



**TECNOLÓGICO NACIONAL DE MÉXICO CAMPUS APIZACO
DEPARTAMENTO DE METAL-MECÁNICA
CARRERA DE INGENIERÍA MECATRÓNICA**

REPORTE DE PROYECTO

**TÍTULO DE PROYECTO
IMPLEMENTACIÓN DE SISTEMA DE MONITOREO PARA
CENTROS DE MISIÓN CRÍTICA**

**NOMBRE DEL ALUMNO
CASTILLO CEREZO LUIS ANGEL**

**NO. DE CONTROL
20370701**

**EMPRESA
TEKSAR LABS SA de CV**

**CARRERA
INGENIERIA MECATRONICA**

**SEMESTRE
DECIMO SEMESTRE**



**PERIODO DE REALIZACION
13 DE ENERO AL 16 DE MAYO DEL 2025**



Instituto Tecnológico de Apizaco
Metal-Mecánica

Tzompantepec, Tlaxcala, **13/agosto/2025**

Oficio No. MM-446/2025

Asunto: Liberación de Proyecto para Titulación Integral.

ISRAEL JORGE SÁNCHEZ SÁNCHEZ
JEFE DE LA DIVISIÓN DE ESTUDIOS PROFESIONALES
P R E S E N T E

Por este medio informo que ha sido liberado el siguiente proyecto para Titulación integral:

Alumno (a):	LUIS ANGEL CASTILLO CEREZO
Carrera:	INGENIERÍA MECATRÓNICA
No. De Control:	20370701
Nombre del Proyecto:	"IMPLEMENTACIÓN DE SISTEMA DE MONITOREO PARA CENTROS DE MISIÓN CRÍTICA".
Producto:	TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL.

Agradezco de antemano su valioso apoyo en esta importante actividad para la formación profesional de nuestros egresados.

ATENTAMENTE

Excelencia en Educación Tecnológica®
Pensar para Servir, Servir para Triunfar®

JORGE AGUILAR VÁZQUEZ
JEFE DEL DEPTO. METAL-MECÁNICA
SECRETARÍA DE EDUCACIÓN PÚBLICA
TECNOLÓGICO NACIONAL
DE MÉXICO
INSTITUTO TECNOLÓGICO DE APIZACO
DEPARTAMENTO DE
METAL MECÁNICA



RAFAEL ORDOÑEZ FLORES
ASESOR

c.p.- Archivo.
JAV*petry.



2025
Año de
La Mujer
Indígena

Av. Instituto Tecnológico No. 418, San Andrés Ahuashuatepec,
Municipio de Tzompantepec, Tlaxcala, Mex. C.P. 90491 Tel.
[241] 4172010 Ext. 124, e-mail: mecanica@apizaco.tecnm.mx
tecnm.mx | apizaco.tecnm.mx





Tzompantepec, Tlaxcala, 11/Marzo/2026

LUIS ANGEL CASTILLO CEREZO
EGRESADO(A) DE LA CARRERA DE INGENIERÍA MECATRÓNICA
CON NÚMERO DE CONTROL 20370701.
P R E S E N T E.

Por este medio, me permito informar a usted que por aprobación de la comisión revisora asignada para valorar el trabajo que mediante la opción **TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL** y cuyo tema es: **"IMPLEMENTACIÓN DE SISTEMA DE MONITOREO PARA CENTROS DE MISIÓN CRÍTICA"**, conforme a lo establecido en el procedimiento para la obtención del Título Profesional en el Instituto Tecnológico, la División de Estudios Profesionales a mi cargo le otorga la:

AUTORIZACIÓN DE IMPRESIÓN

Debiendo entregar **1 USB** del mismo, apropiadamente empastados, a la brevedad, para presentar su Acto de Recepción Profesional.

Sin otro particular por el momento me despido.

ATENTAMENTE

Excelencia en Educación Tecnológica
Pensar para Servir, Servir para Triunfar®

CECILIA YARELY ARREGUÍN LARA
JEFA DE LA DIVISIÓN DE ESTUDIOS PROFESIONALES



ccp. Archivo
CYAL/Gvm*



AGRADECIMIENTOS

Quiero agradecer a todas las personas que hicieron posible la realización de este proyecto y que, de distintas maneras, me acompañaron a lo largo de este camino.

En primer lugar, quiero agradecer a mis padres, quienes estuvieron presentes en todo momento, brindándome su apoyo incondicional y acompañándome incluso durante aquellas largas noches de desvelo. Gracias por estar siempre a mi lado, por impulsarme a seguir adelante y por darme la confianza necesaria para llegar hasta este momento.

A mis profesores, quienes fueron una parte fundamental de mi formación. En especial, quiero agradecer al Dr. Ordóñez, por ser uno de esos profesores que, con su manera de enseñar, hacen que uno llegue a amar aún más su carrera. De igual manera, agradezco a la profesora Guadalupe, al profesor Benjamín y al profesor Castañeda, por compartir conmigo sus conocimientos y enseñanzas, de los cuales pude aprender muchísimo tanto para mi formación profesional como para la realización de este proyecto.

Agradezco profundamente a Enrique Preza y a Roberto Díaz por su amabilidad, confianza y por permitirme formar parte de su equipo durante todo el camino de mis prácticas profesionales. Gracias por compartir conmigo su experiencia, por sus consejos y por brindarme la oportunidad de aprender y desarrollarme profesionalmente. Su acompañamiento fue fundamental para que pudiera llevar a cabo este proyecto de manera satisfactoria.

Por último, pero no menos importante, quiero agradecer a todos mis amigos que estuvieron a mi lado durante este proceso. Gracias por escucharme, acompañarme y compartir conmigo tantas experiencias. Su apoyo me permitió ver las cosas desde diferentes perspectivas y encontrar ánimo incluso en los momentos más complicados.

RESUMEN

Este reporte describe la implementación de un sistema de monitoreo para centros de misión crítica, desarrollado durante la residencia profesional en Teksar Labs. El objetivo principal es implementar una solución que permitiera la supervisión en tiempo real de los aires de precisión en los centros de datos, UPS, RPDU, por ejemplo, parámetros ambientales, consumo de energía, tomando también en cuenta el estado de equipos. Las actividades realizadas incluyeron armado de gabinetes, configuración de gateways, configuración de módems, instalación de gabinetes y monitoreo de los datos, por ejemplo, la selección de hardware con relevancia en que tipos de sensores estaríamos usando para hacer mediciones y el software que usaremos para el monitoreo de estas. Los resultados más importantes comprenden que los equipos estén funcionando de manera óptima, que no tengan fugas de líquidos y que estén encendidos el tiempo que este establecido, por ejemplo, la implementación exitosa del sistema, la mejora en la eficiencia del monitoreo, la reducción de tiempos de respuesta ante incidentes dados por el poleo de nuestros gateways. Puedo concluir que la implementación del sistema de monitoreo contribuye significativamente a la confiabilidad y disponibilidad de los centros de misión crítica, proporcionando una herramienta esencial para la toma de decisiones y la gestión de operaciones.

INDICE

Contenido

Capítulo I Introducción	1
1.- Introducción:	2
1.2.- Problemas por resolver (planteamiento del problema).....	4
1.3.- Objetivos	5
1.3.1.- Objetivo General.	5
1.3.2.- Objetivos Específicos.	5
1.4.- Justificación.....	5
Capítulo II Marco Teórico.....	8
2.- Marco Teórico:	1
2.1.- IdeaPad 3 14itl05	1
2.2.- Suministro De CFE En Centro De Datos	2
2.3.- Plantas De Emergencia	2
2.4.- Transferencia (Cambio De Suministro De Energía)	4
2.5.- UPS (Uninterruptible Power Supply),	5
2.5.1.- Funciones principales	5
2.5.2.- Tipos de UPS	6
2.6.- Unidades de Distribución de Energía (PDU).....	6
2.7.- RPDU (Rack Power Distribution Unit)	7
2.7.1.- Características principales:	8
2.7.2.- Tipos comunes de RPDUs:	9
2.7.3.- Aplicaciones:	9
2.8.- Aires De Precisión.....	9
2.8.1.- Características técnicas	10
2.8.2.- Tipos de configuración	10
2.8.3.- Importancia en centros de datos.....	10
2.9.- Centro de Datos	11
2.9.1.- Características principales	11
2.9.2.- Clasificación y tipos.....	12
2.9.3.- Importancia en la infraestructura tecnológica	12
2.9.4.- Centros de misión crítica: importancia y características	12
3.- Sensor De Apertura De Puerta O Contacto Seco	13
4.- Sensor De Temperatura – Humedad	14
5.- Antena De Monitoreo Y Enlace IoT	14
6.- Sensor De Diesel	14
6.1.- Funciones principales	15

6.2.- Principios de funcionamiento.....	15
6.3.- Aplicación en centros de datos.....	15
7.- CPM-20	16
7.1.- Funciones principales	16
7.2.- Características técnicas	16
7.3.- Interfaz y alimentación	16
8.- Monitoreo De Infraestructura De Ti: Definición Y Propósito	17
9.- Thingsboard Y Protocolos De Comunicación	19
10.- Protocolo Modbus	20
11.- Arquitectura Basada En Computación En La Nube Y Sistema Operativo Linux.....	21
Capítulo III Desarrollo del Proyecto	23
3.1.- Procedimiento Y Descripción De Las Actividades Realizadas.....	24
<i>Ilustración 1</i>	24
3.2.- Elaboración Del Sistema De Demostración Con Sensores Inalámbricos.....	24
<i>Ilustración 2</i>	25
<i>Ilustración 4</i>	25
3.3.- Desarrollo De Sistema De Pruebas Para Medición De Energía Eléctrica	26
<i>Ilustración 6</i>	26
3.4.- Presentación de funcionalidades del sistema	26
<i>Ilustración 7</i>	27
<i>Ilustración 9</i>	27
3.5.- Preparación De Equipos Para Implementación En Campo	28
<i>Ilustración 11</i>	28
<i>Ilustración 12</i>	29
<i>Ilustración 13</i>	29
3.6.- Instalación Del Sistema En Campo	29
3.6.1.- Sensores De Humedad Y Temperatura	29
<i>Ilustración 14</i>	30
<i>Ilustración 15</i>	30
3.6.2.- Sensores De Líquidos	30
<i>Ilustración 18</i>	32
<i>Ilustración 19</i>	32
3.6.3.- Sensores De Aire.....	32
<i>Ilustración 20</i>	33
<i>Ilustración 21</i>	33
<i>Ilustración 22</i>	34
<i>Ilustración 24</i>	34

<i>Ilustración 25</i>	35
<i>Ilustración 26</i>	35
3.6.4.- Sensores De Puerta (Contacto Seco)	36
<i>Ilustración 28</i>	36
3.6.5.- GATEWAY (IBeacon).....	36
<i>Ilustración 29</i>	37
3.6.6.- Tableros Eléctricos	37
<i>Ilustración 30</i>	37
<i>Ilustración 32</i>	38
<i>Ilustración 33</i>	38
<i>Ilustración 34</i>	39
<i>Ilustración 35</i>	39
<i>Ilustración 36</i>	40
<i>Ilustración 37</i>	40
<i>Ilustración 38</i>	41
3.6.7.- Montaje De Gabinetes.....	41
<i>Ilustración 39</i>	41
<i>Ilustración 40</i>	42
<i>Ilustración 41</i>	42
<i>Ilustración 42</i>	43
3.6.8.- Revision De Conexiones De Internet En El Sitio	43
<i>Ilustración 43</i>	43
<i>Ilustración 44</i>	44
<i>Ilustración 45</i>	44
<i>Ilustración 46</i>	45
3.6.9.- Configuración De Equipos En Sitio	45
<i>Ilustración 47</i>	46
<i>Ilustración 49</i>	46
<i>Ilustración 51</i>	47
3.7.- Revision De Equipos Por Medio De Thingsboard Y SNMP	47
3.7.1.- Sensores En Sitio Y Visualización En Thingsboard	47
3.7.2.- Conexiones De Equipos Con SNMP Y Thingsboard	48
<i>Ilustración 52</i>	49
<i>Ilustración 53</i>	49
<i>Ilustración 54</i>	50
<i>Ilustración 55</i>	50
3.7.3.- Schneider Electric InRow	51

<i>Ilustración 56</i>	51
3.7.4.- PDU PANDUIT	51
<i>Ilustración 58</i>	52
<i>Ilustración 59</i>	52
3.7.5.- PDU Chatsworth	53
<i>Ilustración 61</i>	53
3.7.6.- Thingsboard Y Su Entorno Grafico (Dashboards)	53
<i>Ilustración 63</i>	54
<i>Ilustración 64</i>	54
<i>Ilustración 65</i>	54
3.7.7.- Dashboards De Cuartos Monitoreados	55
Bunker 1	55
<i>Ilustración 66</i>	55
<i>Ilustración 67</i>	56
Bunker 2	56
<i>Ilustración 68</i>	56
<i>Ilustración 69</i>	56
Cuarto Eléctrico 1	57
<i>Ilustración 70</i>	57
Cuarto Eléctrico 2	57
<i>Ilustración 71</i>	57
Cubicaciones	58
<i>Ilustración 72</i>	58
3.8.- Documentación Del Proyecto	58
CAPÍTULO IV RESULTADOS	59
Resultados:	60
Planos:	61
Graficas:	¡Error! Marcador no definido.
Manuales:	61
Programas:	62
En los programas utilizados en este proyecto, se utilizaron los siguientes programas: ..	62
Normativas:	62
Conclusiones, recomendaciones, experiencia profesional adquirida.	62
Conclusiones	62
Recomendaciones	63
Experiencia Profesional Adquirida	64
Competencias desarrolladas:	65

Capítulo I

Introducción

1.- Introducción:

En la era digital actual, los centros de misión crítica se han convertido en pilares fundamentales para el funcionamiento de numerosas organizaciones. Estos centros, que albergan la infraestructura tecnológica esencial para las operaciones diarias, demandan altos niveles de disponibilidad, confiabilidad y seguridad. Cualquier interrupción o falla en estos entornos puede tener consecuencias graves, desde pérdidas económicas hasta daños a la reputación.

En este contexto, el monitoreo efectivo de los centros de misión crítica se vuelve indispensable. Un sistema de monitoreo adecuado permite supervisar en tiempo real el estado de los equipos, las condiciones ambientales, el consumo de energía y otros parámetros críticos, facilitando la detección temprana de problemas, la optimización del rendimiento y la toma de decisiones informadas.

Este reporte describe la implementación de un sistema de monitoreo integral para E-Global, enfocado en la supervisión de los factores ambientales y eléctricos de los equipos a monitorear. El sistema desarrollado tiene como objetivo principal mejorar la gestión de los centros de misión crítica, garantizando su funcionamiento continuo y eficiente.

De este modo vemos que Servicios Electrónicos Globales S.A. de C.V. (**E-Global México**), es una empresa con aproximadamente 25 años de experiencia en el sector financiero mexicano, especializada en el procesamiento de pagos electrónicos con tarjeta. Desempeña un rol clave en la infraestructura del sistema de pagos con tarjeta en México, proporcionando servicios centrales como la conmutación y el enrutamiento de transacciones entre comercios, adquirentes y emisores.

Entre sus principales funciones destacan el procesamiento y la gestión del flujo de información y fondos relacionados con pagos con tarjeta. Además, E-Global ofrece soluciones personalizadas en medios de pago, adaptadas a las necesidades específicas de sus clientes, entre los que se encuentran grandes minoristas y los principales bancos del país, como BBVA Bancomer, Citibanamex y HSBC México.

La empresa goza de una reputación laboral generalmente positiva, según evaluaciones en plataformas como CompuTrabajo, donde se destacan aspectos como el buen ambiente laboral, el apoyo al personal y los salarios competitivos.

En cuanto a tecnología, E-Global ha implementado herramientas avanzadas como:

- Oracle, para la optimización del tiempo de procesamiento de transacciones;

- CyberArk, para la protección de sistemas y datos sensibles mediante la gestión de accesos privilegiados;
- INETCO Insight, para el monitoreo en tiempo real, la detección de fraudes y el análisis de rendimiento.

La compañía también explora el uso de inteligencia artificial con miras a integrarla en sus operaciones, buscando mayor eficiencia e innovación.

En el ámbito regulatorio, E-Global fue mencionada por la COFECE en 2023 por posibles barreras a la competencia. Sin embargo, cuenta con las autorizaciones del Banco de México para operar como cámara de compensación y realizar actividades relacionadas.

La importancia de E-Global México radica en su papel como soporte esencial para el comercio, al facilitar que los establecimientos acepten pagos electrónicos de forma eficiente, lo cual resulta clave para el crecimiento del comercio electrónico y la economía moderna, además, impulsa la economía digital al garantizar el funcionamiento confiable de las transacciones con tarjeta, fortaleciendo la confianza en los medios de pago electrónicos; su constante inversión en tecnología de seguridad permite proteger tanto a los usuarios como a las empresas frente al fraude, asegurando la integridad de las operaciones; al mismo tiempo, su infraestructura contribuye a una mayor eficiencia del sistema financiero mexicano al permitir que las transacciones se procesen con rapidez y seguridad.

Actúa también como conmutador, desempeñando un rol crítico en la interconexión entre comercios, adquirentes y emisores, lo que asegura la interoperabilidad del sistema de pagos con tarjeta; finalmente, su capacidad para desarrollar soluciones personalizadas le permite adaptarse a las necesidades del mercado y brindar a las empresas herramientas para ofrecer experiencias de pago más adecuadas a sus clientes.

En su impacto en el mercado, E-Global facilita la aceptación de pagos electrónicos en comercios y contribuye a la seguridad de las transacciones para los usuarios finales. Su trayectoria se caracteriza por una evolución estable, con una constante inversión en tecnología y adaptación a los cambios regulatorios.

El presente reporte se estructura de la siguiente manera: el Capítulo 2 presenta el marco teórico que sustenta el proyecto, el Capítulo 3 detalla el desarrollo de las actividades realizadas, el Capítulo 4 muestra los resultados obtenidos, y finalmente, se presentan las conclusiones, recomendaciones y la experiencia profesional adquirida.

1.2.- Problemas por resolver (planteamiento del problema)

Actualmente, la gestión de los centros de misión crítica en E-Global presentaba las siguientes problemáticas, falta de visibilidad en tiempo real, no se contaba con un sistema centralizado que permita monitorear de forma continua el estado de todos los componentes y equipos de la infraestructura. Esto dificulta la identificación rápida de posibles fallas y solucionarlos de manera oportuna.

En algunas ocasiones se debe de revisar los tiempos de respuesta elevados ante estos incidentes, ya que la detección de problemas se realiza de forma reactiva, lo que ocasionaba tiempos de inactividad prolongados y afectan la disponibilidad de los servicios.

Podemos tener en cuenta también nos afecta la falta de datos para la toma de decisiones ya que no se dispone de información detallada y precisa sobre el rendimiento de los sistemas, lo que dificultaba la optimización de los recursos y la planificación de futuras mejoras.

Este tipo de problemas por lo regular generan ciertos inconvenientes como:

- Interrupciones en el servicio, ya que las fallas no detectadas a tiempo pueden provocar interrupciones en los servicios críticos, lo que afecta en la productividad de la empresa y la satisfacción de sus clientes.
- Costos elevados, porque en los tiempos de inactividad y la necesidad de realizar reparaciones de emergencia estos generan costos adicionales para la empresa.

En la parte de los riesgos de seguridad:

- Falta de monitoreo adecuado aumentaba el riesgo de incidentes de seguridad, como accesos no autorizados o ataques cibernéticos.

Por lo tanto, puedo decir que se identificó la necesidad de implementar un sistema de monitoreo integral que permitiera:

- Obtener visibilidad en tiempo real del estado de la infraestructura de los equipos.
- Reducir los tiempos de respuesta ante incidentes.
- Proporcionar datos precisos para la toma de decisiones.
- Mejorar la disponibilidad y confiabilidad de los centros de misión crítica.

Podemos decir que este proyecto se enfocó en la implementación de un sistema de monitoreo para recabar la información esencial de los temas ambientales y eléctricos de los equipos, con el objetivo de abordar las problemáticas mencionadas y mejorar la gestión de los centros de misión crítica de los equipos en E-Global.

1.3.- Objetivos

1.3.1.- Objetivo General.

Implementar un sistema de monitoreo para centros de misión crítica, supervisando variables eléctricas y ambientales para evitar fallas en dichos centros.

Implementar un sistema de monitoreo integral para los centros de misión crítica de E-Global que permita la supervisión en tiempo real de los tableros eléctricos encargados de suministrar energía a un centro de datos, monitorear aires de precisión, UPS, PDUs, en los centros de datos, con el fin de mejorar la disponibilidad, confiabilidad y eficiencia de la infraestructura.

1.3.2.- Objetivos Específicos.

- Analizar los requerimientos de monitoreo de los centros de misión crítica, identificando los parámetros críticos a supervisar y las necesidades de los clientes.
- Seleccionar el hardware y software adecuado para el sistema de monitoreo, considerando la escalabilidad, la compatibilidad y el costo-beneficio.
- Diseñar la arquitectura del sistema de monitoreo, definiendo la topología, los protocolos de comunicación y la estructura de la base de datos.
- Implementar el sistema de monitoreo, configurando los dispositivos de adquisición de datos, el software de monitoreo y las interfaces de usuario.
- Realizar pruebas de funcionamiento del sistema de monitoreo, verificando su correcto desempeño y la precisión de los datos obtenidos.
- Elaborar la documentación del sistema de monitoreo, incluyendo manuales de usuario y guías de administración.
- Capacitar al personal encargado de la operación y mantenimiento del sistema de monitoreo.

1.4.- Justificación

La implementación de un sistema de monitoreo para los centros de misión crítica de E-Global, se justifica porque en la actualidad estos centros desempeñan un papel fundamental en el funcionamiento de las organizaciones al albergar la infraestructura tecnológica que soporta los procesos de negocio críticos siendo esencial su disponibilidad y confiabilidad para garantizar la continuidad operativa la productividad y la competitividad de la empresa además el monitoreo eficiente de los centros de misión crítica.

Estos se han vuelto una necesidad debido a la creciente complejidad de los sistemas además del aumento de las amenazas de seguridad y la demanda de

servicios ininterrumpidos requiriendo un sistema de monitoreo adecuado para supervisar en tiempo real.

El fin de monitorear la infraestructura es el detectar y resolver problemas de forma proactiva optimizando el rendimiento y garantizar el cumplimiento de los niveles de servicio, alineándonos con las tendencias actuales de la gestión en los centros de datos, que enfatizan la importancia de la automatización, la visibilidad y el análisis de datos para mejorar la eficiencia y la resiliencia de la infraestructura.

Estos nos proporcionan beneficios para E-Global como la mejora de la disponibilidad y confiabilidad al detectar y prevenir fallas antes de que causen interrupciones en el servicio reduciendo el tiempo de inactividad de los sistemas además de hacer la reducción de los tiempos de respuesta ante incidentes, al generar alertas automáticas ante situaciones anómalas, permite que el personal de soporte técnico pueda identificar y resolver problemas de forma más rápida y eficiente.

La optimización en el uso de los recursos se logró mediante la provisión de datos detallados sobre el rendimiento de los sistemas, el consumo de energía y la utilización de los recursos. Esto permitió identificar áreas de mejora y optimizar la asignación de recursos, generando ahorros en los costos operativos y una mayor eficiencia en el uso de la infraestructura.

También se facilitó la toma de decisiones al contar con información precisa y oportuna para los responsables de la gestión de los centros de misión crítica. Esta información permitió una mejor planificación de la capacidad, la implementación de mejoras en la infraestructura y la alineación de la tecnología con los objetivos estratégicos del negocio.

En cuanto a la seguridad, el sistema permitió monitorear constantemente los parámetros críticos de la infraestructura, detectar posibles amenazas y responder de forma proactiva para proteger los sistemas y los datos. Esto contribuyó significativamente a fortalecer la seguridad general de los centros de misión crítica.

El proyecto tuvo un impacto notable en la forma en que se gestionan los centros de misión crítica de E-Global, al introducir una herramienta centralizada y automatizada que permite supervisar de forma integral el estado de la infraestructura. Esta solución mejoró la visibilidad, el control y la eficiencia de las operaciones, promoviendo una gestión más proactiva mediante la detección temprana de problemas y la prevención de fallas. Asimismo, redujo la dependencia de la resolución reactiva de incidentes, permitiendo anticiparse a las necesidades de la infraestructura.

Además, el proyecto tuvo un impacto positivo en la cultura organizacional, al fomentar una mayor conciencia sobre la importancia de la disponibilidad y confiabilidad de los sistemas. También promovió la colaboración entre las distintas áreas involucradas en la gestión de la infraestructura.

La viabilidad del proyecto fue posible gracias al apoyo y colaboración del personal de la empresa, así como a la disponibilidad de los recursos necesarios para implementar el sistema de monitoreo, incluyendo hardware, software, personal técnico y tiempo. El desarrollo se realizó dentro del periodo establecido para la residencia profesional, cumpliendo con los objetivos planteados y respetando tanto el plazo como el presupuesto asignado.

Capítulo II Marco Teórico

2.- Marco Teórico:

El marco teórico que sustenta este proyecto se apoya en conceptos fundamentales y tecnologías clave que permiten la implementación efectiva de un sistema de monitoreo robusto, especialmente diseñado para operar en entornos de alta criticidad como los centros de datos.

El presente proyecto se fundamenta en el monitoreo de infraestructura de TI en centros de misión crítica, instalaciones clave para garantizar la continuidad operativa de organizaciones en sectores como finanzas, salud, telecomunicaciones y manufactura. Estos entornos se caracterizan por su alta disponibilidad, necesidad de redundancia y estrictos requerimientos de seguridad, tanto física como lógica.

El monitoreo de infraestructura es esencial para supervisar en tiempo real el estado, rendimiento y uso de los recursos tecnológicos, permitiendo detectar fallas, prevenir interrupciones, optimizar recursos y garantizar la eficiencia operativa.

2.1.- IdeaPad 3 14itl05

La Lenovo IdeaPad 3 14ITL05 es una laptop económica de 14 pulgadas, ideal para estudiantes o tareas de oficina ligera. Está disponible en múltiples configuraciones, con opciones que varían en procesador, memoria y almacenamiento.

Características principales:

- Pantalla: 14" HD (1366x768) o Full HD (1920x1080), panel TN, antirreflejo, 220 nits.
- Procesadores: Desde Intel Celeron 6305 hasta Intel Core i5-1135G7 (11ª Gen).
- Gráficos: Integrados Intel UHD o Iris Xe, según el CPU.
- Memoria RAM: 4GB u 8GB DDR4 (sistema con RAM soldada + ranura SO-DIMM; hasta 12GB máx).
- Almacenamiento: SSD de 128GB a 512GB; algunos modelos incluyen HDD adicional.
- Batería: 35Wh (hasta 6 h) o 45Wh (hasta 8.5 h), con soporte RapidCharge.
- Conectividad y puertos: Wi-Fi 5, Bluetooth 5.0, USB-A, USB-C (según modelo), HDMI, lector SD, jack combo.
- Extras: Webcam con obturador físico, altavoces estéreo, micrófonos duales, TPM 2.0.

- Construcción: Chasis de policarbonato (ABS), peso aprox. 1.5 kg, colores como Abyss Blue.
- Sistema operativo: Windows 10 o 11 Home, con Microsoft 365 Personal en algunos modelos.

2.2.- Suministro De CFE En Centro De Datos

El suministro eléctrico proporcionado por la Comisión Federal de Electricidad (CFE) en un centro de datos es un componente fundamental para garantizar la continuidad operativa de los sistemas críticos. En este tipo de instalaciones, el suministro debe ser altamente confiable, estable y cumplir con los estándares de calidad eléctrica necesarios para evitar interrupciones, fluctuaciones de voltaje o armónicos que puedan dañar los equipos o comprometer la disponibilidad de los servicios.

CFE ofrece distintos niveles de tensión (media y alta tensión), dependiendo de la demanda energética del centro de datos, que suele ser considerablemente alta. La conexión se realiza generalmente mediante una subestación dedicada o transformadores propios que permiten un control más preciso del suministro. Además, los centros de datos suelen contar con contratos especiales de tarifa industrial o de demanda controlada, lo que permite una mejor planificación del consumo y la facturación.

Para cumplir con los niveles de disponibilidad exigidos (como los establecidos por los estándares TIER del Uptime Institute), el suministro de CFE se complementa con sistemas redundantes de respaldo como UPS (sistemas de alimentación ininterrumpida), generadores eléctricos, bancos de baterías y sistemas de monitoreo en tiempo real. En algunos casos, se instalan fuentes de energía alternativa o acuerdos con CFE para servicios prioritarios en caso de contingencias.

2.3.- Plantas De Emergencia

Las plantas de emergencia son componentes críticos en la infraestructura de un centro de datos, ya que garantizan la continuidad del suministro eléctrico en caso de una interrupción del servicio proporcionado por la red pública, como el de la CFE. Estas plantas están diseñadas para activarse automáticamente cuando se detecta una falla en la red eléctrica, suministrando energía a los sistemas esenciales hasta que se restablezca el servicio o se tomen medidas correctivas.

Estas unidades suelen operar con motores diésel de alto rendimiento, aunque en algunos casos también se utilizan motores a gas natural o biocombustibles, dependiendo de las políticas ambientales o de sostenibilidad de la organización.

Están conectadas a través de tableros de transferencia automática (ATS), que permiten conmutar de forma rápida y segura entre la energía de la red y la energía de respaldo.

El diseño de las plantas de emergencia en centros de datos debe seguir criterios estrictos de redundancia y capacidad, de acuerdo con los niveles TIER. Por ejemplo, un centro de datos TIER III o IV debe contar con al menos una planta de emergencia adicional (N+1 o 2N) para asegurar la disponibilidad continua del servicio, incluso si una unidad falla o requiere mantenimiento.

Además, estos sistemas deben incluir monitoreo constante, control de emisiones, silenciadores para reducir el ruido y tanques de combustible de gran capacidad que aseguren su funcionamiento durante lapsos prolongados, en algunos casos hasta por 24 o 48 horas. La correcta instalación, mantenimiento y pruebas periódicas son esenciales para asegurar que las plantas de emergencia respondan de forma inmediata y eficaz cuando se necesiten.

La integración entre las plantas de emergencia y los sistemas de alimentación ininterrumpida (UPS) es fundamental para garantizar una transición fluida y sin interrupciones en el suministro eléctrico dentro de un centro de datos. Ambos sistemas trabajan en conjunto para asegurar la continuidad operativa, especialmente en situaciones de fallo de la red eléctrica.

Cuando ocurre una interrupción del suministro por parte de la CFE, el sistema UPS es el primero en entrar en acción. Este sistema, alimentado por baterías internas, proporciona energía instantánea y continua a los equipos críticos, sin ningún retardo perceptible. Su función es cubrir ese breve lapso, usualmente de unos segundos, que tarda la planta de emergencia en arrancar y estabilizar su salida eléctrica.

Una vez que la planta de emergencia está en funcionamiento y suministra corriente eléctrica de forma estable, el sistema UPS transfiere la carga desde sus baterías hacia la fuente generada por la planta. De este modo, el UPS actúa como un puente que evita interrupciones o daños por picos de voltaje, protegiendo servidores, sistemas de almacenamiento y equipos de red. Esta interacción se realiza de manera automática mediante los tableros de transferencia (ATS), que detectan la presencia de energía proveniente de la planta y ajustan la distribución de carga.

La coordinación entre UPS y planta debe estar cuidadosamente diseñada para asegurar compatibilidad eléctrica, capacidad adecuada según la carga crítica y sincronización precisa en la conmutación. Además, ambos sistemas deben someterse a pruebas periódicas de arranque, carga y transferencia para validar su funcionamiento conjunto.

Este tipo de arquitectura eléctrica híbrida es clave para mantener la alta disponibilidad requerida por centros de datos clasificados bajo estándares TIER, asegurando que ningún evento de corte energético afecte la operación continua de los servicios.

2.4.- Transferencia (Cambio De Suministro De Energía)

En los centros de datos, la continuidad del suministro eléctrico es fundamental para garantizar la disponibilidad de los servicios y la integridad de los datos. Una de las tecnologías clave para lograr esta continuidad es el sistema de transferencia de energía, el cual permite cambiar de forma controlada la fuente de alimentación de la carga crítica cuando se presenta una falla o interrupción en la red eléctrica principal.

El componente central de este sistema es el **tablero de transferencia automática (ATS, por sus siglas en inglés: Automatic Transfer Switch)**. Su función es detectar de manera instantánea la pérdida total o parcial del suministro eléctrico proveniente de la red pública (como el servicio de la Comisión Federal de Electricidad, CFE) y transferir la carga hacia una fuente alternativa, usualmente una planta de emergencia. Este proceso se realiza en cuestión de segundos y de forma automatizada, sin necesidad de intervención humana, minimizando el impacto sobre los sistemas operativos del centro de datos.

Una vez que el suministro principal se restablece y permanece dentro de los parámetros eléctricos adecuados de voltaje y frecuencia, el ATS realiza nuevamente la transferencia, devolviendo la alimentación a la red pública y desconectando la planta de emergencia. Este sistema también incluye funciones de retardo programado para permitir la estabilización del generador antes de aplicar la carga, así como una fase de enfriamiento posterior antes de apagar el generador.

El mecanismo de transferencia puede ser:

- **Automático**, como en la mayoría de los centros de datos modernos, donde la transición entre fuentes ocurre de manera inmediata.
- **Manual**, en instalaciones donde se requiere intervención humana por razones de control o seguridad.

Además, existen configuraciones de **transferencia con o sin interrupción**, dependiendo del nivel de criticidad de las operaciones. En sistemas más avanzados, se puede implementar una transferencia sin tiempo de corte perceptible, lo cual es esencial en aplicaciones que no toleran ni siquiera interrupciones breves.

La implementación de sistemas de transferencia eléctrica confiables es indispensable en la arquitectura energética de los centros de datos, ya que actúan como puente de continuidad entre las diferentes fuentes de energía y los sistemas de respaldo como UPS y plantas de emergencia, asegurando una operación ininterrumpida ante cualquier contingencia.

2.5.- UPS (Uninterruptible Power Supply),

Un UPS, o sistema de alimentación ininterrumpida, es un dispositivo electrónico diseñado para proporcionar energía temporal y estable a equipos críticos cuando se interrumpe el suministro eléctrico principal. Su función principal es garantizar la continuidad operativa de los sistemas conectados, protegiéndolos además contra anomalías en la red como caídas de tensión, sobrevoltajes, fluctuaciones y ruidos eléctricos que pueden dañar componentes sensibles o causar pérdida de datos.

2.5.1.- Funciones principales

- **Suministro de energía de respaldo:** Proporciona alimentación durante cortes breves de energía, permitiendo el apagado controlado de sistemas críticos o el funcionamiento temporal hasta que entre en marcha un generador.
- **Regulación de voltaje:** Estabiliza la tensión de entrada, compensando sobrevoltajes y bajadas de línea.
- **Protección eléctrica:** Filtra picos, transientes y ruidos que pueden afectar la electrónica sensible.
- **Gestión y monitoreo:** Muchos modelos permiten supervisar el estado de la batería, el voltaje de entrada/salida y eventos eléctricos, a través de software especializado o interfaces de red.

El UPS actúa como una barrera entre la red eléctrica y los equipos, permitiendo mantener su funcionamiento por un tiempo limitado tras un corte energético, tiempo durante el cual es posible apagar los sistemas de forma segura o permitir que entre en funcionamiento una fuente de energía alternativa como un generador. En su estructura básica, un UPS incluye una batería, un inversor que transforma la corriente continua (DC) en corriente alterna (AC), un rectificador que convierte la energía de entrada AC en DC para cargar la batería, y un circuito de bypass que permite el paso directo de la energía en ciertas condiciones de mantenimiento o falla del sistema.

2.5.2.- Tipos de UPS

1. **Offline (Standby):** Activa la batería solo cuando detecta una falla en el suministro. Es básico y adecuado para cargas pequeñas.
2. **Línea interactiva:** Corrige automáticamente pequeñas fluctuaciones de voltaje sin usar la batería, y la activa si ocurre un corte total.
3. **Online (Doble conversión):** Proporciona la mayor calidad de energía, ya que siempre alimenta la carga desde el inversor, eliminando completamente las variaciones del suministro. Es ideal para entornos críticos como centros de datos o infraestructura médica.

La implementación de sistemas UPS es indispensable en áreas donde la disponibilidad y confiabilidad energética son factores determinantes, como centros de datos, instalaciones médicas, infraestructura de telecomunicaciones y entornos industriales. Su uso permite no solo evitar interrupciones en el servicio, sino también preservar la integridad de los equipos, proteger la información y mantener la operatividad ante fallas inesperadas de la red.

2.6.- Unidades de Distribución de Energía (PDU)

En un centro de datos, la gestión adecuada de la energía eléctrica no se limita únicamente a su generación o respaldo, sino también a su distribución eficiente y segura hasta cada uno de los equipos de TI. Para ello, se utilizan las **Unidades de Distribución de Energía o PDU (Power Distribution Units)**, dispositivos esenciales que permiten distribuir la energía eléctrica desde las fuentes principales (como tableros, UPS o generadores) hacia los racks o gabinetes que alojan servidores, switches, sistemas de almacenamiento, entre otros.

Una PDU cumple con varias funciones críticas:

- **Distribución ordenada y segura de energía:** Permite canalizar múltiples salidas de energía desde una única entrada, lo cual facilita la organización del cableado y minimiza riesgos eléctricos.
- **Monitoreo del consumo eléctrico:** En modelos avanzados (PDU inteligentes o monitoreadas), se pueden medir parámetros como voltaje, corriente, potencia consumida por fase, temperatura ambiente y humedad, lo que contribuye a una administración energética más precisa.
- **Gestión remota y control de puertos:** Las PDU inteligentes permiten encender, apagar o reiniciar equipos de forma remota, lo cual resulta crucial

en centros de datos distribuidos o cuando se requiere intervención sin presencia física.

- **Protección eléctrica:** Algunas PDU integran protecciones contra sobrecargas, cortocircuitos o picos de voltaje, ayudando a proteger los equipos sensibles conectados a ellas.

Existen diversos tipos de PDU según su nivel de funcionalidad:

- **PDU básicas:** Distribuyen energía sin capacidad de monitoreo. Se utilizan en entornos con requerimientos simples.
- **PDU monitoreadas:** Permiten visualizar el consumo energético en tiempo real, ayudando a prevenir sobrecargas.
- **PDU conmutadas:** Añaden funciones de control remoto, como el encendido/apagado de salidas individuales.
- **PDU inteligentes (intelligent or metered-by-outlet):** Combinan monitoreo detallado por cada toma, control remoto y conectividad por red.

A continuación se muestran los modelos utilizados en el sitio en donde se realizaron las modificaciones:

- CHATSWORTH **P3-1F0E3**
- ORACLE **RMII_PDU15KVA-1_LV**
- PANDUIT **PP11024-0015**
- PANDUIT **PP11224-009**

En cuanto al diseño físico, las PDU pueden instalarse de manera **vertical (0U)** en los laterales del rack, o de forma **horizontal (1U o 2U)** ocupando espacios dentro del mismo. Su selección depende de factores como el espacio disponible, la densidad de carga por rack y la necesidad de redundancia.

Las PDU son, por tanto, un componente indispensable en la infraestructura eléctrica de los centros de datos modernos. No solo garantizan una distribución de energía organizada y confiable, sino que también contribuyen significativamente a la eficiencia energética, la seguridad operativa y la capacidad de gestión remota, aspectos esenciales para mantener la alta disponibilidad de los sistemas críticos.

2.7.- RPDU (Rack Power Distribution Unit)

Las RPDUs son una versión avanzada y especializada de las Unidades de Distribución de Energía (PDU), diseñadas específicamente para montarse en los racks o gabinetes de servidores dentro de centros de datos. Su función principal es

distribuir de manera eficiente y controlada la energía eléctrica desde la fuente (como UPS o generadores) hacia los dispositivos de TI alojados en el mismo rack.

A diferencia de las PDU tradicionales, las RPDUs están orientadas a entornos de misión crítica y ofrecen capacidades superiores de **monitoreo, control remoto, eficiencia energética y seguridad**.

2.7.1.- Características principales:

- **Montaje directo en racks (0U, 1U, etc.):** Se instalan verticalmente en los costados del rack (0U) o horizontalmente ocupando unidades de espacio (1U o más), lo que maximiza el uso del espacio sin interferir con el cableado o los equipos.
- **Medición precisa:** Las RPDUs pueden medir el consumo de energía en tiempo real a nivel de entrada (por fase), por grupo de tomas o incluso de forma individual por cada salida (en modelos avanzados), proporcionando datos como:
 - Voltaje
 - Corriente (Amperios)
 - Potencia (kW, kVA)
 - Consumo energético acumulado (kWh)
 - Factor de potencia
- **Control remoto:** En las RPDUs con capacidad de conmutación ("switched"), cada toma de corriente puede ser encendida o apagada de forma remota a través de interfaces web, SNMP, Modbus o REST API. Esto permite reiniciar equipos bloqueados o gestionar el arranque secuencial sin intervención física.
- **Supervisión ambiental:** Algunas RPDUs incluyen puertos para sensores ambientales (temperatura, humedad, flujo de aire, presencia de agua), lo que amplía su utilidad como parte del sistema integral de monitoreo de infraestructura.
- **Seguridad y alertas:** Pueden configurarse para enviar alarmas por sobrecargas, picos de corriente, condiciones ambientales críticas o intentos de acceso no autorizado. También es posible establecer umbrales de operación seguros.

2.7.2.- Tipos comunes de RPDUs:

- **Basic RPDUs:** Distribuyen energía sin monitoreo ni control remoto.
- **Monitored RPDUs:** Permiten monitoreo de consumo eléctrico, pero no ofrecen control remoto de las salidas.
- **Switched RPDUs:** Agregan control remoto de tomas individuales, junto con monitoreo.
- **Metered-by-Outlet RPDUs:** Monitorean el consumo por cada toma, ideal para entornos con múltiples clientes (colocation) o para análisis detallado de carga.

2.7.3.- Aplicaciones:

Las RPDUs son fundamentales en centros de datos modernos que requieren alta disponibilidad, visibilidad total del consumo energético, gestión remota y eficiencia operativa. Se utilizan en:

- Racks de servidores y almacenamiento.
- Centros de datos empresariales.
- Entornos con políticas estrictas de eficiencia energética y sostenibilidad (como ISO 50001 o LEED).

2.8.- Aires De Precisión

Los **aires acondicionados de precisión** son sistemas de climatización diseñados específicamente para controlar de manera constante y precisa las **condiciones ambientales** en espacios donde la estabilidad térmica es crucial, como centros de datos, salas de servidores, laboratorios, centros de telecomunicaciones y otras instalaciones de misión crítica. A diferencia de los sistemas de aire acondicionado convencionales, los equipos de precisión no solo se enfocan en el confort térmico, sino en mantener una operación continua con un control riguroso de **temperatura, humedad y calidad del aire**.

A continuación se muestran los modelos utilizados en el sitio en donde se realizaron las modificaciones:

- **VERTIV. Modelo DS105ASD1EI9DF0**
- **LIEBERT. Modelo DS105ASD0EI747A**
- **SCHNEIDER. Modelo ACRD600P**

2.8.1.- Características técnicas

Los aires de precisión destacan por sus capacidades superiores en comparación con los equipos tradicionales. Entre sus características más importantes se encuentran:

- **Control de temperatura estable y preciso**, generalmente con tolerancias de ± 1 °C.
- **Regulación de humedad relativa**, que puede mantenerse típicamente entre el 40 % y 60 %, según las necesidades del equipo electrónico.
- **Operación 24/7/365**, diseñados para funcionar de manera continua sin interrupciones.
- **Flujo de aire constante y de alta eficiencia**, que asegura la correcta circulación y evita la formación de puntos calientes.
- **Filtración de partículas y polvo**, para garantizar un ambiente limpio y seguro para los dispositivos electrónicos sensibles.

2.8.2.- Tipos de configuración

Dependiendo del diseño del centro de datos y de los requerimientos de enfriamiento, los sistemas de aire acondicionado de precisión pueden adoptar distintas configuraciones:

- **Downflow (flujo descendente)**: El aire frío se distribuye por debajo del piso falso y asciende a través de las rejillas hasta alcanzar los racks.
- **Upflow (flujo ascendente)**: Utilizado en instalaciones sin piso elevado; el aire frío sale por la parte superior del equipo y se canaliza hacia los servidores.
- **InRow o Close-Coupled**: Equipos instalados directamente entre los racks, que permiten un control térmico más localizado y eficiente.
- **Overhead o de techo**: Montados en el techo o suspendidos para liberar espacio en el piso técnico.

2.8.3.- Importancia en centros de datos

En un **centro de datos**, el control térmico es un componente esencial para preservar la integridad de los equipos electrónicos, los cuales generan una elevada carga térmica durante su funcionamiento. Una temperatura excesiva o una humedad inadecuada puede reducir la vida útil de los servidores, aumentar las fallas electrónicas e incluso provocar interrupciones en los servicios críticos. Por ello, los aires de precisión permiten:

- **Prevenir sobrecalentamientos.**
- **Asegurar la continuidad operativa.**
- **Mejorar la eficiencia energética mediante el uso de tecnologías como enfriamiento por agua, free cooling o economizadores.**
- **Integrarse a sistemas de monitoreo para la gestión en tiempo real.**

En resumen, los aires acondicionados de precisión representan una infraestructura indispensable para mantener las **condiciones ambientales óptimas y constantes**, necesarias para el correcto funcionamiento de un centro de datos moderno. Su diseño robusto, alta eficiencia y capacidad de integración los convierten en una solución clave dentro de los entornos de alta disponibilidad.

2.9.- Centro de Datos

Un **centro de datos**, también conocido como *data center*, es una instalación física especialmente diseñada para albergar, operar y proteger una gran cantidad de equipos de tecnología de la información (TI), tales como **servidores, sistemas de almacenamiento, dispositivos de red y plataformas de telecomunicaciones**. Su función principal es garantizar la **disponibilidad continua y segura** de los servicios digitales, aplicaciones empresariales, procesos de datos y sistemas críticos de una organización.

Los centros de datos representan un componente fundamental dentro de las infraestructuras de misión crítica debido a que concentran los recursos computacionales que soportan operaciones esenciales en sectores como las finanzas, salud, telecomunicaciones, manufactura, educación y gobierno. Su diseño está orientado a cumplir con estándares estrictos de **redundancia, confiabilidad, eficiencia energética y seguridad**.

2.9.1.- Características principales

Los centros de datos cuentan con una serie de características que los distinguen de otras instalaciones tecnológicas:

- **Alta disponibilidad:** Se diseñan para operar de manera ininterrumpida, implementando esquemas de redundancia eléctrica (como UPS, plantas de emergencia y transferencias automáticas), redes tolerantes a fallos y climatización de precisión.
- **Infraestructura crítica:** Incluyen componentes especializados como sistemas de distribución eléctrica, monitoreo ambiental, control de acceso,

detección y supresión de incendios, y enlaces de comunicaciones redundantes.

- **Seguridad física y lógica:** Integran mecanismos avanzados para proteger tanto el acceso físico (cámaras de seguridad, tarjetas de acceso, biometría) como el acceso lógico a los sistemas y datos almacenados.
- **Gestión energética eficiente:** Debido a su elevado consumo energético, los centros de datos incorporan tecnologías para la administración eficiente de la energía, como unidades de distribución eléctrica inteligentes (RPDUs), monitoreo remoto de consumo y sistemas de enfriamiento optimizados.

2.9.2.- Clasificación y tipos

Según su escala y propósito, los centros de datos pueden clasificarse en:

- **Centros de datos empresariales (privados):** Infraestructura dedicada al uso exclusivo de una organización.
- **Centros de datos de colocation:** Espacios compartidos donde múltiples clientes alojan sus equipos dentro de un mismo entorno físico, gestionado por un proveedor externo.
- **Centros de datos en la nube o hiperescala:** Instalaciones de gran tamaño operadas por proveedores globales como Amazon Web Services, Microsoft Azure o Google Cloud, que ofrecen servicios escalables a través de Internet.

2.9.3.- Importancia en la infraestructura tecnológica

La creciente digitalización de procesos empresariales y gubernamentales ha convertido a los centros de datos en una parte indispensable de la economía digital moderna. Su adecuada gestión garantiza la continuidad operativa, la integridad de los datos y la calidad del servicio prestado por las organizaciones.

En el contexto de este proyecto, el centro de datos representa el entorno físico donde se implementa el sistema de monitoreo propuesto. Comprender su funcionamiento y sus exigencias operativas permite diseñar una solución tecnológica alineada con los requerimientos de confiabilidad, eficiencia y seguridad que demanda una infraestructura de misión crítica.

2.9.4.- Centros de misión crítica: importancia y características

Los centros de misión crítica son instalaciones que albergan la infraestructura tecnológica esencial para el funcionamiento ininterrumpido de una organización. Estos centros son considerados el núcleo operativo de sectores que requieren una disponibilidad constante, como los servicios financieros, la atención médica, las

telecomunicaciones, la manufactura y otros ámbitos donde la interrupción de servicios representa un alto impacto económico y operativo.

Sus principales características incluyen:

- **Alta disponibilidad:** Estos centros deben estar operativos las 24 horas del día, los 365 días del año. Cualquier tiempo de inactividad, por mínimo que sea, puede tener consecuencias graves. Por ello, su diseño contempla tolerancia a fallos y redundancia de componentes críticos como servidores, fuentes de alimentación, sistemas de enfriamiento, enlaces de red y sistemas de respaldo energético.
- **Redundancia:** Se implementan arquitecturas que duplican o triplican elementos clave del sistema para garantizar la continuidad operativa ante cualquier falla técnica o corte inesperado. Esto incluye configuraciones como N+1, 2N o incluso 2(N+1), en donde cada elemento esencial cuenta con respaldo automático.
- **Seguridad física y lógica:** Se exige un nivel de seguridad elevado, tanto a nivel físico (control de accesos, vigilancia, detección de incendios, protección contra desastres naturales) como a nivel lógico (firewalls, sistemas de detección de intrusos, encriptación, control de accesos digitales). La protección de la información confidencial y de los activos tecnológicos es prioritaria.

Una gestión eficiente de estos entornos demanda la integración de estrategias avanzadas, prácticas operativas bien definidas y soluciones tecnológicas de alto nivel que aseguren no solo su continuidad operativa, sino también su eficiencia energética y sostenibilidad a largo plazo.

3.- Sensor De Apertura De Puerta O Contacto Seco.

Este sensor de puerta o ventanas con tecnología Bluetooth® LE 5.0, posee un sensor magnético en el interior que puede ser usado para el monitoreo remoto de puertas para garantizar la seguridad de los activos, equipos o cosas.

Cabe mencionar que este mismo sensor es utilizado para los sensores de presencia de voltaje o sensores de líquidos, a diferencia que en estos se añaden los aditamentos para que cumpla con la funcionalidad requerida de alertar en caso de ausencia de voltaje o de la presencia de líquidos.

4.- Sensor De Temperatura – Humedad

Es un sensor de temperatura y humedad basado en Bluetooth® LE 5.0. Proporciona registros de historial para ayudar a los usuarios a realizar un seguimiento y monitoreo de datos con alta precisión. Es una opción ideal para el monitoreo de la cadena de frío, el monitoreo de depósitos y almacenamiento, o el monitoreo de centros de datos.

Se puede configurar en un área específica para monitorear la temperatura y la humedad relativa del aire en tiempo real. La información de los problemas climáticos es enviada como una alerta y poder atender de manera oportuna la operación del o los equipos y a su vez seguir monitoreándolo en tiempo real.

5.- Antena De Monitoreo Y Enlace IoT

Es una puerta de enlace más rápida y segura con una potente CPU Bluetooth® LE y Wi-Fi y cifrado empresarial WPA 2.0 para seguridad y transmisión de datos, G1 recopila datos de Bluetooth® de los sensores y otros dispositivos IoT que sean compatibles, y luego los envía a la nube. Wifi/Ethernet. Es una gran opción para todas las aplicaciones de la industria.

Se puede utilizar ampliamente en diferentes industrias verticales, como centros comerciales, aeropuertos, supermercados, lugares de entretenimiento, conciertos, hospitales, escuelas, museos, empresas, centros de datos, unidades administrativas, departamentos gubernamentales, fábricas, logística, etc. haciendo posible el seguimiento de activos, el control de acceso, la promoción publicitaria, el posicionamiento en interiores y la automatización y seguimiento de la industria.

6.- Sensor De Diesel

Un sensor de diésel es un dispositivo electrónico diseñado para monitorear el nivel y/o flujo de combustible diésel en un tanque o sistema de almacenamiento. Este tipo de sensor es fundamental en entornos donde el suministro continuo de energía depende de plantas de emergencia, las cuales utilizan diésel como fuente primaria de combustible. En instalaciones críticas como centros de datos, hospitales o instalaciones industriales, garantizar la disponibilidad del combustible es vital para

asegurar la operación de los generadores ante fallas en el suministro eléctrico principal.

6.1.- Funciones principales

El sensor de diésel cumple con diversas funciones que permiten un control preciso y confiable del combustible almacenado:

- **Medición de nivel:** Detecta el volumen de diésel presente en el tanque en tiempo real.
- **Detección de fugas o pérdidas:** Al identificar cambios anómalos en los niveles, permite activar alertas tempranas ante posibles fugas.
- **Control de llenado y vaciado:** Facilita la automatización del proceso de llenado y previene el desbordamiento o el vaciado total del tanque.
- **Monitoreo remoto:** Cuando está integrado en un sistema de monitoreo (como plataformas SCADA o IoT), permite el control a distancia del estado del combustible.

6.2.- Principios de funcionamiento

Los sensores de diésel pueden funcionar bajo distintos principios tecnológicos, entre los más comunes se encuentran:

- **Ultrasónicos:** Utilizan ondas ultrasónicas para medir la distancia entre el sensor y la superficie del líquido.
- **Capacitivos:** Detectan variaciones en la capacidad eléctrica entre dos electrodos, la cual cambia en función del nivel del líquido.
- **Flotadores magnéticos:** Emplean un flotador con un imán que se desplaza a lo largo de una guía, activando sensores en diferentes posiciones.
- **Presión hidrostática:** Miden la presión ejercida por la columna de líquido para determinar su altura.

6.3.- Aplicación en centros de datos

En el contexto de los centros de datos, los sensores de diésel se instalan en los tanques de combustible de las plantas de emergencia. Su implementación permite llevar un registro constante del nivel de combustible, generar alertas automáticas en caso de niveles críticos o pérdidas, y asegurar que los generadores dispongan de la cantidad necesaria de diésel para operar durante cortes prolongados del suministro eléctrico convencional. Además, al integrarse con sistemas de monitoreo basados en protocolos como Modbus RTU o TCP/IP, estos sensores pueden ser

supervisados a distancia, lo que mejora la capacidad de respuesta y la eficiencia operativa del personal de mantenimiento.

7.- CPM-20

El **CPM-20** es un medidor digital diseñado para el monitoreo avanzado de parámetros eléctricos en sistemas de distribución de energía. Se emplea comúnmente en paneles de control, monitoreo de motores y generadores, redes industriales, y sistemas de gestión energética. Su propósito principal es proporcionar una supervisión detallada y precisa del comportamiento eléctrico para mejorar la eficiencia, detectar anomalías y mantener la calidad del suministro.

7.1.- Funciones principales

- Medición de voltaje, corriente, frecuencia, potencia activa, reactiva y aparente, factor de potencia y energía consumida.
- Análisis de distorsión armónica total (THD), útil para evaluar la calidad de la energía eléctrica.
- Registro de valores máximos y mínimos, así como medición de demanda.
- Cálculo de costos eléctricos y estimación de emisiones de CO₂ basadas en el consumo energético.

7.2.- Características técnicas

- Entradas de voltaje: 40 a 600 V (fase-neutro), configurable.
- Entradas de corriente: 0 a 5 A (opcional 0 a 1 A).
- Precisión:
 - Energía activa/reactiva: ± 0.5 %.
 - Frecuencia: ± 0.2 %.
 - THD: ± 1 %.
- Comunicación: Puerto RS485 con protocolo Modbus RTU, compatible con sistemas SCADA y plataformas de monitoreo remoto.
- Entradas y salidas digitales (DI/DO): permiten el monitoreo de estados lógicos o la activación remota de dispositivos externos.

7.3.- Interfaz y alimentación

- Pantalla LED de 16 dígitos, con actualización de datos cada 0.5 segundos.

- Alimentación: voltaje de entrada entre AC 85–265 V o DC 100–300 V.
- Montaje en panel, con dimensiones de 96 x 96 x 71 mm y peso aproximado de 400 gramos.
- Protección: nivel IP50 en el frontal y IP20 en la carcasa posterior.

8.- Monitoreo De Infraestructura De Ti: Definición Y Propósito

En este contexto, el **monitoreo de infraestructura de TI** se convierte en un pilar fundamental para la gestión proactiva de centros de datos complejos. Este concepto hace referencia al conjunto de herramientas, procesos y metodologías empleadas para supervisar en tiempo real el estado, el rendimiento y el comportamiento de todos los elementos que integran la infraestructura tecnológica.

Esta supervisión abarca servidores, sistemas de almacenamiento, dispositivos de red, sistemas de energía y climatización, así como cualquier otro componente que forme parte del ecosistema operativo del centro.

Los objetivos clave del monitoreo de infraestructura de TI son:

1. **Garantizar la disponibilidad de los servicios y aplicaciones críticas:** Un sistema de monitoreo efectivo permite verificar continuamente que los servicios tecnológicos estén en funcionamiento. En caso de incidentes o caídas, se emiten alertas automáticas que permiten actuar de forma inmediata y minimizar los tiempos de inactividad.
2. **Detección temprana y diagnóstico de fallos:** Al recopilar datos en tiempo real sobre el comportamiento de cada componente, es posible identificar tendencias anómalas, degradaciones progresivas del rendimiento o señales tempranas de fallos, lo que facilita una intervención preventiva en lugar de reactiva.
3. **Optimización de recursos tecnológicos:** A través del análisis de métricas de uso, como la carga de trabajo de los servidores, la utilización del ancho de banda o el consumo de energía, se pueden ajustar cargas, balancear recursos y tomar decisiones informadas para maximizar la eficiencia operativa y reducir costos innecesarios.

8.1.- Monitoreo aplicado en centros de misión crítica

Para una cobertura completa del estado del centro de datos, es necesario implementar distintos tipos de monitoreo, cada uno con un enfoque específico:

En la implementación de un sistema de monitoreo para centros de misión crítica, uno de los componentes clave es el monitoreo de infraestructura física crítica. Este tipo de monitoreo permite supervisar en tiempo real variables esenciales para el funcionamiento continuo del centro, como:

- **Variables eléctricas:** voltaje, corriente, calidad de la energía, balanceo de cargas, consumo por área o equipo.
- **Variables mecánicas:** estado de UPS, plantas de emergencia, compresores, motores y bombas.
- **Condiciones ambientales:** temperatura, humedad, calidad del aire (PM2.5, CO₂, VOC), detección de líquidos y apertura de puertas.

Con soluciones como esta, la supervisión se realiza a través de sensores inteligentes conectados vía red celular, sin afectar la red del cliente, con visualización remota, generación de alertas automáticas y análisis predictivo mediante inteligencia artificial.

Este monitoreo permite prevenir fallas, reducir tiempos de respuesta ante incidentes, optimizar recursos y garantizar la continuidad operativa y la disponibilidad de servicios críticos.

Este tipo de monitoreo se enfoca en supervisar todos los elementos físicos esenciales para el funcionamiento continuo y seguro del centro de misión crítica. Incluye:

- **Sistemas eléctricos:** UPS, plantas de emergencia, conmutadores, distribución de energía (PDU)
- **Sistemas de climatización:** aires acondicionados de precisión, control de temperatura y humedad
- **Sensores ambientales:** temperatura, humedad, detección de humo o agua, apertura de puertas
- **Condiciones físicas del entorno:** vibraciones, fugas, acceso físico no autorizado

¿Por qué es relevante en la implementación?

Cuando se implementa un sistema de monitoreo para un centro de misión crítica, el **monitoreo de infraestructura física** permite:

- **Detectar fallas antes de que ocurran interrupciones**
- **Evitar daños por sobrecalentamiento o humedad**

- **Proteger el entorno físico ante accesos indebidos o emergencias**
- **Automatizar alertas** para el personal de mantenimiento o seguridad

Cada tipo de monitoreo se complementa para ofrecer una visión integral de la salud operativa de la infraestructura y permitir una gestión más precisa y oportuna.

9.- Thingsboard Y Protocolos De Comunicación

En este proyecto se implementó un sistema de monitoreo basado en la plataforma **ThingsBoard**, una solución de código abierto que permite la recolección, visualización y análisis de datos provenientes de sensores y dispositivos IoT. ThingsBoard fue seleccionada por su arquitectura flexible, escalable y personalizable, lo que la hace especialmente adecuada para entornos críticos.

Sus principales funcionalidades incluyen:

- Creación de paneles de visualización interactivos y configurables, adaptados a las necesidades específicas del usuario.
- Configuración de reglas de automatización y alertas personalizadas.
- Soporte para múltiples protocolos de comunicación (MQTT, CoAP, HTTP, SNMP, entre otros).

La comunicación con los equipos de aire de precisión responsables del control ambiental se estableció mediante el **protocolo SNMP (Simple Network Management Protocol)**, un estándar ampliamente utilizado en redes IP. SNMP permitió obtener información detallada sobre parámetros como:

- Temperatura del aire en tiempo real.
- Niveles de humedad relativa.
- Flujo de aire y estado del ventilador.
- Alertas de funcionamiento o error del sistema HVAC.

9.1.- Sensores integrados para el monitoreo ambiental y físico

Con el fin de supervisar las condiciones ambientales dentro del centro de datos, se integró un conjunto diverso de sensores especializados:

- **Sensores de temperatura y humedad:** Instaurados en puntos estratégicos de la sala de servidores, permiten detectar variaciones que puedan poner en riesgo el correcto funcionamiento de los equipos y activar alertas preventivas.

- **Sensores de fuga de líquidos:** Estos dispositivos se instalaron en zonas críticas donde una acumulación de agua podría causar daños severos a la infraestructura tecnológica. Su función es detectar fugas con rapidez y emitir una alerta temprana.
- **Sensores de estado de aire:** Supervisan el funcionamiento del sistema de ventilación, detectando interrupciones o cambios anómalos en el flujo de aire que podrían afectar la refrigeración.
- **Sensores de puertas:** Implementados como medida de seguridad física, estos sensores detectan aperturas no autorizadas, ayudando a controlar el acceso a las instalaciones y a prevenir intrusiones.

10.- Protocolo Modbus

El protocolo Modbus es un estándar de comunicación serial abierto que fue desarrollado en 1979 por la empresa Modicon, actualmente parte de Schneider Electric. Su función principal es permitir la comunicación entre múltiples dispositivos electrónicos en entornos industriales, tales como sensores, actuadores, medidores de energía, PLCs (controladores lógicos programables), entre otros. Modbus es ampliamente reconocido por su simplicidad, fiabilidad y por ser un protocolo de código abierto, lo cual ha facilitado su adopción en múltiples aplicaciones de automatización y control.

Modbus opera bajo una arquitectura maestro-esclavo, también conocida como cliente-servidor. En este modelo, el dispositivo maestro es el encargado de iniciar la comunicación y de enviar solicitudes a uno o más dispositivos esclavos. Los dispositivos esclavos solamente responden a las solicitudes del maestro y no pueden iniciar comunicaciones por sí mismos. Esta estructura jerárquica es útil para mantener un control organizado en redes industriales.

Existen diversas variantes del protocolo Modbus que se adaptan a distintos medios físicos y entornos. Modbus RTU (Remote Terminal Unit) es una de las implementaciones más comunes y utiliza comunicación serial (como RS-232 o RS-485) con un formato binario, lo que lo hace más eficiente en la transmisión de datos. Modbus ASCII, por otro lado, también utiliza comunicación serial pero en formato ASCII, lo que facilita su lectura por humanos, aunque reduce la eficiencia en comparación con Modbus RTU. Finalmente, Modbus TCP/IP es una versión moderna del protocolo que opera sobre redes Ethernet, encapsulando los mensajes Modbus dentro de paquetes TCP/IP, lo cual permite su integración con redes de datos modernas y sistemas SCADA (Supervisory Control and Data Acquisition).

En términos de estructura, un mensaje Modbus RTU está compuesto por una dirección de esclavo, un código de función que define la operación a realizar (como leer o escribir datos), un campo de datos que varía según la operación, y una verificación de errores mediante un CRC (Cyclic Redundancy Check). En el caso de Modbus TCP, en lugar de un CRC se utiliza un encabezado MBAP (Modbus Application Protocol Header) que contiene información adicional como el identificador de transacción, protocolo y longitud del mensaje.

El protocolo Modbus utiliza códigos de función específicos para realizar distintas operaciones. Entre los más utilizados se encuentran los códigos para lectura de bobinas (outputs digitales), lectura de entradas digitales, lectura de registros de retención (holding registers), lectura de entradas analógicas, así como la escritura de bobinas y registros únicos o múltiples. Estos códigos permiten una amplia variedad de funciones de monitoreo y control dentro de un sistema.

Entre las principales ventajas de Modbus se encuentran su simplicidad de implementación, la facilidad para integrarse con equipos de diferentes fabricantes, y su estabilidad en entornos industriales con ruido electromagnético. Al ser un protocolo ampliamente adoptado y soportado, ofrece una gran compatibilidad para proyectos de integración y monitoreo.

Modbus es utilizado ampliamente en aplicaciones de automatización industrial, control de sistemas eléctricos, supervisión de variables ambientales, sistemas HVAC (calefacción, ventilación y aire acondicionado), monitoreo de plantas de energía, iluminación inteligente, y sistemas de gestión de edificios. Su versatilidad, confiabilidad y facilidad de integración lo convierten en uno de los protocolos más relevantes en el ámbito de la industria 4.0 y el Internet Industrial de las Cosas (IIoT).

11.- Arquitectura Basada En Computación En La Nube Y Sistema Operativo Linux

La arquitectura del sistema de monitoreo fue diseñada con un enfoque en la **computación en la nube**, lo que permitió aprovechar ventajas clave como:

- **Escalabilidad:** La infraestructura puede crecer fácilmente conforme aumentan las necesidades de monitoreo o se integran nuevos sensores.
- **Flexibilidad y accesibilidad:** El personal de operaciones puede acceder a los datos desde cualquier lugar, facilitando la supervisión remota y la gestión de incidentes.

- **Centralización de la información:** Todos los datos de monitoreo se agrupan en una misma plataforma, permitiendo su análisis consolidado y en tiempo real.

Para el mantenimiento y desarrollo del sistema, se utilizó **Linux** como sistema operativo, debido a su estabilidad, seguridad, flexibilidad y amplia compatibilidad con soluciones de código abierto. Linux permitió configurar, personalizar y automatizar tareas dentro de la plataforma ThingsBoard, así como establecer scripts de monitoreo, gestionar servicios y realizar integraciones eficientes con los sensores conectados.

Capítulo III

Desarrollo del Proyecto

3.1.- Procedimiento Y Descripción De Las Actividades Realizadas

Durante las primeras semanas se llevó a cabo un proceso de capacitación intensiva con el objetivo de familiarizarse con el entorno tecnológico de la empresa, incluyendo la arquitectura de los sistemas de monitoreo, el uso de la plataforma ThingsBoard, el protocolo SNMP y la configuración de equipos en entornos Linux. Se revisaron conceptos clave relacionados con el monitoreo ambiental en centros de datos, así como la operación de sensores inalámbricos y dispositivos de precisión.

En la siguiente imagen (**Ilustración 1**) podemos ver un diagrama el cual nos explica un poco del trabajo de implementación de monitoreo y comunicación que se lleva a cabo en la empresa E-Global:

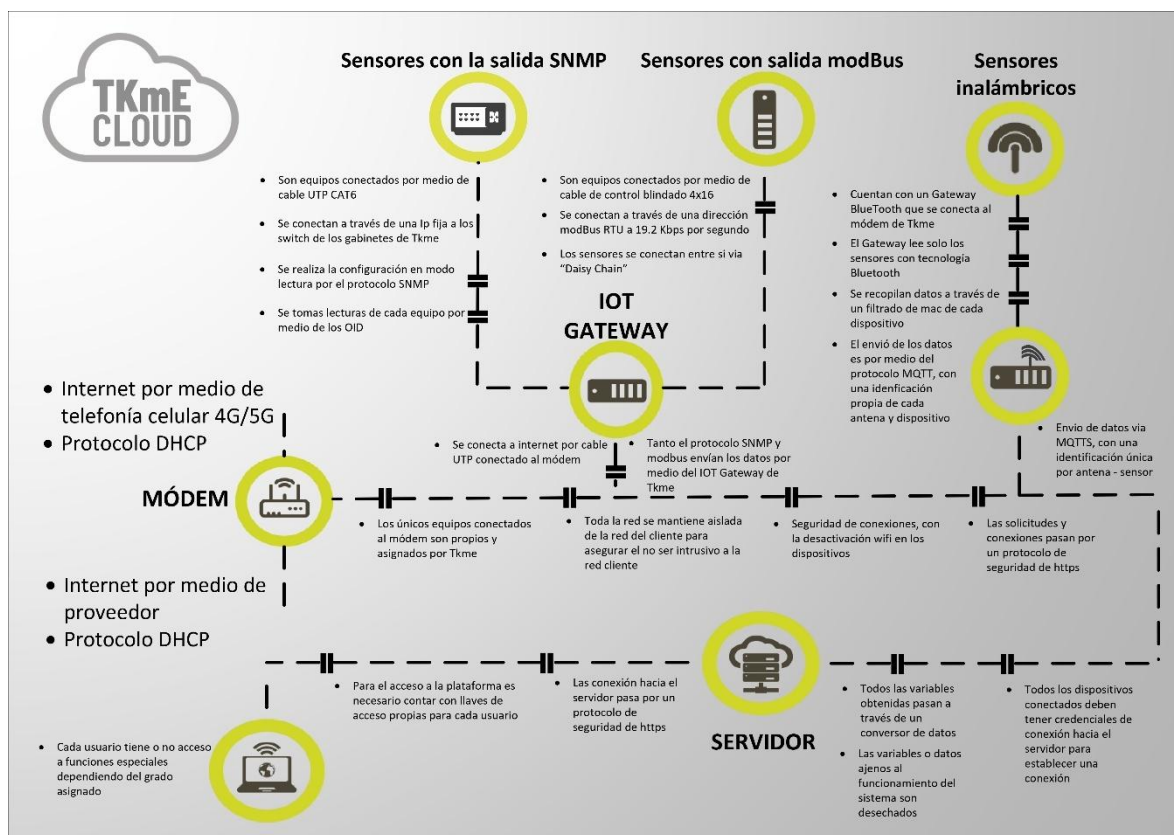


Ilustración 1 Implementación del nuevo modelo de comunicación. (Autoría Propia)

3.2.- Elaboración Del Sistema De Demostración Con Sensores Inalámbricos

Se diseñó e implementó un sistema de monitoreo funcional utilizando sensores inalámbricos para la detección de variables ambientales como temperatura, humedad, fugas de líquidos y apertura de puertas. Esta etapa incluyó la integración

de los sensores con la plataforma ThingBoard, la generación de dashboards personalizados y la configuración de alertas automatizadas. Se realizaron pruebas locales para verificar la conectividad, precisión de datos y fiabilidad del sistema.

En las siguientes fotografías (**Ilustraciones 2 y 3**) se muestran los gabinetes en proceso de armado en el cual se implementaron los materiales primordiales para el correcto funcionamiento.



Ilustración 2 Brandeo de gabinetes (Autoría Propia)

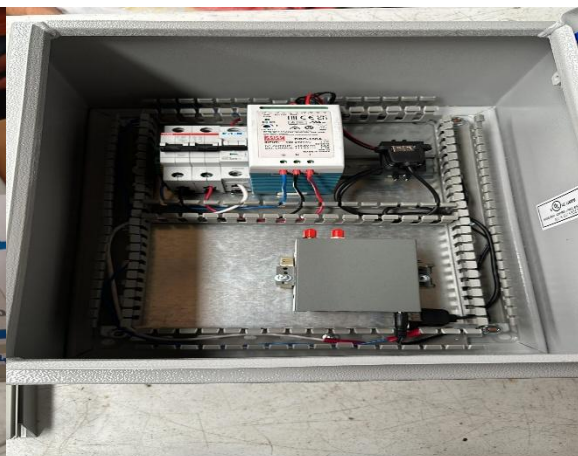


Ilustración 3 Instalación de equipos (Autoría Propia)

En esta etapa del proyecto se desarrollaron prototipos de gabinetes que servirán como base para la instalación de los componentes de monitoreo. Las imágenes siguientes (**Ilustraciones 4 y 5**) nos ilustran tanto el diseño físico de los gabinetes como el proceso de identificación visual mediante el brandeo. Además, se muestran los primeros elementos que fueron integrados en los prototipos con el fin de realizar pruebas funcionales y validar el correcto funcionamiento del sistema antes de su implementación definitiva.



Ilustración 4 Vista lateral de gabinete (Autoría Propia)



Ilustración 5 Brandeo final (Autoría Propia)

3.3.- Desarrollo De Sistema De Pruebas Para Medición De Energía Eléctrica

En paralelo, se inició la integración de sensores orientados a la medición de consumo eléctrico (CPM 20) (**Ilustración 6**) con el fin de complementar el monitoreo ambiental. Se configuraron sensores especializados capaces de registrar parámetros como voltaje, corriente y potencia, permitiendo así un análisis más amplio del entorno del centro de datos. Estas pruebas sirvieron para validar la capacidad de la plataforma para procesar múltiples tipos de variables en tiempo real.



Ilustración 6 Pruebas con CPM 20 (Autoría Propia)

3.4.- Presentación de funcionalidades del sistema

Una vez validadas las funcionalidades principales, se llevó a cabo una presentación técnica ante el personal de la empresa, como podremos ver en las (**Ilustraciones 7 y 8**), a continuación, son para demostrar la operatividad del sistema desarrollado. Se mostró la visualización gráfica de variables, el sistema de alertas en tiempo real y la arquitectura de integración de sensores. Esta actividad permitió recibir retroalimentación para ajustes antes de la implementación en campo.



Ilustración 7 Gabinete de pruebas TKME (Autoría Propia) Ilustración 8 Equipos en prueba (Autoría Propia)

En esta fase se documenta la preparación y ejecución de las pruebas de funcionamiento de todos los sensores conectados al gabinete principal. Las imágenes presentadas muestran las conexiones establecidas tanto para la alimentación eléctrica como para la comunicación de datos. Se puede observar cómo se suministra energía al gabinete, además del enlace entre el módem y el Gateway. Este último se encarga de recibir la información proveniente de los sensores instalados en su entorno inmediato, y posteriormente transmitirla hacia la plataforma en la nube, la cual, en este caso, corresponde al servicio de ThingsBoard, encargado del monitoreo y visualización remota.

En las imágenes siguientes (**Ilustraciones 9 y 10**) podemos darnos cuenta, como fue el desarrollo de la práctica, en la cual se montó todo el sistema y como fue el proceso de configuración y conexión eléctrica hacia el gabinete, además de las comunicaciones con nuestra plataforma en la nube.

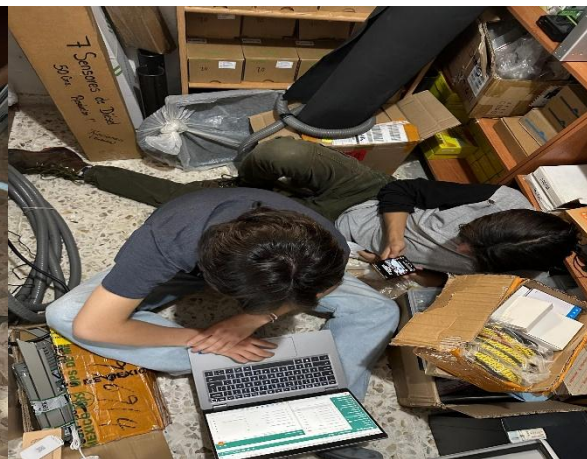


Ilustración 9 Conexiones de equipos (Autoría Propia)

Ilustración 10 Supervisión de pruebas (Autoría Propia)

3.5.- Preparación De Equipos Para Implementación En Campo

Se procedió a la configuración y preparación de los equipos que serían instalados en los centros de datos. Esto incluyó la calibración de sensores, configuraciones de gateways, la configuración de red, la instalación de sistemas operativos y el diseño de planes de contingencia para garantizar la operación continua del sistema en condiciones reales.



Ilustración 11 Creación del sensor de aire (Autoría Propia)

En las imágenes mostradas a continuación se documentan dos procesos clave del sistema de monitoreo. En la parte superior (**Ilustración 11**), se observa el ensamblaje de un sensor de flujo de aire, el cual incorpora un sensor de puerta con contacto seco, acompañado de un mecanismo tipo paleta. Este dispositivo permite detectar el flujo constante de aire proveniente de los equipos de climatización InRow o perimetrales; al mantenerse activado por el paso del aire, se puede confirmar que dichos sistemas se encuentran en funcionamiento.

En la parte inferior se presenta la configuración y verificación de una Raspberry Pi 4, la cual será utilizada como herramienta de visualización de datos provenientes de los equipos a monitorear. Esta comunicación se establece mediante el protocolo SNMP, en conjunto con la plataforma ThingsBoard para su análisis y gestión. Adicionalmente, se muestra un sensor de nivel de diésel conectado tanto a una torreta indicadora como al gateway correspondiente, el cual proporciona información precisa sobre el nivel de combustible en el tanque de la planta de emergencia. Esto permite una intervención oportuna ante cualquier posible deficiencia en el suministro.

En las imágenes que se ven a continuación (**Ilustraciones 12 y 13**), podemos ver como fue la configuración de nuestra raspberry pi 4 y de los modelos de sensores de diesel utilizados en las instalaciones.

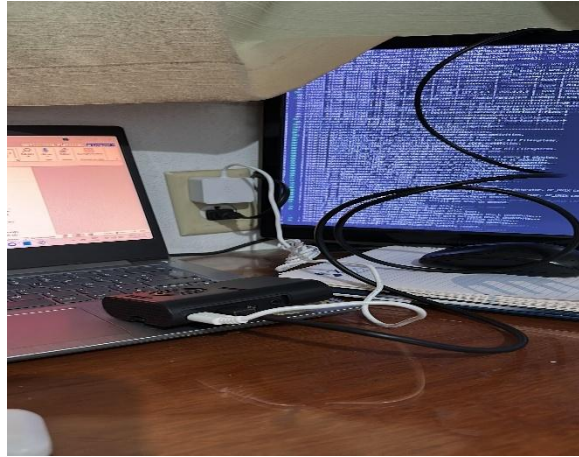


Ilustración 12 Configuración de Raspberry Pi (Autoría Propia)

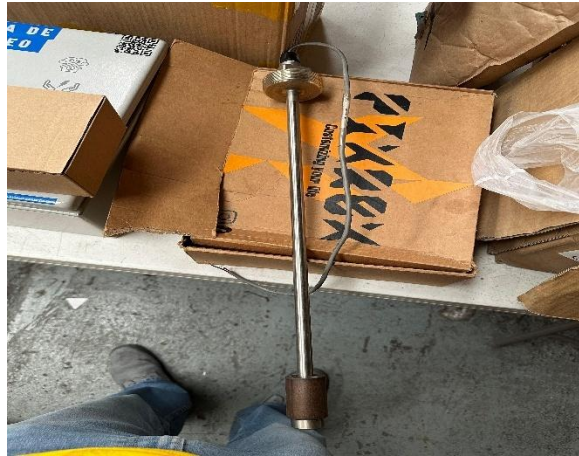


Ilustración 13 Sensor de Diesel (Autoría Propia)

3.6.- Instalación Del Sistema En Campo

Durante esta fase se realizó la implementación física del sistema de monitoreo en las instalaciones de los centros de misión crítica. Se llevó a cabo la conexión de los sensores ambientales y de seguridad, la puesta en marcha de los servidores de monitoreo y la verificación de la comunicación entre los dispositivos y la nube. Se realizaron pruebas en sitio para asegurar la correcta operación del sistema en condiciones reales.

3.6.1.- Sensores De Humedad Y Temperatura

A continuación, se muestran dos imágenes (**Ilustraciones 14 y 15**) en donde se describe el proceso de instalación de los equipos dentro de la empresa E-Global, comenzando con los sensores de temperatura y humedad. Estos dispositivos fueron estratégicamente ubicados en el exterior de los racks, específicamente en posiciones que permiten obtener una lectura representativa y precisa de las

condiciones del aire en el interior del cuarto de servidores. Esta ubicación garantiza una medición más fiable del entorno térmico general, en lugar de concentrarse únicamente en las condiciones internas de cada rack, lo que resulta esencial para una gestión ambiental efectiva del centro de datos.



Ilustración 14 Vista Frontal del sensor de Temperatura y Humedad (Autoría Propia)



Ilustración 15 Instalación de sensor de Temperatura y Humedad (Autoría Propia)

3.6.2.- Sensores De Líquidos

A continuación, se muestran en las siguientes imágenes (**Ilustraciones 16 y 17**), la instalación de los sensores de detección de líquidos. Estos sensores fueron colocados preferentemente en la parte central, de los aires de precisión y también de los equipos InRow, dentro de los cuartos de racks. En las imágenes que se muestran a continuación podemos ver las ubicaciones estratégicas que permiten una detección precisa y oportuna de posibles fugas de líquidos en las zonas críticas de enfriamiento. Su función es alertar de manera inmediata ante la presencia de humedad o derrames, lo que permite tomar acciones correctivas rápidas para evitar daños a los equipos sensibles o interrupciones en la operación del centro de datos.

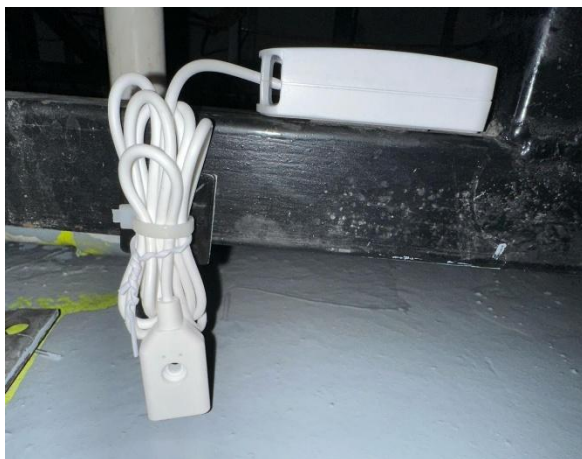


Ilustración 16 Colocación en Aire Perimetral (Autoría Propia)

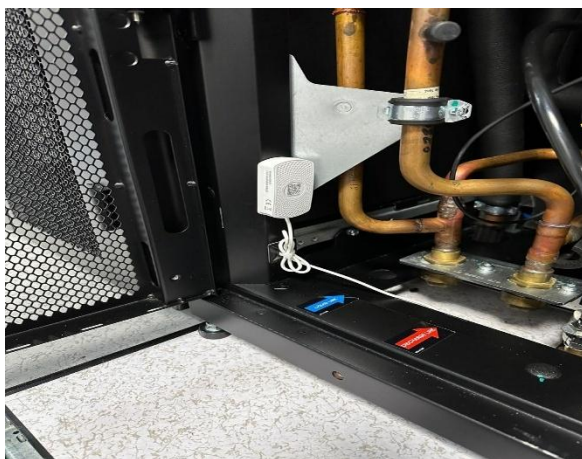


Ilustración 17 Colocación en Aire InRow (Autoría Propia)

En las imágenes presentadas se observa el proceso de instalación de los sensores de detección de líquidos. Estos dispositivos deben ser colocados de forma que ambas terminales tengan contacto directo con el suelo (**ilustración 18**), garantizando una correcta detección de fugas. La ubicación recomendada es en las zonas donde se encuentren las charolas de drenaje de los sistemas de aire acondicionado, tanto InRow como perimetrales.



Ilustración 18 Colocación correcta de Sensor (Autoría Propia)

Esta disposición permite que, en caso de presentarse una fuga de líquido, el sensor pueda detectarla oportunamente. La señal generada es enviada automáticamente a la plataforma en la nube, permitiendo una respuesta rápida por parte del personal encargado del monitoreo.

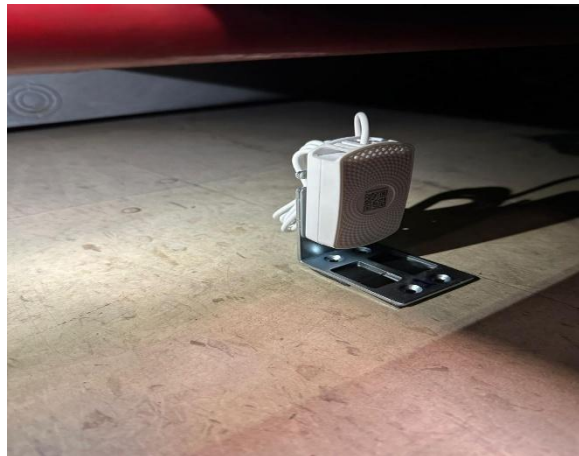


Ilustración 19 Vista de Sensor de Líquidos (Autoría Propia)

3.6.3.- Sensores De Aire

En esta etapa del proyecto, se realizó la instalación de sensores de flujo de aire en los sistemas de climatización. En el caso de los aires de precisión perimetrales (**Ilustración 20**), los sensores se colocaron en los ventiladores ubicados debajo del piso falso, como se muestran en las dos imágenes siguientes. Estos sensores se activan únicamente cuando el aire acondicionado está encendido y se mantienen operativos hasta que otro equipo de enfriamiento entre en funcionamiento o el sistema permanezca activo de forma continua.

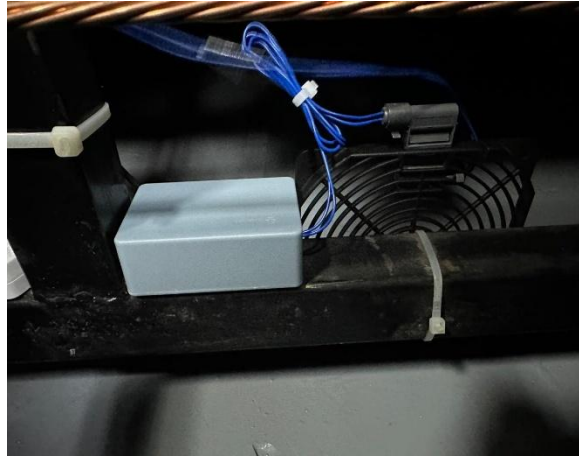


Ilustración 20 Colocación en Aire Perimetral (Autoría Propia)



Ilustración 21 Ubicaciones óptimas para el sensor (Autoría Propia)

En cuanto a los equipos InRow, los sensores se instalaron directamente frente a la corriente de aire expulsada por estos dispositivos, **(Ilustraciones 22 y 23)**. Esta ubicación permite verificar en tiempo real que el flujo de aire se mantenga constante y que los equipos de enfriamiento estén funcionando correctamente, lo que es fundamental para preservar las condiciones ambientales óptimas dentro del cuarto de racks.



Ilustración 22 Sensor En Aire InRow (Autoría Propia) Ilustración 23 Ubicación en Aire InRow (Autoría Propia)

A continuación se presentan las posiciones estratégicas utilizadas para la colocación de los sensores de flujo de aire (**Ilustraciones 24 y 25**). La correcta ubicación de estos dispositivos era fundamental para asegurar el movimiento del componente mecánico tipo “papalote”, el cual actúa como indicador del paso de aire. Si dicho elemento no se activaba, no era posible detectar el funcionamiento del sistema de climatización.



Ilustración 24 Ubicación Aire Perimetral (Autoría Propia)



Ilustración 25 Ubicación Aire Perimetral (Autoría Propia)

Durante el proceso de instalación se identificaron algunas complicaciones, principalmente relacionadas con la orientación del sensor, ya que en algunos casos el flujo de aire era adecuado, pero el sensor no respondía correctamente debido a una mala colocación del “papalote”. Esto evidenció la importancia de una instalación precisa para asegurar lecturas confiables.

Las siguientes imágenes (**Ilustración 26 y 27**), ilustran el proceso de instalación de los sensores de flujo de aire, detallando las posiciones adecuadas según el tipo de sistema de climatización presente. Se consideraron distintas configuraciones, tanto para unidades de aire de precisión tipo *InRow* como para equipos perimetrales, determinando ubicaciones óptimas que permitieran obtener lecturas precisas y representativas del funcionamiento del sistema. La correcta disposición de estos sensores fue clave para asegurar una supervisión efectiva del flujo de aire dentro de los cuartos de equipos.



Ilustración 26 Ubicación Aire InRow (Autoría Propia)

Ilustración 27 Ubicación Aire Perimetral (Autoría Propia)

3.6.4.- Sensores De Puerta (Contacto Seco)

En esta sección se detalla la instalación del sensor de apertura de puerta, el cual fue colocado estratégicamente en la parte interior del cuarto de equipos. Esta ubicación garantiza que el sensor no pueda ser manipulado ni retirado desde el exterior, fortaleciendo así las medidas de seguridad física. El sensor fue instalado dentro del marco de la puerta, lo que permite obtener lecturas precisas sobre el acceso, registrando cualquier apertura o cierre y contribuyendo al monitoreo integral del entorno y la protección del equipamiento crítico.

Lo que podemos ver en la siguiente imagen, (**Ilustraciones 28**), son la correcta colocacion de los sensores de puerta, los cuales nos avisaran si se accede al sitio de manera inadecuada o si se mantiene en un lapso mayor de tiempo de manera abierta.



Ilustración 28 Ubicación de Sensor de puerta (Autoría Propia)

3.6.5.- GATEWAY (IBeacon)

En esta sección se presenta la herramienta utilizada para la recolección de datos del sistema de monitoreo: el Gateway. Este dispositivo se instala en cada uno de los cuartos donde se han distribuido los sensores, permitiendo una gestión segmentada y eficiente de la información. Como podemos ilustra en la siguiente (**Ilustración 29**), los gateways se colocan estratégicamente en el techo de cada sala, y se conectan a un switch PoE, mediante un cable RJ45.



Ilustración 29 Colocación de Gateway (Autoría Propia)

Esta conexión no solo permite la transmisión de datos, sino que también suministra energía al Gateway, eliminando la necesidad de una fuente de alimentación adicional. Finalmente, los datos recopilados por los sensores se transmiten a la nube a través de la conexión proporcionada por un módem, que enlaza el Gateway con la red, asegurando la disponibilidad remota y centralizada de la información.

3.6.6.- Tableros Eléctricos

En esta sección se describe el procedimiento de instalación de los sensores de monitoreo eléctrico en los tableros ubicados en los cuartos de UPS. La integración se realizó tanto en los tableros de entrada como en los de salida de los sistemas UPS, con el objetivo de medir parámetros eléctricos como voltajes y corrientes en ambos extremos del flujo de energía. En las imágenes siguientes (**Ilustraciones 30 y 31**) se muestran una vista de los tableros en los que se trabajaron.

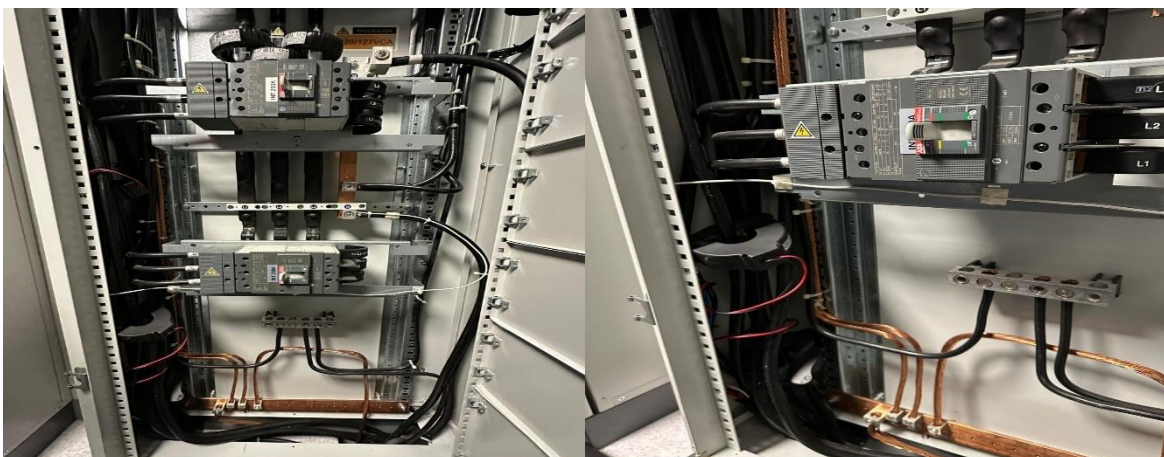


Ilustración 30 Vista general del tablero (Autoría Propia) *Ilustración 31 Vista lateral (Autoría Propia)*

Dado que se trabaja con una red trifásica, se cuenta con tres fases de 120 V cada una y un conductor neutro. Para la conexión, se utilizó un cable de control tipo

10x16, el cual alimenta el medidor de potencia CPM. De este cable, tres conductores se conectan a las entradas del CPM correspondientes a cada fase: L1, L2 y L3, mientras que el conductor del neutro se conectó a la barra de neutros del tablero. Para asegurar una correcta conexión, cada cable de fase fue terminado con una terminal tipo espada y fijado firmemente a la barra correspondiente, garantizando una conducción eléctrica confiable. Como se pueden ver en la imagen siguiente (**Ilustración 32**).



Ilustración 32 Cableado hacia el CPM 50 (Autoría Propia)

Posteriormente, se instalaron transformadores de corriente (TC) de relación 800/5 A, como se ven en las imágenes siguientes (**Ilustración 33 y 34**), tanto en la entrada como en la salida de los UPS. Cada TC se conectó a través de dos conductores provenientes del CPM, en las imágenes se ilustra las conexiones, uno para cada fase, lo cual permite la medición de la corriente en tiempo real. Los cables se empalmaron con conectores adecuados, se prensaron (“poncharon”) correctamente y se aislaron con materiales apropiados para evitar contactos eléctricos accidentales.



Ilustración 33 Instalación de Transformadores de Corriente (Autoría Propia)



Ilustración 34 Ubicación de los transformadores (Autoría Propia)

Una vez conectados los transformadores de corriente, se procedió a abrazar con cada uno de ellos las líneas correspondientes a cada fase. Es importante observar la dirección del flujo de corriente para asegurar una lectura correcta, ya que una inversión podría reflejar valores negativos. En las imágenes siguientes (**Ilustraciones 35 y 36**), se muestra la correcta colocación de los transformadores de corriente. En caso de detectar esta situación, basta con invertir la orientación del TC para corregirla.



Ilustración 35 Correcta colocación de los Transformadores (Autoría Propia)



Ilustración 36 Colocación en otra locación (Autoría Propia)

Para garantizar seguridad en el trabajo dentro del tablero eléctrico, se utilizó cable de control blindado, el cual ayuda a minimizar riesgos en caso de cortocircuitos o fallas eléctricas, tanto internas como externas. Además, se siguieron estrictamente las normas de seguridad eléctrica, incluyendo el uso completo de equipo de protección personal (EPP), herramientas dieléctricas y un tapete de neopreno para el aislamiento del operario respecto al suelo, reduciendo así el riesgo de electrocución durante las maniobras de instalación.

En estas imágenes (**Ilustraciones 37 y 38**) se muestran los resultados finales de esta instalación en el tablero eléctrico.

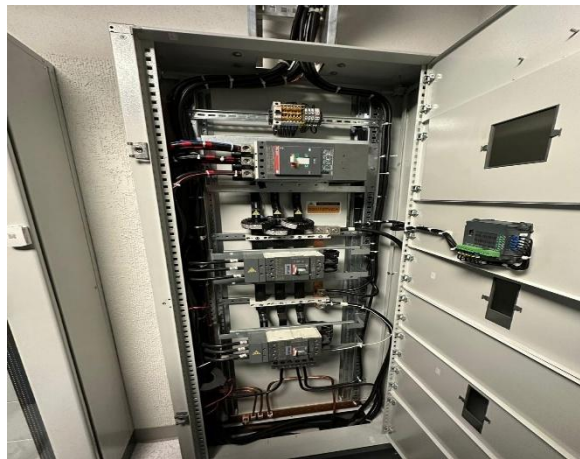


Ilustración 37 Resultado final de tablero (Autoría Propia)

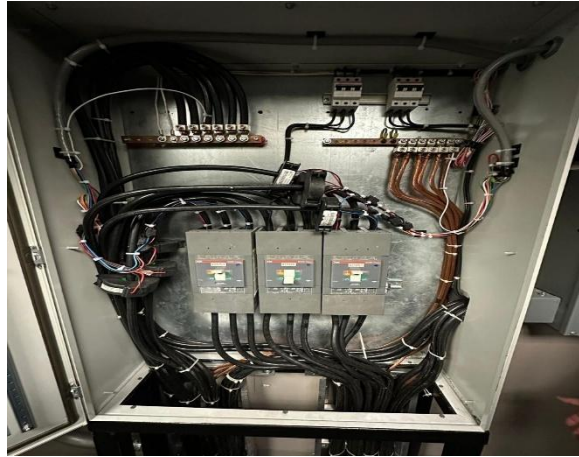


Ilustración 38 Diferente tablero con la misma operación (Autoría Propia)

3.6.7.- Montaje De Gabinetes

En esta sección se describe el proceso de instalación y montaje de los gabinetes dentro de las instalaciones de la empresa. Inicialmente, se identificó la ubicación más adecuada para su colocación, considerando aspectos como el acceso a cableado estructurado, ventilación y proximidad a los equipos a monitorear. En las imágenes siguientes se ven las instalaciones de los gabinetes de la empresa.



Ilustración 39 Gabinete de swtiches con pasos (Autoría Propia)



Ilustración 40 Gabinete principal con pasos (Autoría Propia)

Previo al montaje definitivo, se realizaron adecuaciones físicas en los gabinetes, creando pasos para permitir el enrutamiento ordenado de los cables de comunicación hacia los switches instalados. En las imágenes anteriores (**Ilustraciones 39 y 40**), se muestran los pasos creados en los gabinetes para así hacer pasar los cables de un gabinete a otro. Además, se habilitaron aperturas laterales destinadas al paso de los conductores eléctricos que alimentan los contactores integrados en el sistema.



Ilustración 41 Gabinete conectado a la alimentación (Autoría Propia)



Ilustración 42 Punteo de Switches (Autoría Propia)

Una vez concluido el montaje físico, se procedió a conectar los gabinetes a la red de alimentación eléctrica (**Ilustración 41**), verificando el funcionamiento correcto de los componentes. Tras encender los contactores y comprobar su operatividad, se implementó un puente entre los switches (**Ilustración 42**), con el objetivo de establecer conectividad de red entre todos los gabinetes, centralizando la comunicación a través del gabinete principal.

3.6.8.- Revision De Conexiones De Internet En El Sitio

Antes de proceder con la conexión definitiva de los dispositivos al sistema de monitoreo, es esencial llevar a cabo pruebas preliminares de conectividad y funcionamiento de red. Estas imágenes (**Ilustraciones 43 y 44**), representan las pruebas que aseguran que todos los equipos se comuniquen correctamente y estén listos para su integración operativa.



Ilustración 43 Conexiones en gabinete principal (Autoría Propia)

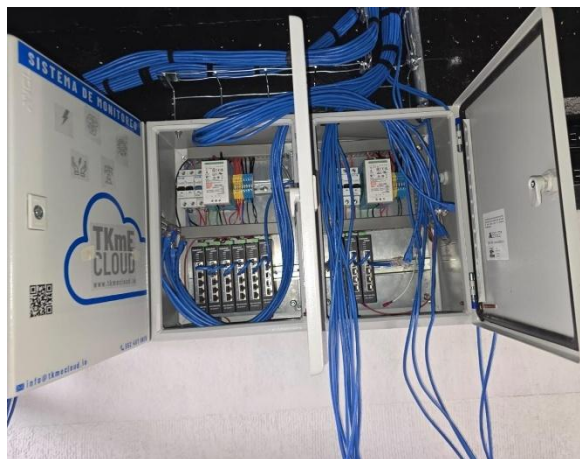


Ilustración 44 Conexiones en Bunker 2 (Autoría Propia)

El proceso comienza verificando que el gabinete principal cuente con alimentación eléctrica estable, mediante las conexiones de corriente adecuadas. Una vez confirmada la energización, se conecta el módem con acceso a Internet a uno de los switches instalados dentro del gabinete. A este switch también se conectan el IoT Gateway y la Raspberry Pi 4, los cuales actuarán como concentradores de datos y visualización en tiempo real de los sensores instalados.

Adicionalmente, se conecta una laptop al puerto Ethernet (**Ilustración 45**) el cual se muestra en la siguiente figura, del cual esta restante del módem para realizar la configuración de red. En esta etapa, es necesario cambiar la configuración de red de la laptop, deshabilitando el modo DHCP y asignándole manualmente una dirección IP estática dentro del mismo rango de red que el módem y los dispositivos conectados. Esto permite una comunicación directa sin interferencias del servidor de direcciones.

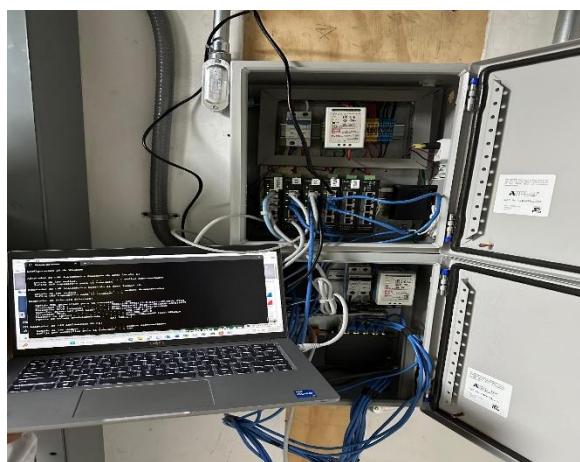


Ilustración 45 Pruebas de conexión a red (Autoría Propia)

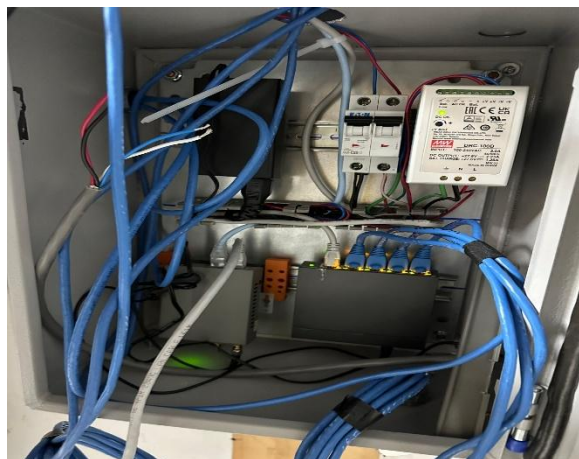


Ilustración 46 Conexiones en Switch principal (Autoría Propia)

Una vez configurada la red, se procede a realizar pruebas de conectividad mediante el uso del comando “ping” hacia las direcciones IP de los dispositivos. Esta prueba permite validar que los paquetes de red llegan correctamente a cada equipo y que estos responden sin pérdidas ni latencia excesiva. Una respuesta positiva confirma que el IoT Gateway, la Raspberry Pi y los demás dispositivos están correctamente enlazados y preparados para iniciar el monitoreo de datos a través de la plataforma en la nube (ThingBoard).

Estas pruebas resultan fundamentales, ya que permiten detectar fallas tempranas de comunicación, errores de configuración o posibles conflictos de red antes de pasar a la etapa de operación continua del sistema.

3.6.9.- Configuración De Equipos En Sitio

En esta etapa del proyecto se describe el proceso de configuración de dispositivos de red y monitoreo, entre los cuales se incluyen RPDUs (Power Distribution Units inteligentes), aires de precisión tipo InRow y unidades perimetrales. El objetivo principal de esta configuración es integrar dichos equipos al sistema de monitoreo en la nube, asegurando una comunicación eficiente y estable dentro del segmento de red definido para el proyecto.



Ilustración 47 Equipo PDU Panduit (Autoría Propia)

Ilustración 48 Ip default del equipo (Autoría Propia)

El primer paso consiste en verificar si los equipos cuentan con una dirección IP predeterminada de fábrica como se ilustra en la **(Ilustración 48)**, y si disponen de una interfaz de administración accesible, desde la cual sea posible modificar la configuración de red. Este análisis inicial es fundamental para garantizar que el dispositivo pueda integrarse correctamente al esquema de direccionamiento del sistema.

Una vez identificada la IP por defecto del equipo, se realiza una conexión directa desde una laptop al dispositivo. Para lograr esta comunicación inicial, se asigna manualmente una dirección IP estática a la laptop, correspondiente al mismo segmento de red del equipo. Posteriormente, se emplea la herramienta de línea de comandos (CMD) para ejecutar un “ping” a la IP del dispositivo como se muestra en la siguiente **(Ilustración 49)**, con el fin de confirmar que existe conectividad y que el equipo está respondiendo correctamente.



Ilustración 49 Realización de Ping al equipo (Autoría Propia)

Ilustración 50 Display de Aire InRow (Autoría Propia)

Tras verificar la comunicación, se procede a cambiar la configuración de red del equipo desde su interfaz, asignándole una nueva dirección IP estática acorde al segmento de red del sistema de monitoreo. Una vez completado este cambio, se ajusta nuevamente la configuración de red de la laptop para que se encuentre dentro del nuevo rango. Esto permite acceder nuevamente al dispositivo, ahora bajo su nueva dirección IP, y continuar con su configuración avanzada o integración al entorno de monitoreo.

Este procedimiento se repite para cada uno de los equipos que se integrarán al sistema, asegurando así una topología de red coherente, organizada y segura. Una configuración adecuada desde el inicio evita conflictos de red, facilita el mantenimiento y mejora la eficiencia del monitoreo remoto.



Ilustración 51 Vista general del equipo InRow

3.7.- Revision De Equipos Por Medio De Thingsboard Y SNMP

3.7.1.- Sensores En Sitio Y Visualización En Thingsboard

Esta fase del proyecto representa uno de los puntos más críticos y relevantes, ya que se centra en el monitoreo integral de todos los dispositivos previamente instalados, asegurando que operen de manera continua y eficiente. La supervisión se realiza mediante la plataforma de visualización y análisis *ThingsBoard*, la cual permite observar en tiempo real el estado de cada sensor implementado.

En total, se distribuyeron sensores en cuatro ubicaciones distintas dentro de la empresa, adaptando la solución de monitoreo a las características y necesidades de cada sitio. Los dispositivos instalados en estos espacios incluyeron sensores de temperatura y humedad, sensores de flujo de aire, sensores de detección de

líquidos, y sensores de puerta o control de acceso al site. Estos elementos proporcionan datos clave para el mantenimiento de condiciones ambientales seguras y controladas en áreas críticas como salas de racks y centros de datos.

Cada sensor está conectado a un *IoT Gateway*, el cual cumple la función de recolectar los datos generados por los dispositivos en campo. A su vez, el Gateway transmite esta información al servidor en la nube mediante un módem con conectividad a Internet. La plataforma *ThingsBoard* actúa como interfaz gráfica y punto central de gestión, permitiendo a los responsables del sistema visualizar en tiempo real el estado operativo de todos los sensores, generar alertas ante eventos críticos, y tomar decisiones de mantenimiento o intervención correctiva de manera remota y oportuna.

Este esquema de monitoreo no solo facilita la supervisión constante del entorno tecnológico de la empresa, sino que también mejora la eficiencia operativa y contribuye a garantizar la continuidad del servicio en infraestructuras críticas.

3.7.2.- Conexiones De Equipos Con SNMP Y Thingsboard

En esta fase del proyecto se abordó la configuración del protocolo SNMP (*Simple Network Management Protocol*) para establecer comunicación entre los equipos a monitorear y el equipo central de gestión, en este caso, una computadora portátil. Este proceso es esencial para integrar dispositivos inteligentes a un sistema de monitoreo remoto que permita la recolección eficiente de datos operativos.

Una vez que a cada dispositivo (como RPDUs, aires de precisión o UPS) se le asignó una dirección IP estática acorde al segmento de red definido, se procedió a configurar la dirección IP de la computadora portátil también dentro de dicho segmento, como se muestran en las dos imágenes siguientes (**Ilustraciones 52 y 53**). Posteriormente, se realizó una prueba de conectividad mediante comandos básicos como ping desde la terminal (CMD), verificando así la correcta comunicación con los equipos.

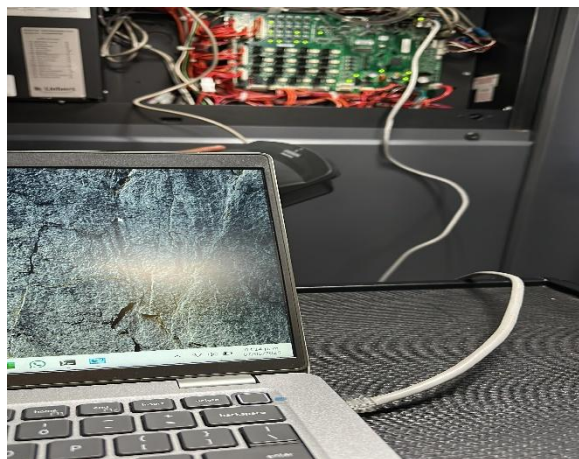


Ilustración 52 Conexión de laptop a equipo (Autoría Propia)

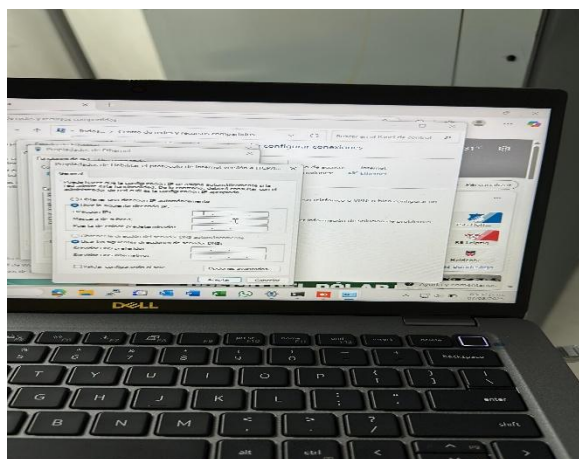


Ilustración 53 Cambio de DHCP a IP static (Autoría Propia)

Con la conectividad establecida, se accedió a la interfaz web de los dispositivos mediante un navegador, desactivando previamente el Wi-Fi para asegurar que toda la comunicación ocurriera a través de la red cableada. Luego del acceso mediante credenciales administrativas, se ingresó a la configuración del protocolo SNMP. Dentro de esta sección, se configuraron los usuarios autorizados y se registró la IP de la computadora gestora como dispositivo confiable, permitiendo así la consulta remota de datos.

Para validar el funcionamiento del protocolo SNMP, se utilizaron herramientas como nmap (**Ilustración 54**), que permite escanear la red para identificar dispositivos conectados y puertos abiertos, y snmpwalk, (**Ilustración 55**), una utilidad que consulta y recupera información estructurada de los equipos a través de sus OIDs (*Object Identifiers*). Estos OIDs representan valores específicos como temperatura, humedad, consumo energético, entre otros.

PDU adicional de la marca Chatsworth. En cada uno de ellos se realizaron ajustes en la red, integración mediante protocolos de comunicación como SNMP, y se habilitaron funcionalidades que permiten su supervisión remota desde la plataforma de monitoreo utilizada en el proyecto.

3.7.3.- Schneider Electric InRow

En las siguientes imágenes (**Ilustraciones 56 y 57**), se pueden observar diversos parámetros clave correspondientes al funcionamiento de un aire de precisión tipo InRow. Estos datos permiten una supervisión detallada del comportamiento térmico y de humedad dentro del cuarto de equipos. Entre los principales valores monitoreados se encuentran el punto de ajuste de enfriamiento, la temperatura mínima de entrada del aire al bastidor del grupo, y el estado del control de flujo activo. Asimismo, se visualizan variables relacionadas con la regulación de humedad, como la demanda y salida de humidificación y deshumidificación grupal, además de la temperatura del punto de rocío. También se registran parámetros críticos como la demanda y salida de enfriamiento, la demanda de recalentamiento, el flujo de aire grupal y la temperatura máxima de entrada al bastidor. Esta información es fundamental para asegurar el funcionamiento óptimo y continuo del sistema de climatización en entornos críticos como los centros de datos.

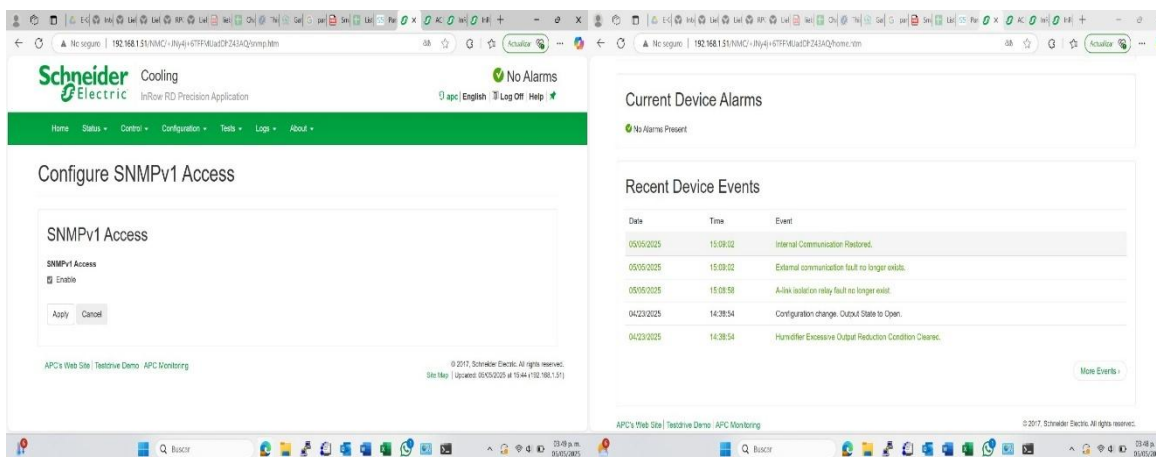


Ilustración 56 Configuración SNMP (Autoría Propia)

Ilustración 57 Status del equipo (Autoría Propia)

3.7.4.- PDU PANDUIT

De igual forma, en las interfaces de los PDU (Unidades de Distribución de Energía) se pueden observar múltiples parámetros eléctricos relevantes para el monitoreo y diagnóstico del consumo energético en los cuartos de equipos. Entre los valores más destacados se encuentran las corrientes, los voltajes, la potencia activa (W), la potencia aparente (VA), el factor de potencia y la energía acumulada en kilowatt-hora (kWh). Estos indicadores permiten evaluar la eficiencia energética y la estabilidad del suministro en tiempo real.

Además, para cada uno de los PDU es posible consultar lecturas específicas como las corrientes RMS, los valores RMS de voltaje y las cargas distribuidas por línea (**Ilustración 59**). Esta información es esencial para prevenir sobrecargas, optimizar el balance de cargas entre fases y garantizar un suministro eléctrico seguro y constante en entornos críticos como los centros de datos.

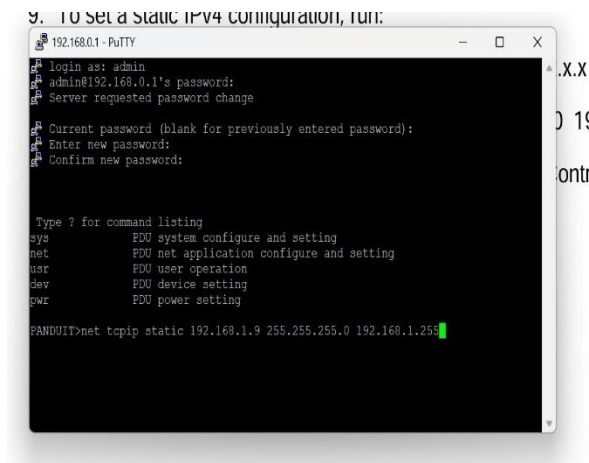


Ilustración 58 Cambio de Ip default Ip deseada (Autoría Propia)

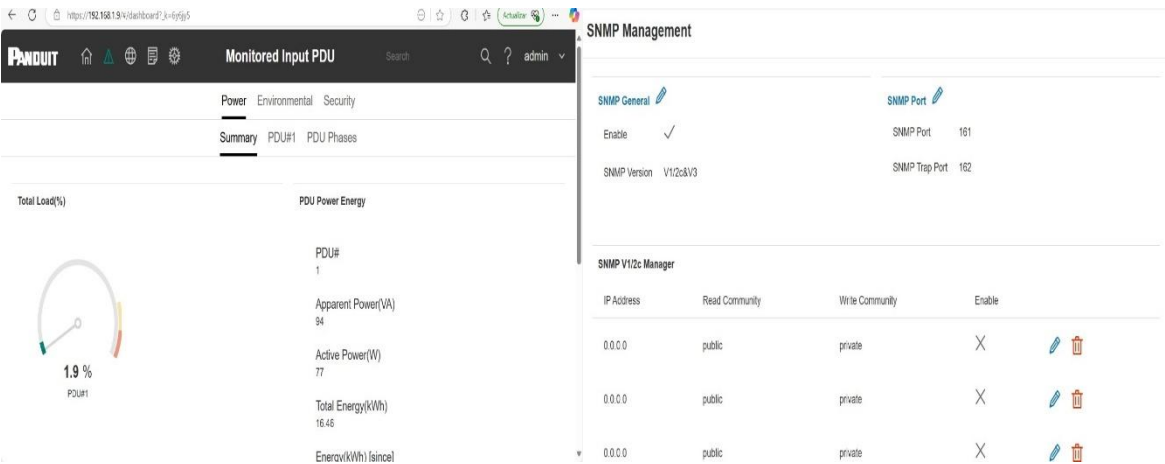


Ilustración 59 Interfaz de PDU Panduit (Autoría Propia) Ilustración 60 Apartado de SNMP (Autoría Propia)

3.7.5.- PDU Chatsworth

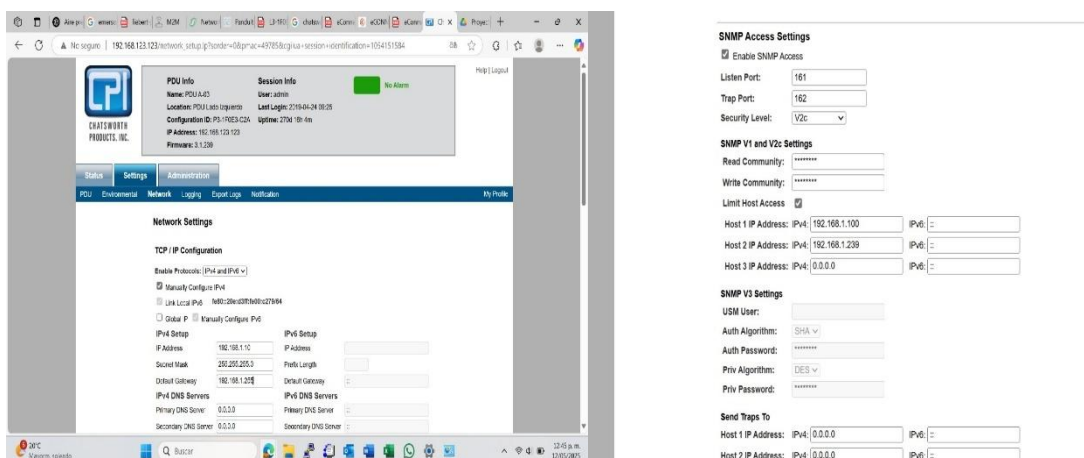


Ilustración 61 Interfaz de PDU Chatsworth (Autoría Propia) Ilustración 62 Información de SNMP (Autoría Propia)

3.7.6.- Thingsboard Y Su Entorno Grafico (Dashboards)

En las capturas de pantalla correspondientes a la interfaz de la plataforma ThingsBoard, se puede apreciar de manera organizada y centralizada el monitoreo integral de todos los dispositivos implementados por la empresa TKME. La visualización incluye (**ilustraciones 63, 64 y 65**), cada uno de los equipos conectados, tales como los medidores de energía modelo CPM-20, los IoT Gateways responsables de la recolección y transmisión de datos, así como los distintos dispositivos configurados mediante el protocolo SNMP.

Asimismo, se identifican claramente los distintos cuartos o zonas en las que se encuentran distribuidos los sensores ambientales, los cuales permiten supervisar parámetros críticos como temperatura, humedad, flujo de aire, presencia de líquidos y acceso físico. Esta vista general facilita una gestión remota eficiente, el análisis de condiciones ambientales en tiempo real y la capacidad de respuesta ante cualquier anomalía en la infraestructura crítica del centro de datos.

Dispositivos Filtro de dispositivo Include customer entities + ↺ 🔍								
☐	Fecha de creación ↓	Nombre	Perfil de dispositivo	Etiqueta	Estado	Customer name	Groups	Es gateway
☐	2025-05-08 14:06:46	SNMP InRow	snmp		Activo			☐
☐	2025-05-08 14:06:46	SNMP PDU8	snmp		Activo			☐
☐	2025-05-08 14:06:46	SNMP PDU9	snmp		Activo			☐
☐	2025-05-06 11:39:27	SNMP Aire	snmp		Activo			☐
☐	2025-03-24 21:03:11	Cuarto eléctrico 2	Dispositivos_S1S4		Activo			☐
☐	2025-03-24 21:02:56	Cuarto eléctrico 1	Dispositivos_S1S4		Activo			☐
☐	2025-03-24 21:02:34	Bunker2	Dispositivos_S1S4		Activo			☐
☐	2025-03-24 21:01:45	Bunker1 y cubricaciones	Dispositivos_S1S4		Activo			☐

Ilustración 63 Visualización de SNMP (Autoría Propia)

☐	2025-02-03 16:44:32	CPM13	CPMDevice		Inactivo			☐
☐	2025-02-03 16:42:40	CPM12	CPMDevice		Inactivo			☐
☐	2025-02-03 16:41:50	CPM11	CPMDevice		Inactivo			☐
☐	2025-02-03 16:40:37	CPM10	CPMDevice		Inactivo			☐
☐	2025-02-03 16:39:15	CPM9	CPMDevice		Inactivo			☐
☐	2025-02-03 16:38:15	CPM8	CPMDevice		Inactivo			☐
☐	2025-02-03 16:37:02	CPM7	CPMDevice		Inactivo			☐
☐	2025-02-03 16:11:10	CPM6	CPMDevice		Inactivo			☐

Ilustración 64 Visualización de CPM 20 (Autoría Propia)

☐	Fecha de creación ↓	Nombre	Perfil de dispositivo	Etiqueta	Estado	Customer name	Groups	Es gateway
☐	2025-02-03 16:07:43	CPM5	CPMDevice		Inactivo			☐
☐	2025-02-03 16:06:44	CPM4	CPMDevice		Inactivo			☐
☐	2025-02-03 16:05:48	CPM3	CPMDevice		Inactivo			☐
☐	2025-02-03 16:04:47	CPM2	CPMDevice		Inactivo			☐
☐	2025-02-03 16:03:03	CPM1	CPMDevice		Inactivo			☐
☐	2025-01-30 16:19:32	IoTGateway	default		Activo			☒

Ilustración 65 Visualización de IoT Gateway (Autoría Propia)

3.7.7.- Dashboards De Cuartos Monitoreados

A continuación, se presentan los dashboards **68, 69, 70, 71 y 72**), diseñados para la visualización y supervisión en tiempo real de las variables ambientales de los diferentes cuartos monitoreados, los cuales incluyen: Bunker 1 (**Ilustraciones 66 y 67**), Bunker 2 (**Ilustraciones 68 y 69**), Cuarto Eléctrico 1 (**Ilustración 70**), Cuarto Eléctrico 2 (**Ilustración 71**) y la sala de Cubicaciones (**Ilustración 72**).

Cada uno de estos paneles de control fue configurado en la plataforma ThingsBoard, permitiendo observar de forma clara y estructurada los datos recopilados por los sensores instalados. Entre las variables monitoreadas se encuentran la temperatura, la humedad relativa, el flujo de aire, la presencia de líquidos y el estado del acceso físico a cada cuarto.

La implementación de estos dashboards permite una gestión eficiente del entorno físico de la infraestructura crítica, ya que ofrece alertas tempranas, históricos de datos y visualizaciones dinámicas que facilitan la toma de decisiones técnicas en tiempo real. Gracias a esta integración, es posible mantener condiciones óptimas de operación para los equipos y garantizar la seguridad de las instalaciones.

Bunker 1

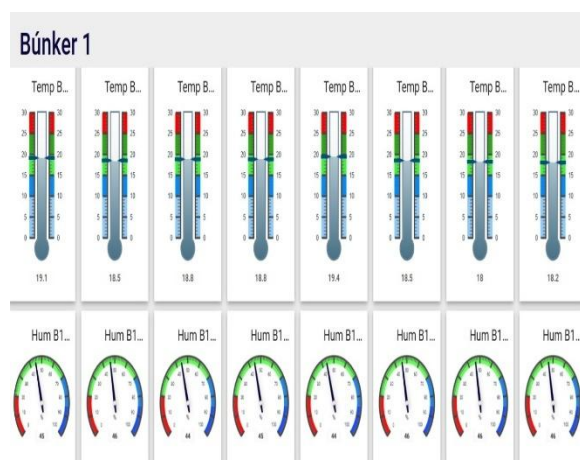


Ilustración 66 Temperatura y Humedad (Autoría Propia)

Búnker 1

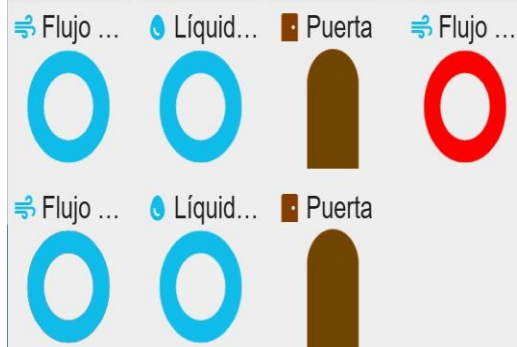


Ilustración 67 Flujo de Aire, Líquidos y Puerta (Autoría Propia)

Bunker 2

Búnker 2

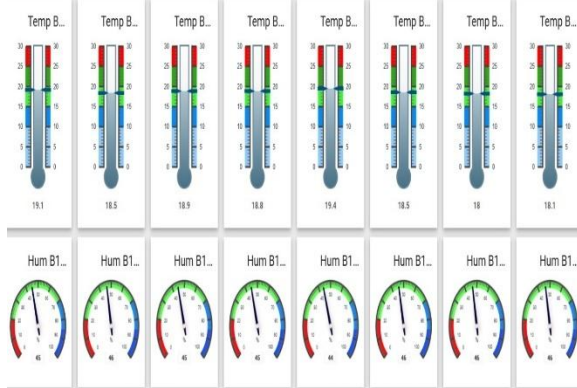


Ilustración 68 Temperaturas y Humedad (Autoría Propia)

Búnker 2

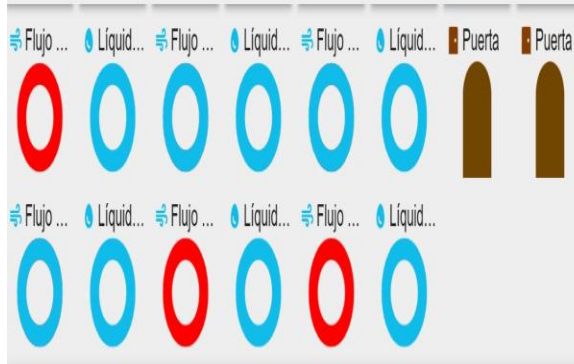


Ilustración 69 Flujo de Aire, Líquidos y Puerta (Autoría Propia)

Cuarto Eléctrico 1

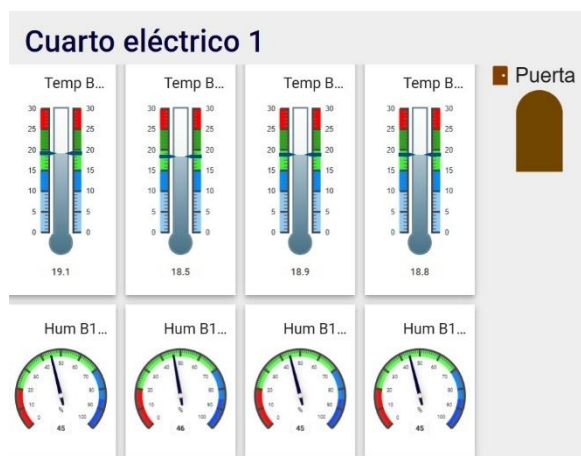


Ilustración 70 Temperatura, Humedad y Puerta (Autoría Propia)

Cuarto Eléctrico 2

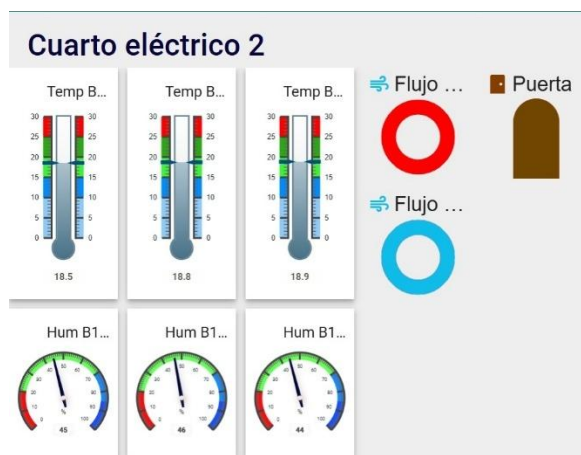


Ilustración 71 Temperatura, Humedad, Flujo de Aire y Puerta (Autoría Propia)

Cubicaciones



Ilustración 72 Temperatura, Humedad y Puerta (Autoria Propia)

3.8.- Documentación Del Proyecto

Finalmente, se elaboró la documentación técnica del sistema desarrollado, incluyendo diagramas de conexión, manuales de usuario, procedimientos de instalación y mantenimiento, y un análisis de los resultados obtenidos. Esta documentación es esencial para garantizar la continuidad operativa, facilitar futuras actualizaciones y servir como referencia para otros proyectos similares dentro de la empresa.

CAPÍTULO IV

RESULTADOS

Resultados:

A lo largo del desarrollo del proyecto se obtuvieron resultados altamente satisfactorios en términos de supervisión, control y visibilidad remota de las condiciones ambientales y energéticas de los cuartos críticos de la empresa. El sistema implementado permitió una supervisión integral de variables esenciales como temperatura, humedad, flujo de aire, presencia de líquidos y control de acceso, mediante sensores estratégicamente ubicados que enviaban información en tiempo real a la plataforma ThingsBoard. Esto permitió no solo detectar condiciones anómalas, sino también anticipar posibles fallos o situaciones de riesgo.

En cuanto a la gestión energética, se incorporaron medidores inteligentes (CPM) para la supervisión de los tableros eléctricos que alimentan los UPS, así como PDU inteligentes de marcas como Panduit y Chatsworth, con capacidad para brindar datos detallados de voltaje, corriente, potencia activa, potencia aparente, consumo energético, entre otros. Estos equipos fueron integrados utilizando el protocolo SNMP, lo que facilitó su incorporación a la red de monitoreo y permitió su visualización desde la misma plataforma centralizada.

Se realizaron configuraciones específicas para cada equipo, como la asignación de IPs estáticas y la validación de la comunicación mediante comandos especializados como ping, nmap y snmpwalk. A través de estos procesos se pudo confirmar la disponibilidad de los equipos y la correcta lectura de los datos mediante los OID respectivos. De esta forma se aseguró que cada dispositivo estuviera correctamente integrado a la red y aportara información útil para la operación.

También se logró una efectiva comunicación entre los gateways IoT y los sensores distribuidos en los distintos cuartos. Estos dispositivos, conectados mediante switches PoE y módems con acceso a Internet, recopilaban y transmitían la información de forma continua hacia la nube, permitiendo la supervisión remota desde cualquier lugar. En la plataforma ThingsBoard se diseñaron dashboards personalizados por cada sitio monitoreado, incluyendo variables como temperatura, humedad, presencia de líquidos, flujo de aire y estado de puertas, lo que facilitó un control ordenado y visualmente claro.

Otro resultado destacable fue la incorporación de sensores especiales, como los de nivel de diésel conectados a torretas visuales y gateways, permitiendo conocer de forma precisa el nivel de combustible en las plantas de emergencia. Esto agregó un valor significativo a la gestión preventiva y al mantenimiento operativo de los sistemas de respaldo energético.

Por último, también se desarrollaron gabinetes físicos personalizados para alojar el hardware necesario del sistema de monitoreo. Estos gabinetes fueron fabricados tomando en cuenta la organización interna, la ventilación, la estética corporativa y la seguridad eléctrica. Se realizaron pruebas de funcionamiento, verificación de

conexiones, puenteo de switches y pruebas de conexión de red antes de su montaje final en las ubicaciones definidas.

En conjunto, los resultados obtenidos confirman el éxito del proyecto al proporcionar una solución de monitoreo integral, precisa y confiable, que optimiza la gestión de infraestructura crítica y permite una reacción inmediata ante cualquier irregularidad que pudiera presentarse. Esta solución, además de ser robusta y funcional, es escalable, lo que permite adaptarla fácilmente a nuevas ubicaciones o futuras necesidades operativas.

Planos:

Respecto a los planos de la empresa, estos contienen información sensible relacionada con la infraestructura física y operativa de la organización. El compartir estos documentos representa un riesgo porque:

1. **Comprometen la seguridad física:**
Los planos pueden revelar la ubicación de servidores, cuartos de control, rutas de evacuación, accesos restringidos o sistemas de energía, lo cual podría ser aprovechado por personas con intenciones maliciosas.
2. **Exponen vulnerabilidades:**
Al mostrar cómo está distribuida la infraestructura, se podrían identificar puntos débiles en la seguridad, accesos no protegidos o rutas críticas, lo que aumenta el riesgo de sabotaje o robo.
3. **Son información confidencial:**
En muchos casos, estos documentos forman parte de los **activos estratégicos de la empresa**, y su divulgación puede violar políticas internas, contratos de confidencialidad o normativas de protección de datos.
4. **Ponen en riesgo la continuidad del contrato:**
Un acceso no autorizado a esta información puede afectar directamente la operación del negocio y su capacidad de respuesta ante emergencias.

Como una alternativa se muestran los documentos de los equipos en los cuales se implementaron los monitoreos de mejora.

Manuales:

A continuación se presenta un link de Google drive en el cual se pueden encontrar todos los documentos relacionados con el proyecto y sus implementaciones.
https://drive.google.com/drive/folders/1MfdvZcXLeGx7mtok3JELp2v8W7Z8Ee3t?usp=drive_link

Programas:

En los programas utilizados en este proyecto, se utilizaron los siguientes programas:

-Modbus Poll

-Putty

-Thingsboard

Normativas:

1.- NORMA OFICIAL MEXICANA NOM-004-STPS-1999, SISTEMAS DE PROTECCION Y DISPOSITIVOS DE SEGURIDAD EN LA MAQUINARIA Y EQUIPO QUE SE UTILICE EN LOS CENTROS DE TRABAJO

2.- NORMA OFICIAL MEXICANA NOM-009-STPS-2011, CONDICIONES DE SEGURIDAD PARA REALIZAR TRABAJOS EN ALTURA

3.- NORMA OFICIAL MEXICANA NOM-017-STPS-2024, EQUIPO DE PROTECCIÓN PERSONAL-SELECCIÓN, USO Y MANEJO EN LOS CENTROS DE TRABAJO

4.- NORMA OFICIAL MEXICANA NOM-022-STPS-2015, ELECTRICIDAD ESTÁTICA EN LOS CENTROS DE TRABAJO-CONDICIONES DE SEGURIDAD

5.- NORMA OFICIAL MEXICANA NOM-026-STPS-2008, COLORES Y SEÑALES DE SEGURIDAD E HIGIENE, E IDENTIFICACION DE RIESGOS POR FLUIDOS CONDUCTIVOS EN TUBERIAS

6.- NORMA OFICIAL MEXICANA NOM-029-STPS-2011, MANTENIMIENTO DE LAS INSTALACIONES ELECTRICAS EN LOS CENTROS DE TRABAJO-CONDICIONES DE SEGURIDAD

7.- NORMA OFICIAL MEXICANA NOM-033-STPS-2015, CONDICIONES DE SEGURIDAD PARA REALIZAR TRABAJOS EN ESPACIOS CONFINADOS

8.- NORMA OFICIAL MEXICANA NOM-036-1-STPS-2018, FACTORES DE RIESGO ERGONÓMICO EN EL TRABAJO-IDENTIFICACIÓN, ANÁLISIS, PREVENCIÓN Y CONTROL. PARTE 1: MANEJO MANUAL DE CARGAS.

Conclusiones, recomendaciones, experiencia profesional adquirida.

Conclusiones

El desarrollo e implementación del sistema de monitoreo ambiental y energético en los centros de datos de la empresa representó un proyecto integral que abarcó

múltiples áreas técnicas, desde la instalación física de sensores hasta la configuración lógica de redes y protocolos de comunicación como SNMP. Se logró diseñar e implementar una solución robusta capaz de recopilar datos en tiempo real sobre parámetros críticos como temperatura, humedad, presencia de líquidos, apertura de puertas, niveles de diésel y flujo de aire de los sistemas de climatización, entre otros.

La correcta colocación de los sensores en puntos estratégicos dentro del cuarto de racks, como en los aires de precisión, bandejas de condensación y puertas de acceso, permitió capturar lecturas precisas y confiables. La incorporación de gateways IoT energizados mediante switches PoE facilitó una instalación limpia y funcional, mientras que la integración de la plataforma ThingsBoard permitió la visualización remota de los datos y la generación de alertas en caso de anomalías.

También se logró integrar exitosamente el monitoreo de dispositivos inteligentes como RPDUs y UPS mediante el protocolo SNMP, lo cual amplió la cobertura del sistema hacia el consumo energético y el estado de los dispositivos críticos. Este enfoque no solo optimiza la operación del centro de datos, sino que también mejora la capacidad de respuesta ante fallas y eventos de riesgo, garantizando mayor continuidad operativa y protección de los activos tecnológicos.

En términos generales, el proyecto cumplió con los objetivos técnicos propuestos, aportando un sistema escalable y eficiente que fortalece la infraestructura crítica de la organización mediante el uso de tecnologías modernas y prácticas de instalación profesional.

Recomendaciones

1. **Mantenimiento Preventivo Regular:** Se recomienda establecer un calendario de mantenimiento para verificar el estado físico y funcional de los sensores, gateways, RPDUs y demás equipos. Esto ayudará a prevenir fallas y asegurar lecturas precisas a largo plazo.
2. **Pruebas de Red y Comunicación:** Es importante realizar revisiones periódicas de la conectividad de red, especialmente en los enlaces entre gateways y la nube, así como entre los dispositivos SNMP y la plataforma de monitoreo. Problemas de conectividad pueden afectar la integridad de los datos.
3. **Filtrado de Datos SNMP:** Se debe continuar optimizando el filtrado de OIDs para que el sistema muestre únicamente información relevante. Esto mejora la usabilidad del panel de monitoreo y facilita la toma de decisiones.

4. **Capacitación del Personal:** Para asegurar la sostenibilidad del sistema, se recomienda capacitar al personal interno en el uso de la plataforma ThingsBoard, interpretación de datos y mantenimiento básico de la infraestructura instalada.
5. **Expansión del Sistema:** La solución actual tiene potencial de escalar a otros sitios o edificios. Se recomienda evaluar nuevas áreas de monitoreo, como consumo de energía por rack, control de acceso con autenticación biométrica, o sensores de humo/gases para detección temprana de incendios.
6. **Seguridad Física y de Red:** Asegurar la protección física de sensores y gabinetes es clave. Asimismo, se deben implementar medidas de ciberseguridad para proteger la red y los dispositivos IoT de posibles accesos no autorizados.

Experiencia Profesional Adquirida

Durante el desarrollo de este proyecto, se adquirió una valiosa experiencia profesional en diversas áreas clave de la ingeniería, particularmente en infraestructura crítica y tecnologías de monitoreo. Entre las principales competencias desarrolladas se encuentran:

- **Instalación y cableado estructurado:** Se profundizó en el manejo y organización de cableado de datos y energía dentro de entornos controlados, respetando estándares de seguridad y buenas prácticas.
- **Protocolos de comunicación:** La implementación de SNMP permitió comprender cómo se realiza la comunicación entre dispositivos inteligentes y plataformas de monitoreo, incluyendo la interpretación de OIDs y el uso de herramientas como snmpwalk y nmap.
- **Redes y direccionamiento IP:** Se fortalecieron conocimientos sobre redes, configuración de direcciones IP estáticas, segmentos de red, conectividad por Ethernet y pruebas de comunicación.
- **Plataformas IoT y nube:** Se obtuvo experiencia práctica en el uso de plataformas como ThingsBoard, incluyendo la visualización de datos, creación de dashboards y configuración de alertas remotas.
- **Monitoreo ambiental en centros de datos:** Se comprendió la importancia de mantener condiciones ambientales óptimas para el correcto funcionamiento de la infraestructura tecnológica, y cómo un sistema de

monitoreo bien diseñado puede prevenir fallas y mejorar la eficiencia energética.

- **Seguridad eléctrica y uso de EPP:** Al trabajar en tableros eléctricos y con equipos de alta potencia como UPS, se aprendió la importancia del equipo de protección personal, del uso de herramientas dieléctricas y del trabajo seguro con energía trifásica.
- **Documentación técnica y validación de pruebas:** Se practicó la documentación estructurada de pruebas, instalación y configuración, una habilidad clave en entornos industriales o de ingeniería de misión crítica.

En resumen, este proyecto no solo fortaleció habilidades técnicas específicas, sino que también desarrolló una mentalidad profesional enfocada en la planeación, ejecución responsable y validación de resultados, competencias altamente valoradas en la industria tecnológica y de infraestructura crítica.

Competencias desarrolladas:

1. Instalación y mantenimiento de sensores ambientales

- Capacidad para instalar sensores de temperatura, humedad, fugas de líquidos, puertas y flujo de aire en puntos estratégicos del centro de datos.
- Comprensión del comportamiento físico de los sensores y su correcta orientación para lecturas precisas.

2. Cableado estructurado y energización de dispositivos

- Dominio del uso de cables RJ45, cables de control blindado y líneas de energía tipo 10x16.
- Habilidad para energizar gateways IoT mediante switches PoE y distribuir alimentación eléctrica en gabinetes.

3. Configuración de redes y direccionamiento IP

- Asignación de direcciones IP estáticas acorde al segmento de red de trabajo.
- Conexión de dispositivos a la red mediante protocolos TCP/IP, configuración de puentes de red entre switches y gateways.

4. Manejo de plataformas IoT (ThingsBoard)

- Integración de sensores con la nube utilizando IoT Gateways.

- Creación y personalización de dashboards para visualización remota de datos en tiempo real.

5. Implementación de monitoreo SNMP

- Conocimiento en la configuración de equipos con interfaz SNMP como UPS, RPDUs y aires InRow/perimetrales.
- Uso de herramientas de consola como nmap y snmpwalk para descubrimiento de dispositivos, obtención de OIDs y filtrado de datos relevantes.

6. Seguridad en instalaciones eléctricas

- Aplicación de protocolos de seguridad eléctrica en tableros trifásicos.
- Uso adecuado de equipo de protección personal (EPP), herramienta dieléctrica y tapetes aislantes para intervención segura.

7. Diagnóstico y solución de fallas

- Capacidad para identificar problemas de lectura en sensores, como colocaciones incorrectas o conexiones defectuosas.
- Realización de pruebas de conectividad con comandos como ping y revisión de rutas de datos hasta la nube.

8. Trabajo en equipo y comunicación técnica

- Colaboración efectiva en un entorno profesional, siguiendo procedimientos estandarizados.
- Documentación clara y detallada de procesos técnicos para futuras referencias y mantenimiento.

9. Planificación e implementación de infraestructura tecnológica

- Evaluación del sitio y diseño de rutas de cableado, espacios para gabinetes y organización de equipos.
- Ejecución de un proyecto integral desde su fase de diseño hasta su monitoreo final.

10. Adaptabilidad al entorno profesional

- Desarrollo de habilidades prácticas aplicadas a un entorno real de trabajo.
- Capacidad para adaptarse a diferentes escenarios y necesidades técnicas en infraestructura crítica.

Fuentes de Información: IEEE o APA

- [1] Lenovo, *IdeaPad 3 14/ITL05*, 14-inch Laptop, various models and release dates. [Online]. Available: <https://www.google.com/search?q=https://pcsupport.lenovo.com/uy/en/products/laptops-and-netbooks/3-series/ideapad-3-14itl05>. [Accessed: May 3, 2025].
- [2] Revista Energy Management, "Electrificación para data centers," 09-Ene-2014. [En línea]. Disponible en: <https://e-management.mx/2014/01/09/electrificacion-para-data-centers/>.
- [3] MDC Data Centers, "CFE: Mexico's new telecom player | MDC Data Centers," *MDC Data Centers Blog*, 06-Oct-2021. [En línea]. Disponible en: <https://www.google.com/search?q=https://www.mdcdatacenters.com/blog/cfe-mexicos-new-telecom-player/>.
- [4] BNH Generators, "How to choose the right power generator for data center infrastructure," *BNH Generators Blog*. [En línea]. Disponible en: <https://bnhgenerators.com/es/how-to-choose-the-right-power-generator-for-data-center-infrastructure/>.
- [5] ATN Ingeniería y Servicios, "¿Qué es una planta de emergencia y cómo puede ayudar a garantizar la disponibilidad de la infraestructura? - ATN Ingeniería y Servicios." [En línea]. Disponible en: <https://www.google.com/search?q=https://atn.com.mx/planta-de-emergencia-o-de-luz/>.
- [6] Tier 4, "Sistema de distribución eléctrica en un centro de datos - Tier 4." [En línea]. Disponible en: <https://www.google.com/search?q=https://www.tier4.mx/blog/sistema-de-distribucion-electrica-en-un-centro-de-datos/>.
- [7] Greentology, "El desafío del suministro de energía en los centros de datos - Greentology." [En línea]. Disponible en: <https://www.google.com/search?q=https://www.greentology.com/es/el-desafio-del-suministro-de-energia-en-los-centros-de-datos/>.
- [8] Vertiv, "¿Qué es un PDU para racks?," [En línea]. Disponible en: <https://www.vertiv.com/es-latam/about/news-and-insights/articles/educational-articles/what-is-a-rack-pdu/>.

[9] Diez características esenciales de las PDUs modernas - Cad&Lan. [En línea]. Disponible en: <https://www.cadlan.com/noticias/diez-caracteristicas-esenciales-de-las-pdus-modernas/>

[10] ¿Qué es una PDU en los centros de datos y por qué es importante? - E-Abel. [En línea]. Disponible en: <https://www.eabel.com/es/que-es-una-pdu-en-los-centros-de-datos/>

[11] AP7900B - Unidad PDU para rack con conmutación de 1 U, 15A, 100/120V, (8) 5-15. [En línea]. Disponible en: <https://www.se.com/pe/es/product/AP7900B/unidad-pdu-para-rack-con-conmutaci%C3%B3n-de-1-u-15a-100-120v-8-515/>

[12] ¿Qué es un centro de datos? Cómo funciona un centro de datos | Fortinet. [En línea]. Disponible en: <https://www.google.com/search?q=https://www.fortinet.com/es/resources/cyberglossary/data-center>

[13] Todo lo que Debes Saber sobre Centros de Datos: Definición, Roles y Normas. [En línea]. Disponible en: <https://www.aprendaredes.com/todo-lo-que-debes-saber-sobre-centros-de-datos-definicion-roles-y-normas/>

[14] Aire acondicionado de precisión en los centros de datos: Manteniendo la frescura de la tecnología - Gesttor. [En línea]. Disponible en: <https://gesttor.com/blog/aire-acondicionado-precision-centros-datos/>

[15] Principales diferencias entre un aire acondicionado de precisión y uno de confort - ATN Ingeniería y Servicios. [En línea]. Disponible en: <https://atn.com.mx/aire-acondicionado-de-precision-vs-de-confort/>

[16] ADTEK Electronics Co., Ltd., "*CPM-20 Series - Multifunction Power Meter*," [Online]. Available: <https://www.google.com/search?q=https://www.adtek.com.tw/product/multifunction-power-meter-cpm-20-series/>. [Accessed: May 3, 2025].

[17] ADTEK Electronics Co., Ltd., "*Dispositivo de medición de potencia multifunción - CPM-20 Series*," [Online]. Available: [The Google Search result points to the same English link as above: <https://www.google.com/search?q=Dispositivo+de+medici%C3%B3n+de+potencia+multifunci%C3%B3n+-+CPM-20+Series+-+ADTEK+Electronics+Co.,+Ltd+-+contador+el%C3%A9ctrico+de+potencia+aparente+de+potencia+activa>]. [Accessed: May 3, 2025].

[18] Cuerva, "*Qué es un UPS, qué tipos de SAI existen y cómo funciona*," 15-dic-2023. [Online]. Available: <https://cuervaenergia.com/es/comunidad/construccion-e-instalacion/que-es-un-ups/>. [Accessed: May 5, 2025].

- [19] Intercompras Blog, "*Sistemas de alimentación ininterrumpida (UPS): Guía para proteger tu equipo en 2024*," [Online]. Available: <https://intercompras.com/blog/sistemas-de-alimentacion-ininterrumpida-ups-guia-para-proteger-tu-equipo-en-2024/>. [Accessed: May 5, 2025].
- [20] PowerSun SAS, "*¿Qué es una UPS?*," [Online]. Available: <https://www.google.com/search?q=https://www.powersun.com.co/que-es-una-ups/>. [Accessed: May 5, 2025]
- [21] Servicios Electrónicos Globales, S.A. de C.V. (E-Global México), "Acerca de Nosotros," [Online]. Available: [No se dispone de un enlace directo a una página "Acerca de Nosotros" específica en los resultados de búsqueda. Se infiere su existencia por su actividad y presencia en el mercado]. [Accessed: May 3, 2025].
- [22] Banco de México, "Autorización a Servicios Electrónicos Globales, S.A. de C.V. para organizarse y operar como cámara de compensación para pagos con tarjetas," 03-may-2018. [Online]. Available: <https://www.banxico.org.mx/marco-normativo/autorizaciones-para-organizarse-y-operar-como-cama/%7B0E7DF823-D18A-9826-7658-36897DB5A883%7D.pdf>. [Accessed: May 3, 2025].
- [23] Comisión Federal de Competencia Económica, "COFECE identificó barreras a la competencia en el mercado de procesamiento de pagos con tarjeta," 14-nov-2023. [Online]. Available: <https://www.cofece.mx/cofece-identifico-barreras-a-la-competencia-en-el-mercado-de-procesamiento-de-pagos-con-tarjeta/>. [Accessed: May 3, 2025].
- [24] INETCO, "E-Global Leverages INETCO Insight for Real-Time Fraud Analytics and Operations Performance," [Online]. Available: <https://www.inetco.com/es/resources/case-studies/e-global-fraud-analytics-and-operations-performance/>. [Accessed: May 3, 2025].
- [25] Fintech México, "Resumen Ejecutivo - Radiografía del Ecosistema Fintech en México," p. 10, [Online]. Available: <https://fintech-mexico.squarespace.com/s/Resumen-Ejecutivo.pdf>. [Accessed: May 3, 2025].
- [26] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787-2805,¹ 2010.
- [27] ASHRAE, *Thermal Guidelines for Data Processing Environments*. Atlanta, GA: American Society of Heating, Refrigerating and Air-Conditioning Engineers,² Inc., 2016.
- [28] W. Stallings, *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*. Boston: Addison-Wesley Longman Publishing Co., Inc., 1999.

[29] ThingBoard. *ThingBoard Documentation*. [Online]. Available: <https://www.google.com/search?q=https://thingboard.io/docs/>

[30] A. S. Tanenbaum, *Modern Operating Systems*. Upper Saddle River, NJ: Prentice Hall, 2008.

[31] NIST, "Recommended Security Controls for Federal Information Systems," National³ Institute of Standards and Technology, Special Publication 800-53, Revision 4, 2013.