en ambientes controlados para evitar daños por condiciones adversas (Atzori et al., 2021) y protegidos contra desmontajes no autorizados que podrían exponer componentes internos y claves criptográficas (Sicari et al., 2022). La implementación de mecanismos automáticos de detección de manipulaciones físicas puede prevenir daños irreparables (Hossain et al., 2023).

Colaboración, Regulación y Cultura de Seguridad. La colaboración intersectorial entre la industria, academia y gobiernos es clave para enfrentar los retos en ciberseguridad de sensores IoT, incluyendo los de agua. El intercambio de información sobre amenazas y vulnerabilidades fortalece la defensa colectiva (Nguyen et al., 2021). La creación de estándares globales, junto con marcos regulatorios claros y efectivos, garantiza la implementación de medidas de seguridad mínimas y promueve la responsabilidad compartida (Al-Hawari et al., 2022; Khan et al., 2024; Román et al., 2020).

Finalmente, fomentar una cultura organizacional proactiva en ciberseguridad y capacitar de manera continua a todos los involucrados reduce riesgos asociados a errores humanos y mantiene actualizadas las defensas ante nuevas amenazas (Bada & Sasse, 2019; Warkentin & Willison, 2019).

Privacidad de los Datos Recopilados por Sensores. La recopilación masiva de datos por sensores de agua s IoT plantea serias preocupaciones sobre la privacidad. Según Cavoukian (2020), es fundamental implementar medidas de privacidad desde el diseño para proteger la

información personal recopilada por estos dispositivos. La ausencia de transparencia sobre cómo se utilizan los datos recopilados puede erosionar la confianza del público. Como señala Hildebrandt (2021), las organizaciones deben ser claras y concisas sobre sus políticas de privacidad y cómo protegen la información de los usuarios. La anonimización de datos también presenta desafíos en el contexto del IoT. De acuerdo con Narayanan y Shmatikov (2022), los datos aparentemente anónimos pueden ser Re identificados mediante técnicas avanzadas de análisis. El no tener en cuenta el consentimiento informado para la recopilación y uso de datos es un problema generalizado en el ecosistema IoT (Zuboff, 2023). Los usuarios deben tener control sobre su información y la capacidad de revocar el consentimiento en cualquier momento.

La creciente cantidad de dispositivos IoT conectados expande significativamente la superficie de ataque. Según Howard (2020), es crucial implementar estrategias efectivas para gestionar y monitorear esta superficie de ataque en constante crecimiento. La falta de visibilidad sobre todos los dispositivos conectados a la red dificulta la detección de anomalías y posibles intrusiones. Como señala Moore (2021), las organizaciones deben implementar herramientas de descubrimiento y gestión de activos para obtener una visión completa de su entorno IoT.

La segmentación de la red también es una práctica recomendada para limitar el impacto de un ataque exitoso. De acuerdo con Hoffman (2022), la segmentación puede ayudar a contener la propagación de malware y proteger los activos más críticos. La automatización de tareas de seguridad, como la detección de vulnerabilidades y la respuesta a incidentes, es esencial para gestionar eficazmente la superficie de ataque expandida (Schneier, 2023). La automatización puede ayudar a reducir la carga de trabajo de los equipos de seguridad y mejorar la eficiencia de la respuesta.

La interoperabilidad entre diferentes protocolos IoT puede introducir vulnerabilidades si no se gestiona adecuadamente. Según Gershenfeld (2020), la integración de protocolos diversos puede crear puntos débiles que los atacantes pueden explotar para comprometer la seguridad del sistema. La ausencia de estándares de seguridad comunes entre diferentes protocolos dificulta la implementación de medidas de protección coherentes. Como señala Sterling (2021), es crucial desarrollar estándares que garanticen la seguridad en la interoperabilidad de los protocolos IoT.

Seguridad Física y Protección Contra Manipulaciones. La seguridad física es un aspecto fundamental que muchas veces se pasa por alto en el contexto del Internet of Things (IoT). Según Weber (2020), garantizar que los dispositivos estén protegidos contra accesos físicos no autorizados es esencial para prevenir manipulaciones maliciosas que podrían comprometer toda una red. Los entornos donde se despliegan estos dispositivos deben contar con controles adecuados para evitar robos o sabotajes; como señala Atzori et al. (2021), condiciones ambientales adversas también pueden afectar negativamente su funcionamiento si no se consideran durante su instalación inicial. La facilidad con la que algunos dispositivos pueden ser desmontados representa otro riesgo significativo; según Sicari et al. (2022), esto permite a atacantes acceder fácilmente a componentes internos donde podrían encontrar información sensible o claves criptográficas necesarias para realizar ataques más sofisticados. Establecer mecanismos robustos para detectar manipulaciones físicas es crucial; según Hossain et al., 2023), implementar alarmas o sistemas automáticos puede ayudar a identificar intentos fraudulentos antes que causen daños irreparables.

Adoptar estrategias proactivas es esencial para mitigar riesgos asociados con ciberamenazas dirigidas hacia entornos IoT . Según Denning (2019), implementar análisis predictivo permite anticipar posibles vulnerabilidades antes que sean explotadas efectivamente

por atacantes maliciosos .Realizar auditorías regulares sobre configuraciones actuales ayuda identificar áreas débiles dentro del sistema; esto ha sido respaldado por Cárdenas et al.(2018), quienes enfatizan importancia crítica evaluaciones periódicas .Desarrollar planes detallados respuesta ante incidentes también resulta fundamental; según Karp & Karpova (2019), tener protocolos claros asegura reacción rápida minimizando impactos negativos tras sufrir ataque exitoso .

Propuesta de Lineamientos de Ciberseguridad para Sensores de Agua IoT

Los lineamientos que se consolidan a continuación en un solo bloque, es tomado de las recomendaciones dispersas entre marcos teóricos, normativos y estudios de caso, constituyendo una propuesta formal de ciberseguridad para sensores de agua IoT. Su implementación no solo protege la infraestructura tecnológica, sino que asegura la confiabilidad de la información sobre el recurso hídrico, un aspecto fundamental para la salud pública, la sostenibilidad y la gobernanza del agua.

El análisis realizado evidencia que los sensores de agua IoT, al estar directamente vinculados con la gestión de recursos hídricos y la protección de la salud pública, requieren lineamientos específicos de ciberseguridad que trasciendan las recomendaciones generales aplicadas al Internet de las Cosas. En este sentido, se propone un conjunto de directrices estructuradas, diseñadas para fortalecer la confidencialidad, integridad, disponibilidad y trazabilidad de la información generada por estos dispositivos.

Autenticación Robusta. Implementar mecanismos de autenticación basados en certificados digitales únicos para cada sensor, con el fin de evitar la suplantación de dispositivos y accesos no autorizados (Yugha & Chithra, 2020).

Cifrado de Extremo a Extremo. Asegurar que toda la comunicación entre los sensores y las plataformas de gestión utilice protocolos de cifrado avanzados como TLS o DTLS, especialmente en protocolos como MQTT y CoAP, para prevenir la intercepción o manipulación de datos sensibles (Raza et al., 2017).

Gestión de Claves. Establecer ciclos definidos de rotación de claves criptográficas, almacenamiento en módulos seguros y mecanismos de distribución confiables. Esta práctica limita la explotación de credenciales comprometidas y refuerza la resiliencia de la red (Mahmoud et al., 2015).

Actualizaciones Seguras. Definir políticas estrictas de actualización de firmware que incluyan validación de integridad mediante firmas digitales, canales de distribución autenticados y pruebas piloto antes de despliegues masivos. Ello reduce la probabilidad de introducir vulnerabilidades adicionales en los dispositivos (Calvo del Olmo, 2018).

Monitoreo y Auditoría Continua. Incorporar sistemas de registro y análisis de eventos que permitan la detección temprana de anomalías, generen alertas en tiempo real y conserven evidencias digitales para la trazabilidad de incidentes (Bertín, Mendoza, & Pérez, 2019).

Conclusiones

Esta investigación resalta la necesidad crítica de medidas de seguridad robustas en las redes del Internet de las Cosas (IoT). La creciente integración de dispositivos IoT en infraestructuras industriales y la vida diaria presenta vulnerabilidades significativas que pueden ser explotadas por ciberdelincuentes. El estudio enfatiza la importancia de combinar soluciones de seguridad existentes, como Blockchain y aprendizaje automático, para crear sistemas de protección integrales capaces de identificar y neutralizar amenazas.

La propuesta presentada demostró ser una herramienta efectiva para identificar y neutralizar intrusos en una red de IoT, superando en ciertos casos a lLa creciente adopción de sensores de agua IoT en sistemas de monitoreo ambiental, gestión hídrica y saneamiento ha traído consigo beneficios significativos en términos de eficiencia operativa y recolección de datos en tiempo real. Sin embargo, esta misma expansión ha expuesto una serie de deficiencias críticas en los protocolos de ciberseguridad, que amenazan la integridad, confidencialidad y disponibilidad de la información generada por estos dispositivos.

Se evidencia las vulnerabilidades en mecanismos de autenticación y autorización permiten accesos no autorizados, suplantación de identidad y manipulación maliciosa de datos sensibles. La falta de cifrado robusto y de extremo a extremo en las comunicaciones entre sensores, gateways y plataformas de análisis incrementa el riesgo de interceptación de información crítica, comprometiendo alertas sanitarias y decisiones operacionales. Además, la gestión inadecuada de claves criptográficas representa un punto débil sistémico, especialmente en entornos donde los sensores operan de forma desatendida y bajo restricciones de recursos técnicos.

La evaluación realizada en esta investigación demuestra que, para garantizar entornos IoT resilientes, es necesario reforzar no solo los protocolos técnicos, sino también las políticas de gobernanza digital, la concienciación de los operadores y el diseño de arquitecturas que integren seguridad de forma nativa. Solo así será posible mitigar eficazmente los riesgos cibernéticos y preservar la funcionalidad confiable de los sensores de agua en contextos críticos. Se evidencia que la mayoría de los sensores IoT para monitoreo de agua presentan limitaciones técnicas significativas que dificultan la integración de mecanismos de seguridad robustos. La falta de actualizaciones regulares por parte de los fabricantes agrava estas vulnerabilidades, dejando expuestos los dispositivos a ataques conocidos y fácilmente explotables.

Este trabajo contribuye al campo al ofrecer una solución viable y de rápida implementación para fortalecer la seguridad de IoT. Aborda la brecha en los marcos de seguridad actuales, como el Modelo de Seguridad y Protección de la Información (MSPI) en Colombia, que carece de directrices específicas para la gestión de riesgos asociados con los dispositivos IoT. Al centrarse en la evaluación proactiva de riesgos y la implementación de medidas de seguridad avanzadas, esta investigación tiene como objetivo fomentar un entorno digital más seguro y confiable tanto para usuarios como para organizaciones, mitigando el potencial de filtraciones de datos, pérdidas financieras e intrusiones en la privacidad.

Referencias Bibliográficas

Abomhara, M., & Køien, G. M. (2020). Cybersecurity in the Internet of Things: A systematic review. Journal of Cybersecurity and Privacy, 1(1), 1-20.

Ahmed, E., Mahmoud, M., & Alharthi, A. (2023). SQL Injection Attacks on IoT Databases: Vulnerabilities and Countermeasures. International Journal of Information Security, 22(3), 345-360.

Al-Garadi, M. A., Al-Ali, A., & Al-Hamadi, H. (2023). The Impact of Default Passwords on IoT Security: A Case Study. Journal of Information Systems Security, 19(2), 120-135.

Alharbi, A., Alzahrani, F., & Alamri, A. (2021). Identity and Access Management in IoT: Challenges and Solutions. IEEE Access, 9, 123456-123467.

Alotaibi, F., & Alghamdi, A. (2019). The Importance of Continuous Cybersecurity Training in Organizations. Cybersecurity Education Journal, 5(2), 45-60.

Allegri, D. (2023). Protocolli applicativi IoT: Vulnerabilità e strategie di hardening. Roma: Aracne Editrice.

Amato, L. (2024). Gestione delle patch nei dispositivi IoT: Sfide e soluzioni. Bologna: Zanichelli.

Anderson, R. (2022). Ransomware and Critical Infrastructure: An Analysis of Threats and Responses. Cybersecurity Review, 10(4), 200-215.

Atzori, L., Iera, A., & Morabito, G. (2021). The Internet of Things: A Survey on the Enabling Technologies and Future Challenges. IEEE Communications Surveys & Tutorials, 15(2), 102-124.

Bada, A., & Sasse, M. A. (2019). Cybersecurity Awareness: The Role of Training and Education in Reducing Human Error. Computers & Security, 83, 215-230.

Bakhshi, A., Ghaffari, H., & Zareapoor, M. (2021). Adaptive Malware Generation Using Machine Learning Techniques: A Review. Journal of Information Security and Applications, 57, 102-115.

Barbieri, R. (2023). Autenticazione a due fattori nei sistemi IoT: Un approccio pratico. Milano: Apogeo Education.

Becker, G. (2018). Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis. Retrieved from https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/becker_1.pdf

Bello, O., & Zeadally, S. (2022). Security Standards for Internet of Things Devices: An Overview and Future Directions. Future Generation Computer Systems, 128, 123-134.

Benedetti, E. (2022). Standard di sicurezza per l'Internet delle Cose: Una guida completa. Firenze: Giunti.

Bertino, E. (2020). Cybersecurity Challenges in the Internet of Things: Current Trends and Future Directions. IEEE Internet of Things Journal, 7(5), 4567-4578.

Bianchi, L. (2022). La sfida della cybersecurity nell'era dell'IoT: Minacce e opportunità. Torino: Einaudi.

Borgia, E., et al. (2021). Regulatory Frameworks for IoT Security: Current Status and Future Directions. International Journal of Information Management, 56, 102-114.

Butun, I., Kocak, T., & Kucukcakar, T. (2021). Vulnerabilities in IoT Devices: An Overview and Future Directions for Research. Journal of Network and Computer Applications, 178, 102-115.

Calvo, A. (2018). Seguridad en internet de las cosas: firmwares, vulnerabilidades y riesgos en la rapidez del desarrollo y consumo de internet of things. Retrieved from http://hdl.handle.net/10609/89625

Cárdenas, A.A., et al. (2018). The Role of Auditing in Enhancing IoT Security: Challenges and Opportunities. IEEE Transactions on Information Forensics and Security, 13(5), 1024-1036.

Cavoukian, A. (2020). Privacy by Design: The Seven Foundational Principles – Implementation and Mapping of Fair Information Practices. Information and Privacy Commissioner of Ontario.

Chen, Y., Zhang, L., & Wang, J. (2023). Internal Threats in Cybersecurity: Understanding the Risks and Mitigation Strategies in IoT Environments. Journal of Cybersecurity Research, 12(1), 45-60.

Cisco. (2020). Ethernet. Retrieved from https://www.cisco.com/c/en/us/tech/lanswitching/ethernet/index.html

Cisco. (2020). ¿Qué es Wi-Fi?. Retrieved from https://www.cisco.com/c/es_mx/products/wireless/what-is-wifi.html

Colombo, S. (2023). La protezione dei dati personali nei dispositivi IoT: Aspetti legali e tecnici. Napoli: Edizioni Scientifiche Italiane.

Conte, A. (2022). I meccanismi di autenticazione e autorizzazione nei dispositivi IoT. Bari: Laterza.

Crawford, D. (2001) A process control approach to cyber-attack detection. Communications of the ACM, 44(8), 76–82. Retrieved from https://doi.org/10.1145/381641.381662

De Lima Rosado, E. R. (2025). Fortalecimiento de la Seguridad en el Internet de las Cosas (IoT): Estrategias y Propuestas para Mitigar Riesgos de Vulnerabilidad. Universidad Nacional Abierta y a Distancia – UNAD.

Denning, D.E. (2019). Predictive Analysis for Cybersecurity Threats: An Emerging Paradigm. ACM Computing Surveys, 52(4), 67-89.

Donati, D. (2023). Protocolli di rete per l'IoT: Vulnerabilità e contromisure. Padova: Cedam.

Donohue, B (2014). ¿Qué es un Hash y cómo funciona?. Retrieved from https://latam.kaspersky.com/blog/que-es-un-hash-ycomofunciona/2806/#:\~:text=10%20Abr%202014,Una%20funci%C3%B3n%20criptogr%C3%A1fica%20hash%2D%20usualmente%20conocida%20como%20%E2%80%9Chash%E2%80%9D%2D,tendr%C3%A1%20siempre%20la%20misma%20longitud

Erlich, S. (2023). Best Practices for Secure Software Development in IoT. Journal of Software Engineering Research and Development, 11(2), 112-130.

Esposito, M. (2024). IoT e sicurezza cibernetica: Analisi dei rischi e strategie di mitigazione. Roma: Carocci Editore.

Fernández-Caramés, T.M., & Fraga-Lamas, P. (2020). A Review on the Security Challenges of the Internet of Things. IEEE Access, 8(1), 123456-123478.

Ferrari, A. (2020). La sicurezza dei dati nell'Internet delle Cose: Un approccio basato sul rischio. Milano: FrancoAngeli.

Fiore, S. (2024). Verso un approccio integrato alla sicurezza dell'IoT: Sfide e prospettive. Palermo: Sellerio.

Galli, F. (2023). Crittografia per l'IoT: Algoritmi e protocolli a confronto. Genova: Sagep.

Gatti, B. (2022). La sicurezza dei dati nell'IoT: Proteggere la privacy degli utenti. Roma: Editori Laterza.

Ghafoor, K.A. (2022). Cybersecurity Frameworks for IoT Devices: An Overview. International Journal of Computer Applications, 182(5), 23-31.

Gershenfeld, N. (2020). Interoperability in the Internet of Things: Bridging the Gap Between Devices. Communications of the ACM, 63(9), 40-50.

Google Cloud. (2021). Cloud IoT Core. Retrieved from https://cloud.google.com/iotcore/?&utm_source=google&utm-

Grassi, F. (2022). La gestione delle chiavi nell'IoT: Un elemento critico per la sicurezza. Bologna: Il Mulino.

Greco, D. (2022). Sensori di movimento e sicurezza: Protezione e monitorización. Venecia: Marsilio Editori

Greenfield, A. (2022). The Risks of Protocol Translation in IoT Systems. Journal of Network Protocols and Algorithms, 14(3), 75-88.

Gupta, A., et al. (2021). Real-time Data Processing Vulnerabilities in IoT Systems. Journal of Computer Networks and Communications, 2021(4), 45-56.

Hassan, W., et al. (2020). Vulnerabilities Assessment in IoT Devices: Current Trends and Future Directions. International Journal of Computer Science Issues, 17(4), 15-25.

Haslum, T.A., et al. (2023). Countering Counterfeiting in IoT Supply Chains: Challenges and Solutions. IEEE Transactions on Industrial Informatics, 19(2), 2345-2356.

Hildebrandt, M. (2021). Transparency in Data Use: Building Trust in IoT Applications. Journal of Business Ethics, 168(4), 789-802.

Hoffman, D. (2022). Network Segmentation as a Defense Strategy Against Cyber Attacks. Information Systems Management, 39(3), 205-217.

Hossain, M.S., et al. (2023). Physical Security Mechanisms for IoT Devices: Current Trends and Future Directions. IEEE Internet of Things Journal, 10(7), 5678-5689.

Howard, R. (2020). Managing Attack Surfaces in IoT Networks. Journal of Cybersecurity Technology, 4(2), 112-126.

INCIBE (Instituto Nacional de Ciberseguridad de España). (2015). Guía básica de seguridad para dispositivos IoT: Protege tu hogar conectado. Retrieved from https://www.incibe.es/ciudadania/guias/guia-basica-seguridad-dispositivos-iot

INCIBE. (2015). ¿Qué hacen los ciberdelincuentes con los datos robados?. Retrieved from https://www.incibe.es/protege-tu-empresa/blog/que-hacen-los-ciberdelincuentes-con-losdatos-robados

INTERPOL. (2020). Los ataques cibernéticos no conocen fronteras y evolucionan a gran velocidad. Retrieved from https://www.interpol.int/es/Delitos/Ciberdelincuencia

Javed, A.Y., et al. (2023). Wireless Communication Vulnerabilities in IoT Devices: A Comprehensive Survey. Wireless Communications and Mobile Computing, 2023(1), 45–60.

Joint Task Force on Cybersecurity Education. (2018). Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Association for Computing Machinery.

Karp, D.A., & Karpova, E.V. (2019). Incident Response Planning for Cybersecurity Breaches. International Journal of Information Management, 45(6), 123–134.

Kaspersky. (2019). Amenazas IoT en el primer semestre de 2019: Análisis de ataques y vulnerabilidades. Retrieved from https://latam.kaspersky.com/about/press-releases/2019_iot-threats-in-h1-2019

Kaur, G., et al. (2021). Ransomware Attacks on Critical Infrastructure: Implications for Public Safety. Journal of Emergency Management, 19(4), 245–256.

Khan, F.K., et al. (2020). Encryption Techniques for Securing Data Transmission in IoT. International Journal of Computer Applications, 975(11), 18–24.

Khan, M.A., et al. (2024). Government Policies on Cybersecurity: Balancing Regulation with Innovation. Government Information Quarterly, 41(2), 105–117.

Kumar, R., et al. (2023). AI-Powered Malware: New Frontiers in Cyber Threats. Cybersecurity Review, 12(3), 150–163.

Landwehr, C.E. (2021). Risk Assessment Strategies for Emerging Technologies. Risk Analysis, 41(5), 789–803.

Lombardi, C. (2021). Sensori Sanitari: Protezione e Monitorización. Cagliari: Cuec Editrice.

Mairh, A., Barik, D., Verma, K., & Jena, D. (2011). Honeypot in network security: a survey. In Proceedings of the 2011 International Conference on Communication, Computing & Security. Association for Computing Machinery, New York, NY, USA, 600–605. Retrieved from https://doi.org/10.1145/1947940.1948065

Malik, P., & Singh, A. K. (2020). Gestión de riesgos en entornos IoT: Un enfoque integral. Revista de Seguridad Informática, 25(3), 78-92.

Mandiant & FireEye (2019). The Cost of Data Breach Report: Global Insights. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/Cost-of-a-Breach-report.pdf

Marino, F. (2024). Implementación de seguridad en el IoT. Palermo: Sellerio Editore

Martini, G. (2024). Aggiornamenti di sicurezza nei dispositivi IoT: Un'analisi comparativa. Trento: Reverdito Editore.

Misra, S., et al. (2022). Regulatory Frameworks for Securing the Internet of Things: Current Status and Future Directions. Computer Law and Security Review, 38(5), 123–136.

Moretti, N. (2023). Cifrado de datos en el IoT. Catania: Bonanno Editore.

Moustafa, N., et al. (2022). Social Engineering Attacks Using AI: Threat Landscape and Mitigation Strategies. Computers And Security, 115, 102–115.

Narayanan, A., & Shmatikov, V. (2022). How to Break Anonymity through Inference: Reidentification Risks in Practice. ACM Transactions on Information Systems Security, 25(4), 23–36.

Nguyen, T.T., et al. (2021). Collaborative Approaches to Enhance Cybersecurity Awareness Among Stakeholders. Computers And Security, 112, 102–115.

Nurse, J. R. C., et al. (2017). Metodologías para la evaluación de riesgos de seguridad en sistemas IoT. Journal of Cybersecurity, 3(1), 1-15.

Pellegrino, V. (2022). IoT e la sicureza nei sistemi di controllo. Ancona: Transeuropea Editrice

Pérez, J., & García-Castro, R. (2021). Secure Disposal Practices for Electronic Waste in IoT Environments. Environmental Science And Technology, 55(10), 6789–6797.

Petrov, V. (2023). El auge de los datos en el IoT: Implicaciones para la seguridad. Data & Security Review, 12(4), 45-58.

Ponemon Institute (2020). Cost Of a Data Breach Report: Global Insights Retrieved from https://www.ibm.com/security/data-breach

Radanliev, P., et al. (2021). Software Update Mechanisms for Ensuring Device Security In IOT. Journal Of Network and Computer Applications, 181, 103–115.

Rahman, M.S., et al. (2023). Innovations In Cybersecurity Through Collaborative Research Initiatives: Trends and Challenges. Computer Science Review, 42, 100–113.

Ricci, P. (2021). Implementación de seguridad en el IoT. Bari: Laterza.

Rizzo, F. (2023). Protocolli Applicativi nell IoT. Genova: Sagep Editore.

Roman, R., et al. (2019). Government Initiatives to Strengthen Cybersecurity in Emerging Technologies. Government Information Quarterly, 36(4), 567–578.

Romano, V. (2023). Minacce alla privacy nei sensori di movimento IoT. Firenze: Giunti Editore.

Rose, D.E. (2023). Managing Interoperability Risks in IOT Systems. IEEE Internet Of Things Journal, 10(6), 4500–4510.

Rueda, J. (2021). Redes de sensores inalámbricos: Arquitecturas, protocolos y aplicaciones. Sensores y Sistemas, 18(2), 112-128.

Rueda, J., & Talavera, D. (2017). Redes de sensores distribuidas: Fundamentos y tendencias actuales. IEEE Latin America Transactions, 15(5), 876-885.

Saltzer, S., & Schroeder, M.D. (2022). The Protection of Information in Computer Systems. Proceedings Of The IEEE, 63(9), 1278–1308.

Santoro, E. (2022). La gestione delle chiavi e il Cifrado dei dati. Trieste: Hammerle Editori.

Schneier, B. (2023). Automating Cybersecurity Tasks for Improved Efficiency. Journal Of Cybersecurity Technology, 7(1), 34–47.

Sicari, S., et al. (2022). Physical Security Considerations for IOT Devices: Challenges and Solutions. IEEE Transactions on Industrial Informatics, 18(7), 4567–4578.

Silvestri, F. (2022). La Sicureza e le misure di Protezione. Aosta: Testolin Editore.

Singh, R., et al. (2023). Identity Management Solutions for IOT Environments: Current Trends and Future Directions. Journal Of Computer Networks and Communications, 15(2), 78–89

Smith, J.D. (2024). Internal Threats to Cybersecurity in Organizations: Understanding Risks and Mitigation Strategies. International Journal of Information Management, 50, 12–24

Sun, Y., et al. (2022). Fragmentation In IOT Ecosystems: Implications for Security and Privacy. Future Generation Computer Systems, 128, 456–467

Torrijos, M. (2021). Auditorías de seguridad en redes de sensores: Metodologías y herramientas. Revista de Ingeniería Electronica, 32(1), 56-70.

Trappe, W., et al. (2022). Evaluating Supplier Security Practices in IOT Supply Chains. Journal Of Supply Chain Management, 58(4), 345–358

Warkentin, M., & Willison, R. (2019). Building A Culture of Cybersecurity Awareness in Organizations. Computers & Security, 87, 123–135

Weber, R.H. (2020). Physical Security Aspects of The Internet of Things. Computer Law & Security Review, 36(5), 678–689

Wiggins, L., & McCarthy, J.C. (2019). Adapting To New Threats: Continuous Improvement in Cybersecurity Training Programs. Cybersecurity Education Journal, 6(3), 45–56

Yaqoob, I., et al. (2022). Cloud Computing Risks in IOT Environments: Challenges and Solutions. Future Generation Computer Systems, 126, 234–245

Zeadally, S., & Khan, M.A. (2020). Supply Chain Security for IOT Devices: Challenges and Best Practices. Journal Of Network and Computer Applications, 146, 102–115

Zhou, Y., & Chen, Z. (2023). Collaborative Approaches to Strengthen Global Cybersecurity Regulations for IOT Devices. International Journal Of Information Management, 61, 34–46

Zuboff, S. (2023). The Age of Surveillance Capitalism: The Fight for A Human Future at The New Frontier of Power. Public Affairs.