Simulación de un sistema de monitoreo automatizado de cuartos técnicos mediante IoT con análisis predictivo basado en Inteligencia Artificial y estrategias de Ciberseguridad.

Juan David Avendaño Rodríguez
Juan Diego Hernández Ramírez
Tomás Esteban Puchana Borda

Universidad Ean

Facultad de ingeniería

Ingeniería de sistemas

Bogotá, Colombia

.

Resumen

La gestión eficiente de infraestructuras de Tecnologías de la Información (TI) es un componente esencial para garantizar la disponibilidad, seguridad y el rendimiento continuo de los sistemas. En un entorno empresarial cada vez más dependiente de soluciones digitales, se vuelve crucial implementar mecanismos automatizados que permitan el monitoreo en tiempo real de servidores, así como la detección temprana de fallas, con el fin de reducir los tiempos de inactividad y optimizar los recursos tecnológicos.

Este trabajo propone la simulación de un sistema de monitoreo automatizado de servidores mediante el uso del Internet de las Cosas (IoT), integrando análisis predictivo basado en Inteligencia Artificial (IA) y estrategias básicas de ciberseguridad. La integración de IA permite procesar datos en tiempo real para anticipar posibles fallos en la infraestructura tecnológica, mejorando así la toma de decisiones y fortaleciendo la resiliencia del entorno digital. Además, se consideran lineamientos fundamentales de ciberseguridad para mitigar riesgos asociados a la conectividad de dispositivos inteligentes.

El enfoque de este estudio busca sentar las bases conceptuales y técnicas para el desarrollo futuro de soluciones más robustas, escalables y adaptables a entornos reales dentro del ámbito de la gestión de infraestructuras de TI. A través de la simulación de un sistema de monitoreo automatizado que integra tecnologías emergentes como el Internet de las Cosas (IoT), inteligencia artificial y principios fundamentales de ciberseguridad.

Palabras clave: IoT, inteligencia artificial, análisis predictivo, monitoreo de servidores, infraestructura IT, ciberseguridad, simulación.

Abstract

Efficient management of Information Technology (IT) infrastructures is essential to ensure system availability, security, and consistent performance. In an increasingly digital business environment, it is crucial to implement automated mechanisms that enable real-time server monitoring and early fault detection, with the goal of minimizing downtime and optimizing technological resources. This study proposes the simulation of an automated server monitoring system based on the Internet of Things (IoT), incorporating predictive analysis powered by Artificial Intelligence (AI) and fundamental cybersecurity strategies. The integration of AI enables real-time data processing to anticipate potential infrastructure failures, thereby improving decision-making and enhancing the resilience of digital environments. Furthermore, basic cybersecurity guidelines are considered to mitigate the risks associated with the connectivity of smart devices. The focus of this study is to lay the conceptual and technical groundwork for the future development of more robust, scalable, and adaptable solutions in real-world IT management scenarios through the simulation of emerging technologies in controlled environments.

Keywords: IoT, artificial intelligence, predictive analysis, server monitoring, IT infrastructure, cybersecurity, simulation.

Contenido

Lista de Figuras **10**

Lista de Tablas **11**

Introducción **12**

Objetivos **16**

Objetivo general *16*

Objetivos específicos *16*

Definición del problema **17**

Justificación **19**

Análisis de Requerimientos **21**

Marco Teórico **23**

Internet de las cosas *23*

Servidores *35*

Inteligencia artificial y análisis predictivo *40*

Análisis de Restricciones **46**

Técnicas: *47*

Económicas y Financieras: *47*

Legales y Normativas: *48*

Ambientales: *48*

Limitaciones del Equipo de Trabajo: *49*

Metodología **50**

Etapa 1. Diseño de la arquitectura IoT *50*

Etapa 2. Análisis predictivo mediante IA *52*

Etapa 3. Integración de ciberseguridad y monitoreo en tiempo real *51*

Etapa 4. Evaluación, validación y documentación final *52*

Resultados **54**

Infraestructura de red y simulación IoT *54*

Base de datos ..... ***¡Error! Marcador no definido.***

Análisis predictivo IA *68*

Análisis de la IA en la base de datos *71*

Costos **79**

Costos directos *79*

Costos indirectos: *81*

Capital de trabajo: *82*

Conclusiones **83**

Recomendaciones ..... ¡Error! Marcador no definido.

Referencias **87**

Lista de Figuras

Figura 1: Composición de infraestructura de red básica. 33

Figura 2: Infraestructura diseñada 54

Figura 3: Tipo de conexión 55

Figura 4: Configuración básica de la red inalámbrica 56

Figura 5: Establecer contraseña y tipo de encriptación 56

Figura 6: Configuración dinámica DCHP 57

Figura 7: Acceso dispositivos IoT 58

Figura 8: Registro de usuario en HTTP del servidor 60

Figura 9: Configuración de los dispositivos IoT 60

Figura 10: Estado de las variables ambientales de la infraestructura de red 61

Figura 11: Conexión de microcontrolador 62

Figura 12: Acceso a entorno MySQL 64

Figura 13: Creación y verificación de base de datos 65

Figura 14: Verificación estructura creada 66

Figura 15: Consulta de datos registrados 68

Figura 16: Consulta de datos registrados #2 68

Figura 17: Conexión de la base de datos con la IA 69

Figura 18: Verificación de la conectividad 70

Figura 19: Lecturas tomadas#1 70

Figura 20: Lecturas tomadas#2 71

Figura 21: Promt#1 análisis de las lecturas 72

Figura 22: Código proporcionado por IA 73

Figura 23: Resultado Visualización de análisis 73

Figura 24: Promt#2 Comportamiento sensores 74

Figura 25: Resultado comportamiento sensores 74

Figura 26: Resultado comportamiento sensores#2 75

Figura 27: Prompt #3 Alertas registradas 75

Figura 28: Resultado alertas registradas 76

Figura 29: Prompt #4 Recomendaciones predictivas 77

Figura 30: Resultado de las predicciones 78

Lista de Tablas

Tabla 1: Dispositivos esenciales en la infraestructura de red. 32

Tabla 2: Costos directos ..... **¡Error! Marcador no definido.**

Tabla 3: Costos indirectos 81

Tabla 4: Capital de trabajo..... 82

Introducción

En un mundo caracterizado por la creciente digitalización de procesos y servicios, la gestión eficiente de infraestructuras de Tecnologías de la Información (TI) se ha convertido en un componente estratégico para garantizar la disponibilidad, el rendimiento y la seguridad de los sistemas informáticos. Las organizaciones, tanto del sector público como privado, enfrentan la necesidad de asegurar la continuidad operativa de sus plataformas tecnológicas, minimizando riesgos y tiempos de inactividad que podrían afectar la productividad, la integridad de los datos o incluso la confianza de los usuarios. En este escenario, el monitoreo automatizado de servidores y redes adquiere una relevancia crítica, ya que permite detectar anomalías y anticipar posibles fallos mediante el análisis constante de variables clave, promoviendo así una gestión eficaz.

En respuesta a esta necesidad, las tecnologías emergentes como el Internet de las Cosas (IoT) y la Inteligencia Artificial (IA) han empezado a desempeñar un papel fundamental en la transformación de los modelos tradicionales de supervisión. El IoT facilita la conexión y comunicación entre dispositivos inteligentes, permitiendo la recolección de datos en tiempo real desde múltiples puntos de una infraestructura tecnológica. Por su parte, la IA, especialmente a través del análisis predictivo, ofrece herramientas para interpretar dichos datos y generar alertas tempranas sobre posibles fallos o irregularidades, contribuyendo a una toma de decisiones más informada, rápida y eficiente. Estas capacidades no solo optimizan el uso de los recursos tecnológicos, sino que también refuerzan la seguridad de los sistemas frente a amenazas cada vez más sofisticadas.

El presente proyecto propone la simulación de un sistema de monitoreo automatizado de servidores, integrando tecnologías IoT, modelos básicos de inteligencia artificial y principios fundamentales de ciberseguridad. A través de un entorno simulado, se busca demostrar el potencial de estas herramientas para mejorar la gestión de infraestructuras TI sin requerir inversiones significativas en hardware. Esta aproximación resulta especialmente útil en contextos académicos y empresariales que requieren soluciones efectivas, escalables y de bajo costo para enfrentar los desafíos de la transformación digital.

El estudio está diseñado para responder la necesidad de contar con herramientas accesibles que faciliten el monitoreo y la gestión de infraestructuras digitales, dentro de entornos que dependan de sistemas tecnológicos para su funcionamiento. El uso de un entorno simulado permite explicar de manera sencilla y práctica conceptos de IoT, IA, y ciberseguridad, sin exigir conocimientos técnicos avanzados ni inversiones en equipos especializados. De esta forma, la propuesta puede ser aplicada para cualquier tipo de público interesado en fortalecer la seguridad y automatización de sus componentes digitales.

Desde una perspectiva empresarial, la implementación de sistemas inteligentes de monitoreo no solo fortalece la estabilidad tecnológica de las organizaciones, sino que también contribuye a prevenir fallas que podrían generar pérdidas económicas, interrupciones operativas o vulnerabilidades en la protección de los datos personales y corporativos. La creciente preocupación por la seguridad de la información en la era digital ha convertido la ciberseguridad en un eje prioritario, tanto para usuarios como para

instituciones. En este sentido, la integración de mecanismos de protección en los sistemas de monitoreo, incluso desde la etapa de simulación, permite evaluar escenarios de riesgo y definir estrategias de mitigación más eficaces (Ramírez, 2023).

Asimismo, la simulación en entornos virtuales como herramienta metodológica permite validar configuraciones, probar soluciones y optimizar el desempeño de los sistemas antes de su implementación en contextos reales. Esto no solo reduce los costos operativos, sino que también minimiza los riesgos asociados a errores de configuración o vulnerabilidades no identificadas. En un entorno donde la ciberseguridad suele estar vinculada a grandes inversiones (Martínez, 2023), el uso de simulaciones representa una alternativa accesible y eficaz para mejorar la protección de la información sin comprometer el presupuesto disponible.

Desde una perspectiva teórica, el estudio contribuye a la expansión del conocimiento en torno a la automatización en la gestión de infraestructuras TI, promoviendo una visión integral que combina IoT, análisis predictivo y ciberseguridad. La metodología basada en simulación no solo facilita la comprensión de estos conceptos, sino que también ofrece un modelo replicable y adaptable a diferentes contextos, lo que refuerza su valor académico y práctico.

Finalmente, este trabajo se enmarca en el campo de las Tecnologías de la Información y la Comunicación (TIC), con énfasis en la protección de la información que se transmite y procesa en entornos digitales. Su desarrollo responde a la necesidad de contar con herramientas inteligentes que permitan supervisar, analizar y proteger infraestructuras tecnológicas críticas, promoviendo así el avance de la automatización y la

transformación digital en diferentes sectores. En suma, la propuesta busca aportar soluciones innovadoras, sostenibles y orientadas al futuro de la gestión tecnológica.

Para el desarrollo del proyecto se plantean varias fases metodológicas para la ejecución de manera ordenada, por lo que, en primer lugar se realizará un diagnóstico de un cuarto de telecomunicaciones mediante encuestas, revisión de documentación y trabajo de campo, con el fin de establecer el estado actual de los dispositivos y el nivel de operación (al ser una simulación, se tomarán bases vistas en entornos cercanos), posteriormente con los resultados del diagnóstico, se seleccionarán los componentes IoT necesarios para el tipo de red que se va a manejar, garantizando que estos dispositivos respondan las necesidades de monitoreo y automatización del cuarto. Luego de esto, se construye la arquitectura de red simulada que permita la conexión y gestión de los sensores IoT destinados a la recolección de datos, en la cuarta etapa, se desarrollarán los módulos de análisis predictivo apoyados en IA, orientados a la identificación de comportamientos anómalos y anticipar fallos potenciales, y por último se evaluará el desempeño de los sistemas simulados a partir de la capacidad de disminuir tiempos de indisponibilidad y de reforzar la seguridad de la infraestructura mediante la aplicación de estándares básicos de ciberseguridad, consolidando así la propuesta integral de monitoreo automatizado seguro.

Objetivos

Objetivo general

Diseñar un sistema automatizado de monitoreo de cuartos de telecomunicaciones basados en tecnologías IoT, integrando modelos de análisis predictivo mediante IA y mecanismos de ciberseguridad para la detección temprana de fallos y protección de la infraestructura informática.

Objetivos específicos

- Diseñar la arquitectura IoT simulada que represente la infraestructura de un cuarto de telecomunicaciones, incorporando sensores virtuales, routers, switches y servidores.
- Integrar mecanismos de ciberseguridad dentro del entorno simulado, aplicando configuraciones de firewall, autenticación, que garanticen la confidencialidad, integridad y disponibilidad de la información transmitida.
- Asociar herramientas de análisis predictivo mediante inteligencia artificial, capaz de procesar y analizar la información generada por los sensores IoT.

Definición del problema

El crecimiento exponencial de la digitalización y el uso masivo de servicios tecnológicos ha convertido a las infraestructuras de Tecnologías de la Información (TI) en un pilar para garantizar la disponibilidad, seguridad y el rendimiento de los sistemas que soportan desde aplicaciones personales hasta operaciones empresariales y gubernamentales críticas. Sin embargo, los métodos tradicionales de monitoreo, que suelen ser manuales y reactivos, resultan insuficientes en un entorno donde la complejidad de las redes y la criticidad de los servicios han aumentado exponencialmente. Estudios recientes señalan que el 72 % de las interrupciones en centros de datos están asociadas a fallos de hardware no detectados a tiempo, lo que ocasiona pérdidas económicas promedio de USD 300.000 por hora de inactividad (Janisar, et al 2024). Esta situación no solo impacta la continuidad operativa, sino que también acelera el desecho prematuro de equipos con vida útil disponible.

El Internet de las Cosas (IoT) se ha posicionado como una herramienta clave para recolectar datos en tiempo real a través de sensores distribuidos. Se estima que para 2025 habrá más de 75 mil millones de dispositivos IoT conectados globalmente, generando cantidades masivas de datos para la supervisión de infraestructuras críticas (Prathyusha, Rao, & Sree, 2023). No obstante, la simple recolección de datos no es suficiente para garantizar la resiliencia tecnológica. Es necesario integrar algoritmos de Inteligencia Artificial (IA) que posibiliten el análisis predictivo. Según Chilongo y Sithik (2024), la IA

aplicada al monitoreo de infraestructuras puede reducir hasta en un 55 % los tiempos de inactividad no planificados, al identificar patrones de fallos antes de que ocurran.

Paralelamente, la interconexión masiva de dispositivos incrementa la superficie de ataque de las organizaciones. De acuerdo con AlSalem, Almaiah y Lutfi (2023), más del 70 % de los dispositivos IoT presentan vulnerabilidades de seguridad conocidas, siendo las más frecuentes la ausencia de cifrado en las comunicaciones y la falta de autenticación robusta. En esta misma línea, Mazhar, Talpur, Hamam et al. (2023) señalan que los ataques distribuidos de denegación de servicio (DDoS) dirigidos a IoT crecieron un 300 % entre 2019 y 2022, convirtiendo estos entornos en objetivos preferenciales para los ciberdelincuentes. Estas cifras ponen de manifiesto que garantizar la integridad, confidencialidad y disponibilidad de los datos en entornos distribuidos es un reto que no puede ser abordado sin estrategias de ciberseguridad integradas.

En este contexto, se identifica la necesidad de diseñar un simulador automatizado de monitoreo de cuartos de telecomunicaciones que combine tres ejes fundamentales: sensores IoT para la recolección de datos en tiempo real, algoritmos de IA para análisis predictivo y estándares mínimos de ciberseguridad. Este enfoque permitirá optimizar la operatividad, reducir los riesgos, prolongar la vida útil de los equipos y disminuir el impacto ambiental asociado al desecho electrónico, ofreciendo así una solución integral para la gestión eficiente de infraestructuras tecnológicas críticas.

Justificación

La creciente dependencia de las organizaciones en las infraestructuras de Tecnologías de la Información (TI) exige el desarrollo de soluciones innovadoras que aseguren su disponibilidad, seguridad y un rendimiento constante. Los métodos tradicionales de monitoreo suelen ser reactivos, lo que aumenta el riesgo de interrupciones y fallos no detectados, generando pérdidas económicas significativas. De acuerdo con Janisar, et al (2024), más del 60 % de las interrupciones de red están relacionadas con la ausencia de mecanismos predictivos de monitoreo, lo que expone tanto la operación como la integridad de la información crítica. En este sentido, el proyecto de simulación de un sistema automatizado de monitoreo de servidores mediante IoT, con análisis predictivo impulsado por Inteligencia Artificial (IA) y estrategias de ciberseguridad, se presenta como una solución eficaz a estas problemáticas.

La relevancia de la propuesta radica en la integración de tecnologías emergentes que optimizan la supervisión en tiempo real, permitiendo prever fallos y mejorar la gestión de los recursos tecnológicos. Desde el punto de vista económico, la adopción de monitoreo predictivo con IA puede reducir los costos de mantenimiento hasta en un 30 % y disminuir en un 55 % los tiempos de inactividad no planificada (Chilongo & Sithik, 2024). Asimismo, la simulación en entornos virtuales minimiza los costos de pruebas físicas y facilita la escalabilidad de las soluciones, haciéndolas accesibles incluso para organizaciones con recursos limitados (Prathyusha, Rao, & Sree, 2023).

En el ámbito académico, el proyecto aporta al conocimiento en las áreas de IoT, IA y ciberseguridad, ofreciendo un modelo replicable y adaptable tanto para la investigación como para la práctica profesional. Desde una perspectiva social, la implementación de sistemas de monitoreo inteligente fortalece la protección de datos sensibles, un aspecto crítico en un entorno donde la ciberdelincuencia genera pérdidas globales estimadas en USD 8 billones en 2023, con proyecciones de llegar a USD 10,5 billones en 2025 (AlSalem et al., 2023).

En términos prácticos, la propuesta demuestra cómo la convergencia entre IoT, IA y ciberseguridad constituye una estrategia robusta para optimizar infraestructuras TI. La disponibilidad de herramientas de simulación incrementa la viabilidad del proyecto, asegurando su cumplimiento dentro de los plazos y objetivos planteados. Finalmente, el proyecto se enmarca en la línea de investigación en Tecnologías de la Información y Comunicación (TIC), contribuyendo a la transformación digital mediante soluciones sostenibles, innovadoras y ajustadas a las necesidades actuales del sector tecnológico.

Análisis de Requerimientos

El prototipo planteado no consiste en la implementación física completa de un sistema de monitoreo en un centro de datos, sino en la construcción de una simulación funcional que represente las condiciones de un cuarto de telecomunicaciones y permita validar la viabilidad técnica del enfoque. Este entorno simulado integrará tres elementos esenciales: sensores virtuales que generen datos en tiempo real, algoritmos de Inteligencia Artificial (IA) para el análisis predictivo y módulos de ciberseguridad que garanticen la protección de la información procesada.

Para la recolección de datos, se utilizarán sensores simulados en Cisco Packet Tracer, configurados para generar información relacionada con parámetros críticos como temperatura, humedad, tráfico de red, consumo eléctrico y latencia en servidores y switches. Estos sensores virtuales permitirán emular escenarios realistas de operación normal y condiciones de fallo, proporcionando la base de datos necesaria para el análisis.

En cuanto al análisis predictivo, se aprovechará un modelo de inteligencia artificial ya existente, que procesará los datos recolectados y aplicará métricas de precisión y sensibilidad para anticipar comportamientos anómalos. El objetivo es que el modelo sea capaz de emitir alertas sobre posibles fallos en los componentes simulados, demostrando cómo la IA puede contribuir a la continuidad de la operación en entornos críticos.

El componente de ciberseguridad se desarrollará igualmente en Cisco Packet Tracer, donde se simulará una arquitectura de red segura. En este entorno se implementarán medidas como cifrado en la transmisión de datos, autenticación de usuarios, segmentación de red mediante VLANs y configuraciones básicas de firewall y control de accesos. También se podrán recrear intentos de intrusión o ataques de denegación de servicio en la red simulada, para validar la capacidad del sistema de responder y mantener los principios de confidencialidad, integridad y disponibilidad de la información.

Finalmente, los requerimientos de viabilidad incluyen contar con un entorno de simulación estable, equipos de cómputo con capacidad de ejecutar Cisco Packet Tracer y MySQL de manera simultánea, así como definir un plan de desarrollo en fases: diseño de la arquitectura simulada, configuración de sensores y red, integración del modelo de IA, y pruebas de seguridad y resiliencia. Al concluir el plazo establecido, se espera disponer de un simulador académico funcional, capaz de ilustrar de forma práctica la interacción entre IoT, IA y ciberseguridad aplicada a la gestión de infraestructuras tecnológicas.

Marco Teórico

Internet de las cosas

El Internet de las Cosas (IoT) es clave en la transformación digital, ya que posibilita la conexión de dispositivos físicos capaces de recolectar, procesar y enviar datos en tiempo real. Esta tecnología no solo facilita la supervisión y el control remoto de infraestructuras, sino que también permite automatizar procesos y tomar decisiones basadas en información constante. En el ámbito del monitoreo de servidores, el IoT se convierte en una herramienta fundamental para mejorar el rendimiento, minimizar el riesgo de fallos y asegurar la continuidad operativa de sistemas tecnológicos esenciales.

Definición y evolución del IoT

El Internet de las Cosas **"**IoT**"** se refiere al conjunto de dispositivos físicos que, equipados con sensores, actuadores y software, se conectan a redes para recopilar, intercambiar y procesar datos sobre su entorno. Estos objetos no solo recopilan información, sino que también pueden detectar cambios o eventos y responder de forma automática o semiautónoma, convirtiéndolos en agentes activos dentro de los sistemas de información. El objetivo principal del IoT es cerrar la brecha entre el mundo físico y su representación digital, permitiendo la creación de servicios que agreguen valor a través de la observación y el control continuo de activos, procesos y entornos. (Barrio, 2022)

Origen del término IoT

El concepto fue acuñado a finales de los años noventa por Kevin Ashton, dentro de proyectos relacionados con la identificación por radiofrecuencia (RFID) en la cadena de suministro. Su idea inicial era sustituir los registros manuales por lecturas automáticas

provenientes de los propios objetos, lo que permitiría hacer un seguimiento en tiempo real de su uso, estado y ciclo de vida. Aunque al principio el foco estaba en las etiquetas RFID para la logística, pronto se dio cuenta de que el concepto era mucho más amplio: cualquier dispositivo capaz de recolectar y transmitir datos podría integrarse en una red de objetos interconectados (Gokhale & Bhat, 2018).

Evolución tecnológica de IoT en sectores industriales y empresariales

El avance del IoT ha sido posible gracias a la reducción de costos de sensores y microcontroladores, el progreso en las comunicaciones inalámbricas, la expansión de la computación en la nube y los avances en el análisis de datos. En sus primeras etapas de adopción, especialmente en las décadas de 2000 y 2010, el IoT estuvo principalmente enfocado en el ámbito industrial (IoT), donde se utilizaba para monitorear máquinas, realizar mantenimiento predictivo y optimizar las cadenas de producción. Más tarde, la expansión de redes móviles de alta velocidad y la incorporación de arquitecturas como el *edge computing* y la computación en la nube facilitaron su adopción en el ámbito empresarial, con aplicaciones como la gestión inteligente de edificios, el seguimiento de activos, el control de inventarios y el análisis predictivo para mejorar la toma de decisiones operativas. (Crespo & Morales, 2023)

Hoy en día, el IoT está presente en una amplia variedad de sectores, como la salud, el transporte, la energía, la agricultura y las ciudades inteligentes, transformando tanto procesos como modelos de negocio. Esto se debe a que genera grandes volúmenes de datos que permiten la automatización y el ofrecimiento de servicios proactivos. Sin embargo, este crecimiento también trae consigo varios retos, como la latencia, la

capacidad de procesamiento, y las preocupaciones relacionadas con la seguridad y la privacidad, especialmente cuando los datos involucran personas o activos críticos. Estas tensiones entre oportunidades y riesgos explican por qué la integración del IoT generalmente va acompañada de iniciativas de analítica avanzada y ciberseguridad.

Arquitectura del IoT

La arquitectura del Internet de las Cosas "IoT" se organiza en un conjunto de capas que facilitan la recolección, transmisión, procesamiento y utilización de los datos generados por los objetos conectados. Aunque existen diferentes enfoques para describirla, el modelo de referencia más común la divide en cuatro niveles principales: percepción, red, procesamiento y aplicación. (Buitrón Ruiz, 2022)

A partir de este punto, para comprender la arquitectura según (Farooq, Waseem, Mazhar, Khairi, & Kamal, 2015) las capas se dividen y se caracterizan por:

Capa de Percepción

Conocida también como capa física, está compuesta por sensores, actuadores, etiquetas RFID y dispositivos capaces de obtener información del entorno físico. Su función es medir parámetros como temperatura, humedad, presión, ubicación, vibración o imágenes, así como llevar a cabo acciones sobre el entorno cuando sea necesario. Esta capa representa el primer punto de contacto entre el mundo físico y el digital, garantizando la precisión y fiabilidad de los datos iniciales. (Farooq, Waseem, Mazhar, Khairi, & Kamal, 2015)

Capa de Red

Es la encargada de transmitir los datos captados hacia los sistemas que los procesarán. Utiliza tanto tecnologías de comunicación cableada (como Ethernet y fibra óptica) como inalámbrica (Wi-Fi, Bluetooth Low Energy, Zigbee, LoRaWAN, redes celulares 4G/5G, entre otras). En esta fase, la interoperabilidad y la eficiencia en la transmisión son esenciales debido a la diversidad de protocolos y dispositivos, por lo que es necesario implementar soluciones que aseguren la compatibilidad y el bajo consumo energético. (Farooq, Waseem, Mazhar, Khairi, & Kamal, 2015)

Capa de Procesamiento

En este nivel, la información recolectada se guarda, analiza y convierte en conocimiento aplicable. Este proceso involucra plataformas como la computación en la nube (*cloud computing*), computación en el borde (*edge computing*) o computación en la niebla (*fog computing*), además de algoritmos de análisis de datos, inteligencia artificial y aprendizaje automático. La capa de procesamiento filtra la información irrelevante, identifica patrones, genera alertas y ejecuta acciones automáticas, creando valor a partir de los datos crudos. (Farooq, Waseem, Mazhar, Khairi, & Kamal, 2015)

Capa de Aplicación

Es la encargada de presentar los datos procesados de forma comprensible y útil para el usuario final o para otros sistemas. Incluye interfaces como paneles de control, aplicaciones móviles, software empresarial o integraciones con sistemas de planificación y gestión. En esta capa se concretan los beneficios del IoT, como monitoreo en tiempo real,

predicciones, mantenimiento automatizado o control remoto de dispositivos. (Farooq, Waseem, Mazhar, Khairi, & Kamal, 2015)

Interconexión de Dispositivos y Sensores

El funcionamiento del IoT depende de la comunicación entre dispositivos diversos. Para facilitar este intercambio de información de manera segura y eficiente, se utilizan protocolos estandarizados como MQTT, CoAP o HTTP/REST, así como formatos ligeros como JSON o XML para estructurar los datos. Los sensores y actuadores no operan de manera independiente; forman redes que colaboran, comparten información y pueden interactuar con sistemas externos, creando un ecosistema conectado que integra hardware, software y servicios. (Buitrón Ruiz, 2022)

En conjunto, esta arquitectura modular asegura que el IoT sea escalable, flexible y capaz de adaptarse a una amplia variedad de contextos, desde aplicaciones industriales y empresariales hasta usos domésticos y de consumo masivo.

El Internet de las Cosas (IoT) ha revolucionado la gestión de infraestructuras críticas, permitiendo una supervisión constante y decisiones fundamentadas en datos en tiempo real. La combinación de sensores inteligentes, redes de comunicación y plataformas de análisis facilita un control detallado de parámetros clave, lo cual es vital en centros de datos, servidores y otros entornos donde la seguridad y la disponibilidad son prioritarias. (National Institute of Standards and Technology, 2020)

Aplicaciones en centros de datos, servidores y entornos críticos

En los centros de datos, el IoT se utiliza para monitorear factores ambientales como la temperatura, humedad, flujo de aire y el consumo de energía. Los sensores distribuidos

envían datos constantemente, lo que ayuda a optimizar el rendimiento de los sistemas de climatización (HVAC) y evitar sobrecalentamientos que podrían dañar el hardware.

En cuanto a los servidores, el IoT facilita la supervisión de métricas de rendimiento como el uso de CPU, memoria, velocidad de transferencia y latencia de red. Los sistemas de análisis predictivo son capaces de identificar anomalías que podrían señalar posibles fallos, lo que permite realizar mantenimiento preventivo antes de que se produzca una interrupción del servicio. (National Institute of Standards and Technology, 2020)

En infraestructuras críticas, tales como instalaciones industriales, centros de control energético, laboratorios o redes de telecomunicaciones, el IoT monitorea el estado de equipos, la integridad de los sistemas eléctricos, la presión de tuberías o las vibraciones de las maquinarias. Este tipo de monitoreo es fundamental en operaciones continuas, ya que un fallo no detectado puede causar pérdidas económicas y riesgos de seguridad importantes. (Talavera et al., 2017)

Ventajas de la automatización en tiempo real

La implementación de la automatización respaldada por el Internet de las Cosas (IoT) presenta importantes ventajas en la gestión de infraestructuras:

- **Minimización del tiempo de inactividad**: La identificación anticipada de fallos ayuda a reducir las interrupciones inesperadas, garantizando la continuidad del servicio (National Institute of Standards and Technology, 2020).
- **Optimización de los recursos**: El monitoreo continuo facilita ajustes en el consumo de energía, distribuye mejor las cargas de trabajo y mejora la eficiencia en las operaciones (National Institute of Standards and Technology, 2020).

- **Mantenimiento predictivo**: A través de algoritmos avanzados, es posible prever el desgaste o deterioro de los componentes, permitiendo programar mantenimientos antes de que ocurran fallos críticos (National Institute of Standards and Technology, 2020).
- **Mayor seguridad**: La vigilancia constante y la generación automática de alertas incrementan la protección frente a riesgos, tanto físicos como cibernéticos (National Institute of Standards and Technology, 2020).
- **Escalabilidad y flexibilidad**: Los sistemas basados en IoT son altamente escalables, lo que permite añadir nuevos sensores o integrar diversas plataformas de gestión de manera sencilla (Buitrón Ruiz, 2022).

Protocolos del Internet de las Cosas

El funcionamiento eficiente de un ecosistema de IoT depende de la correcta implementación de protocolos y estándares que faciliten la comunicación entre dispositivos, pasarelas, servidores y aplicaciones (Buitrón Ruiz, 2022). Dado que los entornos de IoT varían en términos de anchos de banda, necesidades de seguridad y consumo energético, se han desarrollado múltiples protocolos específicos para abordar estos desafíos. Entre los más relevantes se encuentran MQTT, CoAP y HTTP, además de otros como AMQP, LoRaWAN y Zigbee (Buitrón Ruiz, 2022).

MQTT (Message Queuing Telemetry Transport)

Es un protocolo de mensajería ligera que sigue un modelo de publicador/suscriptor y está optimizado para redes con ancho de banda limitado y dispositivos con pocos recursos. Entre sus principales ventajas se destacan el bajo consumo de energía, el soporte

para comunicaciones asincrónicas, su facilidad de implementación y la confiabilidad que ofrece gracias a los niveles de calidad de servicio (QoS). Sin embargo, también presenta ciertas limitaciones, como la ausencia de cifrado nativo, lo que obliga a complementarlo con protocolos como TLS/SSL, y su idoneidad principalmente para el manejo de mensajes cortos, ya que no resulta eficiente en la transferencia masiva de datos (Soni & Makwana, 2017).

CoAP (Constrained Application Protocol)

Es un protocolo diseñado para dispositivos con capacidades limitadas que funciona sobre UDP y emplea un modelo de intercambio similar al de HTTP, aunque de manera más ligera. Entre sus ventajas se encuentran el bajo consumo de recursos, el soporte para comunicaciones multicast, la compatibilidad con HTTP mediante proxies y la capacidad de operar en redes con alta latencia. No obstante, presenta ciertas limitaciones, ya que al estar basado en UDP no garantiza una entrega confiable sin la incorporación de mecanismos adicionales, y su seguridad depende del uso de DTLS, lo que puede dificultar su implementación en entornos críticos (Seoane et al., 2021).

HTTP (Hypertext Transfer Protocol)

HTTP es uno de los protocolos más utilizados en aplicaciones web y también tiene un papel importante en el ámbito del IoT, donde se emplea para integraciones y servicios basados en REST. Sus principales ventajas radican en ser un estándar universal, ampliamente compatible con diferentes plataformas y herramientas, además de facilitar el desarrollo de APIs y ofrecer seguridad nativa mediante el uso de HTTPS. Sin embargo, presenta limitaciones relacionadas con su mayor consumo de ancho de banda y recursos, lo

que lo hace menos eficiente para dispositivos con restricciones de procesamiento o energía (Da Cruz et al., 2019).

En general, la selección del protocolo adecuado para un sistema IoT depende de factores como el tipo de aplicación, las limitaciones de hardware, la necesidad de comunicaciones en tiempo real, la seguridad requerida y la conectividad disponible. Una implementación óptima podría combinar diferentes protocolos, como usar MQTT para telemetría en tiempo real y HTTP/REST para la configuración o el acceso a datos históricos.

La adopción de los protocolos y estándares correctos no solo mejora la eficiencia y escalabilidad del sistema, sino que también asegura su interoperabilidad con otras soluciones, un aspecto esencial para el crecimiento del IoT en entornos industriales, empresariales y domésticos.

Infraestructura de telecomunicación

Existen muchas formas para categorizar las redes, bien sea por sus características físicas o su extensión, pero según su alcance son divididas de la siguiente forma:

PAN (Personal Area Network)

LAN (Local Area Network) = Aprox. 1Km de extensión

MAN (Metropolitan Area Network) = Aprox 50Km de extensión

WAN (Wide Area Network) = +50Km, interconexión de redes de diferentes regiones o incluso países.

Independientemente de la red, la finalidad de esta es el envío correcto y seguro de mensajes e información, para esto se involucran 3 actores: Emisor, medio y receptor, los dispositivos que toman este rol pueden ser los siguientes:

Tabla 1: Dispositivos esenciales en la infraestructura de red.

Nombre	Definición	Cita	Función
Router	Conecta varias redes diferentes y dirige el tráfico de datos para garantizar que la información llegue correctamente al destino	(2025, Cisco Systems, Inc.)	Esencial para interconectar redes LAN y WAN, permitiendo la comunicación global en internet
Switch	Interconecta varios dispositivos dentro de una misma red local, enviando los datos solo al equipo necesario	(2025, Cisco Systems, Inc.)	Optimiza el rendimiento de la red al reducir el tráfico innecesario
Firewall	Filtra y controla el tráfico de red, bloqueando accesos no autorizados y protegiendo la seguridad de la información.	(2025, Cisco Systems, Inc.)	Es un componente clave en la seguridad perimetral de las redes.

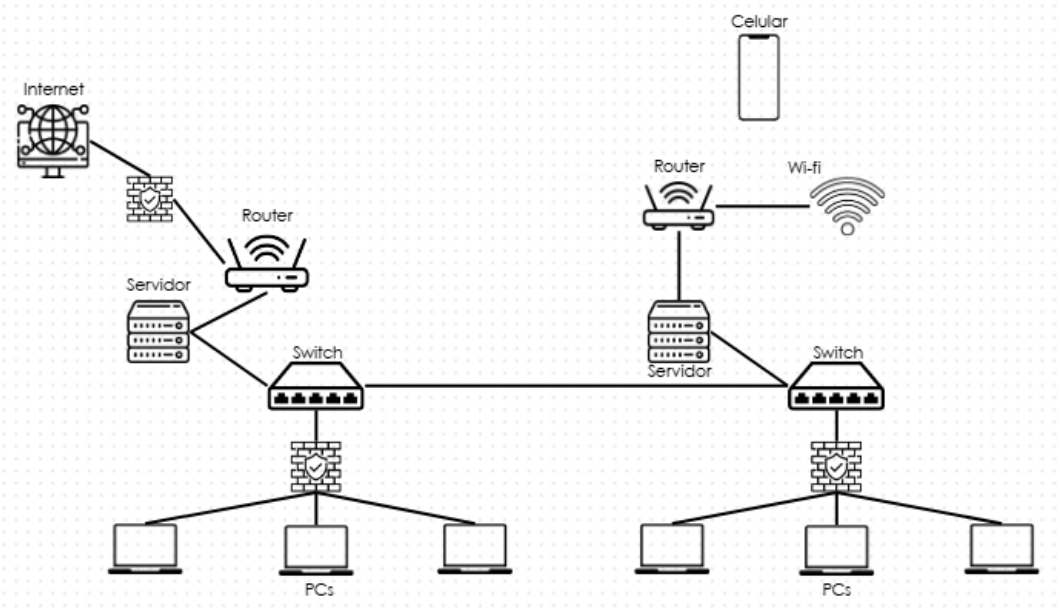
Sniffer	Captura y analiza el tráfico que circula por la red	(2025, Cisco Systems, Inc.)	Es utiliza en las auditorías de seguridad y diagnóstico de fallos en la red
Access Point	Proporciona conexión inalámbrica y enlaza dispositivos con la red cableada	(2025, Cisco Systems, Inc.)	Facilita la movilidad de los usuarios al brindar el acceso inalámbrico

La importancia de implementar este tipo de monitoreo es como el sistema permite detectar incidencias en tiempo real, y reducir significativamente los tiempos de inactividad, con el fin de coordinar acciones correctivas inmediatas y optimizar la utilización de recursos tanto físicos como virtuales. (Marchionni, 2011)

Esta infraestructura, compuesta por redes y dispositivos, es la base sobre la cual se construyen las comunicaciones modernas, asegurando que la información pueda ser transmitida de forma eficiente, segura y con la menor latencia posible.

En la figura 1 se evidencia el funcionamiento de la composición de redes locales interconectadas básicas.

Figura 1: Composición de infraestructura de red básica.



Nota: Elaboración propia (2025).

Este ejemplo presentado en la figura 1 muestra dos empresas interconectadas, donde se evidencia en el esquema de la izquierda, que la conexión a internet llega primero a un *firewall* perimetral, encargado de filtrar y controlar el tráfico antes de entrar a la red interna, después la señal pasa por el *router,* que distribuye la conexión hacia un servidor y un *switch*. El switch enlaza varias computadoras, sin antes no tener un control de seguridad para proteger los equipos finales de amenazas internas o externas. En el esquema de la derecha se observa la misma funcionalidad, solo que esta vez el *router* proporciona conectividad Wi-Fi, permitiendo que dispositivos móviles como un celular se conecten a la red de manera inalámbrica.

La conexión entre los switches de ambos esquemas funciona como un enlace troncal que permiten que las dos redes de tipo LAN se comuniquen entre sí, gracias a este enlace los dispositivos que intervienen dentro de la red pueden compartir recursos, centralizar servicios, mejorar la administración de red y mantener la seguridad segmentada. **(CIS Controls, 2021; Khan et al., 2012).**

Con esto claro, se evidencia la importancia de la disponibilidad de estos cuartos e infraestructuras en todo tiempo.

Servidores

Un servidor se define como un sistema informático, que tiene como objetivo almacenar, procesar y administrar información para ponerla a disposición de otros dispositivos mediante una red de comunicación. Estos sistemas son diseñados para ofrecer servicios o recursos de manera centralizada, lo que permite que múltiples usuarios o aplicaciones accedan de forma simultánea a los mismos datos o funciones. **(Isa et al., 2024).**

Las funciones pueden variar según su propósito, por ejemplo, existen servidores de archivos, que permiten almacenar y compartir documentos entre usuarios, servidores web que alojan páginas y aplicaciones accesibles a través de internet, servidores de bases de datos que gestionan grandes volúmenes de datos de información estructurada, y servidores de correo electrónico que administran el envío y recepción de mensajes. En general pueden centralizar aplicaciones críticas, mejorar la gestión de usuarios y dispositivos y garantizar la seguridad mediante políticas de acceso y estándares de ciberseguridad (Kurose & Ross, 2017).

Debido a la disponibilidad necesaria de manera continua, según Stalling (2020), la robustez o redundancia en el hardware, junto con la implementación de medidas de ciberseguridad, son aspectos fundamentales para garantizar la integridad y disponibilidad de la información que gestionan.

Los servidores están conformados por:

Procesadores: Unidad central de procesamiento, componente que interpreta y ejecuta instrucciones, procesan datos y controla el funcionamiento general del sistema. La CPU de un servidor no es igual a la de un computador debido que esta cuenta con una mayor capacidad de memoria RAM, con optimización del consumo de energía en largas sesiones de cargas de información, mayor potencia de velocidad y entre otros factores que diferencian.

Memoria RAM: Módulos de gran capacidad que permiten el procesamiento de datos en una gran velocidad.

Sistema de refrigeración: Encargados de mantener la temperatura correcta de los componentes dentro de rangos seguros

Placa base: Circuitos principales y conexiones entre todos los componentes.

Fuentes de alimentación: Proveer energía al servidor.

La necesidad de monitorear este tipo de servidor mediante sensores IoT radica en que cada componente es crítico para la continuidad del servicio. Si un procesador empieza a sobrecalentarse, si el ventilador falla o si la memoria RAM presenta errores, el sistema podría degradarse afectando aplicaciones, usuarios y operaciones necesarias de una compañía. Con sensores de temperatura, voltaje, vibración y consumo energético, es posible implementar el sistema de monitoreo predictivo.

Como señalan Kurose y Ross (2017), la proactividad dentro de la gestión de la infraestructura reduce significativamente los tiempos de inactividad y el impacto económico asociado a fallos no previstos. La integración de sensores IoT Y el análisis predictivo mediante Inteligencia artificial, permite anticipar problemas y programar

mantenimientos preventivos, garantizando la disponibilidad, integridad y la confidencialidad de los datos.

Monitoreo de servidores

El monitoreo de servidores busca la observación constante de los parámetros que evidencien el estado físico y lógico de los sistemas que un cuarto de telecomunicaciones compone, permitiendo detectar fallos tempranos y desgastes normales de uso en estos componentes. Los parámetros suelen incluir aspectos ambientales como la temperatura, y humedad, y aspectos más técnicos como el uso de CPU, uso de memoria, latencia de red, estado de ventiladores y fuentes de voltaje. **(Miranda Indio, 2023)**

Debido a la globalización que demanda del uso de la tecnología y fuentes de información gigantes, los pilares tecnológicos del mundo y empresas pequeñas no se pueden conformar con un análisis y monitoreos antiguos manuales que requieren de personal 24 horas al día, los 7 días de la semana, para saber el estado de estos componentes, por lo que la integración de las tecnologías 4.0 da lugar a una automatización correcta que optimizaría procesos a nivel mundial.

Tipos de monitoreo

En el ámbito de los cuartos de telecomunicaciones y centros de datos, el monitoreo es un factor esencial para garantizar la continuidad operativa, la seguridad de la información y el desempeño eficiente de los recursos. Existen diferentes tipos de monitoreo que abarcan desde la supervisión lógica de los sistemas, hasta el control de parámetros físicos y ambientales. Estos enfoques permiten prevenir fallos, responder de

manera oportuna a incidentes y optimizar los procesos internos mediante el uso de tecnologías de automatización e IoT (Al Batahari, 2020)

Monitoreo de seguridad: Es un proceso continuo que permite observar en tiempo real los incidentes de la red, detectando amenazas y exponiendo posibles vulnerabilidades que puedan comprometer la información de la organización. Para lograr una respuesta adecuada, resulta fundamental analizar los datos recolectados, establecer una línea base y definir métricas claras que permitan identificar el rango de funcionamiento correcto de los componentes. (**CIS Controls, 2021).**

La finalidad con este tipo de monitoreo es interpretar el comportamiento de los componentes que funcionan dentro del cuarto de telecomunicaciones, optimizando los procesos y aumentando la respuesta frente a los fallos tempranos.

Monitoreo de infraestructura: Este sistema se centra más hacia inferir el entorno de archivos de una organización y así poder proporcionar respuestas efectivas frente a cualquier amenaza en los canales de comunicación. (Miranda Indio, 2023)

Métricas en el monitoreo.

Según el *National Institute of Standarfs and Technology* (NIST, 2018) el monitoreo continuo es un proceso esencial para lograr identificar cambios en la postura de seguridad y el estado operativo de los sistemas, integrando herramientas automatizadas y técnicas de supervisión proactiva. (NIST SP 800-137, 2011). El monitoreo de los servidores garantiza la continuidad operativa, optimiza el rendimiento y refuerza la seguridad de los sistemas, para esto se debe tener en cuenta que los sensores de IoT manejen métricas como:

- Disponibilidad y tiempo de actividad: Este aspecto se debe medir en como el servidor se encuentra operando de manera correcta y es accesible para los usuarios que dependen de él, mediante un porcentaje de tiempo de este dato. El *uptime* refleja el tiempo continuo en el que el servidor ha estado funcionando sin interrupciones. La métrica estándar busca una disponibilidad cercana al (99.999%) que implica un máximo de inactividad por año de 5.26 minutos. (**Isa et al., 2024)**

  La norma ISO/IEC 27031:2011 recomienda el monitoreo contante de disponibilidad como parte del plan de continuidad de negocio.
- Rendimiento: El uso intensivo y sostenido de una CPU por encima del 85% puede indicar sobrecarga o procesos anómalos (Srinivasan, 2019). Así mismo la RAM al tener una falta de memoria disponible y el uso de memoria swap puede llegar a ralentizar el sistema y provocar errores de asignación, por lo que un control y eliminación de archivos ya no funcionales, es de suma necesidad. (**Miranda Indio, 2023).**
- Seguridad y detección de incidentes: Detección y respuesta antes actividades maliciosas, accesos no autorizados o alteraciones al sistema, para esto se debe de lograr una supervisión de los puertos y servicios de la red e IP del servidor para identificar procesos no autorizados. (NIST SP 800-94). La implementación de controles de monitoreo continuo y correlación de eventos reduce significativamente el tiempo de permanencia de amenazas. (CIS Controls v8, 2021).
- Temperatura y humedad: Mantener entre 18°C y 27°C y una humedad entre el 40% y el 60% para evitar la condensación o electricidad estática. **(Gokhale, Bhat & Bhat, 2018).**
- Ruidos o vibraciones: El exceso de ruido puede indicar fallos en ventiladores o discos duros mecánicos, así mismo las vibraciones prolongadas pueden llegar a causar daños dentro de los discos HDD y afectar la lectura de archivos. **Esteban, Zafra & Ventura, 2022).**

- Detección de humo: Extinción mediante gas limpio que no altere el funcionamiento de los componentes en caso de una detección temprana de humo. **(National Institute of Standards and Technology, 2020)**
- Seguridad física: Control de acceso mediante credenciales, biometría, cámaras de videovigilancia y sensores de apertura en racks. **(IBM, 2024)**

Inteligencia artificial y análisis predictivo

La creciente digitalización de procesos ha impulsado a las organizaciones a adoptar estrategias de monitoreo automatizado para garantizar la disponibilidad y seguridad de sus respectivos sistemas. En este contexto, las tecnologías de ***Iot*** "Internet de las cosas" y la inteligencia artificial se han posicionado como unos de los ejes centrales en la supervisión de infraestructuras tecnológicas (Shlash Mohamed et al., 2024). Estas herramientas no solo permiten la recopilación de datos en tiempo real, sino también la aplicación de análisis predictivo para anticipar fallos, logrando la reducción de costos y de riesgos operativos.

Fundamentos teóricos del análisis predictivo y la IA

Durante los procesos de producción, los sistemas de manufacturación pueden sufrir de errores críticos que no pueden ser controlados debido a distintos fenómenos como la degradación del equipo, procesos ineficientes de trabajo y rotura de material.

Para esto, se comienzan a sugerir distintas técnicas para la detección de fallas tempranas y estimación de deterioro según el tiempo, como la estimación de vida útil (RUL en inglés) con el que las organizaciones se prevén las posibles fallas críticas antes de tener que detener la producción por alguna de estas situaciones. Por lo anterior, es importante incorporar estas técnicas con procesos de análisis predictivo. El análisis predictivo es una técnica analítica avanzada que emplea datos históricos y en tiempo real,

junto con algoritmos estadísticos y de *machine learning* para la identificación de patrones y así predecir eventos futuros. (Mohamed-Larbi & Daoud, 2024)

El enfoque ***SCO-AI*** "Supply Chain Optimization using AI" propuesto en *Predictive analytics on artificial intelligence in supply chain optimization* por (Mohammed et al, 2024)**,** aunque es desarrollado para cadenas de suministro, comparte varios factores comunes con el proceso de monitoreo de redes y servidores. Entre estos factores destacan la integración de análisis en tiempo real, arquitecturas modulares y capacidad de adaptación a entornos cambiantes, lo que permite a los sistemas reaccionar de forma eficaz ante distintos fenómenos.

Ciberseguridad en entornos IoT

Según el área de ciberseguridad de IBM, "la ciberseguridad se refiere a todas las tecnologías, prácticas y políticas para prevenir los ataques cibernéticos o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas informáticos, las aplicaciones, dispositivos, datos, activos financieros y las personas contra el *ransomware* y otros malwares, las estafas de phishing, el robo de datos y otras ciber amenazas".

Existen 3 tipos de amenazas que pueden ser digitales, humanas o físicos.

La seguridad digital se refiere a la protección de los datos y sistemas frente a amenazas cibernéticas. Estas amenazas se mitigan mediante estrategias como el uso de firewalls, sistemas de detección de intrusos y software de encriptación. Por otro lado, la seguridad humana está relacionada con la manipulación de las personas para obtener acceso a información confidencial, ya sea a través de engaños, sabotajes o acciones no intencionales, como abrir o descargar archivos maliciosos enviados mediante técnicas de

phishing. Para reducir estos riesgos, resulta fundamental implementar programas de capacitación y entrenamiento dirigidos al personal, con el fin de que puedan identificar posibles amenazas tanto en correos electrónicos como en intentos de manipulación directa por parte de terceros. Finalmente, la seguridad física se centra en la protección de los componentes tangibles de una organización, tales como la infraestructura, los servers rooms y los data centers. Dentro de este ámbito se consideran riesgos como el robo y los daños no intencionales ocasionados por desastres naturales, los cuales pueden comprometer seriamente la continuidad operativa de las instalaciones y los sistemas de información.

Sea cual sea el tipo de seguridad y amenaza en la que se categorice, la ciberseguridad tiene como objetivo garantizar la confidencialidad, disponibilidad e integridad (CIA) de la información.

La tríada mencionada constituye el marco conceptual esencial para la ciberseguridad en entornos IoT, donde la combinación de dispositivos, las restricciones de recursos y la exposición física incrementan sustancialmente la superficie de ataque y obligan a reinterpretar y aplicar cada uno de estos principios con medidas técnicas concretas y compatibles con las limitaciones del ecosistema. (Roman et al., 2013). La confidencialidad busca mantener la información y los datos manejados en secreto, lo que significa que solo personal autorizado pueda tener acceso y modificar esta información, controles básicos que se usan en esta fase es la encriptación, el control de accesos, y la gestión de parches o actualizaciones, por el lado de la integridad se refiere a como se asegura que la data sea confiable y no sea modificada o destruida por accesos no autorizados, dentro de las soluciones para mitigar este tipo de filtración, se encuentran los

controles de acceso, los *backups* de información, auditorias que registren cronológicamente de como el canal de comunicación reciben y envían información correctamente, y *checksums* el cual es un valor numérico que suma la cantidad de datos por bloque para verificar la integridad de los datos, por último la disponibilidad refiriéndose a que sin importar el momento, hora o día, se tenga acceso a los datos, esto hace referencia a que se deben manejar *backups* de información, tener *softwares antimaleware* de detección de estos, y firewalls.

En la práctica, la aplicación de la CIA en IoT exige decisiones de ingeniería que equilibren seguridad y eficiencia mediante selección de algoritmos criptográficos apropiados a la plataforma, diseño de protocolos con sobrecarga mínima, definiciones explícitas de nivel de servicio y objetivos de recuperación, y un programa de gestión del ciclo de vida que incluya pruebas de resiliencia y auditorías periódicas.

La autenticación en sistemas de información no se limita únicamente a la verificación de identidad de los usuarios, sino que también abarca la identificación y validación de dispositivos que participan en la recolección y transmisión de datos, como ocurre en entornos de IoT. Para garantizar la integridad de la información y la confiabilidad de los procesos de predicción y análisis, se recomienda el uso de mecanismos criptográficos robustos y escalables. Entre estos se encuentran los certificados digitales X.509, documentos electrónicos que asocian una clave pública con la identidad de un usuario, servicio o dispositivo, e incluyen información esencial como algoritmos de cifrado y datos del firmante (Microsoft, 2025). Junto a estos certificados, los protocolos TLS/DTLS permiten establecer canales seguros que garantizan la legitimidad de los datos, mientras que la autenticación multifactor(MFA) integra distintos factores de verificación

(contraseñas complejas, tokens físicos o biometría), reduciendo el riesgo de suplantación de identidad y accesos no autorizados (Khan, Khan, Zaheer, & Khan, 2012).

En este marco, el control de accesos es otro componente esencial de la ciberseguridad. Este se basa en la definición de políticas que determinan qué usuarios o dispositivos tienen permiso para acceder a determinados recursos, operaciones o niveles de privilegio. Las redes suelen vincularse con listas de control de acceso (ACL) en gateways y firewalls, lo que delimita direcciones, protocolos y puertos autorizados, fortaleciendo la seguridad perimetral y reduciendo el riesgo de filtración de información.

La gestión de identidades y accesos (IAM) ha evolucionado hacia soluciones inteligentes que incorporan algoritmos de inteligencia artificial capaces de auditar acciones de los usuarios, detectar patrones anómalos y automatizar la revocación de credenciales en caso de comportamientos sospechosos. Los motores de análisis predictivo, en este sentido, contribuyen a identificar intentos inusuales de autenticación y habilitan respuestas preventivas de forma temprana (Stergiou, Psannis, Kim, & Gupta, 2018).

En entornos distribuidos como los de IoT, las amenazas más comunes incluyen la intercepción de datos, el spoofing, los ataques DDoS y el acceso no autorizado. La intercepción ocurre cuando un atacante captura información en tránsito, lo que puede ser mitigado mediante cifrado de extremo a extremo (E2EE), VPNs y protocolos como TLS/DTLS. El spoofing, por su parte, busca falsificar identidades o direcciones IP para introducir datos falsos en el sistema, y puede ser prevenido con certificados digitales y

validación de integridad de firmware. Los ataques DDoS, que saturan los recursos de red o servidores, suelen mitigarse mediante filtración de tráfico y segmentación de red. Finalmente, el acceso no autorizado se relaciona con credenciales débiles o falta de MFA, lo que se mitiga con políticas de contraseñas robustas, control de acceso basado en roles y auditorías continuas (Khan et al., 2012; Stergiou et al., 2018).

La defensa en profundidad se refuerza con medidas como firewalls, segmentación de red e IDS/IPS. Los firewalls filtran el tráfico según direcciones y protocolos, mientras que la segmentación limita la propagación de ataques. Los sistemas IDS/IPS, por su parte, monitorizan patrones de comportamiento para identificar intrusiones y responder de forma preventiva.

La protección de infraestructuras críticas debe alinearse con normas y marcos regulatorios internacionales. Entre los más relevantes se encuentran:

- ISO/IEC 27001, estándar internacional de gestión de la seguridad de la información, que define políticas, procedimientos y controles para preservar la confidencialidad, integridad y disponibilidad.

- NIST Cybersecurity Framework, que estructura cinco funciones principales: identificar, proteger, detectar, responder y recuperar (NIST, 2018).

- OWASP IoT Top 10, que expone las principales vulnerabilidades en IoT y directrices para mitigarlas.

- GDPR, reglamento europeo que establece principios de privacidad y obligaciones para el tratamiento de datos personales.

Cumplir con estos estándares no solo refuerza la seguridad de la organización, sino que también genera confianza entre los clientes y socios, mostrando el compromiso de la entidad con la protección de la información y la gestión de riesgos cibernéticos. (National Institute of Standards and Technology [NIST], 2018)

Análisis de Restricciones

En la ingeniería, la búsqueda de soluciones innovadoras enfrenta diversas limitaciones que condicionan tanto el diseño como la implementación de cualquier proyecto. Aunque existen múltiples soluciones teóricas para los problemas planteados, el análisis de restricciones es un proceso esencial que permite identificar y evaluar los factores que pueden dificultar o impedir la viabilidad de una solución en el mundo real. Este análisis abarca no solo aspectos técnicos, sino también áreas normativas, económicas, sociales, ambientales, políticas, de salud y seguridad.

El proyecto de simulación de un sistema automatizado de monitoreo de servidores utilizando IoT, IA y ciberseguridad, aunque basado en una simulación de bajo costo, no

está exento de estas limitaciones. A continuación, se describen las restricciones principales que deben ser tenidas en cuenta para asegurar la ejecución exitosa del proyecto:

Técnicas:

Disponibilidad tecnológica: El proyecto se basa en una simulación funcional y no requiere hardware físico. Su viabilidad depende de contar con un software de simulación fiable y un entorno de programación que permita ejecutar simultáneamente aplicaciones como Cisco Packet Tracer y Python. Para garantizar un rendimiento adecuado, el computador debe cumplir con los requisitos mínimos del software de simulación: procesador de al menos 2.5 GHz, 4 GB de memoria RAM y 1.5 GB de espacio disponible en el disco duro para la instalación de los programas.

Capacidad de los equipos: Los equipos de cómputo utilizados por el equipo de trabajo deben tener suficiente capacidad para ejecutar las herramientas de simulación y los modelos de IA sin problemas. Una capacidad limitada podría afectar el rendimiento de la simulación y la capacidad de procesar los datos en tiempo real. Cada equipo cuenta con un procesador multinúcleo (Intel Core i5 o AMD Ryzen 5 o superior), 8 GB de RAM, disco sólido SSD de 256 GB o superior y tarjeta gráfica básica compatible con entornos de simulación e IA. Además, se requiere conexión a internet estable, sistema operativo actualizado (Windows 10/11 o Linux) y periféricos básicos como teclado, ratón y monitor 1080p, para facilitar la visualización de resultados.

Económicas y Financieras:

Disponibilidad de capital: El proyecto se plantea como una solución de bajo costo, ya que no se requieren grandes inversiones en hardware. Esta limitación es una fortaleza del proyecto, ya que se enfoca en demostrar la viabilidad de soluciones accesibles tanto en entornos académicos como en entornos empresariales con recursos limitados. No obstante, debe considerarse que algunos de los programas utilizados para la simulación y el análisis cuentan con licencias proporcionadas por la universidad EAN que podrían expirar durante el desarrollo del proyecto, lo que implicaría la necesidad de renovarlas o adquirir nuevas licencias para garantizar la continuidad de las actividades sin interrupciones.

Costos de prueba: Al utilizar un entorno simulado se minimizan los costos, lo que hace que esta opción sea económicamente accesible y eficaz para el estudio de sistemas de monitoreo automatizado sin exceder el presupuesto disponible.

Legales y Normativas:

Protección de datos personales: Aunque la simulación no utiliza datos reales, la propuesta considera los principios de privacidad y seguridad informática. Se toman como referencia la Ley 1581 de 2012 de Protección de Datos Personales en Colombia y el Reglamento General de Protección de Datos de la Unión Europea (GDPR, 2016/679), que establecen los lineamientos básicos para el tratamiento y resguardo de información digital.

Ambientales:

Desperdicio electrónico: El proyecto contribuye a reducir el desecho prematuro de equipos al centrarse en el mantenimiento predictivo. Esto promueve la optimización de recursos tecnológicos y la disminución del impacto ambiental asociado al reemplazo frecuente de hardware.

Limitaciones del Equipo de Trabajo:

Mano de obra: El proyecto requiere un equipo de trabajo cualificado con la formación y disponibilidad necesarias para desarrollar, operar e implementar la simulación. En este caso, el equipo cuenta con las competencias y el perfil técnico idóneo, incluyendo conocimientos en tecnologías IoT, inteligencia artificial y ciberseguridad, para construir la arquitectura de red simulada, configurar sensores virtuales y desarrollar módulos de análisis predictivo. Por lo tanto, este ítem no representa una restricción para la viabilidad del proyecto.

Al identificar y abordar estas restricciones desde las primeras fases del diseño, el equipo de ingeniería puede orientar la solución hacia una propuesta más robusta y viable. La solución de simulación propuesta aborda directamente estas limitaciones, ya que se centra en un modelo replicable y adaptable que no requiere grandes inversiones y se ajusta a las capacidades técnicas disponibles.

Metodología

El proyecto se desarrollará bajo un enfoque de simulación aplicada y validación experimental, implementado en un entorno virtual controlado que emula las condiciones reales de un cuarto de telecomunicaciones. El diseño metodológico busca garantizar la reproducibilidad del sistema, la trazabilidad de las pruebas y la integración coherente entre los tres ejes del proyecto: IoT, Inteligencia Artificial y Ciberseguridad.

La ejecución se estructura en cuatro etapas consecutivas, cada una con actividades específicas, herramientas definidas, responsables y entregables concretos.

Etapa 1. Diseño de la arquitectura IoT

En esta fase se realizará la planificación técnica y estructuración del entorno de simulación. Se definirá la topología de red, los tipos de sensores a utilizar y los protocolos de comunicación que permitirán la interconexión de los dispositivos IoT.

- Actividades específicas:
    - Identificación de los parámetros ambientales a monitorear (temperatura, humedad, voltaje, consumo eléctrico, tráfico de red, latencia).
    - Diseño lógico y físico de la red en Cisco Packet Tracer, incorporando routers, switches, servidores y nodos IoT.
    - Configuración inicial de los sensores virtuales y del servidor de base de datos para la recepción de datos en tiempo real.

  - Selección y justificación del protocolo de comunicación (MQTT o HTTP/REST) según las limitaciones del entorno simulado.

- Herramientas: Cisco Packet Tracer, diagramas de red, hojas de cálculo para direccionamiento y fichas técnicas de sensores.

- Entregable: Diagrama completo de la red simulada y configuración base del entorno IoT.

Etapa 2. Integración de ciberseguridad y monitoreo en tiempo real

Esta fase se centrará en fortalecer la seguridad de la arquitectura simulada, incorporando mecanismos de protección, autenticación y cifrado. El objetivo es mitigar vulnerabilidades y garantizar la confidencialidad, integridad y disponibilidad (CIA) de la información.

- Actividades específicas:

  - Configuración de firewalls simulados y listas de control de acceso (ACL) en routers y switches virtuales.

  - Aplicación de segmentación de red mediante VLANs para aislar zonas críticas de monitoreo.

  - Implementación de protocolos de autenticación multifactor para los accesos simulados.

- Herramientas: Cisco Packet Tracer.

- Entregable: Informe técnico de configuración de seguridad y evidencias de pruebas de defensa.

Etapa 3. Análisis predictivo mediante IA

En esta etapa se integrará el componente de Inteligencia Artificial orientado al análisis predictivo. El objetivo es crear un modelo capaz de identificar patrones anómalos en los datos recolectados por los sensores y anticipar posibles fallos.

- Actividades específicas:
    - Extracción, limpieza y normalización de los datos generados por la simulación IoT.
    - Asociación de herramientas de IA para el análisis predictivo de los datos generados en la simulación
    - Desarrollo de una interfaz de salida (dashboard o script) que muestre en tiempo real el estado de los servidores y las predicciones del sistema.
- Herramientas: Librerías de IA, MySQL o SQLite para almacenamiento de datos.
- Entregable: Modelo predictivo funcional e integrado al sistema de monitoreo.

Etapa 4. Evaluación, validación y documentación final

La última etapa tiene como propósito validar la funcionalidad del sistema de monitoreo, cuantificar los resultados obtenidos y consolidar la documentación técnica y académica del proyecto.

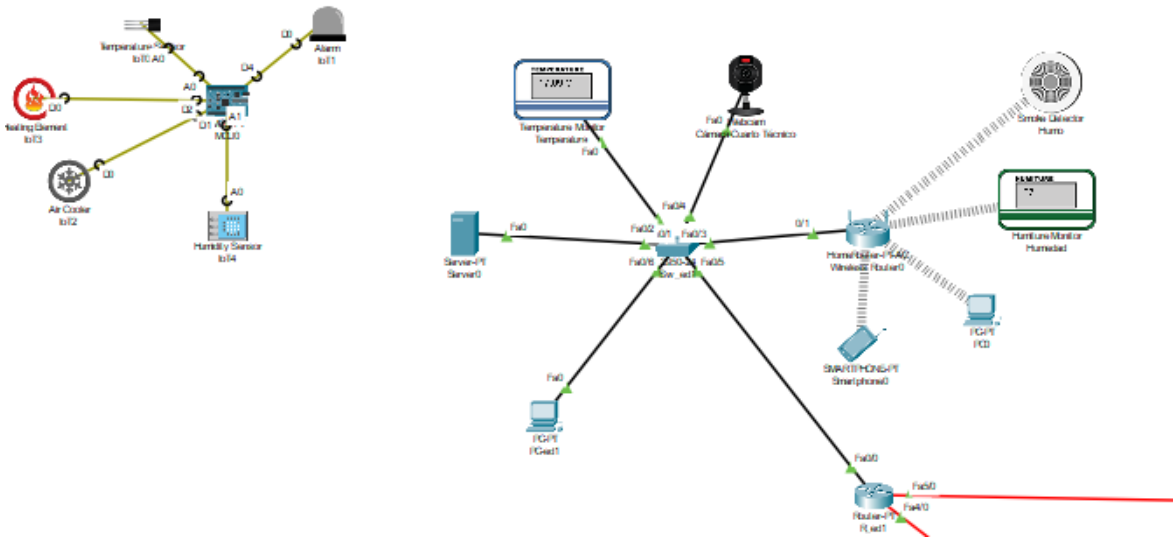
- Actividades específicas:
    - Elaboración del informe técnico y memoria final del proyecto con gráficas, conclusiones y recomendaciones para implementación real.
    - Preparación de la sustentación oral y material visual de apoyo.

Resultados

Infraestructura de red, simulación IoT e integración de mecanismos de ciberseguridad

Una vez realizado el estudio general de los dispositivos necesarios para el funcionamiento correcto de cualquier red de comunicación, se realizó una red que integra hardware de redes y tecnologías IoT que permitan la supervisión en tiempo real de las variables ambientales que puedan llegar a afectar el comportamiento y funcionamiento de estos dispositivos, en la figura #2 se evidencia la composición de la red.

Figura 2: Infraestructura diseñada



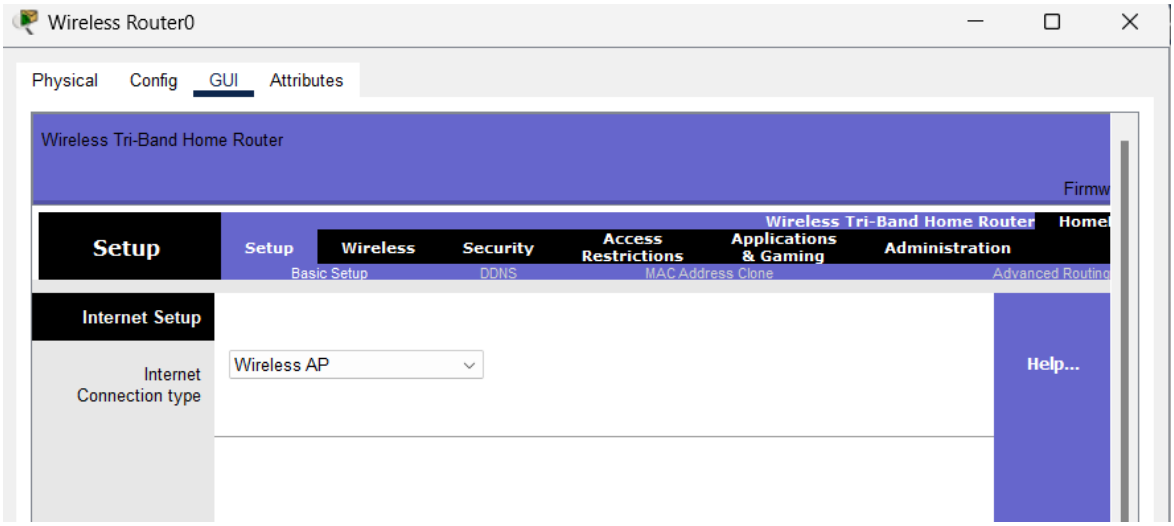
Nota: Elaboración propia (2025).

La red se encuentra dividida en dos segmentos principales, la zona de IoT conformada por el control ambiental que incluye sensores de temperatura, humedad y dispositivos de actuación como el aire acondicionado, y la alarma, por el otro lado se encuentra la administración de red y los dispositivos de monitoreo central, donde se encuentran los datos que se recopilan por los sensores a través de un switch conectado a un

router principal (funcionalidad a gran escala) , que a su vez enlaza con los servidores y dispositivos de los usuarios y administradores que podrán observar el funcionamiento de la red.

Más allá de ver la infraestructura, toca entender el cómo se configuraron los dispositivos para el funcionamiento integral de toda la red y posteriormente el cómo se envían los paquetes de datos entre varios edificios a gran distancia. Para esto primero se modifica el servidor Home-Router inalámbrico para que algunos de los dispositivos IoT puedan acceder a la red, para realizar esto se configura una conexión de tipo Wireless AP, un nombre de red, el canal estándar que va a trabajar, un canal de banda ancha y por último el modo de seguridad, la encriptación y la contraseña del dispositivo. Este proceso se puede observar en las imágenes 3,4 y 5.

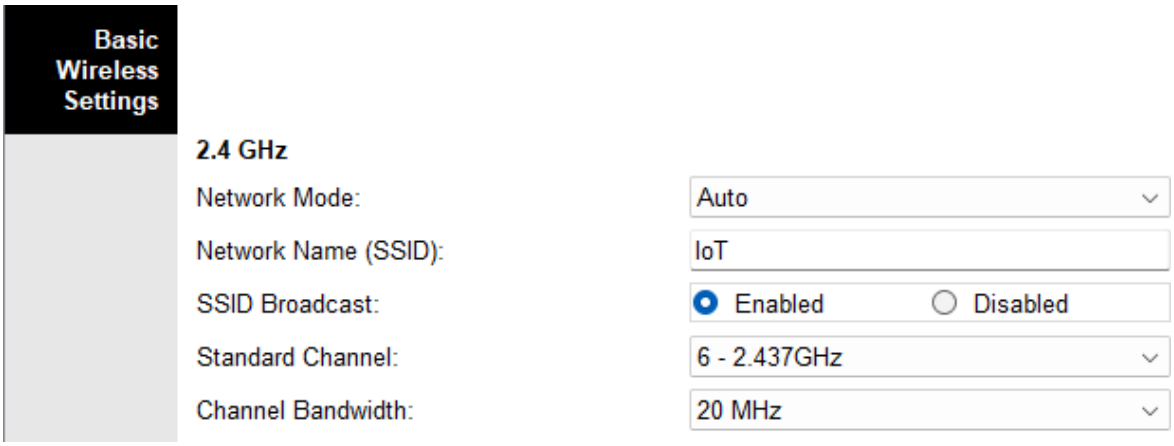
Figura 3: Tipo de conexión



Nota: Elaboración propia (2025). En esta configuración se define el modo de operación del router, el cual ha sido establecido como Wireless Access Point (Wireless AP). Esta modalidad permite que el router funcione como un punto de acceso inalámbrico

dentro de la red IoT, brindando conectividad a los dispositivos inteligentes (sensores, cámaras y monitores) a través de la interfaz Wi-Fi.

Figura 4: Configuración básica de la red inalámbrica

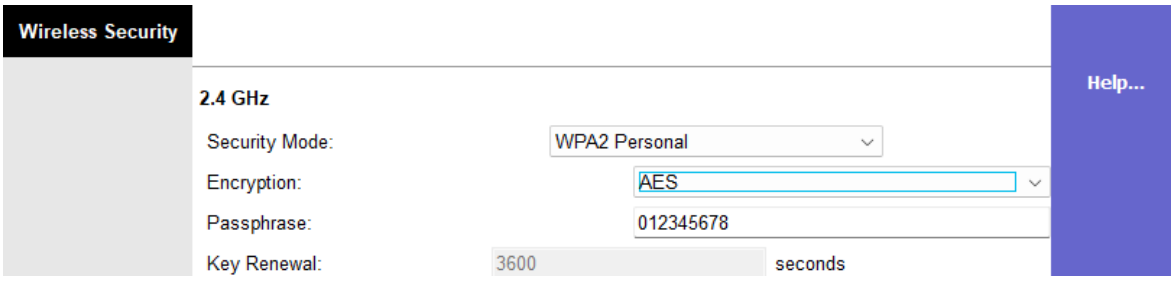


Nota: Elaboración propia (2025).

En esta sección se definen los parámetros fundamentales del enlace Wi-Fi. El modo de red (Network Mode) se configuró en Auto, lo que permite compatibilidad con distintos estándares inalámbricos (802.11b/g/n).

El nombre de la red (SSID) fue designado como IoT, identificando la red específica destinada a los dispositivos del sistema de monitoreo. El SSID Broadcast se mantiene Enabled para que los dispositivos detecten la red y puedan conectarse fácilmente.

Figura 5: Establecer contraseña y tipo de encriptación



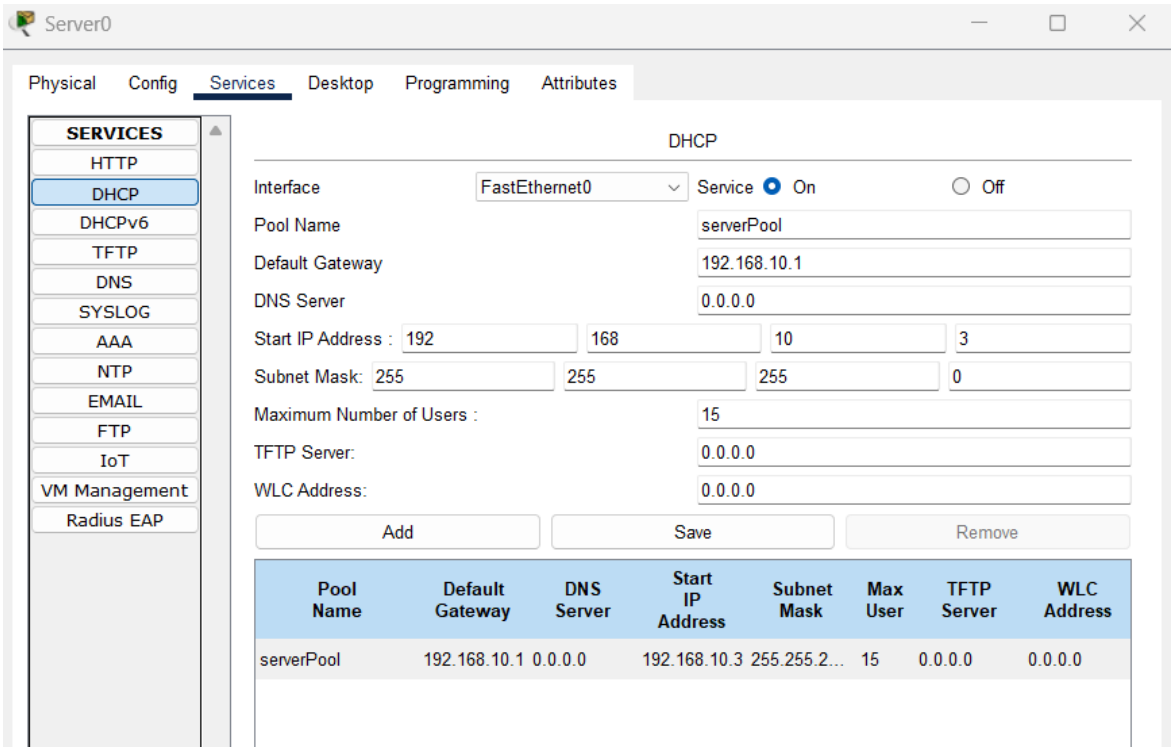
Nota: Elaboración propia (2025). En esta etapa se garantiza la seguridad del enlace inalámbrico mediante la configuración del apartado Wireless Security.

Se seleccionó el modo de seguridad WPA2-Personal con cifrado AES (Advanced Encryption Standard), considerado uno de los estándares más seguros para redes locales. La contraseña de acceso (Passphrase) fue definida como 012345678, la cual permite autenticar el ingreso de los dispositivos IoT a la red inalámbrica.

El parámetro de renovación de clave (Key Renewal) se estableció en 3600 segundos, lo que implica una actualización automática de las claves de cifrado cada hora, reforzando la integridad de la comunicación.

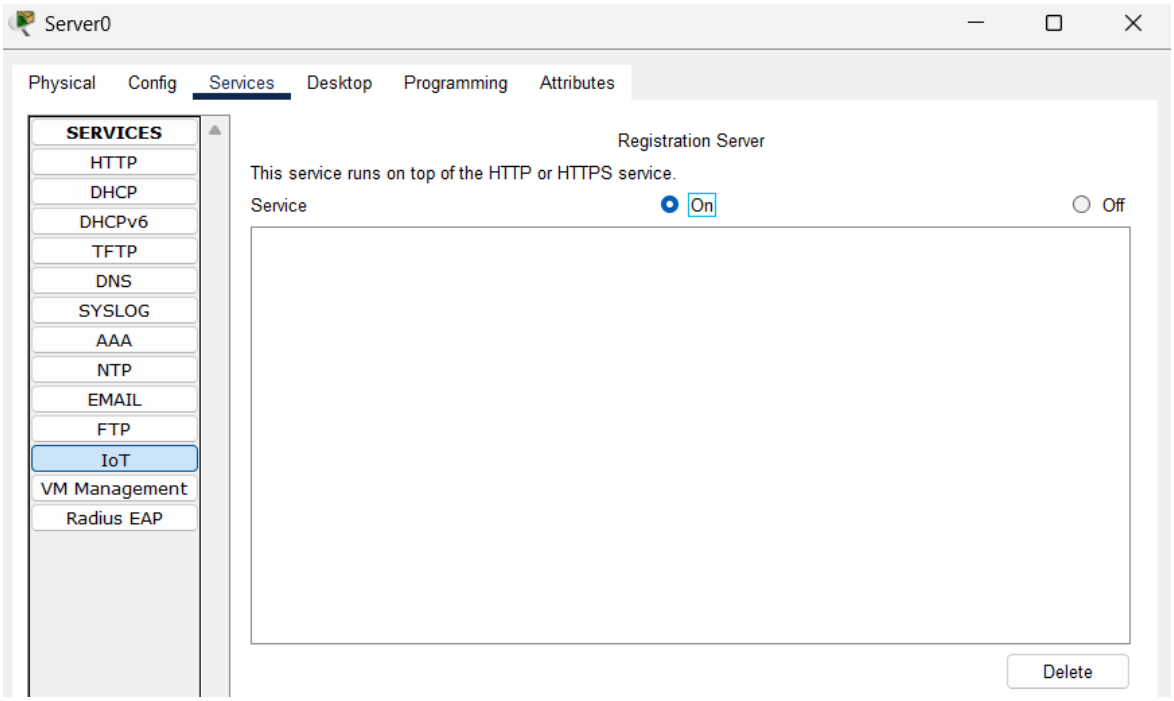
Una vez establecida la conexión por cable e inalámbrica a toda la red, se configura el servidor para que haga un direccionamiento IP de tipo DHCP (Protocolo de configuración dinámica de Host), con una dirección estática para sí mismo la cual es 163.70.0.1 y definiendo una dirección inicial para el protocolo de 163.70.0.10 y un máximo de dispositivos de 15, como se puede observar en la imagen 6, además de esto se establece en el apartado de servicios el protocolo IoT que permitirá dar acceso a estos dispositivos a las direcciones HTTP y HTTPS que se definan en el servidor, como se puede observar en la imagen 7.

Figura 6: Configuración dinámica DCHP



Nota: Elaboración propia (2025).

Figura 7: Acceso dispositivos IoT

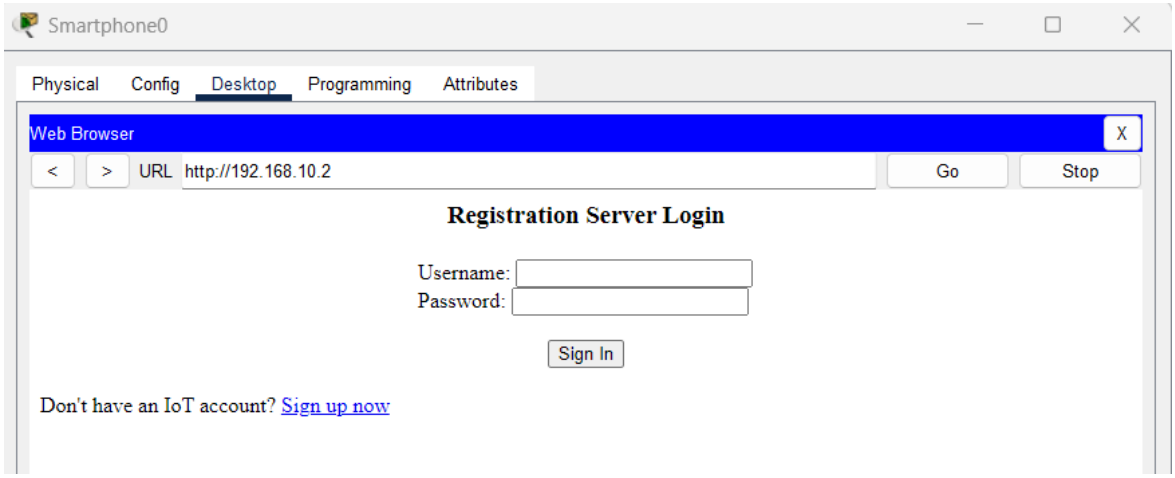


Nota: Elaboración propia (2025).

Con la configuración del router y servidor de la red, se va a crear un registro con acceso a la visualización del monitoreo de los componentes del cuarto, para esto se accede desde un dispositivo como un PC o un Smartphone de la red al apartado de Web Browser y en la barra de búsqueda se coloca la dirección IP del servidor, en nuestro caso 163.70.152.35 al colocarla sale la interfaz mostrada en la imagen 8 donde se registra un usuario nuevo, a pesar del registro, el usuario no va a poder entrar a ver el estado de los dispositivos hasta que sea asignado el permiso, para esto se entra en la configuración de cada dispositivo IoT y en su configuración en el apartado de IoT server se selecciona la opción Remote Server, estableciendo comunicación directa con un servidor remoto que centraliza los datos de todos los sensores IoT. El campo Server Address (163.70.152.35) representa la dirección IP del servidor de monitoreo, al cual el sensor envía periódicamente los valores de detección de humo. Para la autenticación y registro del dispositivo, se asignan las credenciales de usuario: User Name: AdminTest, Password: Admin

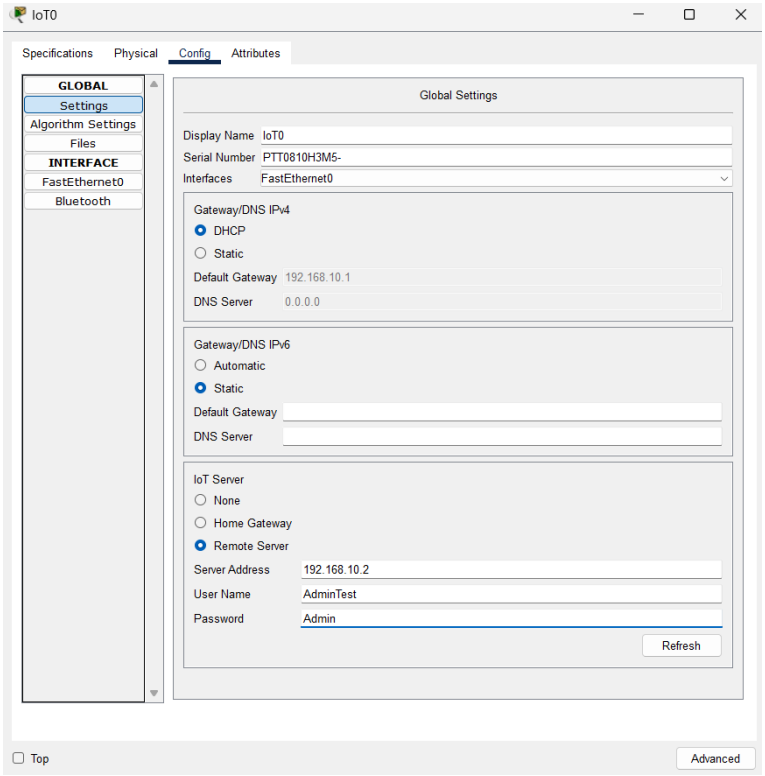
Esta configuración garantiza que el sensor pueda transmitir la información de manera segura al sistema de control, permitiendo generar alertas automáticas en caso de detectar humo o incendios. Además, esta arquitectura posibilita la gestión remota, ya que el servidor IoT puede recibir, almacenar y visualizar los datos a través de una interfaz centralizada o una aplicación móvil vinculada al sistema, así como garantizar la seguridad de que solo los administradores de la red puedan dar permiso a las personas que pueden acceder a esta información

Figura 8: Registro de usuario en HTTP del servidor



Nota: Elaboración propia (2025).

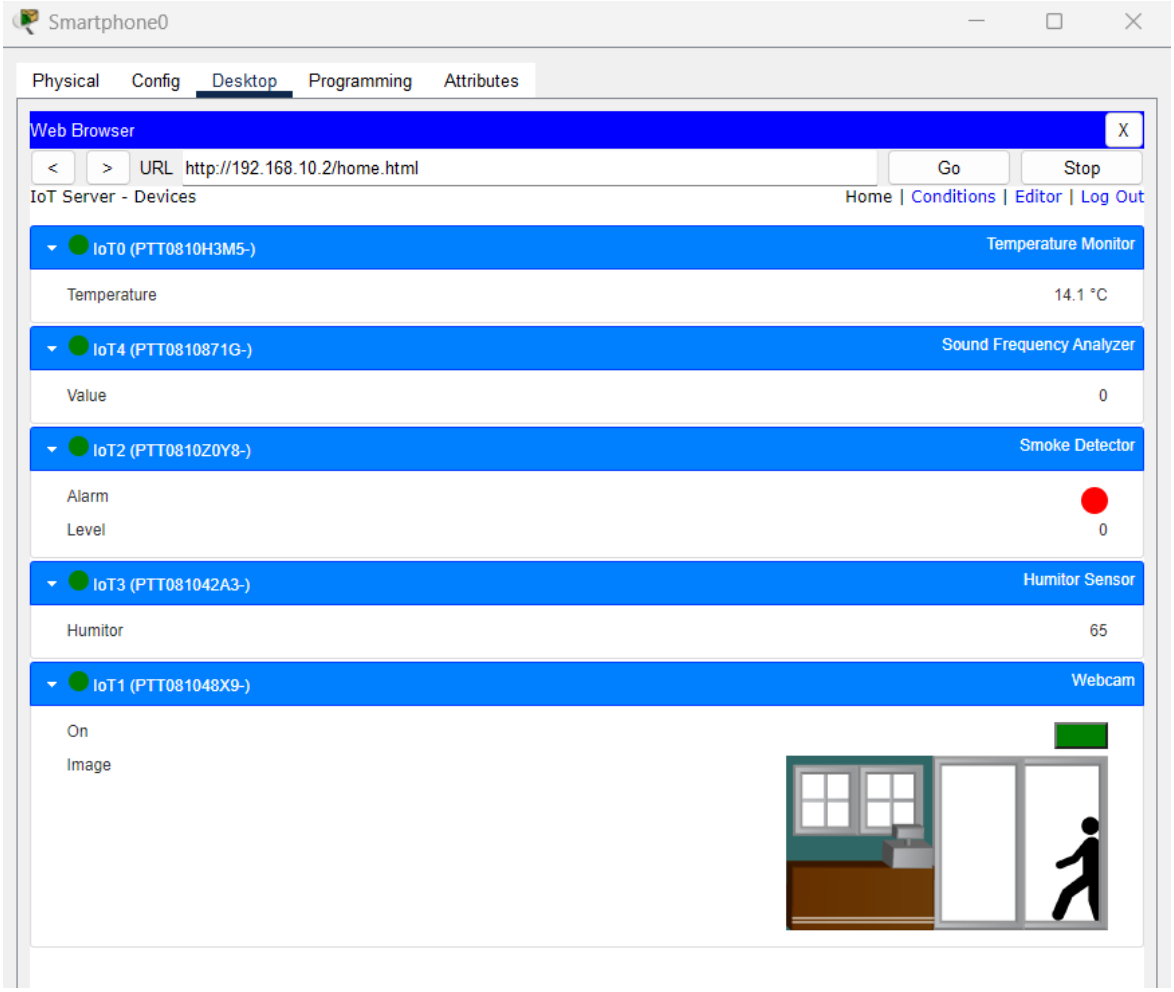
Figura 9: Configuración de los dispositivos IoT



Nota: Elaboración propia (2025).

Una vez realizado este control de accesos, el usuario puede ingresar con sus credenciales y observar el estado ambiental del cuarto técnico y si hay alguna anomalía, como se puede observar en la imagen 10.

Figura 10: Estado de las variables ambientales de la infraestructura de red



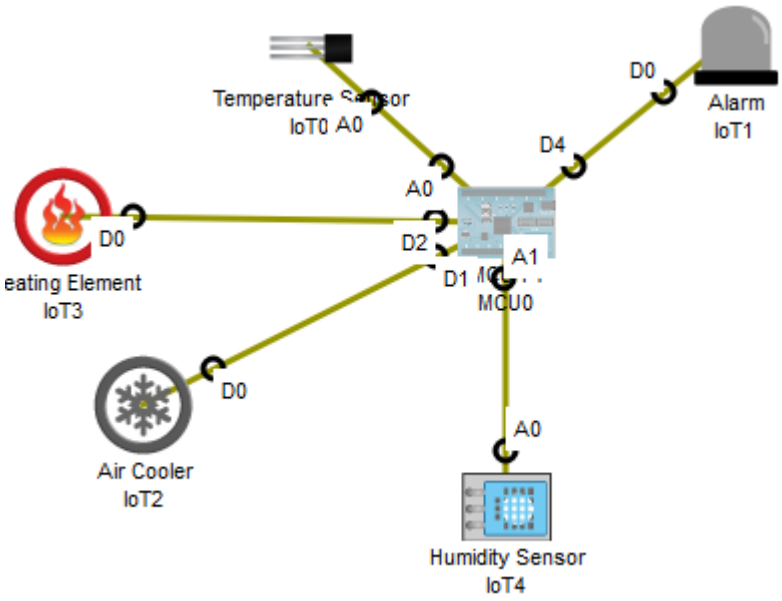
Nota: Elaboración propia (2025).

Por último, se realiza una conexión entre un microcontrolador y los sensores ambientales para que envíen los datos y sean analizados mediante un código de programación y así mismo que los actuadores entren en acción en caso tal de estar en un rango inhabitual, para esto se hace la conexión de los sensores, alarmas, y un sistema dual

de calefacción, se hace la conexión a las entradas analógicas A0 y A1, y a las salidas digitales del controlador dual, esto se puede evidenciar en la imagen #11. Una vez realizada la conexión se accede a la programación del microcontrolador y se hace la codificación que se puede observar dentro del anexo de Cisco Packer Tracer.

El código controla el sistema automático de climatización, lee la temperatura y la humedad mediante los sensores, consulta por red el consumo eléctrico desde un medidor de potencia y, según los datos que llegan, decide activar los accionadores para mantener en un rango correcto los dispositivos hasta que llegue una persona a revisarlo.

Figura 11: Conexión de microcontrolador



Nota: Elaboración propia (2025).

Se puede evidenciar un sistema de control de clima automatizado en el que un microcontrolador (MCU0) recibe información de un sensor de temperatura y un sensor de humedad, y según esos datos activa diferentes dispositivos. Si la temperatura es baja,

enciende el calentador; si es alta, activa el aire acondicionado. Además, una alarma se conecta para avisar cuando los valores están fuera del rango normal. En conjunto, este circuito permite mantener condiciones ambientales estables mediante la lectura de sensores y el control automático de los actuadores.

Integración de mecanismos de ciberseguridad

Una vez configurada y verificado el funcionamiento de toda la infraestructura, se realiza una configuración en los routers que conectan entre varios edificios (según la simulación) unos estándares básicos de ciberseguridad para bloquear y permitir el envío de mensajes a través de la red, esto se realiza entrando al command line interface del router y se establecen parámetros de red y reglas de control de tráfico, en un firewall ASA, se configuran dos interfaces principales, la interna (inside) y la externa (outside). La interfaz interna se asigna a la red confiable con el nivel de seguridad 100 y la dirección IP 163.70.0.2, mientras que la externa se asigna a la red pública con el nivel de seguridad 0 y la dirección IP 200.10.10.2, esto permite que el dispositivo controle el flujo de información entre las redes, garantizando a la protección de la red interna frente a amenazas externas y gestionando las políticas de acceso.

Por otro lado, el router se crean listas de control de acceso (ACL) para permitir a la comunicación ICMP, utilizada en las pruebas de conectividad. Se configura mediante el comando Access-list 101 permit icmp any any echo y Access-list 101 permit icmp any any echo-reply autorizando tanto las solicitudes de eco como las respuestas de eco entre cualquier origen de destino dentro de la misma red. Así se logra que el tráfico básico de

diágnostico pueda fluir entre dispositivos, mientras el firewall gestiona la seguridad general de las conexiones entre las redes internas y externas.

Análisis predictivo mediante IA

Para el desarrollo del proyecto se diseñó e implementó una base de datos relacional en MySQL, con el propósito de almacenar y gestionar la información generada por los sensores simulados en el entorno de trabajo.

La base de datos cumple la función de centralizar los registros de temperatura, humedad y alertas generadas por los módulos de simulación e inteligencia artificial, garantizando la trazabilidad, integridad y consistencia de los datos.

La implementación se realizó en el entorno de línea de comandos de MySQL 8.0, configurado localmente. A continuación, se describen los pasos técnicos, comandos ejecutados y resultados obtenidos que evidencian la correcta creación, configuración y prueba de la base de datos.

Acceso al entorno MySQL: Se accedió al motor MySQL mediante el cliente de línea de comandos, autenticándose con el usuario administrador configurado durante la instalación.

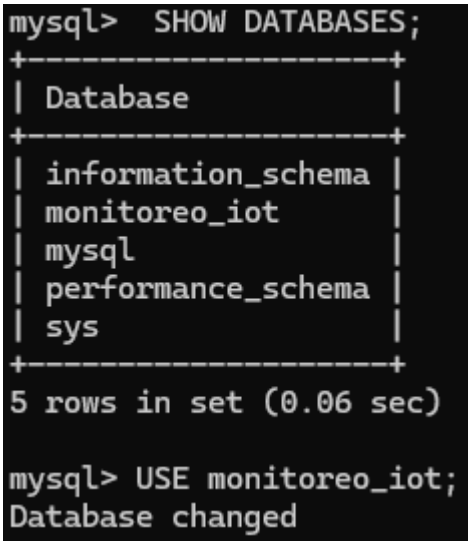
Figura 12: Acceso a entorno MySQL

```
Enter password: ********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.43 MySQL Community Server - GPL

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

Nota: Elaboración propia (2025).

Creación y verificación de la base de datos: Se creó la base de datos monitoreo_iot destinada a almacenar las lecturas y configuraciones del sistema simulado. Posteriormente, se verificó su creación con el comando “SHOW DATABASES”. Y posteriormente se activó el uso de la base creada para ejecutar las operaciones dentro de su contexto.

Figura 13: Creación y verificación de base de datos



Nota: Elaboración propia (2025).

Creación de la estructura de tablas: Se implementaron tres tablas relacionales con claves primarias y foráneas que garantizan integridad referencial:

- **Sensores:** registro de los dispositivos virtuales.
- **Lecturas:** almacenamiento de los valores obtenidos.
- **Alertas:** notificaciones generadas por condiciones críticas.

Comandos ejecutados:

```
CREATE TABLE sensores ( id_sensor INT AUTO_INCREMENT PRIMARY KEY,
    nombre VARCHAR(50), tipo VARCHAR(30), ubicacion VARCHAR(100), estado
    VARCHAR(20) );

CREATE TABLE lecturas ( id_lectura INT AUTO_INCREMENT PRIMARY KEY,
    id_sensor INT, valor FLOAT, unidad VARCHAR(10), fecha_hora DATETIME,
    FOREIGN KEY (id_sensor) REFERENCES sensores(id_sensor) );

CREATE TABLE alertas ( id_alerta INT AUTO_INCREMENT PRIMARY KEY,
    id_sensor INT, descripcion VARCHAR(255), nivel VARCHAR(20), fecha_hora
    DATETIME, FOREIGN KEY (id_sensor) REFERENCES sensores(id_sensor) );
```

Verificación de la estructura creada: Se comprobó la existencia de las tablas y sus campos. Las tres tablas (sensores, lecturas, alertas) se listan correctamente, y su estructura coincide con el modelo diseñado.

Figura 14: Verificación estructura creada

```
mysql> SHOW TABLES;
+------------------------+
| Tables_in_monitoreo_iot |
+------------------------+
| alertas                |
| lecturas               |
| sensores               |
+------------------------+
3 rows in set (0.00 sec)

mysql> DESCRIBE sensores;
+-----------+--------------+------+-----+---------+----------------+
| Field     | Type         | Null | Key | Default | Extra          |
+-----------+--------------+------+-----+---------+----------------+
| id_sensor | int          | NO   | PRI | NULL    | auto_increment |
| nombre    | varchar(50)  | YES  |     | NULL    |                |
| tipo      | varchar(30)  | YES  |     | NULL    |                |
| ubicacion | varchar(100) | YES  |     | NULL    |                |
| estado    | varchar(20)  | YES  |     | NULL    |                |
+-----------+--------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)
```

Nota: Elaboración propia (2025).

Inserción de datos de prueba: Se realizaron pruebas de inserción para validar la operatividad del modelo relacional.

Comandos ejecutados:

```
INSERT INTO sensores (nombre, tipo, ubicacion, estado) VALUES ('Sensor Temperatura 1', 'Temperatura', 'Servidor Principal', 'Activo'), ('Sensor Humedad 1', 'Humedad', 'Rack de Red', 'Activo');

INSERT INTO lecturas (id_sensor, valor, unidad, fecha_hora) VALUES (1, 28.7, '°C', NOW()), (2, 45.3, '%', NOW());
```

Consulta de datos registrados: Se verificó la correcta inserción y vinculación de registros mediante consultas básicas y combinadas.

Figura 15: Consulta de datos registrados

```
mysql> SELECT * FROM sensores;
+-----------+----------------------+-------------+--------------------+--------+
| id_sensor | nombre               | tipo        | ubicacion          | estado |
+-----------+----------------------+-------------+--------------------+--------+
|         1 | Sensor Temperatura 1 | Temperatura | Servidor Principal | Activo |
|         2 | Sensor Humedad 1     | Humedad     | Rack de red        | Activo |
+-----------+----------------------+-------------+--------------------+--------+
2 rows in set (0.01 sec)

mysql> SELECT * FROM lecturas;
+------------+-----------+-------+--------+---------------------+
| id_lectura | id_sensor | valor | unidad | fecha_hora          |
+------------+-----------+-------+--------+---------------------+
|          1 |         1 |  28.7 | °C     | 2025-10-14 14:36:41 |
|          2 |         2 |  45.3 | %      | 2025-10-14 14:36:41 |
+------------+-----------+-------+--------+---------------------+
2 rows in set (0.00 sec)
```

Nota: Elaboración propia (2025).

Figura 16: Consulta de datos registrados #2

```
mysql>
mysql> SELECT s.nombre, l.valor, l.unidad, l.fecha_hora
    -> FROM sensores s
    -> JOIN lecturas l ON s.id_sensor = l.id_sensor;
+----------------------+-------+--------+---------------------+
| nombre               | valor | unidad | fecha_hora          |
+----------------------+-------+--------+---------------------+
| Sensor Temperatura 1 |  28.7 | °C     | 2025-10-14 14:36:41 |
| Sensor Humedad 1     |  45.3 | %      | 2025-10-14 14:36:41 |
+----------------------+-------+--------+---------------------+
2 rows in set (0.00 sec)
```

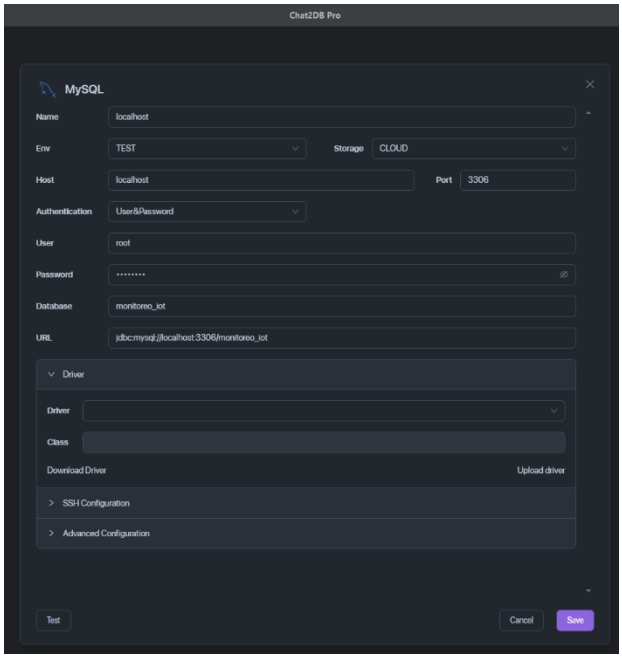
Nota: Elaboración propia (2025).

Análisis predictivo IA

La integración de la Inteligencia Artificial (Chat2DB) con la base de datos se realizó mediante la configuración de un entorno relacional usando MySQL para centralizar

la información generada por los sensores virtuales del simulador. Esta base de datos, denominada ‘monitoreoiot’, almacena los registros de temperatura, humedad y alertas que los módulos de IA generan, garantizando la trazabilidad y consistencia de los datos. La estructura implementada contiene tres tablas principales: sensores, lecturas y alertas, vinculadas por claves foráneas para mantener la integridad referencial

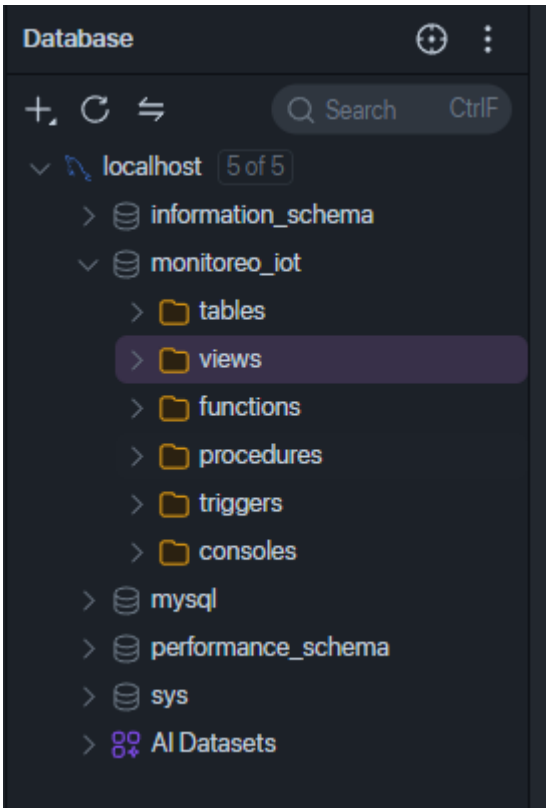
Figura 177: Conexión de la base de datos con la IA



Nota: Elaboración propia (2025).

Para la vinculación de la IA, se definieron puerto, usuario y contraseña de la base de datos en la aplicación de Chat2DB y se verificó la conexión con la misma

Figura 188: Verificación de la conectividad



Nota: Elaboración propia (2025).

Una vez conectada, se muestran los datos tomados directamente de la vinculación con la base de datos, como se muestra en la figura

Figura 199: Lecturas tomadas#1

	id_lectura	id_sensor	valor	unidad	fecha_hora
1	21	1	34.59	°C	2025-10-31 12:07:40
2	22	2	43.49	%	2025-10-31 12:07:40
3	19	1	30.81	°C	2025-10-31 12:06:40
4	20	2	45.23	%	2025-10-31 12:06:40
5	17	1	26.5	°C	2025-10-31 12:05:40
6	18	2	61.92	%	2025-10-31 12:05:40
7	15	1	27.74	°C	2025-10-31 12:04:40
8	16	2	48.47	%	2025-10-31 12:04:40
9	13	1	31.5	°C	2025-10-31 12:03:40
10	14	2	57.77	%	2025-10-31 12:03:40

Nota: Elaboración propia (2025).

Figura 200: Lecturas tomadas#2

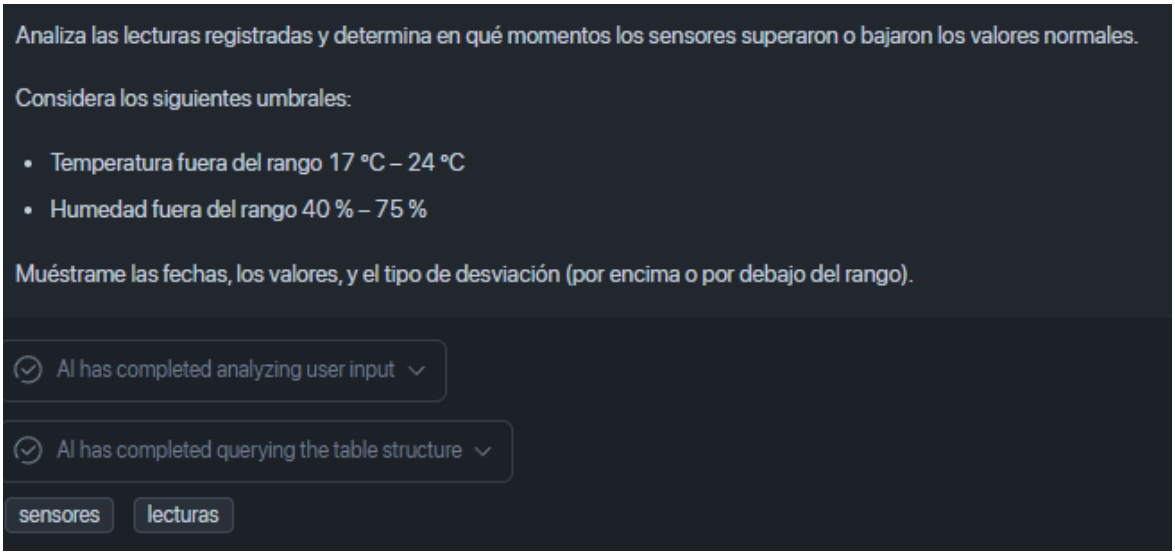
	id_lectura	id_sensor	valor	unidad	fecha_hora
13	9	1	28.68	°C	2025-10-31 12:01:40
14	10	2	67.63	%	2025-10-31 12:01:40
15	7	1	29.35	°C	2025-10-31 12:00:40
16	8	2	47.47	%	2025-10-31 12:00:40
17	5	1	26.31	°C	2025-10-31 11:59:40
18	6	2	56.01	%	2025-10-31 11:59:40
19	3	1	25.57	°C	2025-10-31 11:58:40
20	4	2	60.03	%	2025-10-31 11:58:40
21	1	1	28.7	°C	2025-10-14 14:36:41
22	2	2	45.3	%	2025-10-14 14:36:41

Nota: Elaboración propia (2025).

Análisis de la IA en la base de datos

En la imagen # se evidencia la instrucción inicial que da origen al análisis automatizado de lecturas provenientes de sensores IoT. El objetivo del proceso consiste en identificar los momentos en los que los sensores registran valores fuera de los rangos normales establecidos. Para ello, se definen los umbrales de control: temperatura fuera del rango de 17 °C a 24 °C y humedad fuera del rango de 40 % a 75 %. La solicitud requiere mostrar las fechas, los valores y el tipo de desviación (por encima o por debajo del rango).

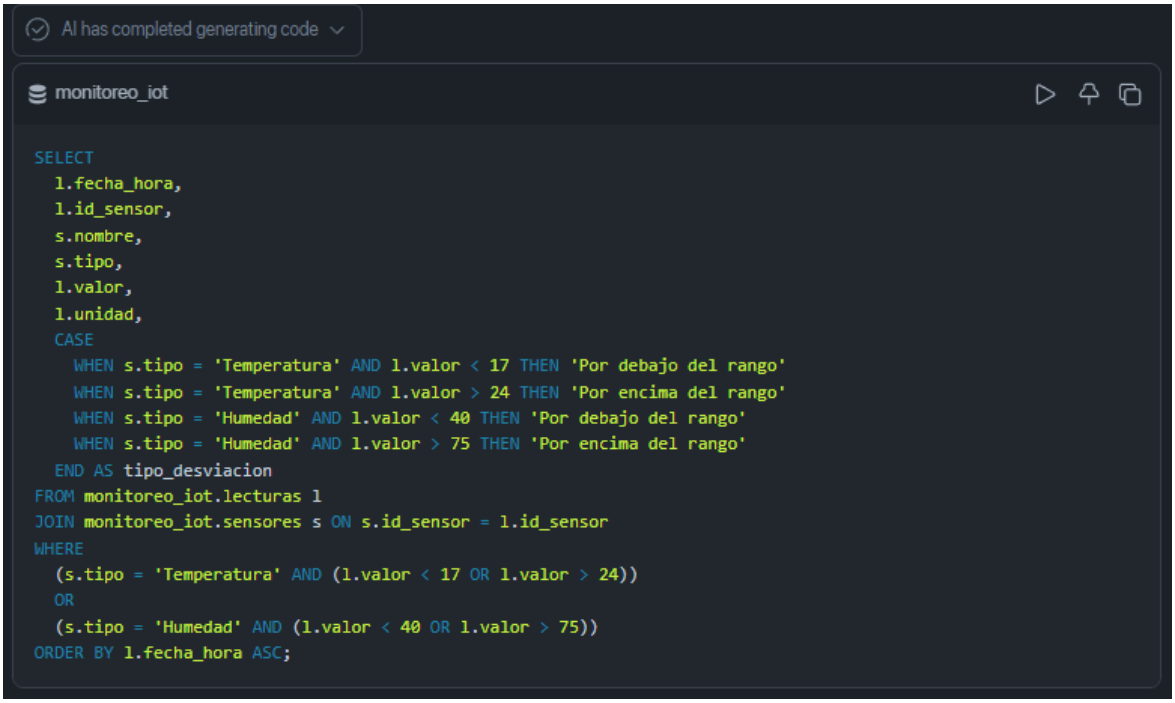
Figura 211: Promt#1 análisis de las lecturas



Nota: Elaboración propia (2025).

Al lanzar el prompt con los rangos, la consulta la IA selecciona las columnas relevantes de las tablas lecturas y sensores, y aplica una estructura condicional CASE para clasificar cada registro según si el valor del sensor se encuentra por debajo o por encima del rango permitido. La unión de ambas tablas (JOIN) permite relacionar las lecturas con la información de identificación del sensor, y el filtro WHERE asegura que solo se muestren las lecturas anómalas. Esta automatización demuestra cómo la IA interpreta lenguaje natural y lo traduce en una consulta SQL funcional y precisa, esto se puede evidenciar en la imagen #.

Figura 222: Código proporcionado por IA



Nota: Elaboración propia (2025).

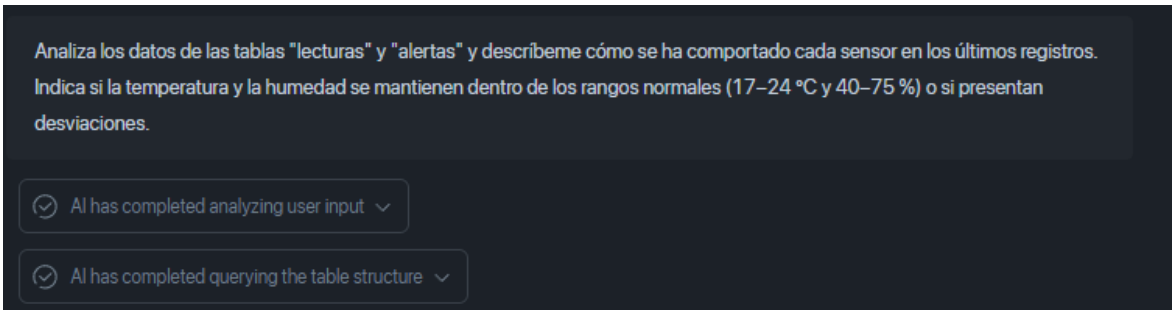
Figura 233: Resultado Visualización de análisis

fecha_hora	id_sensor	nombre	tipo	valor	unidad	tipo_desviacion
2025-10-31 13:16:53	1	Sensor Temperatura 1	Temperatura	24.37	°C	Por encima del rango
2025-10-31 13:17:53	2	Sensor Humedad 1	Humedad	75.11	%	Por encima del rango
2025-10-31 13:19:53	2	Sensor Humedad 1	Humedad	38.26	%	Por debajo del rango
2025-10-31 13:28:53	1	Sensor Temperatura 1	Temperatura	26.06	°C	Por encima del rango
2025-10-31 13:28:53	2	Sensor Humedad 1	Humedad	39.26	%	Por debajo del rango
2025-10-31 13:31:53	1	Sensor Temperatura 1	Temperatura	26.39	°C	Por encima del rango
2025-10-31 13:35:53	1	Sensor Temperatura 1	Temperatura	15.3	°C	Por debajo del rango
2025-10-31 13:37:53	1	Sensor Temperatura 1	Temperatura	25.29	°C	Por encima del rango
2025-10-31 13:39:15	1	Sensor Temperatura 1	Temperatura	24.24	°C	Por encima del rango
2025-10-31 13:39:15	2	Sensor Humedad 1	Humedad	39.42	%	Por debajo del rango

Nota: Elaboración propia (2025).

Una vez dados los valores por la IA, se realiza un nuevo requerimiento que analice los datos combinados de las tablas para describir el comportamiento reciente de cada sensor, verificando si los valores se mantienen dentro de los rangos normales o presentan desviaciones. Este paso amplía el análisis, incorporando las alertas generadas por el sistema de monitoreo.

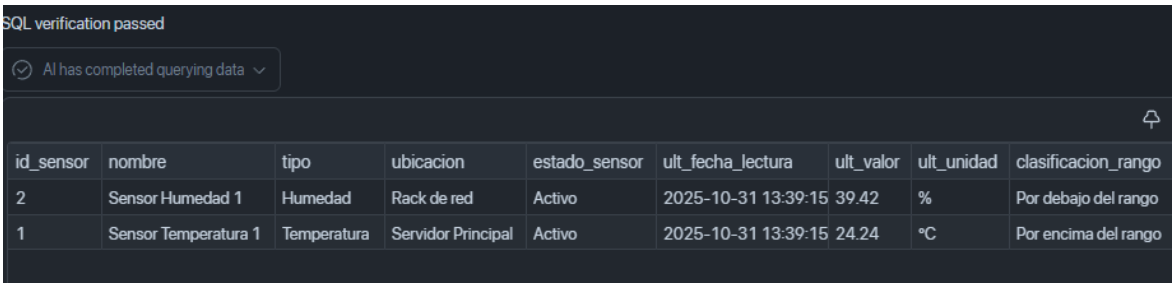
Figura 244: Promt#2 Comportamiento sensores



Nota: Elaboración propia (2025).

En la imagen #, se puede observar los resultados del análisis, donde se evidencia que los dos sensores activos: Sensor Humedad 1, ubicado en el “Rack de red”, y Sensor Temperatura 1, ubicado en el “Servidor Principal”. Ambos se encuentran en estado activo y con lecturas recientes. Los datos revelan que la humedad presenta 39.42 %, situándose por debajo del rango establecido, mientras que la temperatura alcanza 24.24 °C, ubicándose por encima del rango máximo permitido. Esto confirma que ambos sensores presentan desviaciones actuales, reflejando un desbalance ambiental en el cuarto técnico.

Figura 255: Resultado comportamiento sensores


SQL verification passed

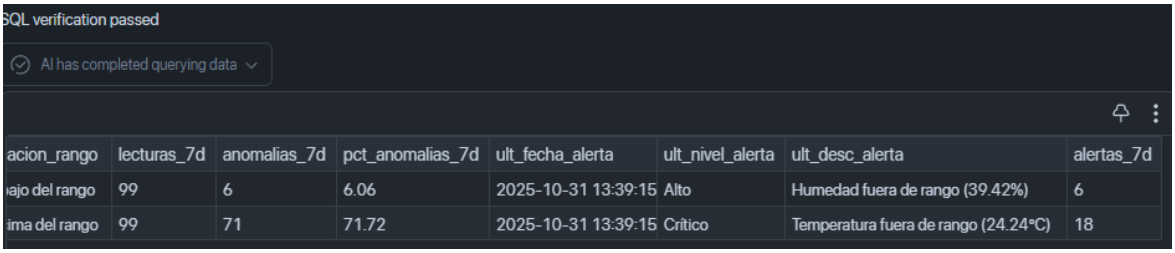
AI has completed querying data

id_sensor	nombre	tipo	ubicacion	estado_sensor	ult_fecha_lectura	ult_valor	ult_unidad	clasificacion_rango
2	Sensor Humedad 1	Humedad	Rack de red	Activo	2025-10-31 13:39:15	39.42	%	Por debajo del rango
1	Sensor Temperatura 1	Temperatura	Servidor Principal	Activo	2025-10-31 13:39:15	24.24	°C	Por encima del rango

Nota: Elaboración propia (2025).

Además de las lecturas recientes, la IA realiza una tabla de alertas que muestra las estadísticas de las anomalías registradas en la ultima semana, se puede observar en la imagen # que las desviaciones por debajo del rango (principalmente en humedad) representan un 6.06 % de las lecturas, mientras que las desviaciones por encima del rango (relacionadas con la temperatura) alcanzan un 71.72 %, clasificadas como de nivel crítico. La IA también identifica el nivel de severidad de las alertas: “Alto” para los valores bajos de humedad y “Crítico” para los excesos de temperatura. Estos resultados indican una tendencia clara de sobrecalentamiento en el entorno monitoreado.

Figura 266: Resultado comportamiento sensores#2


SQL verification passed

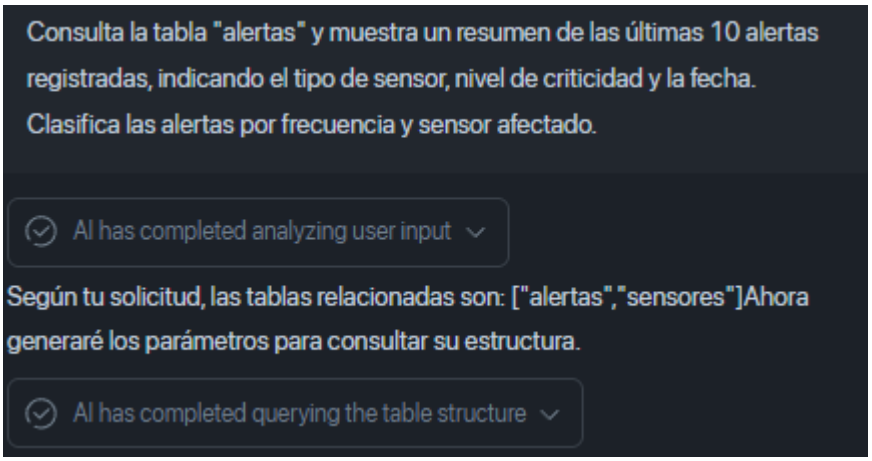
AI has completed querying data

acion_rango	lecturas_7d	anomalias_7d	pct_anomalias_7d	ult_fecha_alerta	ult_nivel_alerta	ult_desc_alerta	alertas_7d
ajo del rango	99	6	6.06	2025-10-31 13:39:15	Alto	Humedad fuera de rango (39.42%)	6
ima del rango	99	71	71.72	2025-10-31 13:39:15	Crítico	Temperatura fuera de rango (24.24°C)	18

Nota: Elaboración propia (2025).

Luego se realiza otra instrucción para que se consulte la tabla “alertas” y genere un resumen de las últimas 10 alertas registradas, indicando el tipo de sensores, nivel de criticidad y la fecha, como se puede evidenciar en la imagen #.

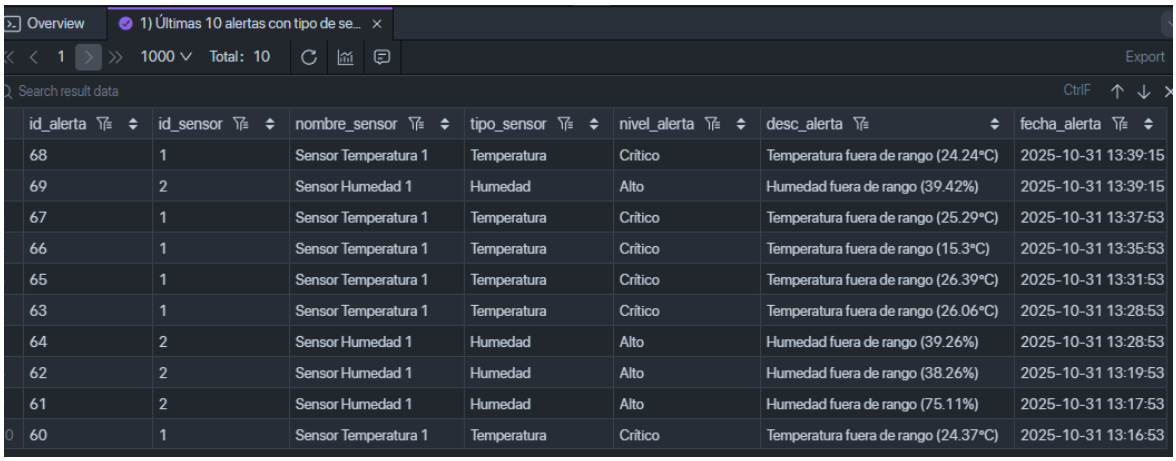
Figura 277: Prompt #3 Alertas registradas



Nota: Elaboración propia (2025).

En la imagen # se muestra la ejecución de dicha consulta, donde se listan las últimas diez alertas activas. Se pueden observar alertas de tipo Crítico para el Sensor Temperatura 1, con descripciones como “Temperatura fuera de rango (24.24 °C)” y “Temperatura fuera de rango (26.06 °C)”, y alertas de tipo Alto para el Sensor Humedad 1, con lecturas de 39.26 % y 75.11 %. Esta evidencia permite visualizar con claridad los momentos más recientes en los que ambos sensores han sobrepasado los límites normales, demostrando que las fluctuaciones son recurrentes y que el sistema de alerta se encuentra funcionando de manera efectiva

Figura 288: Resultado alertas registradas

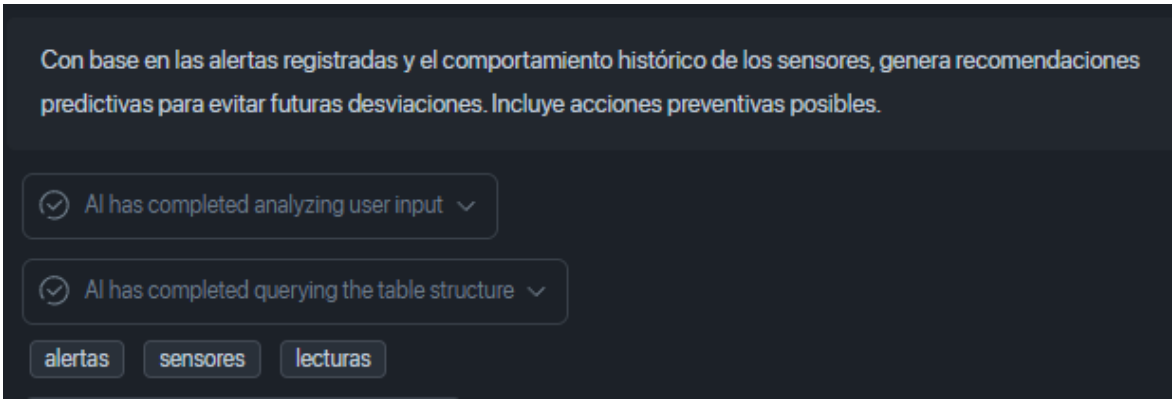


id_alerta	id_sensor	nombre_sensor	tipo_sensor	nivel_alerta	desc_alerta	fecha_alerta
68	1	Sensor Temperatura 1	Temperatura	Crítico	Temperatura fuera de rango (24.24°C)	2025-10-31 13:39:15
69	2	Sensor Humedad 1	Humedad	Alto	Humedad fuera de rango (39.42%)	2025-10-31 13:39:15
67	1	Sensor Temperatura 1	Temperatura	Crítico	Temperatura fuera de rango (25.29°C)	2025-10-31 13:37:53
66	1	Sensor Temperatura 1	Temperatura	Crítico	Temperatura fuera de rango (15.3°C)	2025-10-31 13:35:53
65	1	Sensor Temperatura 1	Temperatura	Crítico	Temperatura fuera de rango (26.39°C)	2025-10-31 13:31:53
63	1	Sensor Temperatura 1	Temperatura	Crítico	Temperatura fuera de rango (26.06°C)	2025-10-31 13:28:53
64	2	Sensor Humedad 1	Humedad	Alto	Humedad fuera de rango (39.26%)	2025-10-31 13:28:53
62	2	Sensor Humedad 1	Humedad	Alto	Humedad fuera de rango (38.26%)	2025-10-31 13:19:53
61	2	Sensor Humedad 1	Humedad	Alto	Humedad fuera de rango (75.11%)	2025-10-31 13:17:53
60	1	Sensor Temperatura 1	Temperatura	Crítico	Temperatura fuera de rango (24.37°C)	2025-10-31 13:16:53

Nota: Elaboración propia (2025).

Para finalizar, la IA hace una recomendación de acciones preventivas que se pueden realizar en base a las alertas que se registran en los pasos anteriores.

Figura 299: Prompt #4 Recomendaciones predictivas



Nota: Elaboración propia (2025).

Al hacer la lectura, la IA realiza las siguientes recomendaciones predictivas:

Sensor temperatura:

Acción principal: Calibrar sensor de temperatura; revisar HVAC/ventilación y aislamiento; programar mantenimiento preventivo

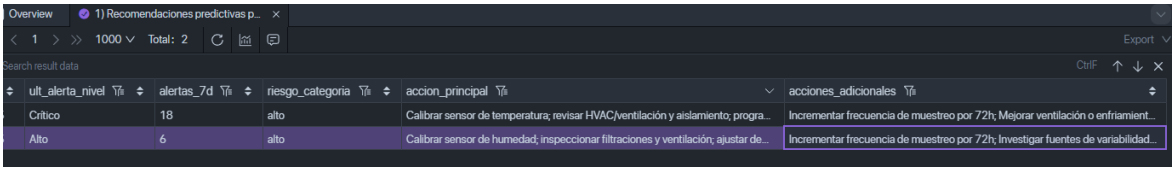
Acciones adicionales: Incrementar frecuencia de muestreo por 72h; Mejorar ventilación o enfriamiento local; Investigar fuentes de variabilidad (aperturas de puertas, procesos)

Sensor humedad:

Acción principal: Calibrar sensor de humedad; inspeccionar filtraciones y ventilación; ajustar deshumidificación

Acciones adicionales: Incrementar frecuencia de muestreo por 72h; Investigar fuentes de variabilidad (aperturas de puertas, procesos)

Figura 30: Resultado de las predicciones



Nota: Elaboración propia (2025).

Costos

Costos directos

Tabla 2: Costos directos

Rol / Concepto	Descripción de actividades	Valor por hora (COP)	Horas estimadas (4 meses)	Costo total (COP)
Especialista en infraestructura IoT	Encargado del desarrollo del sistema de simulación en Cisco Packet Tracer, configuración de dispositivos IoT e integración de sensores virtuales.	$90.000	104 h	$9.360.000
Analista de bases de datos	Diseña y estructura la base de datos del sistema de monitoreo, gestiona la comunicación entre los módulos de simulación y garantiza la integridad de la información almacenada.	$100.000	104 h	$10.400.000
Gerente de proyectos	Planifica, coordina y supervisa las actividades del equipo. Controla tiempos, recursos, cronograma y asegura la calidad técnica y documental del proyecto. Además, consolida los informes y resultados finales.	$120.000	104 h	$12.480.000
Servicios básicos (energía eléctrica e internet)	Consumo energético e internet requeridos para mantener en funcionamiento los equipos de cómputo y la conexión durante el desarrollo del proyecto.	—	—	$560.000
Software de simulación	Uso del entorno Cisco Packet Tracer, licenciado gratuitamente por Cisco Networking Academy para fines educativos.	—	—	$0

Rol / Concepto	Descripción de actividades	Valor por hora (COP)	Horas estimadas (4 meses)	Costo total (COP)
Total costos directos				$32.800.000

El valor total de los costos directos asciende a $32.800.000 COP, concentrándose principalmente en la mano de obra especializada.

El especialista en infraestructura IoT es responsable de la parte técnica y funcional del sistema, garantizando la operatividad del modelo de monitoreo y la correcta interacción entre los sensores virtuales y el entorno de simulación.

El analista de bases de datos asegura el diseño lógico y la consistencia del almacenamiento de la información, integrando los flujos de datos provenientes del sistema IoT con los módulos de análisis predictivo.

Por su parte, el gerente de proyectos cumple un rol estratégico, orientado a la gestión integral del trabajo en equipo, la planificación temporal, la asignación de recursos y la validación técnica de los resultados finales.

Los servicios básicos (energía eléctrica e internet) se incluyen como costos fijos necesarios para la continuidad de las simulaciones y la comunicación entre los miembros del equipo y el asesor.

El software de simulación no representa un gasto monetario, ya que corresponde a una licencia académica gratuita, lo cual contribuye a la sostenibilidad económica del proyecto.

En síntesis, los costos directos reflejan una planificación técnica realista, donde la inversión principal se centra en el capital humano y en el uso eficiente de los recursos tecnológicos, garantizando así la viabilidad académica y económica del sistema de monitoreo automatizado propuesto.

Costos indirectos:

Tabla 3: Costos indirectos

	Descripción	**Costo estimado (COP)**
Imprevistos técnicos	Gastos ocasionales por fallas de software, errores en simulación, reinstalaciones o respaldo de información en la nube.	$200.000
Mantenimiento de equipos	Limpieza, actualización del sistema operativo, instalación de controladores y revisión del rendimiento del computador usado para las simulaciones.	$150.000
Actualización de software	Descarga de nuevas versiones, librerías o herramientas requeridas para mantener la compatibilidad con Python y Cisco Packet Tracer.	$150.000
Subtotal costos indirectos		$500.000

El costo total estimado de los costos indirectos asciende a $500.000 COP, los cuales se destinan principalmente al mantenimiento técnico, actualización de software e imprevistos menores que puedan surgir durante el desarrollo de la simulación. Estos gastos permiten mantener la estabilidad y el correcto funcionamiento de los programas utilizados, garantizando que las herramientas de simulación y análisis operen sin interrupciones.

El mantenimiento del equipo y la actualización de librerías son esenciales para evitar errores de compatibilidad o pérdida de información, aspectos clave en proyectos que

integran componentes de IoT e inteligencia artificial. A pesar de su monto reducido, estos costos representan una inversión estratégica en la confiabilidad y continuidad técnica del proyecto.

Capital de trabajo:

Tabla 4: Capital de trabajo

Concepto	Descripción	Costo estimado (COP)
Fondo operativo	Dinero destinado a cubrir pequeñas necesidades imprevistas (reposición de cables, memorias USB, copias físicas de reportes).	$150.000
Servicios de respaldo digital	Uso de plataformas en la nube (Google Drive, OneDrive, GitHub) o almacenamiento externo para guardar avances y bases de datos.	$100.000
Materiales de apoyo	Impresión de informes, etiquetas o presentaciones finales requeridas para la sustentación.	$100.000
Subtotal costos indirectos		$350.000

El capital de trabajo estimado es de $350.000 COP, destinado a cubrir gastos menores relacionados con la operación, documentación y respaldo del proyecto. Estos recursos permiten garantizar la disponibilidad de materiales básicos como memorias USB, servicios de almacenamiento en la nube y la impresión de informes o presentaciones finales.

Aunque su impacto financiero es limitado, su importancia radica en sostener la organización y seguridad de la información generada durante el desarrollo. De este modo,

el capital de trabajo contribuye a mantener la trazabilidad, respaldo y presentación adecuada de los resultados, fortaleciendo la calidad técnica y académica del proyecto.

Conclusiones

- El desarrollo de este simulador demostró la factibilidad técnica y académica de integrar tecnologías IoT, modelos predictivos de IA y principios de ciberseguridad en el monitoreo automatizado de cuartos de telecomunicaciones.
- La centralización de datos IoT en una base relacional, combinada con la capacidad de análisis predictivo, permite detectar proactivamente anomalías, incrementando la disponibilidad y seguridad de la infraestructura digital.
- La simulación validó que la automatización y monitorización inteligente reduce los tiempos de indisponibilidad y riesgo de fallos, lo que da paso a una potencial reducción de costos operativos y de mantenimiento en escenarios reales
- Adoptar estándares de seguridad en las capas de infraestructura es fundamental para prevenir intrusiones, minimizando las brechas de riesgo asociadas a la proliferación de dispositivos conectados
- La propuesta es replicable y escalable, con opciones de integrar todas las tecnologías en entornos reales y con opciones de cambio según el tamaño, complejidad y criticidad de la infraestructura de la empresa a monitorizar.

Plan de implementación

La implementación de un sistema de monitoreo automatizado de servidores en entornos reales representa un paso fundamental para garantizar la disponibilidad, seguridad y eficiencia operativa de infraestructuras tecnológicas críticas. Este plan surge como respuesta a la necesidad de trasladar los resultados obtenidos en la simulación académica a contextos empresariales y técnicos, donde los desafíos de escalabilidad, interoperabilidad y cumplimiento normativo son más exigentes.

El enfoque propuesto se basa en una metodología estructurada que integra diagnóstico, diseño, instalación, integración de inteligencia artificial y ciberseguridad, capacitación y mejora continua. Cada fase está orientada a asegurar la viabilidad técnica, la sostenibilidad económica y la adaptabilidad a diferentes tipos de infraestructura, permitiendo la detección temprana de fallas, la optimización de recursos y la reducción de tiempos de inactividad en entornos productivos.

Este plan no solo facilita la adopción del sistema en centros de datos y cuartos técnicos, sino que también establece las bases para futuras mejoras y la expansión a otros escenarios de monitoreo, garantizando la trazabilidad, la protección de datos y el cumplimiento de estándares internacionales de seguridad y gestión de TI

1. Diagnostico y levantamiento de infraestructura: Realizar un diagnóstico inicial del cuarto de telecomunicaciones o centro de datos donde se implementará el sistema, con encuestas, revisión documental y auditoría física, para determinar el estado actual de los equipos, redes y riesgos ambientales, asegurando la selección adecuada de sensores y componentes IoT. Además, se debe de definir y priorizar los parámetros críticos a monitorear.
2. Planificación y diseño técnico: Se debe de diseñar una infraestructura lógica y física adaptable al entorno, usando esquemas de red, diagramas y fichas técnicas de los dispositivos, se debe de considerar requisitos de contabilidad, consumo energético y futura expansión para seleccionar hardware adecuado y software en gestión de bases de datos.
3. Instalación de la red IoT y sensores: configurar y hacer pruebas de sistemas de control ambiental automatizados, simulando escenarios de fallo para verificar el funcionamiento de alertas, actuadores y la recolección de datos en tiempo real.

4. Integración de la solución predictiva y ciberseguridad: Implementar el modelo de análisis predictivo mediante IA sobre la base de datos generada en el sistema real, ajustando algoritmos para identificar patrones y emitir alertas tempranas de fallos físicos y lógicos. Al hacer estos pasos se deberá de fortalecer la arquitectura de ciberseguridad con escalabilidad de autenticación multifactorial, certificados digitales, y cifrado extremo a externo (TLS), además de segmentación de la red mediante VLANs, aplicación de firewalls y ACLs (Access Control Lists).
5. Capacitación, pilotos y validación: Formar al personal técnico y administrativo en uso, interpretación y gestión de la plataforma de monitoreo inteligente, poniendo énfasis en respuesta a alertas, incidentes y mantenimiento predictivo.

Referencias

Al Batahari, M. (2020). Servers Room Monitoring System Using Iot. *Engpaper Journal*.

Barra, M., Cillo, T., De Santis, A., Petrillo, U. F., Negro, A., & Scarano, V. (2002). Multimodal monitoring of web servers. *IEEE MultiMedia*, *9*(3), 32-41.

Bhardwaj, A., Dagar, V., Khan, M. O., Aggarwal, A., Alvarado, R., Kumar, M., ... & Proshad, R. (2022). Smart IoT and machine learning-based framework for water quality assessment and device component monitoring. *Environmental Science and Pollution Research*, *29*(30), 46018-46036.

CIS Controls. (2021). *CIS Critical Security Controls v8*. Center for Internet Security.

Dempsey, K. L., Johnson, L. A., Scholl, M. A., Stine, K. M., Jones, A. C., Orebaugh, A., ... & Johnston, R. (2011). Information security continuous monitoring (ISCM) for federal information systems and organizations.

IBM (2024, octubre 11) ¿Qué es la ciberseguridad? *Ibm.com*. https://www.ibm.com/es-es/topics/cybersecurity

Isa, I. S. M., El-Gorashi, T. E., Musa, M. O., & Elmirghani, J. M. (2024). Resilient energy efficient IoT infrastructure with server and network protection for healthcare monitoring applications. *IEEE Access*, *12*, 48910-48940.

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In 2012 10th international conference on frontiers of information technology (pp. 257-260). IEEE.

Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top-Down Approach* (7th ed.). Pearson.

Marchionni, E. A. (2011). *Administrador de servidores* (Vol. 210).

MIRANDA INDIO, M. A. (2023). *ESTUDIO DE FACTIBILIDAD PARA EL MONITOREO DE SERVIDORES MEDIANTE RASPBERRY PI BASADO EN LA INTERNET DE LAS COSAS EN LA UNIDAD INFORMÁTICA DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ* (Bachelor's thesis, Jipijapa-Unesum).

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer networks*, *57*(10), 2266-2279.

Srinivasan, S. (2019). *Cloud Computing Basics*. Springer.

Stallings, W. (2020). *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Addison-Wesley.

Villa Crespo, E., Morales Alonso, I.(2023). *Ciberseguridad IoT y su aplicación en ciudades inteligentes*. Ediciones de la U. https://www-ebooks7-24-com.bdbiblioteca.universidadean.edu.co/?il=35416

Barrio Andrés, M. (2022). Internet de las cosas: (3 ed.). Editorial Reus. https://elibro-net.bdbiblioteca.universidadean.edu.co/es/lc/bibliotecaean/titulos/283884

Gokhale, P., Bhat, O., & Bhat, S. (2018). Introduction to IOT. *International Advanced Research Journal in Science, Engineering and Technology*, *5*(1), 41-44.

Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. (2020). A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors*, *20*(13), 3625. https://doi.org/10.3390/s20133625

Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on internet of things (IoT). *International journal of computer applications*, *113*(1).

Talavera, J. M., Tobón, L. E., Gómez, J. A., Culman, M. A., Aranda, J. M., Parra, D. T., ... & Garreta, L. E. (2017). Review of IoT applications in agro-industrial and environmental fields. *Computers and Electronics in Agriculture*, *142*, 283-297.

Soni, D., & Makwana, A. (2017, April). A survey on mqtt: a protocol of internet of things (iot). In *International conference on telecommunication, power analysis and computing techniques (ICTPACT-2017)* (Vol. 20, No. April, 2017).

Seoane, V., Garcia-Rubio, C., Almenares, F., & Campo, C. (2021). Performance evaluation of CoAP and MQTT with security support for IoT environments. Computer Networks, 197, 108338.

Da Cruz, M. A., Rodrigues, J. J., Lorenz, P., Solic, P., Al-Muhtadi, J., & Albuquerque, V. H. C. (2019). A proposal for bridging application layer protocols to HTTP on IoT solutions. *Future Generation Computer Systems*, *97*, 145-152.

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems, 78*, 964–975.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce

Esteban, A., Zafra, A., & Ventura, S. (2022). Data mining in predictive maintenance systems: A taxonomy and systematic review. *WIREs: Data Mining & Knowledge Discovery*, *12*(5), 1–45. https://doi-org.bdbiblioteca.universidadean.edu.co/10.1002/widm.1471

AlShorman, O., Irfan, M., Saad, N., Zhen, D., Haider, N., Glowacz, A., & AlShorman, A. (2020). A Review of Artificial Intelligence Methods for Condition Monitoring and Fault Diagnosis of Rolling Element Bearings for Induction Motor. *Shock & Vibration*, 1–20. https://doi-org.bdbiblioteca.universidadean.edu.co/10.1155/2020/8843759

Shlash Mohammad, A. A., Khanfar, I. A. A., Al Oraini, B., Vasudevan, A., Mohammad, S. I., & Zhou Fei. (2024). Predictive analytics on artificial intelligence in supply chain optimization. *Data & Metadata*, *3*, 1–9. https://doi-org.bdbiblioteca.universidadean.edu.co/10.56294/dm2024395

Mohamed-Larbi, R., & Daoud, A.-K. (2024). Condition-based maintenance optimisation for multi-component systems using mean residual life. *International Journal of Production Research*, *62*(13), 4831–4855. https://doi-org.bdbiblioteca.universidadean.edu.co/10.1080/00207543.2023.2280882

Buitrón Ruiz, D. F. (2022). Arquitecturas y modelos de referencia para sistemas IoT: Estado del arte de las arquitecturas para sistemas IoT. [Tesis de grado]. Repositorio Digital EPN. https://bibdigital.epn.edu.ec/handle/15000/22368

National Institute of Standards and Technology. (2020). *Consideraciones para la gestión de riesgos a la ciberseguridad y la privacidad de internet de las cosas (IoT)*. NIST. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932207